**Pakiet 1 – elementy składowe pakietu:**

1. **Serwer NAS - 1 sztuka**

Wymagane parametry (jednostka centralna):

**a) Procesor:**

Procesor wielordzeniowy 4-rdzeniowy 64bit, taktowanie min 2,2 GHz

**b) Płyta główna:**

Złącza minimum: 2x USB 3.2.1, 2x 10 GbE SFP+

**c) Pamięć RAM:**

Typ pamięci: DDR4

Pojemność: min. 32 GB

**d) Zasilacz:**

Moc: min. 100 W

**e) Obudowa:** Rack (1U)

**f) Wnęki na dyski:** min. 4

**g) Obsługa SSD cache**

**h) Wnęki dysków SSD M.2:** min. 2

**i)Hot-Swap**

**j) System plików:**

EXT4, EXT3, FAT32, NTFS, HFS+, exFAT

k)**Wymiary(wys. x szer. x gł.):** 43,3 × 430 × 292,12 mm

l)**Minimalny okres gwarancji 36 miesięcy**

Dyski do serwera klasa enterprise: ilość: 4 sztuki

Wymagane minimalne parametry (dyski):

**a) Pojemność:** 8 TB

**b) Interfejs:** SATA III (min. 6Gb/s)

**c) Pamięć podręczna:** min 256 MB

**d) Prędkość obrotowa:** 7200 obr./min

**e)** **Nominalny czas pracy:** min. 2 mln godzin

**f)** **Technologia CMR:** Tak

**g)** **Typ:** korporacyjne, 3.5”

**h) Minimalny okres gwarancji 60 miesięcy**

Akcesoria: ilość: 1 komplet

1. Komplet szyn do montażu w szafie typu RACK 19”
2. Kable zasilające

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**

1. **Ochrona antywirusowa na okres 36 miesięcy**

Typ: Oprogramowanie antywirusowe

Ilość: Licencje serwerowe: 5 szt. ; Licencje przeznaczone do komputerów klasy PC: 110 szt.

Wymagania:

Ochrona antywirusowa systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

* + Microsoft Windows 7 z dodatkiem SP1
  + Microsoft Windows 8.1
  + Microsoft Windows 10
  + Microsoft Windows 11
  + macOS 11 "Big Sur"
  + macOS 10.15 "Catalina"
  + macOS 10.14 "Mojave"

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

* + Microsoft Windows Server 2008 R2
  + Microsoft Windows Server 2012
  + Microsoft Windows Server 2016
  + Microsoft Windows Server 2019
  + Microsoft Windows Server 2022

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

* + Microsoft Internet Explorer
  + Microsoft Edge
  + Mozilla Firefox
  + Google Chrome
  + Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

# Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
26. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
27. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
28. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
29. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
30. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
31. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne (przez pliki wykonywalne rozumie się co najmniej: aplikacje, interpretowalną zawartość Flash, Sliverlight, skrypty oraz makra dokumentów pakietu Office).
32. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
34. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
35. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
36. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
37. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
38. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
39. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
40. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
41. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
42. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
43. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla Firefox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
44. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
45. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
46. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
47. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
48. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
49. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
50. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna” poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
51. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
53. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
54. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
55. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
56. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
57. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy, oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
58. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
59. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
60. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch managment), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
61. Mechanizm aktualizacji aplikacji (patch managment) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
62. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
63. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
64. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
65. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
66. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
67. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
68. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
69. Mechanizm aktualizacji aplikacji (patch managment) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
70. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
71. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
72. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
73. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
74. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
75. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
76. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
77. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
78. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
79. Rozwiązanie posiada możliwość zabezpieczenia zmian w konfiguracji przez użytkownika końcowego przy wykorzystaniu hasła.
80. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
81. *Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.*
82. *Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.*
83. *Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.*
84. *Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.*
85. *Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.*
86. *Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.*
87. *Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.*
88. *Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.*
89. *Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.*

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
26. Z poziomu portalu zarządzającego isnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
27. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
28. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
29. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
30. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
31. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

**3. System ochrony typu EDR na okres 36 miesięcy**

Ilość : Licencje przeznaczone na komputery klasy PC: 110 szt.

Wymagania:

System EDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

* Microsoft Windows 7 z dodatkiem SP1
* Microsoft Windows 8.1 (32-bit i 64-bit)
* Microsoft Windows 10
* Microsoft Windows 11
* MacOS 11 “Big Sur”
* MacOS 10.15 “Catalina”
* MacOS 10.14 “Mojave”

Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

* Microsoft® Windows Server 2008 R2
* Microsoft® Windows Server 2012
* Microsoft® Windows Server 2016
* Microsoft® Windows Server 2019
* Microsoft® Windows Server 2022

Wspierane przeglądarki internetowe:

* Microsoft Edge
* Mozilla Firefox
* Google Chrome
* Safari

Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
   * dostęp do pliku;
   * tworzenie nowego procesu;
   * nawiązane połączenia sieciowe;
   * wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
   * zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
9. Maksymalna ilość wysyłanych danych przez agenta uruchomionego na stacji roboczej z systemami Windows nie przekracza 25MB na 24 godziny.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
11. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
12. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
13. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
14. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
15. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
16. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
17. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
18. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
19. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
20. Każda detekcja zawiera co najmniej następujące informacje:
    * Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
    * Data i czas wystąpienia podejrzanych zdarzeń.
    * Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
    * Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
    * Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
    * Poziom ryzyka, określający istotność danej detekcji.
    * Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
21. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
22. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
23. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
24. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
25. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
26. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
27. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
28. Rozwiązanie monitoruje aplikacje uruchomione na stacjach roboczych i serwerach i oznacza aplikacje zidentyfikowane jako szkodliwe lub potencjalnie niebezpieczne dla użytkownika.
29. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
30. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
31. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
32. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
33. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
34. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
35. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
36. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
37. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
38. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
39. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
40. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
41. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
42. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

**4. Pakiet oprogramowania biurowego**

Ilość: 24 sztuki

Wymagania:

|  |  |
| --- | --- |
| Typ produktu: | Pakiet biurowy zawierający: Edytor tekstu, Arkusz kalkulacyjny, Program pocztowy, Program do prezentacji |
| Zastosowanie: | Biurowe |
| Architektura programu: | 64-Bit |
| Typ DRM: | Platforma producenta jak systemu operacyjnego |
| Rodzaj licencji: | Komercyjna |
| Liczba stanowisk: | 1 |
| Okres licencji: | Dożywotnia |
| Wersja językowa: | Wszystkie języki Eurozone |
| Rodzaj wydania: | Licencja z kluczem aktywacyjnym |
| Dodatkowe informacje: | Kompatybilny z systemami Windows oraz Mac |

Oprogramowanie powinno być dostarczone w najnowszej dostępnej aktualnie wersji.

**5. System do automatyzacji kopii zapasowych – serwery NAS**

**Ilość: 2 szt**

Sprzęt - wymagania:

|  |  |
| --- | --- |
|  | **Charakterystyka  (wymagania minimalne)** |
| Przeznaczenie | Sprzęt do wykonywania kopi zapasowych danych na serwerach fizycznych  i wirtualnych |
| Procesor | Procesor osiągający wynik minimum 4500 punktów w teście PassMark. |
| Obudowa | Typu rack o wysokości 2U i wymiarach maksymalnych 88 mm x 490 mm x 410 mm (wysokość x szerokość x głębokość) wraz z szynami umożliwiającymi montaż w szafie rack w zestawie. |
| Pamięć RAM | 32 GB pamięci SO-DIMM DDR4 ECC |
| Ilość obsługiwanych dysków | Minimum 8 dysków o maksymalnej pojemności 18TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków. |
| Zainstalowane dyski | 8 dysków o pojemności 4TB każdy zgodne z listą kompatybilności oferowanej macierzy oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 5400 RPM,  - pamięć cache: minimum 256MB,  - gwarancja: minimum 36 miesięcy,  - MTBF: minimum 1 milion,  - usługa odzyskiwania danych, |
| Interfejsy sieciowe | 4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation.  Możliwość rozszerzenia o dodatkowe 2 porty 10Gb SFP+ / RJ-45. |
| Porty | Minimum 2 x USB 3.2 1. Generacj 1, 1 x eSATA |
| Wskaźniki LED | Status,HDD1-8, zasilanie,LAN1-4 |
| Obsługa RAID | Basic, JBOD, RAID 0,1,5,6,10, SHR wraz z obsługa dysków typu hot spare. |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. |
| Licencja na Kamery IP | W zestawie licencja na minimum dwie kamery z możliwością rozszerzenia do 40. |
| Maks. liczba kamer IP | Obsługa do 40 kamer. |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| Usługi | Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość utworzenia klastra wysokiej dostępności z dwóch takich samych urządzeń, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów, możliwość wykonywania kopii zapasowej typu bare-metal dla komputerów z systemem Windows oraz wykonywanie kopii zapasowych maszyn wirtualnych z Hyper-V i VMware poprzez centralną konsolę zarządzania. |
| Obsługa migawek | Maksymalna liczba migawek folderów współdzielonych: 1024 |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów |
| Język GUI | Polski |
| Gwarancja i serwis | Minimum 3 lata gwarancji z opcją rozszerzenia do 5 lat. |
| Waga | Maksymalnie 12 kg |
| Pobór mocy | Maksymalnie 65W w trybie pracy. Maksymalnie 30W w trybie hibernacja dysków. |
| Certyfikaty | EAC, VCCI, CCC, RCM, KC, FCC, CE, BSMI |
| System plików | Dyski wewnętrzne Btrfs lub EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) |
| Liczba wolumenów | Do 64 |
| Liczba iSCSI Targetów | Do 128 |
| Liczba iSCSI LUN | Do 256 |
| Liczba kont użytkowników | Do 2048 |
| Liczba grup | Do 256 |
| Liczba folderów udostępnionych | Minimum 512 |
| Ilość jednoczesnych połączeń | Minimum 1000 dla CIFS/AFP/NFS/FTP/WebDAV |
| Głośność pracy | Maksymalnie 45 dB(A) |
| Zasilacz | Redundantny zasilacz o mocy minimalnie 350W |
| Chłodzenie | Minimum 2 wentylatory o rozmiarze 80 mm x 80 mm |
| Usługi dodatkowe | Przeprowadzenie szkolenia z zakresu obsługi systemu operacyjnego macierzy oraz zarządzania zintegrowanym narzędziem do wykonywania kopii zapasowych przez autoryzowanego dystrybutora oferowanego rozwiązania.  Zakres szkolenia powinien obejmować:  - instalację systemu operacyjnego,  - konfigurację pul pamięci oraz wolumenów,  - tworzenie folderów współdzielonych, użytkowników i grup,  - weryfikację ustawień sieciowych oraz kwestii związanych z bezpieczeństwem,  - wykonywanie kopii zapasowych danych składowanych na serwerze,  - włączenie mechanizmu migawek wraz z omówieniem najlepszych praktyk,  - tworzenie kopii zapasowych komputerów PC, serwerów fizycznych oraz maszyn wirtualnych na poziomie plikowym jak i bare-metal,  - zarządzanie przechowywaniem kopii zapasowych oraz ich wersjonowaniem,  - metodykę przywracania kopi oraz postępowania w przypadku awarii komputera lub maszyny wirtualnej,  - nadzorowanie oraz monitorowanie systemem kopii zapasowych oraz systemem operacyjnym,  - Szkolenie powinno potrwać minimum 6 godzin lub więcej jeżeli wszystkie zagadnienia nie zostaną omówione w założonym okresie czasu.  Wykonawca przedłoży do  oferty oświadczenie autoryzowanego partnera producenta ,iż szkolenie przeprowadzone będzie przez certyfikowanych inżynierów posiadających autoryzacje oferowanego  w postepowaniu  produktu |

Oprogramowanie - wymagania:

|  |  |  |
| --- | --- | --- |
|  | Konsola administratora | * Zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows, komputerów, serwerów plików rsync/SMB oraz maszyn wirtualnych VMware vSphere/Microsoft Hyper-V. * Centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych. * Różne metody przywracania, w tym przywracanie całego urządzenia, natychmiastowe przywracanie, szczegółowe odzyskiwanie plików. * Maksymalna wydajność tworzenia kopii zapasowych i pamięci masowej dzięki zastosowaniu funkcji Changed Block Tracking (CBT), narzędzia RCT (Resident Change Tracking) oraz deduplikacji globalnej w miejscu składowania kopii zapasowych. * Elastyczne zasady planowania i przechowywania w celu dostosowywania strategii tworzenia kopii zapasowych. * Szczegółowe logi i raporty umożliwiające śledzenie stanów kopii zapasowych i diagnostykę problemów. |
|  | Komputery osobiste i serwery fizyczne z systemem Windows | * Obsługa systemu plików NTFS. * Tryby tworzenia kopii zapasowej: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu. * Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów oraz przywracanie na poziomie woluminów, natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora na serwerze NAS. * Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu. * Korzystanie z funkcji śledzenia zmiany bloków Changed Block Tracking opartej na usłudze Microsoft VSS do tworzenia przyrostowych kopii zapasowych. * Zdarzenia tworzenia kopii zapasowych wyzwalane zdarzeniami obejmują blokadę ekranu urządzenia, wylogowanie użytkownika i uruchamianie urządzeń. * Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej. * Obsługa wstawiania argumentów (adres IP serwera NAS, nazwa użytkownika, hasło) do instalatora .msi w celu masowego wdrażania programu (agenta). |
|  | Komputery osobiste i serwery fizyczne z systemem Linux | * Obsługa systemu plików ext2, ext3, ext4, XFS. * Tryby tworzenia kopii zapasowych: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu. * Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie na poziomie woluminów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora. Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu. * Korzystanie z funkcji do śledzenia zmiany bloków Changed Block Tracking w oparciu o sterownik migawki systemu Linux w celu wykonywania przyrostowych kopii zapasowych. * Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej. |
|  | Maszyny wirtualne | * Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK. * Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0. * W przypadku tworzenia kopii zapasowych Microsoft Hyper-V wymagany jest wolumin systemowy hosta z co najmniej 512 MB wolnego miejsca w celu zainstalowania narzędzia do przenoszenia danych. * Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu. * Kopia zapasowa bez agentów. * Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej * Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych. * Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora na serwerze NAS. * W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, I ext4. * Kopia zapasowa uwzględniające aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS). * Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V. |
|  | Obsługiwane systemy | Obsługiwane platformy:   1. Windows: Windows 11 (wszystkie wersje), Windows 10 Creators Update, Windows 10, Windows 8.1, Windows 7 SP1. 2. Windows Server: Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 i Windows Server 2022. 3. Linux: CentOS 6.10, 7.8, 8.1, RHEL 6.10, 7.8, 8.1, 8.4, 8.5 Ubuntu 16.04, 18.04, 20.04, Fedora 30, 31, 32, Debian 8.0, 9.0, 10, 11. 4. VMware vSphere: VMware vSphere 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 i 7.0.0 (Obsługiwane wersje VMware vSphere: VMware free ESXi, VMware vSphere Essentials, VMware vSphere Essentials Plus, VMware vSphere Standard, VMware vSphere Advanced, VMware vSphere Enterprise i VMware vSphere Enterprise Plus) 5. Microsoft Hyper-V: Hyper-V 2016 i 2019 (Obsługiwane klastry przełączania awaryjnego Microsoft Hyper-V: Hyper-V 2016 i Hyper-V 2019) 6. Serwery plików:   a) wykorzystujące protokół SMB w wersjach SMB1, SMB2 i SMB3,  b) wykorzystujące protokół rsync w wersji 3.0 lub nowszej. |
|  | Wymagane licencje | Komputery osobiste z systemem Windows:110 szt.  Serwery fizyczne z systemem Windows: 5 szt. |

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**

**6. Przełącznik sieciowy (switch) zarządzalny**

Ilość: 2 szt.   
Wymagania:

Typ obudowy: Do szaf RACK

Zarządzanie: Zarządzalny L2

Dostęp:Wiersz poleceń (CLI)

SNMP v1/v2c/v3

RMON

SNTP

Telnet

Architektura sieci: Gigabit Ethernet

Całkowita liczba portów: 52

Złącza : RJ-45 10/100/1000 Mbps - 48 szt.

SFP+ - 4 szt.

Obsługiwane standardy: IEEE 802.3

IEEE 802.3 u

IEEE 802.3 x

IEEE 802.3 ab

IEEE 802.3 ae

Rozmiar tablicy MAC: 16 k

Ramka Jumbo: 9,216 B

Liczba grup VLAN: 4096

Algorytm przełączania: Store-and-forward

Szybkość przekierowań pakietów: 131 Mb/s

Przepustowość: 176 Gb/s

Bufor pamięci: 3 MB

Warstwa przełączania: 2

Materiał obudowy: Metal

Dodatkowe informacje: Automatyczne krosowanie portów (Auto MDI-MDIX)

Automatyczna negocjacja szybkości połączeń

Automatyczne rozpoznawanie kabla krosowego (MDI/MDIX)

Praca w trybie half i full-duplex

SNMP

Dołączone akcesoria: Kabel zasilający

Gwarancja: 24 miesiące (gwarancja producenta)

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**

**7.** **Przełącznik sieciowy (switch) zarządzalny**

Ilość: 9 szt.

Wymagania:

Typ obudowy: Do szaf RACK

Zarządzanie: Zarządzalny L2

Dostęp: Przeglądarka WWW (GUI)

Wiersz poleceń (CLI)

SNMP v1/v2c/v3

RMON

Telnet

Architektura sieci: Gigabit Ethernet

Całkowita liczba portów: 28

Złącza : RJ-45 10/100/1000 Mbps - 24 szt.

SFP+ - 4 szt.

Obsługiwane standardy: IEEE 802.3

IEEE 802.3 u

IEEE 802.3 x

IEEE 802.3 ab

IEEE 802.3 ae

Rozmiar tablicy MAC: 16 k

Ramka Jumbo: 9,000 B

Liczba grup VLAN: 4096

Algorytm przełączania: Store-and-forward

Przepustowość: 128 Gb/s

Bufor pamięci: 1,5 MB

MTBF: 516 593 h

Dodatkowe informacje: Automatyczne krosowanie portów (Auto MDI-MDIX)

Diagnostyka przewodów

Praca w trybie half i full-duplex

QoS

VLAN

Gwarancja: 24 miesiące (gwarancja producenta)

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**

**8. Przełącznik sieciowy (switch) zarządzalny**

Ilość: 2szt.

Wymagania:

|  |  |
| --- | --- |
| Porty | • 16 Slotów SFP+ 10GE • 1 Port konsolowy RJ45 • 1 Port konsolowy Micro-USB |
| Zasilanie | 100-240 V AC~50/60 Hz |
| Montaż | Montaż w szafie Rack |

| WYDAJNOŚĆ | |
| --- | --- |
| Wydajność przełączania | 320 Gb/s |
| Szybkość przekierowań pakietów | 238.08 Mpps |
| Tablica adresów MAC | 32 K |
| Bufor pakietów | 24 Mb |
| Ramki jumbo | 9 KB |

| FUNKCJE OPROGRAMOWANIA | |
| --- | --- |
| Funkcja Quality of Service | • 8 kolejek priorytetowania • Obsługa priorytetowania 802.1p CoS/DSCP • Tryb harmonogramu priorytetowania: - SP (Strict Priority) - WRR (Weighted Round Robin) - SP+WRR • Kontrola przepustowości - Ograniczanie prędkości transferu w oparciu o port/przepływ danych • Płynniejsze działanie • Działania dla przepływów - Mirror (do obsługiwanego interfejsu) - Redirect (do obsługiwanego interfejsu) - Limit prędkości - QoS Remark |
| Funkcje L2 i L2+ | • Agregacja łączy - Statyczna agregacja łączy - LACP 802.3ad - Do 8 grup agregacji i do 8 portów na grupę • Protokół drzewa rozpinającego (STP) - STP 802.1d - RSTP 802.1w - MSTP 802.1s - Zabezpieczenia STP: ochrona TC, filtrowanie poprzez pakiety BPDU, ochrona Root • Wykrywanie pętli zwrotnych - Oparte na portach - Oparte na VLAN • Kontrola przepływu - Kontrola przepływu 802.3x - Zapobieganie blokowaniu HOL • Mirroring - Port Mirroring - Mirroring procesora - Przesył One-to-One - Przesył Many-to-One - Port wejścia/wyjścia / obydwa porty |
| L2 Multicast | • IGMP Snooping - IGMP v1/v2/v3 Snooping - Fast Leave - IGMP Snooping Querier - Uwierzytelnianie IGMP • Uwierzytelnianie IGMP • MVR • MLD Snooping - MLD v1/v2 Snooping - Fast Leave - MLD Snooping Querier - Konfiguracja grupy statycznej - Ograniczone przekazywanie IP Multicast • Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil |
| Sieci VLAN | • Grupy VLAN - Maks. 4K grup VLAN • Tagowanie 802.1Q VLAN • Adres MAC VLAN: 30 wpisów • Protokół VLAN • Prywatna sieć VLAN • GVRP • VLAN VPN (QinQ) - QinQ oparty na portach - Selective QinQ • Głosowa sieć VLAN |
| Listy kontroli dostępu | • Time-based ACL • MAC ACL - Source MAC - Destination MAC - VLAN ID - User Priority - Ether Type • IP ACL -Source IP - Destination IP - Fragment - IP Protocol - TCP Flag - TCP/UDP Port - DSCP/IP TOS - User Priority • Combined ACL • Packet Content ACL • IPv6 ACL • Policy - Mirroring - Redirect - Rate Limit - QoS Remark • ACL apply to Port/VLAN |
| Bezpieczeństwo transmisji | • Wiązanie adresów IP, MAC i portów - 512 wpisów - DHCP Snooping - Inspekcja ARP - Ochrona źródłowego adresu IPv4: 100 wpisów • Wiązanie adresów IPv6, MAC i portów - 512 wpisów - DHCPv6 Snooping - Wykrywanie ND - Ochrona źródłowego adresu IPv6: 100 wpisów • Ochrona przed atakami DoS • Ochrona portów poprzez ich statyczną/dynamiczną konfigurację - Do 64 adresów MAC na port • Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) • Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC - Przydzielanie VLAN - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius • AAA (w tym TACACS+) • Izolacja portów • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 • Kontrola dostępu w oparciu o IP/port/MAC |
| IPv6 | • IPv6 Dual IPv4/IPv6 • Multicast Listener Discovery (MLD) Snooping • ACL IPv6 • Interfejs IPv6 • Statyczny routing IPv6 • Funkcja neighbor discovery (ND) wykorzystywana przez węzły IPv6 • Path maximum transmission unit (MTU) discovery • ICMP v6 • TCP v6/UDP v6 • Zastosowania protokołu IPv6: - Klient DHCPv6 - Ping6 - Tracert6 - Telnet (v6) - SNMP IPv6 - SSH IPv6 - SSL IPv6 - Http/Https - TFTP IPv6 |
| Cechy przełącznika L3 | • 16 interfejsów IPv4/IPv6 • Routing statyczny - 48 tras statycznych • Wpisy statyczne ARP - 128 wpisów statycznych • Proxy ARP • Gratuitous ARP • Serwer DHCP • DHCP Relay - DHCP Interface Relay - DHCP VLAN Relay • DHCP L2 Relay |
| Funkcje zaawansowane | • Automatyczne wykrywanie urządzeń • Konfiguracje grupowe • Grupowe aktualizacje oprogramowania • Inteligentne monitorowanie stanu sieci • Ostrzeżenia o nietypowych zdarzeniach • Ujednolicony proces konfiguracji • Harmonogram restartu • Bezobsługowa konfiguracja ZTP\* |
| MIBs | • Bazy danych MIB II (RFC1213) • Porty MIB (RFC2233) • Port Ethernet MIB (RFC1643) • Bridge MIB (RFC1493) • P/Q-Bridge MIB (RFC2674) • RMON MIB (RFC2819) • RMON2 MIB (RFC2021) • Radius Accounting Client MIB (RFC2620) • Radius Authentication Client MIB (RFC2618) • Pakiety Ping i Traceroute do interfejsu MIB (RFC2925) • Obsługa prywatnych baz danych MIB TP-Link |

| ZARZĄDZANIE | |
| --- | --- |
| Funkcje panelu zarządzania | • Interfejs graficzny GUI • Interfejs linii poleceń CLI • SNMP v1/v2c/v3 - Trap/Inform - RMON (grupy 1, 2, 3, 9) • Szablon SDM • Klient DHCP/BOOTP • 802.1ab LLDP/LLDP-MED • Autoinstalacja DHCP • Dual Image, Dual Configuration • Monitorowanie zużycia procesora • Diagnostyka kabli • EEE • Odzyskiwanie hasła • SNTP • Logi systemowe |

|  |  |
| --- | --- |
| Certyfikaty | CE, FCC, RoHS |
| Akcesoria | • 2 Przewody zasilające • Instrukcja szybkiej instalacji • Zestaw do montażu w szafie Rack • Gumowe nóżki |
| Wymagania systemowe | Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ or Windows 7/8/10/11, MAC® OS, NetWare®, UNIX® or Linux. |

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**

**9. Moduły światłowodowe SFP +**

Ilość: 30 par

Wymagania:

Komplet modułów SFP+ 10G WDM 1270/1330NM SM 20KM

Komplet dwóch wkładek jednomodowych SFP (stanowiących jedną parę) pracujących dwukierunkowo na jednym włóknie na falach 1270/1330 nm,   
na dystansie wynoszącym do 20 km. Interfejs elektryczny światłowodowego modułu SFP 10G zgodny ze specyfikacjami elektrycznymi SFI. Odbiornik przetwarza szeregowe dane optyczne o prędkości 10 Gbit/s na szeregowe dane elektryczne PECL/CML.

Najważniejsze parametry techniczne:

Wydajność - Typ transceivera SFP: Swiatłowód

Wydajność - Wsparcie dla Single-mode fiber (SMF): Tak

Wydajność - Maksymalny dystans transferu: 20000 m

Wydajność - Tx długości fali (min): 1270 nm

Wydajność - Długość fali RX (min): 1330 nm

Światłowód - Złącze światłowodowe: LC

Cechy - Maksymalna szybkość przesyłania danych: 10000 Mbit/s

Cechy - Certyfikaty: FCC

Dane opakowania - Liczba dołączonych produktów: 2 szt (1 para)

Pozostałe funkcje - Typ interfejsu: SFP+

Szczegóły Techniczne - Certyfikat środowiskowy: CE, RoHS

Klasyfikacja - Kod producenta: EX.6211

Klasyfikacja - EAN: 5902560366211

Klasyfikacja - ID Produktu: 93453651

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**

**10. Zintegrowany system zarządzania infrastrukturą IT**

Ilość nowych licencji: 10szt.

Ilość licencji do odnowienia: 110szt.

Wymagania, jakie system powinien spełniać:

**MONITOROWANIE INFRASTRUKTURY** (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

✓ wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping

✓ wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)

✓ wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci

✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.

✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.

✓ wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.

✓ wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.

✓ wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny. ✓ zablokowania mapy urządzeń przed przypadkową edycją.

✓ serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.

✓ serwerów pocztowych: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), - program ma możliwość wykonywania operacji testowych, - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.

✓ monitorowania serwerów WWW i adresów URL.

✓ cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.

✓ obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.

✓ obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.

✓ obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.

✓ monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych – graficzna prezentacja panelu switcha, - ruchu generowanego przez podłączone do portów stacje robocze.

✓ serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.

✓ wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.

✓ wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program umożliwia również definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

**W ZAKRESIE INWENTARYZACJI** program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.

2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.

3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.

4. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.

5. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.

6. Umożliwia odczytanie numeru seryjnego (klucze licencyjne).

7. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.

9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).

10. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

**Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:**

✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,

✓ tworzenia powiązań między zasobami a urządzeniami,

✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,

✓ wskazania osób uprawnionych do użycia zasobów,

✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,

✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,

✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,

✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,

✓ importu danych z zewnętrznego źródła (.CSV),

✓ przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,

✓ tworzenia powiązań między zasobami a dokumentami w relacji 1:N,

✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,

✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,

✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,

✓ generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,

✓ archiwizacji i porównywania audytów zasobów,

✓ tworzenia kodów kreskowych dla zasobów,

✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,

✓ inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,

✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),

✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Dodatkowo dostępny jest Agent inwentaryzacji na system Android.

**Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:**

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.

2. Informacje o aplikacjach używanych w organizacji.

3. Tworzenie własnych wzorców aplikacji.

4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

5. Informacje o komputerach, na których aplikacja została wykryta.

6. Zarządzanie posiadanymi licencjami.

7. Wskazywanie osób odpowiedzialnych za licencję.

8. Wskazanie użytkowników licencji. 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

10. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.

12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe posiadają możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

✓ Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),

✓ Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

✓ Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,

✓ Informacji o edytowanych przez użytkownika dokumentach,

✓ Historii pracy (cykliczne zrzuty ekranowe),

✓ Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),

✓ Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

✓ Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,

✓ Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail. Program ponadto posiada możliwość:

✓ blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

✓ blokowania ruchu na wskazanych portach TCP/IP,

✓ blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,

✓ wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,

✓ przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),

✓ definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

**PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM**. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten zawiera również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic).

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

**Moduł pomocy zdalnej umożliwia również:**

✓ pobieranie listy użytkowników z Active Directory,

✓ zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,

✓ zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,

✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,

✓ tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii),

✓ automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,

✓ procesowanie zgłoszeń użytkowników z wiadomości e-mail,

✓ tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,

✓ wykonywanie operacji na wielu zgłoszeniach równocześnie,

✓ dołączanie załączników do zgłoszeń,

✓ rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,

✓ szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,

✓ wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,

✓ zrzuty ekranowe (podgląd pulpitu),

✓ dystrybucję oprogramowania przez Agenty,

✓ dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),

✓ zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,

✓ możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,

✓ planowanie nieobecności pracowników helpdesk,

✓ obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,

✓ generowanie raportów obsługi helpdesk,

✓ zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),

✓ zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),

✓ wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

**MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.

3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane.

3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2. Podłączenie/odłączenie urządzenia przenośnego.

**Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.**

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

**WSPIERANIE ZARZĄDZANIA CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW** poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.

2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.

3. Statystyki aktywności podwładnych widoczne dla przełożonego.

4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.

5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.

6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.

7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.

9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.

10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).

11. Wskaźnik czasu poświęconego na aktywność produktywną.

12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.

13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.

14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.

**Portal informacyjny w formie platformy WWW**

Oprogramowanie posiada również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardówwidgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:

✓ Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.

✓ Wyświetlana w trybie jasnym lub nocnym.

Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.

Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:

✓ Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,

✓ Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,

✓ Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW,

✓ Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń,

✓ Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem),

✓ Produktywność dla grupy, Statystyki czasu nieproduktywnego.

**Ochrona przed usunięciem**

Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

**Funkcjonalność Agenta**

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Program dostępny jest w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

**11. Urządzenie ochrony sieciowej typu UTM**

Ilość: 1szt.

Wymagania:

# **Wymagania Ogólne**

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:

* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 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 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

# **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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. 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.

1. 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 5000 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 2000 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.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. 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.
3. 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.

# **Certyfikaty**

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

# **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:

b)     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 36 miesięcy

# **Gwarancja oraz wsparcie**

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# **Rozszerzone wsparcie serwisowe AHB/SOS**

System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
* Przygotowanie urządzenia do zdalnej konfiguracji.
* Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie   
  z wymaganiami użytkownika.
* Minimum 5 godzin zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
* Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

# **Opisy do wymagań ogólnych**

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Wykonawca przedłoży dokument w postaci oświadczenia producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży

# **Szkolenie**

Szkolenie minimum 2 dniowe: DASHBOARD System Information, Administrators, CPU/Memory Usage, License Status SECURITY FABRIC Physical / Logical Topology, Security Rating, Automation

Szkolenie przeprowadzone przez inżyniera posiadającego certyfikacje NSE7 - certyfikat należy przedłożyć przed podpisaniem umowy.

**12. Komputer mobilny (laptop)**

Ilość: 1szt.

Wymagania:

**Procesor** , który według testu PASSMARK CPU MARK osiąga wynik co najmniej 10000 punktów.

- posiadający minimum 4 rdzenie fizyczne

- 64 bitowy

**Pamięć RAM:** co najmniej 16 GB z możliwością rozszerzenia do 32 GB (możliwość domontowania modułu pamięci 16 GB) i z częstotliwością taktowania minimum 3200 MHz typ DDR 4

**Karta graficzna:** zintegrowana podstawowa obsługująca rozdzielczość FULL HD 1920 x1080

**Dysk SSD:**  minimum 512GB

**Ekran:** o przekątnej od 15 do 16 cali matowy FULL HD 1920x1080

**Kamera przy ekranie:** z matrycą HD

**Wbudowany mikrofon**

**Wbudowane głośniki** stereo

**Klawiatura US** z wyodrębnionym blokiem numerycznym

**Wielofunkcyjny touchpad standardowy**

**Wyjście słuchawkowe**

**Wejście mikrofonowe**

**Wejścia USB 3.0 -** minimum 3 standard A

**Czytnik kart micro SD**

**Wejście USB 3.1 typ C**

**Gniazdo HDMI standardowe**

**Gniazdo LAN RJ45 10/100/1000**

**Karta WIFI** obsługująca co najmniej standardy(802.11 a/b/g/n/ac)

**Moduł Bluetooth** obsługujący co najmniej standard 5.0

**System Windows 10 Pro w wersji polskiej preinstalowany**

**Gwarancja minimum 24 miesiące**

**Torba podróżna do laptopa** – przeznaczona do zamawianego komputera minimum 2 komorowa (osobna komora na laptopa i osobna na zasilacz i inne akcesoria). Każda komora powinna mieć zapięcie na zamek błyskawiczny. Torba powinna być wyposażona w uchwyt w stylu rączki oraz pasek do zawieszenia torby na ramieniu.

**Dostarczany sprzęt powinien być fabrycznie nowy nieużywany – nie powinien zawierać żadnych elementów używanych. Powinien pochodzić z polskiej dystrybucji.**