Cyberbezpieczny Samorząd – Wdrażanie nowoczesnych rozwiązań cyberbezpieczeństwa w Gminie Stężyca

(Postępowanie znak: GPiOS.0271.9.2025)

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa, instalacja, uruchomienie, konfiguracja z dostosowaniem do istniejącej infrastruktury informatycznej Serwera wraz z oprogramowaniem i licencjami, zapewniające ochronę systemów informatycznych, zapewnienie funkcjonowania Urzędu Gminy Stężyca w zgodności z KRI oraz uoKSC oraz kształtowanie kultury cyberbezpieczeństwa wśród pracowników.

1. Podstawy normatywne opracowania dokumentacji CPV:
   48820000 - Serwery
   30233000-1 Urządzenia do przechowywania i odczytu danych
   32420000-3 Urządzenia sieciowe
   48000000 - Pakiety oprogramowania i systemy informatyczne
   48219700 - Pakiety oprogramowania do serwera komunikacyjnego
   48620000-0 Systemy operacyjne
   72263000 - Usługi wdrażania oprogramowania
   72265000 - Usługi konfiguracji oprogramowania

2. Dostarczony sprzęt winien być:
   1) nowy tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów poprawnej pracy,
   2) wolny od wad technicznych,
   3) wolny od wad prawnych,
   4) pochodzących z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych,
   5) dostarczony w oryginalnych opakowaniach producenta sprzętu dla danego produktu, zaopatrzony w etykiety identyfikujące dany produkt,
   6) kompletny, w tym m.in. posiadać pełne okablowanie zapewniające funkcjonalność, oprogramowanie, licencję itp.

3. W skład urządzeń objętych przedmiotem zamówienia wchodzi:

1) Serwer

Wymagane minimalne parametry techniczne komponentu Serwer (1 kpl.)
Wymagana ilość 1 sztuka
Obudowa typu RACK o wysokości max. 3U wyposażony w szyny ruchome oraz elementy do montażu w szafie serwerowej pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej

Zainstalowany min. 2 procesory 8 rdzeniowe w architekturze x64, cache 12MB przeznaczony do pracy ciągłej (serwerowy)
Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta serwera, trwale oznaczona (na laminacie płyty głównej) z nazwą producenta oferowanego serwera i dedykowana dla danego urządzenia. Płyta główna powinna umożliwiać zainstalowanie 2 procesorów oraz pamięci RAM
min. 96 GB DDR4 RDIMM o częstotliwości pracy 3200 MT/s
Zainstalowane min. 7 dysków, każdy o pojemności min. 1.2 TB, o parametrach min. 12Gb/s, , Hot-Plug 2.5. do intensywnego odczytu wymienny bez wyłączania systemu Uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
Zainstalowany sprzętowy kontroler dyskowy RAID SAS/SATA 0/1/5/6/10/50/60
Karta graficzna zintegrowana z płytą główną umożliwiająca wyświetlanie rozdzielczości min. 1280x1024.
Zintegrowany kontroler zdalnego dostępu umożliwiający administratorom monitorowanie, zarządzanie, aktualizowanie, rozwiązywanie problemów i naprawę z dowolnego miejsca i bez użycia agentów. Niezależnie od obecności lub stanu systemu operacyjnego lub hiperwizora.
Wbudowana w płytę główną dwu portowa karta sieciowa z min 2 portami 1Gbit/s. Dodatkowo zainstalowana dwu portowa karta 10Gbit/s SFP+. Interfejsy sieciowe muszą pochodzić od tego samego producenta.
na przednim panelu: min. 1 port USB min. 1 port micro USB min. 1 złącze video analogowe lub cyfrowe na tylnym panelu: min. 1 złącze video analogowe lub cyfrowe min. 1 port USB 2.0 min. 1 port USB 3.0 min. 2 porty RJ-45 Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy
Min. 2 zasilacze o mocy co najmniej 700W, redundancyjne, dedykowane do zaoferowanego sprzętu zwymiarowane do wewnętrznych podzespołów, wymienne bez wyłączania systemu
W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe.
System operacyjny – fabrycznie nowy, nieużywany, nie pochodzący z recyklingu, z licencją na czas nieoznaczony, nie naruszający praw osób trzecich. System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowanym urządzeniu komputerowym. Zabrania się instalowania lub preinstalowania systemu operacyjnego w jakimkolwiek środowisku wirtualnym. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta. MS Windows Server 2025 Standard wersja polskojęzyczna z nieujawnianym wcześniej, nieaktywowanym wcześniej kluczem licencyjnym, pochodzący z oficjalnej sieci dystrybucji firmy Microsoft® wraz z licencjami dostępowymi CAL User dla 20 lub równoważne. Warunki równoważności: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.

2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2012 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server.
5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i 2 środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

a) zarządzania użytkownikami,

b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,

c) możliwości przydzielania praw dostępu do zasobów sieciowych,

d) instalacji zdalnej oprogramowania z pakietów msi,

e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 8,8.1, 10. 11.

10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre.
12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP dla dostępu administracyjnego.
13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra.
16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra.
17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ipv4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
22. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1;
23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory.
24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte musza być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

Wymagania dla równoważnych licencji dostępowych dla użytkownika:

- Licencja dostępowa dla użytkownika umożliwiająca połączenie i wykorzystywanie wszystkich

dostępnych funkcjonalności serwera Microsoft Windows Server 2022 z wdrożoną rolą Active Directory. - Każda z licencji umożliwia użytkownikowi na dostęp z dowolnego urządzenia do zasobów serwera.
Certyfikat ISO 9001:2015 oraz ISO 27001:2023 w zakresie dostarczania usług serwisowych do urządzeń oraz wdrożeń systemów informatycznych i oprogramowania – Wykonawca, zobowiązany jest załączyć wymagany certyfikat do oferty.
Zamawiający wymaga od Wykonawcy lub podwykonawcy zatrudnienia na podstawie umowy o pracę minimum 6 osób wykonujących wskazane czynności w trakcie realizacji zamówienia. W celu weryfikacji zatrudniania, przez wykonawcę lub podwykonawcę, Zamawiający wymaga złożenia oświadczenia wykonawcy lub podwykonawcy wraz z ofertą.
Co najmniej 36 miesięczna gwarancja, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 2 godzin roboczych
Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu wraz z migracją danych z obecnego systemu posiadanego przez Zamawiającego. Wdrożenie: • Montaż fizycznych składników rozwiązania, podłączenie i konfiguracja interfejsów sieciowych, • konfiguracja interfejsów zarządzających serwerami, aktualizacja oprogramowania sprzętowego. Konfiguracja urządzeń sieciowych w odniesieniu do rozwiązania wirtualizacyjnego, • Instalacja systemów operacyjnych (np. serwer Windows), aktualizacja. • Konfiguracja usługi bazującej na oprogramowaniu definiowanym magazynem. • Konfiguracja usług klastra dotyczących wirtualizacji, definiowanie sieci wirtualnych, • Instalacja i konfiguracja maszyn wirtualnych (np. serwer Windows). • Tworzenie wzorcowego obrazu maszyny wirtualnej (np. serwer Windows). • Instalacja oprogramowania do zarządzania kopiami zapasowymi na dedykowanym serwerze, • konfiguracja lokalnych zasobów serwera jako repozytorium kopii zapasowych, konfiguracja zadań • tworzenia kopii zapasowych dla danego środowiska, weryfikacja kopii zapasowej - przywrócenie • wybranej maszyny • Konfiguracja serwera VPN • Migracją danych z obecnego systemu posiadanego przez Zamawiającego wraz z obecnie wykorzystywanym • oprogramowaniem. • Weryfikacja funkcjonowania środowiska. • Włączenie funkcji serwera usług katalogowych na wybranej maszynie wirtualnej. • Konfiguracja polityk usług katalogowych dotyczących urządzeń i użytkowników. • Konfiguracja profili użytkowników. • Konfiguracja dostępu do wybranych zasobów. • Instalacja usług serwera terminalowego na maszynie wirtualnej i konfiguracja usług zdalnego • dostępu dla użytkowników. • Konfiguracja dostępu terminalowego na wszystkich hostach(komputerach klienckich) • Migracja obecnych profili użytkowników do serwera terminalowego • Konfiguracja połączeń VPN dla dostępów zdalnych na urządzeniach mobilnych

2) Oprogramowanie Antywirusowe

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe)

Oprogramowanie do wykonywania kopii zapasowych (1 kpl.)

Wykonawca musi mieć wdrożony oraz stosować zintegrowany system zarządzania jakością i bezpieczeństwem informacji zgodny z wymaganiami norm ISO 9001 oraz 27001 minimum w zakresie wdrożeń systemów informatycznych oraz oprogramowania. Dostarczone rozwiązanie musi mieć możliwość jednoczesnej pracy dla 20 użytkowników końcowych oraz dwóch serwerów w okresie 24 miesięcy.
Wspierane systemy operacyjne
Systemy Operacyjne Komputerów

- Windows 11 October 2024 Update (24H2)
- Windows 11 October 2023 Update (23h2)
- Windows 10 November 2022 Update (22H2)
- Windows 11 September 2022 Update (22H2)
- Windows 11 (initial release)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial release)
- Windows 8.1
- Windows 8
- Windows 7 SP1

Windows Tablet oraz systemy wbudowane
Windows 10 IoT Enterprise
Windows Embedded 8.1 Industry
Windows Embedded 8 Standard
Windows Embedded Standard 7
Windows Embedded Compact 7
Windows Embedded POSReady 7
Windows Embedded Enterprise 7

Windows ARM64 desktop
Windows 11 October 2024 Update (24H2)
Windows 10 November 2022 Update (22H2)
Windows 11 September 2022 Update (22h2)
Windows 10 November 2021 Update (21H2)

Systemy operacyjne serwera
Windows Server 2025 64x
Windows Server 2022 Core
Windows Server 2022
Windows Server 2019 Core
Windows Server 2019
Windows Server 2016
Windows Server 2016 Core
Windows Server 2012 R2
Windows Server 2012
Windows Small Business Server (SBS) 2011
Windows Server 2008 R2

Systemy Operacyjne Linux i wersja kernel

Oparte o RPM
RHEL 7.x - 3.10.0 (build 957) 64-bit
RHEL 8.x - 4.18.0 64-bit
RHEL 9.x - 5.14.0 64-bit
Oracle Linux 7.x (UEK) - 4.18.0 64-bit
Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit
Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit
Oracle Linux 8.x (RHCK) – 4.18.0 64-bit
Oracle Linux 9.x (UEK) – 5.15.0 64-bit
Oracle Linux 9.x (RHCK) – 5.14.0 64-bit
CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit
CentOS 8 Stream - 4.18.0 64-bit
CentOS 9 Stream - 5.14.0 64-bit
Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit
AlmaLinux 8.x - 4.18.0 64-bit
AlmaLinux 9.x - 5.14.0 64-bit
Rocky Linux 8.x - 4.18.0 64-bit
Rocky Linux 9.x - 5.14.0 64-bit
CloudLinux 7.x - 3.10 (build 957) 64-bit
CloudLinux 8.x - 4.18.0 64-bit
Miracle Linux 8.x - 4.18.0 64-bit
Kylinv10 RHEL - 4.19.90 64-bit

Oparte o Debian
Debian 9 - 4.9.0 32-bit/64-bit
Debian 10 - 4.19 32-bit/64-bit
Debian 11 - 5.10 32-bit/64-bit
Debian 12 – 6.1.0 64-bit
Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit
Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit
Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit
Ubuntu 22.04.x - 5.15 / 5.19 64-bit
Ubuntu 23.04.x – 6.2.0 64-bit
Ubuntu 24.04.x – 6.8.0 64- bit
PopOS 22.04.x – 6.2.6 64-bit
Pardus 21 – 5.10.0 64-bit
Mint 20.x – 5.4.0 64-bit
Mint 21.x – 5.15.0 64-bit
Mint 22.x – 6.8.0.x 64-bit
Zorin OS – 6.5.x 64-bit
Linux Mint Debian Edition 6 – 6.1.x 64-bit

Oparte o SUSE
SLES 12 SP4 - 4.12.14-x 64-bit
SLES 12 SP5 - 4.12.14-x 64-bit
SLES 15 SP1 - 4.12.14-x 64-bit
SLES 15 SP2 - 5.3.18-x 64-bit
SLES 15 SP3 - 5.3.18-x 64-bit
SLES 15 SP4 – 5.14.21 64-bit
SLES 15 SP5 – 5.14.21 64-bit
SLES 15 SP6 – 6.4.x 64-bit

SLED 15 SP4 – 5.14.21 64-bit
openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit

Cloud based Linux
AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit
Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit
Amazon Linux 2023 – 6.1.x 64-bit
Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit
Azure Mariner 2 - 5.15 64-bit

Linux dla ARM

Oparte o RPM
RHEL 8.x – 4.18.0-x
RHEL 9.x – 5.14
AlmaLinux 9.x – 5.14
Rocky Linux 9.x – 5.14

Oparte o Debian
Debian 11 – 5.10 / 6.1
Debian 12 – 6.1.0.x
Ubuntu 20.04.x – 5.15
Ubuntu 22.04.x – 5.15 / 5.19
Ubuntu 24.04.x – 6.8.0.x

Oparte o SUSE
SLES 15 SP4 – 5.14.21-x
openSUSE Leap 15.4-15.5 – 5.14.21-x

Oparte o chmurę
Amazon Linux v2 – 5.10
Amazon Linux 2023 - 6.1

Systemy Operacyjne Mac OS X
macOS Sequoia (15.x)
macOS Sonoma (14.x)
macOS Ventura (13.x)
macOS Monterey (12.x)
macOS Big Sur (11.x)

Obsługiwane Środowiska Microsoft Exchange
Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2019 z rolą Edge Transport lub Mailbox
- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox

Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG).

Ochrona środowisk wirtualnych (SVE)

1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej.
2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:
   a) OVA
   b) XVA

c) VHD
d) VHDX
e) VMDK

Środowiska wspierane:

- VMware vSphere and vCenter Server:
  - version 6.5
  - version 6.7, including update 1, update 2a and update 3
  - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d
  - version 8.0, including update 1, update 2
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix Xen Hypervisor: 8.4.
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor), 2022, 2025
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition)

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Interfejs oraz pomoc techniczna świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
13. Możliwość dodawania wykluczeń na podstawie:
    a) Plik
    b) Folder
    c) Rozszerzenie
    d) Proces
    e) Hash pliku
    f) Hash certyfikatu
    g) Nazwa zagrożenia
    h) Wiersz poleceń
    i) IP/maska
14. Skanowanie poczty opartej o protokoły IMAP, MAPI, POP3 i SMTP w czasie rzeczywistym.

15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.
16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
17. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji.
18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS.
19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
21. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
22. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
23. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
24. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
25. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
26. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
27. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
30. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
31. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
32. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
33. Wbudowany IDS.
34. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
35. Możliwość tworzenia list sieci zaufanych.
36. Możliwość dezaktywacji funkcji zapory sieciowej.
37. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
38. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
39. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
    a) Możliwość wymuszenia funkcji DEP systemu Windows.
    b) Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.
41. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

-Pierwszy dostęp.
-Dostęp do poświadczeń.
-Wykrycie.
-Crimeware.
-Ruch boczny.

42. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach:

3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4

43. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux.
44. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.
45. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
46. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
47. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.
48. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON).
49. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).

Stacje robocze i serwery

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail

do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux.

12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5. Możliwość skanowania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
2. Możliwość integracji wielu domen Active Directory.
3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.

11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
12. Możliwość generowania raportu co godzinę.
13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
14. Możliwość dodania etykiety do stacji roboczej.
15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.
17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.
18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim.
20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:
    -Zakres adresów IP/IP.
    -Adres bramy.
    -Adres serwera WINS.
    -Adres serwera DNS.
    -Połączenie DHCP sufiksów DNS.
    -Punkt końcowy może rozwiązać hosta.
    -Typ sieci.
    -Nazwa hosta.
22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
23. Możliwość naprawy instalacji agenta z poziomu konsoli.
24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS.
28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
33. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.

34. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
35. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
    a) Ukierunkowane ataki.
    b) Podejrzane pliki i ruch w sieci.
    c) Exploity.
    d) Ransomware.
    e) Grayware.
36. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
37. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:
    a) Tolerancyjny.
    b) Normalny.
    c) Agresywny.
38. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:
    a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora.
    b) Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem.
    c) Możliwość ręcznego przesłania adresu URL.
    d) W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
39. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
40. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.
41. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania.
42. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
43. Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB.
44. Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.
45. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać:
    a) Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji:
       -Przeglądarka
       -Sieć
       -System operacyjny
       -Luki

System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów.

    b) System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk.
    c) System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość.
    d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach.
f) System pozwala na wykrywanie podatności w oparciu o standardy bezpieczeństwa zgodne z: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU).
g) System musi mieć możliwość określenia, które konkretnie zapisy standardów bezpieczeństwa: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU) nie są spełnione w wyniku wykrytej błędnej konfiguracji.

46. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
47. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
48. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
49. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure.
50. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak:
    a) Zarządzane punkty końcowe.
    b) Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne.
    c) Pięć rodzajów najczęściej blokowanych zagrożeń.
    d) Podział zagrożeń na urządzenia takie jak stacje robocze i serwery.
    e) Status incydentów bezpieczeństwa, które wystąpiły.
    f) Stan modułów punktów końcowych.
    g) Ocena ryzyka firmy.
    h) Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
    i) Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware.
51. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Firmy
    b) Raporty
    c) Licencjonowanie
    d) Konta
    e) Pakiety
    f) Incydenty
    g) Sieć
    h) Kwarantanna
    i) Integracje
    j) Event Push Service
    k) Polityki
52. Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
53. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać:
    a) Pobieranie przez partnera plików z kwarantanny podległych firm.
    b) Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm.
    c) Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego.

54. Profil firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej. Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne.
55. System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Linux i macOS.
56. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii.
57. Konsola administracyjna umożliwia zmianę motywu dla interfejsu spośród jasnego, ciemnego lub wybranego automatycznie w oparciu o ustawienia systemowe.
58. System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas, który wynosi 15 minut, 30 minut, 1 godzina, 2 godziny, 4 godziny. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania.
59. Centrum integracji – Panel umożliwiający zarządzanie integracjami z rozwiązaniami zewnętrznymi tj. Vmware vCenter, Veeam Backup & Replication, Microsoft Active Directory, Vmware Tanzu, Microsoft Exchange (on-premises), SecurityCoach (KnowBe4).
60. Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB.
61. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie:

a) ID.
b) Ostatnia aktualizacja.
c) Status.
d) Osoba przydzielająca.
f) Data utworzenia.
g) Priorytet.
h) Ocena szkodliwości w skali 0-100.
i) Podmioty.
j) Zasoby.
k) Ostatnia faza killchain.
l) Wykonane czynności.
m) Skorelowane incydenty.
n) Typ incydentu.

62. System umożliwia wygenerowanie i pobranie zestawu informacji z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje:
    a) Windows

- Logi zainstalowanego agenta.
- Dziennik zdarzeń Windows.
- Informacje o systemie.
- DnsCache.
- Webcache.
- Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY).
- Harmonogram zadań.
- Historia Powershell (jeśli włączono).

    b) Linux
        - Podstawowy log pomocy technicznej zainstalowanego agenta.
        - Certyfikaty.
        - Autorun i usługi.
        - Informacje sieciowe.
        - Informacje systemowe.
        - Zainstalowane pakiety.
    c) macOS
        - Podstawowy log pomocy technicznej zainstalowanego agenta.
        - Autorun.
        - Lista procesów.
        - Informacje sieciowe.

- Informacje o systemie.

63. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:

a) historia powłoki.
b) wczytywanie bibliotek .dll z podejrzanej lokalizacji.
c) Sesje logowania z użyciem jawnych danych uwierzytelniających.
d) Arp cache.
e) Ip forwarding.
f) Lista zamontowanych nośników.
g) Konfiguracja ip tables.
h) Połączenia TLS które używają certyfikatów self-signed.
i) Używane rozszerzenia w przeglądarce Chrome.
j) Używane rozszerzenia w przeglądarce Firefox.
k) Używane rozszerzenia w przeglądarce Safari.
l) Źródła apt w systemach Linux.
m) Wyświetlanie zainstalowanych pakietów DEB.
n) Wyświetlanie zainstalowanych pakietów RPM.
o) Pakiety Python zainstalowane w systemie.
p) Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux).
q) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS.
r) Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona.
s) Wykrywanie czy SecureBoot jest włączony.
t) Lista zapamiętanych sieci bezprzewodowych.
u) Wykrywa, czy zmienił się domyślny folder startowy użytkownika.
w) Wykrywa, czy zmienił się domyślny folder startowy maszyny.

64. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna:

a) Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i innych.
b) Automatyczne działania zapobiegawcze są zależne od wyboru kategorii.
c) Tworzenie reguł musi być określone poprzez wybór operatora np. „to”, „zawiera”, „jest jednym z” itp.
d) Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia.
e) Zapewniać możliwość tworzenia zapytań YARA.
f) Umożliwiać określenie priorytetu kolejności automatyzacji.
g) Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).

EDR-Endpoint Detection and Response
Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.

Wspierane systemy operacyjne

A. Systemy desktopowe
   a) Windows 11 October 2024 Update (24H2)
   b) Windows 11 October 2023 Update (23H2)
   c) Windows 10 November 2022 Update (22H2)
   d) Windows 11 September 2022 Update (22H2)
   e) Windows 11 (initial release)
   f) Windows 10 November 2021 Update (21H2)
   g) Windows 10 May 2021 Update (21H1)
   h) Windows 10 October 2020 Update (20H2)
   i) Windows 10 May 2020 Update (20H1)
   j) Windows 10 May 2019 Update (19H1)
   k) Windows 10 October 2018 Update (Redstone 5)

l) Windows 10 April 2018 Update (Redstone 4)
m) Windows 10 Fall Creators Update (Redstone 3)
n) Windows 10 Creators Update (Redstone 2)
o) Windows 10 Anniversary Update (Redstone 1)
p) Windows 10 November Update (Threshold 2)
q) Windows 10 (initial release)
r) Windows 8.1
s) Windows 8
t) Windows 7 SP1

B. Systemy operacyjne dla serwerów:

a) Windows Server 2025 64x
b) Windows Server 2022 Core
c) Windows Server 2022
d) Windows Server 2019 Core
e) Windows Server 2019
f) Windows Server 2016
g) Windows Server 2016 Core
h) Windows Server 2012 R2
i) Windows Server 2012
j) Windows Small Business Server (SBS) 2011
k) Windows Server 2008 R2

C. MacOS:

a) macOS Sequoia (15.x)
b) macOS Sonoma (14.x)
c) macOS Ventura (13.x)
d) macOS Monterey (12.x)
e) macOS Big Sur (11.x)

D. Linux
Oparte o RPM
RHEL 7.x - 3.10.0 (build 957) 64-bit
RHEL 8.x - 4.18.0 64-bit
RHEL 9.x - 5.14.0 64-bit
Oracle Linux 7.x (UEK) - 4.18.0 64-bit
Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit
Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit
Oracle Linux 8.x (RHCK) – 4.18.0 64-bit
Oracle Linux 9.x (UEK) – 5.15.0 64-bit
Oracle Linux 9.x (RHCK) – 5.14.0 64-bit
CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit
CentOS 8 Stream - 4.18.0 64-bit
CentOS 9 Stream - 5.14.0 64-bit
Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit
AlmaLinux 8.x - 4.18.0 64-bit
AlmaLinux 9.x - 5.14.0 64-bit
Rocky Linux 8.x - 4.18.0 64-bit
Rocky Linux 9.x - 5.14.0 64-bit
CloudLinux 7.x - 3.10 (build 957) 64-bit
CloudLinux 8.x - 4.18.0 64-bit
Miracle Linux 8.x - 4.18.0 64-bit
Kylinv10 RHEL - 4.19.90 64-bit

Oparte o Debian

Debian 9 - 4.9.0 32-bit/64-bit
Debian 10 - 4.19 32-bit/64-bit
Debian 11 - 5.10 32-bit/64-bit
Debian 12 – 6.1.0 64-bit
Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit
Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit
Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit
Ubuntu 22.04.x - 5.15 / 5.19 64-bit
Ubuntu 23.04.x – 6.2.0 64-bit
Ubuntu 24.04.x – 6.8.0 64- bit
PopOS 22.04.x – 6.2.6 64-bit
Pardus 21 – 5.10.0 64-bit
Mint 20.x – 5.4.0 64-bit
Mint 21.x – 5.15.0 64-bit
Mint 22.x – 6.8.0.x 64-bit
Zorin OS – 6.5.x 64-bit
Linux Mint Debian Edition 6 – 6.1.x 64-bit

Oparte o SUSE
SLES 12 SP4 - 4.12.14-x 64-bit
SLES 12 SP5 - 4.12.14-x 64-bit
SLES 15 SP1 - 4.12.14-x 64-bit
SLES 15 SP2 - 5.3.18-x 64-bit
SLES 15 SP3 - 5.3.18-x 64-bit
SLES 15 SP4 – 5.14.21 64-bit
SLES 15 SP5 – 5.14.21 64-bit
SLES 15 SP6 – 6.4.x 64-bit
SLED 15 SP4 – 5.14.21 64-bit
openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit

Cloud based Linux
AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit
Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit
Amazon Linux 2023 – 6.1.x 64-bit
Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit
Azure Mariner 2 - 5.15 64-bit
Komponenty EDR
Główne elementy:

1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania.
2. Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR.
3. Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.

Wykrywanie podejrzanej aktywności
Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.

1. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.
2. Zgłaszanie naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.

2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa. 3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami: a) Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia. b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej. c) System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa. Incydenty 1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość: b) Filtrowania zdarzeń. c) Zakończenia procesów. d) Dodania procesów do czarnej listy. e) Dodania procesów do białej listy. f) Izolacji hosta. g) Przesłania pliku do Sandbox. h) Sprawdzenia informacji o pliku w Google. i) Sprawdzenia informacji o pliku w VirusTotal. 2. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego. 3. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. 4. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii: 5. a) Hash MD5 lub SHA256. j) b) Pełna ścieżka do aplikacji. k) c) Reguła połączenia. 6. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV. 7. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania. 8. Możliwość wygenerowania i wyeksportowania listy incydentów do pliku .csv.

3) Oprogramowanie menadżera logów

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Oprogramowanie menadżera logów (1 kpl.)
Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne, rejestrowanie logów aktywności użytkowników i zdarzeń bezpieczeństwa. Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o

aktualizacji
Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
Odwzorowanie struktury organizacji w oparciu o Active Directory
Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci
Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów programu
Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
Utworzenie własnych typów elementów wyposażenia
Łączenie elementów wyposażenia w zestawy
Przypisywanie zasobu do wielu zestawów
Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
Przypisywanie sprzętu do konkretnych osób, sprzętu do wybranej firmy
Automatyczne wyznaczanie 'Głównego użytkownika' komputera
Wiązanie wielu rekordów wyposażenia z użytkownikiem
Przypisywanie sprzętu do dowolnej lokalizacji
Definiowanie własnych, dowolnych atrybutów sprzętu
Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
Dowolna treść kodu kreskowego
Określanie loga firmy oraz użycia go na wydrukach
Grupowa zmiana domeny/grupy roboczej zasobu
Informacje o sprzęcie
Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
Wykrywanie komputerów typu All-In-One
Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)
Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
Odczyt informacji o module TPM, D3Dscore z WinSAT
Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu, wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika), tworzenie zestawów: Komputer + Monitor, Komputer + drukarka lokalna, host + maszyny wirtualne, wykrywanie czy komputer jest maszyną

wirtualną
Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
Określanie informacji o wykorzystywanej wirtualizacji
Podgląd zestawów, do których należy zasób
Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
Definiowanie szczegółowych informacji finansowych, bazy dostawców sprzętu i oprogramowania
Obsługa walut w danych finansowych
Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) oraz automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
Agent odczytuje identyfikator SID komputera
Określanie adresu interfejsu webowego urządzenia sieciowego, typu gwarancji dla zasobu, wpływu biznesowego wybranego zasobu
Tworzenie własnych typów gwarancji
Określanie ikony dla typów zasobów
Integracja z Dell API
Wyszukiwanie i identyfikacja duplikatów zasobów
Geolokalizacja komputerów z agentem
Raporty zasobów
Raport dodanych załączników
Automatyczne tworzenie historii zmian sprzętu
Raport zbiorczy historii zmian w sprzęcie
Ewidencja zdarzeń serwisowych
Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
Informacja na temat pojemności dysków twardych oraz wolnego miejsca
Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu, jako załącznik protokołu przekazania dla całego zestawu
Kreator szablonów wydruków WYSIWYG
Definiowanie dedykowanych profili protokołów
Zapisywanie protokołów podczas generowania jako załącznik do zasobu
Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia
Wydruk lub zapis do pliku raportów ze szczegółami sprzętu
Porównywarka wyników skanowania sprzętu
Dzienniki zdarzeń systemu Windows
Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu
Geolokalizacja komputerów z agentem
Zarządzanie zasilaniem
Zdalne włączanie i wyłączenie komputerów
Obsługa SecureOn przy WakeOnLan
Tworzenie harmonogramów wyłączania i włączania komputerów
Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart
Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik
Możliwość przerwania / odłożenia zadania na żądanie użytkownika
Wymuszenie wylogowania użytkownika przed wyłączeniem komputera
Raport zadań jednorazowych oraz harmonogramów

Monitoring obciążenia CPU
Funkcje dodatkowe
Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych
Podpisywanie skryptów Powershell certyfikatem
Wykonywanie skryptów w kontekście sesji użytkownika lub usługi
Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika
Wykonywanie zadań dla wszystkich komputerów
Edytor skryptów z funkcją kolorowania składni
Wykorzystywanie predefiniowanych skryptów
Import informacji o wyposażeniu z pliku CSV
Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL)
Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)
Generowanie kodów paskowych, QR dla każdego elementu wyposażenia
Obsługa kodów QR
Archiwum zasobów
Przeniesienie utylizowanego wyposażenia do archiwum
Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
Zarządzanie sprzętem przez aplikacje mobilną
Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu
Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych
Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej
Grupowa zmiana atrybutów
Personalizacja statusów zasobów
Zarządzanie oprogramowaniem
Licencje
Inwentaryzacja licencji
Automatyczne tworzenie licencji na podstawie kluczy produktów
Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego
Import licencji z pliku tekstowego
Automatyczne generowanie historii zmian w licencji
Określanie statusu licencji
Tworzenie własnych atrybutów licencji, notatek oraz załączników w dowolnym formacie do licencji, licencji z poziomu rozliczenia audytu legalności, licencji z poziomu raportu kluczy licencji, zestawów licencji
Relacja licencji z użytkownikiem, firmą, działem, lokalizacją
Zmiana typu licencji dla wybranej grupy
Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
Przypisywanie licencji do komputera
Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.), ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska, licencji przeznaczonych do przyszłego zakupu, kluczy seryjnych i przypisywanie do licencji
Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją
Określenie wpływu biznesowego wybranej licencji
Skanowanie oprogramowania

Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
Śledzenie zmian w stanie zainstalowanego oprogramowania
Zdalny skan komputerów (bieżący lub okresowy)
Zmiana priorytetu skanowania oprogramowania
Skan komputerów niepodłączonych do sieci
Wysyłanie wyników skanowania offline na serwer FTP (Audyt)
Przekazywanie konfiguracji wzorcowej dla skanera offline
Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
Określanie masek plików dla publikacji elektronicznych (e-book)
Skan plików skompresowanych
Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
Wbudowane profile skanowania (np. profil wzorcowy)
Definicja własnych ustawień skanowania
Porównywanie wyników skanowania oprogramowania
Wykrywanie plików multimedialnych
Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta
Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)
Audyt oprogramowania
Rozliczanie pakietów aplikacji, systemów operacyjnych, licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji
Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.
Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji
Funkcje
Mechanizm informujący o nowej bazie wzorców oprogramowania
Definiowanie własnych wzorców oprogramowania
Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
Wykrywanie kluczy/identyfikatorów programów
W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office

Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd., oraz informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
"Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi), dezinstalacja oprogramowania
Utworzenie harmonogramu dezinstalacji oprogramowania
Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej, zainstalowanych aktualizacji systemu Windows
Kontrola wykorzystania sprzętu i oprogramowania
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne
Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach
Odczyt informacji o kontal lokalnych komputera, wraz z odczytem grup do, których konto należy
Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
Określanie firmy do której należy użytkownik, przełożonego dla użytkownika
Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy), 'statusu użytkownika' (Zatrudniony, zwolniony, itd.)
Zarządzanie stanowiskami użytkowników
Przeniesienie rekordu użytkownika do archiwum
Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika
Odczytywanie informacji o użytkownikach z Active Directory oraz AAD
Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD)
Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
Podgląd zdjęcia przypisanego do użytkownika
Przypisywanie do użytkownika załączników (pliki), notatek do użytkownika
Ewidencja zdarzeń przypisanych do użytkowników
Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory
Raporty
Analiza aktywności użytkowników
Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko
Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
Analiza przerw w pracy, jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków), aktywności mikrofonu oraz kamery, wykorzystania poszczególnych aplikacji w czasie, czasu działania aplikacji, na pierwszym planie oraz sumarycznie
Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika
Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
Statystyki najczęściej wykorzystywanych aplikacji, wykorzystania komputerów przez

poszczególnych użytkowników, aktywności użytkownika i grup użytkowników

Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin

Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników, Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)

Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)

Monitoring wydruków na drukarkach sieciowych, użytkowników stacji terminalowych

Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.), o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca

Raport zbiorczy historii zmian w rekordach użytkowników

Funkcje

Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.

Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń

Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych

Automatycznie budowana baza informacji o napędach zewnętrznych

Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)

Odczyt i blokada urządzeń PTP/MTP

Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM

Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy

Informacje o ostatnio zalogowanych osobach na stacjach klienckich

Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje

Komentowanie przerw pracy

Kategoryzacja przerwy w pracy na podstawie komentarza

Kontrola wykorzystania Internetu

Funkcje

Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)

Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW

Kategoryzacja stron internetowych

Import stron WWW z pliku lub ze schowka

Slowniki kategorii stron WWW

Blokada dostępu do witryn zgodnie z harmonogramem, trybu incognito w przeglądarce Google Chrome

Raporty

Raporty dotyczące aktywności użytkowników w Internecie

Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)

Monitoring stron internetowych dla protokołu http \ https (Edge, Chrome, Opera, Vivaldi, Firefox)

Analiza liczby wejść na poszczególne strony lub domeny

Kategoryzacja odwiedzanych domen i stron

Raport informujący o plikach pobranych przez przeglądarki WWW, informujący o danych wysłanych przez przeglądarki (bez Firefox)

Monitoring plików pobieranych przez przeglądarki internetowe
Helpdesk
Obsługa
Rejestracja i obsługa zgłoszeń
Obsługa zgłoszeń w modelu Kanban
Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny)
Edycja zgłoszeń powiązanych w oknie zgłsozenia bieżącego
Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii
Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów
Opis zgłoszenia w formacie HTML
Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent
Tworzenie notatek dla zgłoszeń
Zapisywanie wersji roboczej komentarza
Archiwizacja zgłoszeń
Monitoring czasu pracy nad incydentem (time tracking)
Raport ewidencji czasu pracy nad zgłoszeniem
Informacja o czasie reakcji do podjęcia zgłoszenia
Dodanie prywatnego komentarza
Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia
Dodanie załączników do incydentów, również do komentarza
Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie, uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń
Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń
Wydruk historii zgłoszenia
Widok kalendarza (Planowanie rozwiązania incydentów)
Korelacja incydentu z elementem zasobów
Raport zbiorczy historii zmian
Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej
Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania
Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA
Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu
Określenie wpływu biznesowego wybranego zgłoszenia
Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email
Duplikacja i replikacja zgłoszeń
Powiadomienia o liczbie nieprzeczytanych zgłoszeń
Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł
Konfiguracja
Architektura drzewa dla kategorii zgłoszeń
Tworzenie szablonów odpowiedzi
Cykliczne raportowanie Listy incydentów
Tworzenie własnych dodatkowych atrybutów dla zgłoszeń

Personalizowane szablony wiadomości email z możliwością ustawienia stałego załącznika
Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu, e-mail o zbliżających się terminach realizacji incydentu (Deadline)
Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)
Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)
Obsługa wielu kont pocztowych (Import + notyfikację email)
Tworzenie własnych trybów oraz priorytetów incydentów
Personalizacja widoku raportu listy incydentów
Profile zgłaszających w helpdesk
Personalizacja kolorów statusów zgłoszeń
Automatyczne przypisywanie zgłoszeń do użytkowników
Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego
Konfiguracja maksymalnej wielkości załącznika
Moduł połączeń zdalnych
Operacje na plikach i katalogach
Zarządzanie procesami i rejestrem
Monitoring pracy wykonywanej na komputerze
Zdalny podgląd pulpitów wielu stacji (Funkcja Company Online)
Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
Wysyłanie wiadomości do użytkowników
Uruchamianie na stacjach programów z wiersza poleceń Command Line
Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego
Przejęcie kontroli nad stacją roboczą
Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu
Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
Obsługa wielu monitorów dla podglądu pulpitu
Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu
Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
Połączenie pulpitem zdalnym w konfiguracji NAT-NAT
Zarządzanie usługami systemu Windows
Raport Sesje zdalnego pulpitu
Wybór adresu IP, na którym ma być zestawione połączenie DirectPC, portu, na którym klient nasłuchuje połączenia zdalnego
Wykorzystanie protokołu autorskiego lub MS RDP do połączeń zdalnych
Baza wiedzy
Wbudowana baza wiedzy
Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk
Kopiowanie artykułów
Edytor HTML
Osadzanie załączników w treści artykułów
Osadzanie multimediów w treści artykułów

Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych
Szybkie kopiowanie wpisów bazy wiedzy
Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk oraz mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów
Informacja o liczbie odsłon artykułu bazy wiedzy
Bezpośrednie linkowanie artykułów bazy wiedzy
SLA
Definiowanie planów umów SLA, czasu obowiązywania umów SLA, czasu pracy działów wsparcia technicznego, dni wolnych na podstawie kalendarza świąt i dni wolnych, czasów reakcji oraz realizacji zgłoszenia
Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji
Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie
Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA
Centralne repozytorium załączników
Funkcje
Załączniki przechowywane w centralnym repozytorium
Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu)
Dodawanie i modyfikacja załączników z poziomu innych zasobów
Załączniki typu: link, udział oraz plik
Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura
Historia zmian załącznika
Zarządzanie użytkownikami
Funkcje
Raportowanie aktywności pracy
Przeglądanie ostatnio zgłoszonych incydentów
Powiązanie użytkownika z licencją
Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów
Cykliczne, automatyczne generowanie raportów
Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze
Zgłoszenia dotyczące wniosków nieobecności użytkowników
Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności
Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika
Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory
Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO
Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych
Planowanie dni wolnych w widoku kalendarza, zastępstw podczas nieobecności
Raportowanie cykliczne
Użytkownicy
Raport historia sesji, Nośniki danych, Operacje na plikach, wydruków, użycia aplikacji, nagłówków okien, odwiedzonych stron WWW
Najczęściej odwiedzane strony internetowe
Raport Wysyłane pliki, czasu pracy przy komputerze

Zasoby

Raport historii zasobów, informujący o nowych zasobach, informujący o nadchodzących terminach w zasobach, Zasoby zarchiwizowane, Systemy Operacyjne

Podstawowe

Raport Informacje o autoryzowanych agentach

Oprogramowanie

Raport zainstalowanego oprogramowania, Szczegóły plików

Helpdesk

Raport incydentów (Helpdesk), czasu pracy nad zgłoszeniem, Czasy SLA

Automatyzacja

Lista dostępnych reguł

Ogólne

Zakończenie asysty serwisowej AS lub AS Plus

Wygaśnięcie certyfikatu SSL

Kończące się licencje na agenta

Zapełniona baza danych

Zbyt duży rozmiar folderu cache

Zasoby

Brak połączenia od agenta, Brak wolnej przestrzeni na dysku, Ostrzeżenie od Windows Security Center, Zakończenie skanowania sprzętu, Dodanie zasobu, Zmiana zasobu, Usunięcie zasobu, Zakończenie okresu gwarancyjnego, Zakończenie umowy serwisowej, Powielenie zasobów

Oprogramowanie

Zmiana oprogramowania, Zakończenie skanowania oprogramowania, Zamknięcie audytu

Licencje

Dodanie/Zmiana/Usunięcie/Wygaśnięcie licencji, Planowana wymiana licencji

Użytkownicy

Dodanie/Zmiana/Usunięcie/Logowanie/Wylogowanie użytkownika

Helpdesk

Dodanie/Zmiana/Usunięcie zgłoszenia, Brak aktywności w zgłoszeniu

Lista dostępnych Akcji

Wykonywanie skryptu na podstawie zdefiniowanej reguły

Wysłanie powiadomienia w konsoli Master / Konsola Web na podstawie zdefiniowanej reguły, powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)

Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły

Dodanie komentarza (dla reguł Helpdesk)

Wysyłka wiadomości SMS

RODO

Funkcje

Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie

Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie

Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia

Wstępne wypełnienie wniosków o zmianę dostępu

Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji
Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych
Archiwizacja zbiorów
Definiowanie czynności przetwarzania
Przypisywanie zbioru danych do czynności przetwarzania
Przydzielanie dostępów do czynności przetwarzania
Zapisywanie historii zmian wniosków o dostęp do zbiorów
Dodawanie historycznych dostępów oraz wniosków o dostęp
Filtrowanie użytkowników w raporcie Dostępy
Raporty
Raport zbiorczy Czynności przetwarzania, Zbiory danych, zinwentaryzowanych dostępów, zinwentaryzowanych powierzeń, zinwentaryzowanych dokumentów, historii naruszeń bezpieczeństwa, wniosków o dostęp, dostępy
Sygnalista
Funkcje
Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej
Usuwanie metadanych z załączników zgłoszeń, danych osobowych ze zgłoszeń
Podział interfejsu na publiczny oraz dla wewnętrzny
Dashboard podsumowujący wykorzystanie portalu sygnalisty
Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła
Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka, stron publicznych (dostępnych dla sygnalistów)
Obsługa wielu języków stron publicznych
Natywne wsparcie języka ukraińskiego
Definiowany limit załączników
Wyróżnienie zgłoszeń o przekroczonym czasie reakcji
Raporty
Raport zgłoszeń, Historia zmian, Statystyka zgłoszeń
Pozostały czas na przyjęcie zgłoszenia/ do zakończenia
Widgety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane
Portal Web
Funkcje
Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu
Dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów
Widok “Mój dzień” zawierający oś czasu z aktywnością użytkownika
Rozbudowane filtry dla raportów tabelarycznych
Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami
Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji
Raporty dla każdego modułu w formie tabelarycznej
Obsługa helpdesk oraz bazy wiedzy, modułu RODO, modułu automatyzacja, modułu Sygnalita
Automatyczne logowanie przy pomocy aplikacji
Logowanie za pomocą poświadczeń domenowych (SSO), konta AzureAD lub AAD
Wydruk raportów tabelarycznych
Kontrola statystyk użytkowników
Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja,

zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania)
Przełączanie wersji językowej bez ponownego logowania do systemu
Nawigacja Breadcrumb
Funkcjonalności ogólne
Określanie praw dostępu do grup zasobów lub użytkowników
Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
Wersja angielska (en-US) interfejsu użytkownika
Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
Odczytywanie struktury organizacji z Active Directory
Skaner sieci wykorzystywany do wykrywania nowych urządzeń
Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta
Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
Definiowanie nieograniczonej liczby użytkowników systemu
Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy, Pracownicy
Indywidualny login i hasło dla poszczególnych użytkowników
Automatyczne logowanie do systemu
Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)
Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego
Określanie ról użytkowników - zarządzanie grupami
Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
Zgodny z pracą w sieciach WLAN
Podgląd aktualnych zadań serwera
Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami
Wyszukiwanie danych w tabelach raportów
Dowolne definiowania grup sprzętu i użytkowników
Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
Definiowanie i zapamiętywanie własnych widoków
Eksport danych bezpośrednio do MS Excel
Budowa zestawień metodą drag'n'drop
Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
Mechanizm kompresji pakietów danych przesyłanych przez Agenta
Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)

Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server
Mechanizm zdalnego pobierania bieżących aktualizacji do programu
Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
Dostęp do bazy wiedzy systemu
Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
Personalizacja pakietu instalacyjnego agenta
Określanie polityki haseł dla systemu
Zmiana języka systemu podczas logowania
Określenie numeru BDO przy definiowaniu rekordu firmy
Opcja resetu hasła podczas logowania
Globalne wyszukiwanie obiektów w systemie
Utworzenie atrybutów jako lista/słownik
Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
Wyszukiwarka ustawień w opcjach systemowych
Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
Skanowanie lasu domen
Budowa personalizowanego pakietu instalacyjnego
Automatyczne zamknięcie konsoli Master po zakończeniu sesji
Logowanie do portalu Web za pomocą mechanizmu Single Sign On
Logowanie operacji kont serwisowych
Security Key - dodatkowa metoda uwierzytelniania klientów przed połączeniem do serwera
Logowanie nieudanych prób uwierzytelnienia
Eksport danych diagnostycznych oraz dzienników operacji
Integracja z SMS API
Dodatkowe informacje
Kreator instalacyjny ułatwiający wdrożenie systemu
Aplikacja Master\Server\ Agent w wersji x64
Rozproszona architektura systemu: Serwer, Master, Agent (Możliwa praca każdego z komponentów na różnych komputerach)
Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019/2022 32/64 bit)
Praca w oparciu o PostgreSQL 10 lub nowszy
Szyfrowane połączenie pomiędzy serwerem programu, a bazą danych
Obsługa systemów operacyjnych - Agent: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
Obsługa systemów operacyjnych - Master : Windows Server 2008R2, Windows Server 2012,

Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
Obsługa systemów operacyjnych - Serwer: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert)
Sterowniki systemowe są podpisane certyfikatem Extended Validation (EV) Code Signing Certificate (GlobalSign) i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.
Oprogramowanie z licencją bez ograniczeń czasowych dla 1 konsoli zarządzającej Master oraz 20 Agentów z Asystą Serwisową na 2 lata.
Asysta Serwisowa winna być świadczona wyłącznie przez producenta oprogramowania i powinna zawierać bezpłatny dostęp do wszelkich uaktualnień programu, nowych wersji oraz bazy wzorców aplikacji, wielokanałowy dostęp do pomocy technicznej – telefon, e-mail, on-line

4) Macierz dyskowa

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Macierz dyskowa (1 kpl.)
Wymagana ilość 1 sztuka
Typ Online
Obudowa typu RACK o wysokości max. 2U wyposażony w szyny oraz elementy do montażu w szafie serwerowej, pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej
Urządzenie montowane jest do szafy RACK 19"
Zainstalowany min. sześciordzeniowy procesor ze sprzętowym mechanizmem szyfrowania AES 256bit i architekturze 64-bitów
min. 16 GB UDIMM DDR5 z możliwością rozbudowy
Obsługa min. 12 dysków oraz trybu RAID Single Disk, JBOD, RAID 0, 1, 5, 6, 10, 5 + hot spare, zabezpieczającą przed utratą danych
Kompatybilność dysków: 3,5-calowe dyski twarde SATA, 2,5-calowe dyski twarde SATA, 2,5-calowe dyski SSD SATA
Zainstalowane 12 dysków kązdy o parametrach minimum 4000 GB, Mix Use 6Gbps, 3.5, MTBF 1200000 godzin, uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
Wspierane systemy operacyjne min.: Apple Mac OS 10.10, Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12, IBM AIX 7, Solaris 10, Microsoft Windows 7, 8, 10, 11, Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 , 2022, 2025, Microsoft® Hyper-V
Wpierane przeglądarki: Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox
Obsługa RTRR (ang. Real-Time Remote Replication) umożliwiająca wykonywanie kopii zapasowych zarówno w czasie rzeczywistym jak i według harmonogramu
SNMP V2, V3
Zdalny dostęp min: PPTP, L2TP/IPSec, OpenVPN, Wake on LAN (WOL), Ramka Jumbo

Wbudowany serwer FTP z funkcjami SSL, TLS 1.3 oraz serwer VPN oraz MySQL,
Maksymalna ilość połączenie FTP min. 1000
Ochrona dostępu do sieci z funkcją automatycznego blokowania: SSH, Telnet, HTTP(S), FTP, CIFS/SMB, AFP
Min. 4 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) Min. 2 porty USB 3.2 Gen 2 (10 Gb/s), 2 porty USB 2.0
Ochrona systemu operacyjnego przed podwójnych rozruchem z wykorzystaniem pamięć flash min. 4 GB
Maksymalny wolumen min. 250 TB
Minimalny interwał migawki 5 minut
Pobór mocy: Tryb pracy, typowy maksimum 400 W
Min. 2 zasilacze o mocy co najmniej 500W, redundancyjne, dedykowane do zaoferowanego sprzętu zwymiarowane do wewnętrznych podzespołów, wymienne bez wyłączania systemu
Dźwiękowe ostrzeżenie systemowe
System chłodzenia min 3 wbudowane wetylatory
Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
Co najmniej 24 miesięczna gwarancja, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 2 godzin roboczych
W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe.
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu, wdrożenie: ● Montaż fizycznych składników rozwiązania, podłączenie i konfiguracja interfejsów sieciowych, konfiguracja interfejsów zarządzających serwerami, aktualizacja oprogramowania sprzętowego. ● Instalacja oprogramowania do zarządzania kopiami zapasowymi, konfiguracja, konfiguracja zadań tworzenia kopii zapasowych dla danego środowiska, weryfikacja kopii zapasowej - przywrócenie wybranej maszyny

5) Oprogramowanie do wykonywania kopii zapasowych

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Oprogramowanie do wykonywania kopii zapasowych (1 kpl.)
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej

Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla conajmniej trzech pamięci masowych to takiej puli.
Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.
Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS)
Oprogramowanie musi posiadać integracje z systemami typu SIEM
Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu.

Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications oraz logi audytowe i sign-in.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych
Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych
Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR
Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux
Rozwiązanie musi wspierać system operacyjny macOS
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu, wdrożenie: ● Instalacja oprogramowania do wykonywania kopii zapasowych, konfiguracja, konfiguracja zadań tworzenia kopii zapasowych dla danego środowiska, weryfikacja kopii zapasowej - przywrócenie wybranej maszyny

6) UTM

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) UTM - (1 kpl.)
Wymagana ilość 1 sztuka System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. Interfejsy, Dysk, Zasilanie: 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC. Parametry wydajnościowe: 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4.4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 Mbps. Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 10000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 5000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. Gwarancja oraz wsparcie 1. System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegają-cym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (ad-vanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

7) Switch zarządzalny

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Przełączniki sieciowe 24 porty(3 kpl.)
Wymagana ilość 3 sztuki
Typ zarządzalny gigabitowy switch
Obudowa typu RACK wyposażony w szyny oraz elementy do montażu w szafie serwerowej, pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej
Urządzenie montowane jest do szafy RACK 19"
Funkcja przełączania, tworzenia kopii lustrzanych lub agregowania na port
Inter-VLAN routing, routing statyczny i funkcjonalność serwera DHCP
Obsługa aplikacji mobilnych zapewniająca funkcjonalność udostępniania urządzenia, mapowania sieci i zarządzania ruchem w systemie z dowolnego miejsca poprzez zewnętrzny kontroler
Min. 24 gigabitowe porty RJ45 10/100/1000 Mb/s, 16 portów PoE+ 802.3af/at, 8 portów PoE++ 802.3bt
dwa porty 10Gbit/s SFP+
Przepustowość przełączania min 86 Gb/s
Całkowita przepustowość non-blocking: min 43 Gb/s
Dotykowy wyświetlacz prezentujący informacje o stanie połączeń z przeznaczeniem do łatwego monitorowania i szybkiego rozwiązywania problemów
Funkcje przełączania warstwy 2: IGMP snooping, STP/RSTP z priorytetami i wyłączaniem na poziomie portu, Izolacja portów, Kontrola burzowa,Voice VLAN, Port mirroring, Agregacja portów LACP, Ograniczenie szybkości transmisji multicast / broadcast, Blokowanie adresów MAC, Kontrola przepływu, Kontrola 802.1X, Ramki Jumbo, Ochrona pętli własnej,DHCP snooping / Guarding, Limitowanie szybkości egress, LLDP-MED, Port ograniczony według MAC, Izolacja urządzenia za pomocą ACL
Funkcje przełączania warstwy 3: DHCP dla sieci zarządzanych lokalnie, Przekaźnik DHCP, Routing między sieciami VLAN na tym samym przełączniku, Statyczne routowanie między lokalnymi sieciami, Izolacja sieci za pomocą ACL
Obsługa zewnętrznego interfejsu wejściowego DC jako dodatkowa funkcja zasilania do tworzenia kopii zapasowych w przypadku awarii wewnętrznego zasilacza.
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu wraz z ustawieniem reguły filtrowania kontroli listy dostępu oraz polityki bezpieczeństwa w oparciu o zaporę ogniową
Co najmniej 24 miesięczna gwarancja, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 2 godzin roboczych

Serwisowe zgłoszenia za pomocą kodów QR**.** W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Przełączniki sieciowe 8 portów (6 kpl.)
Wymagana ilość 6 sztuk
Typ zarządzalny gigabitowy switch pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej
Obsługa aplikacji mobilnych zapewniająca funkcjonalność udostępniania urządzenia, mapowania sieci i zarządzania ruchem w systemie z dowolnego miejsca poprzez zewnętrzny kontroler
Min. 8 portów GbE RJ45, 4 porty PoE/PoE+
dwa porty 10Gbit/s SFP+
Przepustowość przełączania min 86 Gb/s
Całkowita przepustowość non-blocking: min 43 Gb/s
Dotykowy wyświetlacz prezentujący informacje o stanie połączeń z przeznaczeniem do łatwego monitorowania i szybkiego rozwiązywania problemów
Funkcje przełączania warstwy 2: Zarządzanie IGMP, STP / RSTP z priorytetami i wyłączaniem na poziomie portu, Izolacja portu, Kontrola burzowa, VLAN głosowa, Lustrzane porty, Agregacja portów LACP, Ograniczenie przepustowości multicast / broadcast, Blokowanie adresów MAC, Kontrola przepływu, Kontrola 802.1X, Ramki Jumbo, Ochrona pętli własnej, Zarządzanie DHCP snooping / guard, Ograniczenie szybkości egress, LLDP-MED, Port ograniczony według adresu MAC, Izolacja urządzenia za pomocą ACL
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu wraz z ustawieniem reguły filtrowania kontroli listy dostępu oraz polityki bezpieczeństwa w oparciu o zaporę ogniową
Co najmniej 24 miesięczna gwarancja, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 2 godzin roboczych
Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Przełącznik sieciowe 4 porty (1 kpl.)

Wymagana ilość 1 sztuka	
Porty LAN	5x 10/100/1000 Mbit/s Ethernet
Liczba rdzeni procesora	min. 2
Taktowania procesora	min. 880 MHz
Liczba wątków	4

Pamięć RAM	256 MB
Pamięć wewnętrzna	minimum 12 MB FLASH
Napięcie wejściowe	8V - 30V DC
Maksymalny pobór mocy	10 W
Maksymalny pobór mocy bez osprzętu	5 W
Typ PoE	Pasywne PoE
Napięcie wejściowe PoE	8V - 30V
Slot na kartę pamięci	microSD
Port USB	1x USB
Monitor temperatury PCB	Tak
Monitor napięcia	Tak
Przycisk trybu pracy	Tak
Wsparcie serwera Dude	Tak
Sygnalizacja	diody LED
Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) wewnętrzny punkt dostępowy (1 kpl)	
Wymagana ilość 1 sztuka	
Typ: wewnętrzny punkt dostępowy	
Standard pracy minimum 802.11ax	
Standardy Wi-Fi: 02.11a/b/g, 4/ 5/ 6	
Pasma: 5 GHz 4x4 MU-MIMO i OFDMA z szybkością radiową 4,8 Gb/s, 2,4 GHz 2x2 MIMO i OFDMA z szybkością radiową 573,5 Mb/s	
Interfejs: Ethernet, Bluetooth,	
VLAN 802.1Q,	
Ilość obsługiwanych klientów jednocześnie minimum 300, Izolacja ruchu gości	
Zasilanie 802.3at, PoE+	
Zabezpieczenia bezprzewodowe: WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3), Izolacja ruchu gości	
Minimum stopień ochrony IP54	
Waga z mocowaniem maksimum 600 g	
Mocowanie Ścienne oraz Sufitowe	
W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe.	
Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.	
Co najmniej 24 miesięczna gwarancja, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 2 godzin roboczych w godzinach pracy Zamawiającego tj.: Poniedziałek: 8:00 - 16:00, Wtorek - Piątek: 7:00 - 15:00	
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu • Montaż fizycznych składników rozwiązania, podłączenie i konfiguracja interfejsów sieciowych, konfiguracja interfejsów zarządzających serwerami, aktualizacja oprogramowania sprzętowego. • Utworzenie odseparowanych podsieci oraz izolacja ruchu według zlecenia Zamawiającego.	

• Zabezpieczenie dostępu bezprzewodowego do zasobów sieciowych • Montaż bezprzewodowych punktów dostępowych we wskazanych lokalizacjach • Konfiguracja podsieci UTM, przełącznik, punkt dostępowy • Utworzenie sieci „Dla Gości" uniemożliwiającej dostęp do zasobów Zamawiającego.

8) Network Attached Storage – NAS

Wymagane minimalne parametry techniczne komponentu (wymagania jakościowe) Network Attached Storage – NAS (1 kpl.)
Wymagana ilość 1 sztuka
Typ Online
Obudowa typu RACK o wysokości max. 2U wyposażony w szyny oraz elementy do montażu w szafie serwerowej, pochodzący z oficjalnego kanału dystrybucji na rynek Unii Europejskiej
Urządzenie montowane jest do szafy RACK 19",
Zainstalowany min. dwurdzeniowy procesor ze sprzętowym mechanizmem szyfrowania AES 256bit i architekturze 64-bitów
min. 8 GB SODIMM DDR4 z możliwością rozbudowy
Obsługa min. 4 dysków oraz trybu RAID Single Disk, JBOD, RAID 0, 1, 5, 6, 10, 5 + hot spare, zabezpieczającą przed utratą danych
Kompatybilność dysków: 3,5-calowe dyski twarde SATA, 2,5-calowe dyski twarde SATA, 2,5-calowe dyski SSD SATA
Zainstalowane min. 4 dysków, 4000 GB, Mix Use 6Gbps, 3.5, MTBF 1200000 godzin, Uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
Wspierane systemy operacyjne min.: Apple Mac OS 10.10, Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12, IBM AIX 7, Solaris 10, Microsoft Windows 7, 8, 10, 11, Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 , 2022
Wpierane przeglądarki: Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox
Obsługa RTRR (ang. Real-Time Remote Replication) umożliwiająca wykonywanie kopii zapasowych zarówno w czasie rzeczywistym jak i według harmonogramu
SNMP V2, V3
Zdalny dostęp min: PPTP, L2TP/IPSec, OpenVPN, Wake on LAN (WOL), Ramka Jumbo
Wbudowany serwer FTP z funkcjami SSL, TLS 1.3 oraz serwer VPN oraz MySQL
Ochrona dostępu do sieci z funkcją automatycznego blokowania: SSH, Telnet, HTTP(S), FTP, CIFS/SMB, AFP
Min. 2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) Min. 2 porty USB 3.2 Gen 2 (10 Gb/s), 2 porty USB 2.0 Min. 1 Wyjście HDMI
Ochrona systemu operacyjnego przed podwójnych rozruchem z wykorzystaniem pamięć flash min. 4 GB
Maksymalny wolumen min. 250 TB

Minimalny interwał migawki 5 minut
Pobór mocy: Tryb pracy, typowy maksimum 36 W
Dźwiękowe ostrzeżenie systemowe
Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
Co najmniej 24 miesięczna gwarancja, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 4 godzin roboczych w godzinach pracy Zamawiającego tj.: Poniedziałek – Piątek 7:30 – 15:30
W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe
W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu, wdrożenie: • Montaż fizycznych składników rozwiązania, podłączenie i konfiguracja interfejsów sieciowych, konfiguracja interfejsów zarządzających serwerami, aktualizacja oprogramowania sprzętowego. • Instalacja oprogramowania do zarządzania kopiami zapasowymi, konfiguracja, konfiguracja zadań tworzenia kopii zapasowych dla danego środowiska, weryfikacja kopii zapasowej - przywrócenie wybranej maszyny

1. Zamawiający dopuszcza oferowanie materiałów lub rozwiązań równoważnych, pod warunkiem, że zagwarantują one wykonanie zamówienia w zgodzie z treścią zapytania ofertowego oraz zapewnią uzyskanie parametrów technicznych i użytkowych nie gorszych od założonych w wyżej wymienionych dokumentach. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji, na Wykonawcy ciąży obowiązek każdorazowego przedłożenia Zamawiającemu stosownych dokumentów, stwierdzających, że proponowane materiały, dostawy i technologia zamienne spełniają (nie są gorsze) warunki/parametry techniczne i użytkowe zawarte w dokumentacji postępowania. Obowiązek udowodnienia równoważności powiązań technicznych i użytkowych leży wyłącznie po stronie Wykonawcy. We wszystkich przypadkach wymagania techniczne mają pierwszeństwo przed standardami producenta
2. Wymagane minimalne parametry techniczne komponentów wymienionych w ust. 3 stanowią wymagania jakościowe w rozumieniu art. 246 ust. 2 ustawy Pzp.
3. W przypadku, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały normy, znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, charakteryzujące określone produkty lub usługi, oznacza to, że zamawiający nie mógł opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na normy, znaki towarowe,

patenty, pochodzenie, źródło lub szczególny proces należy odczytywać z wyrazami „lub równoważne”.

4. Wykonawca ponosi odpowiedzialność za jakość i ilość przekazanego sprzętu.
5. Wymagany termin wykonania zamówienia to maksymalnie 60 dni roboczych od dnia podpisania umowy.
6. Wykonawca będzie związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
7. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny.
8. Podstawą do płatności jest prawidłowo wystawiona faktura, po zaakceptowaniu protokołu zdawczego.
9. Po zaakceptowaniu przez strony protokołu zdawczego i wystawieniu faktury - w terminie 14 dni.