Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest system antywirusowy zarządzany centralnie z licencją na 2 lata (180 licencji)spełniający następujące wymagania:

System Operacyjny Windows:

Systemy Operacyjne Komputerów

Pełne wsparcie:

Windows 11 (initial)
Windows 10 November 2021 Update (21H2)
Windows 10 May 2021 Update (21H1)
Windows 10 October 2020 Update (20H2)
Windows 10 May 2020 Update (20H1)
Windows 10 November 2019 Update (19H2)
Windows 10 May 2019 Update (19H1)
Windows 10 October 2018 Update (Redstone 5)
Windows 10 April 2018 Update (Redstone 4)
Windows 10 Fall Creators Update (Redstone 3)
Windows 10 Creators Update (Redstone 2)
Windows 10 Anniversary Update (Redstone 1)
Windows 10 November Update (Threshold 2)
Windows 10
Windows 8.1
Windows 8
Windows 7

Windows Tablet oraz systemy wbudowane

Pełne wsparcie

Windows 10 IoT Enterprise
Windows Embedded 8.1 Industry
Windows Embedded 8 Standard
Windows Embedded Standard 7
Windows Embedded Compact 7
Windows Embedded POSReady 7
Windows Embedded Enterprise 7

Systemy operacyjne serwera

Pełne wsparcie
Windows Server 2019 Core
Windows Server 2019
Windows Server 2016
Windows Server 2016 Core
Windows Server 2012 R2
Windows Server 2012
Windows Small Business Server (SBS) 2011
Windows Server 2008 R2

Systemy Operacyjne Linux

Ubuntu 14.04 LTS lub wyższy
Red Hat Enterprise Linux / CentOS 6.0 lub wyżej
SUSE Linux Enterprise Server 11 SP4 lub wyższy
OpenSUSE Leap 42.x
Fedora 25 lub wyższy
Debian 8.0 lub wyższy
Oracle Linux 6.3 lub nowszy
Amazon Linux 2
Amazon Linux AMI 2016.09 lub nowszy

Systemy Operacyjne Mac OS X

macOS Big Sur(11.0)
macOS Catalina (10.15)
macOS Mojave (10.14)
macOS High Sierra (10.13)
macOS Sierra (10.12)
OS X El Capitan (10.11)

Wymagania Ochrony Mobile[3]

- Apple iPhone i tablety iPad (iOS 8.1+)
- Smartfony i tablety z Google Android (4.2+)

Obsługiwane Środowiska Microsoft Exchange

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2019 z rolą Edge Transport lub Mailbox
- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox
- Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox

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

Ochrona środowisk wirtualnych (SVE)

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

Środowiska wspierane:

- VMware vSphere & vCenter Server 7.0 update 1, 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (including Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism with AOS 5.6, 5.11, 5.18 STS
- Nutanix Prism with AHV 20170830.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog[3]
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość dodawania wykluczeni na podstawie

a. Plik
b. Folder
c. Rozszerzenie
d. Proces
e. Hash pliku
f. Hash certyfikatu
g. Nazwa zagrożenia
h. Wiersz poleceń
i. IP/maska

13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Praca programu musi być niezauważalna dla użytkownika.
29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
32. Możliwość odblokowania ustawień programu po wpisaniu hasła
33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu
34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)

35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
40. Wbudowany IDS
41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji
43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
44. Możliwość tworzenia list sieci zaufanych.
45. Możliwość dezaktywacji funkcji zapory sieciowej.
46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware
48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa)
50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
52. System zarządzania ryzykiem^2 – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
    a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

-Ochrony przeglądarki internetowej

-Sieć i poświadczenia

-Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

a) Możliwość wymuszenia funkcji DEP systemu Windows

b) Możliwość wymuszenia relokacji modułów (ASLR)

<u>Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.</u>

54. Ochrona poczty(add-on[1,2]) – mechanizm pozwalający na ochronę poczty Office 365 lub Microsoft Exchange z wykorzystaniem serwera pośredniczącego.

55. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:

-Wczesny dostęp

-Dostęp do poświadczeń

-Wykrycie

-Crimeware

56. Pełne Szyfrowanie dysków(add-on[1])
57. Zarządzanie aktualizacjami oprogramowania firm trzecich(add-on[1)]
58. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

    Formaty plików jakie mogą być odzyskane:

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

    Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

59. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
    a) Ukierunkowane ataki
    b) Podejrzane pliki i ruch w sieci
    c) Exploity
    d) Ransomware
    e) Grayware
60. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego
61. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
    a) Tolerancyjny
    b) Normalny
    c) Agresywny
62. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku

a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora

b) Możliwość przesłania archiwum zabezpieczonego hasłem

c) Możliwość przesłania adresu URL

d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.

63. Wbudowany sandbox musi działać w trybie monitorowania i blokowania

64. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny

65. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.

66. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.

67. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB

68. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB

78.Telemetria[2] - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk(wymaga TLS 1.2 lub wyższy)

79. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu)

2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.

3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.

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

6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

Stacje robocze i serwery Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

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

20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.

2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.

3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.

4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.

5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.

6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.

7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.

8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.

9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.

10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.

11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.

12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. Dwa typy konsoli administracyjnej:
   - Konsola Cloud – serwer administracyjny po stronie producenta
   - Konsola On-premise – lokalny serwer administracyjny
2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
4. Możliwość integracji Domeny Active Directory w obu typach konsoli.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Możliwość generowania raportu co godzinę.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
18. Możliwość dodania etykiety do stacji roboczej.

19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
20. Możliwość przechowywania kwarantanny maksymalnie 180 dni
21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[3]
25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
26. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
27. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie

    -Zakres adresów IP/IP

    -Adres bramy

    -Adres serwera WINS

    -Adres serwera DNS

    -Połączenie DHCP sufiksów DNS

    -Punkt końcowy może rozwiązać hosta

    -Typ sieci

    -Nazwa hosta
28. Integracja z serwerem Syslog[3]
29. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator
30. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni[2]
31. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem[2]
32. Funkcja pojedynczego logowania – Single Sign-on (SSO)[2]
33. Możliwość naprawy instalacji z poziomu konsoli[2]

34. Raport streszczający[2] - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

    -Zarządzane punkty końcowe

    -Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne

    -Pięć najczęściej blokowanych zagrożeń

    -Podział zagrożeń na urządzenia takie jak stacje robocze i serwery

    -Status incydentów bezpieczeństwa które wystąpiły

    -Stan modułów punktów końcowych

    -Ocena ryzyka firmy

    -Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

    -Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

35. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Pakiety
    b) Sieć
    c) Kwarantanna
    d) Licencjonowanie
    e) Integracje
    f) Polityki
    g) Raporty
    h) Konta
    i) Firmy[2]
36. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na okrślenie godziny kiedy te maszyny będą usuwane
37. Możliwość określenia własnego serwera NTP[3]

38. Integracja z vCenter Server[3]
39. Integracja z Xen Server[3]
40. Integracja z nutanix Prism Element[3]
41. Możliwość integracji z Amazon EC2
42. Intergracja z Azure[3]
43. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.
44. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
45. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.
46. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
47. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
48. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
49. Pion firmy[2] - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:
    a) Lotnictwo
    b) Rolnictwo
    c) Automotive
    d) Usługi komercyjne
    e) Doradztwo
    f) Energia
    g) Usługi finansowe
    h) Rząd
    i) Opieka zdrowotna
    j) Technologie
    k) Transport
    l) Non-profit
    m) Górnictwo
    n) Media

50. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. (3)
51. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym
52. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. (3)
53. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
54. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
55. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS
56. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
57. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
58. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS
59. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1
60. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych(2).
61. Możliwość skanowania SSL dla połączeń RDP(2)
62. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.

EDR-Endpoint Detection and Response

Wspierane systemy operacyjne

A. Systemy desktopowe

- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

B. Systemy operacyjne dla serwerów:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

C. MacOS:

- OS X El Capitan (10.11.x) i nowsze

D. Linux

- Ubuntu 14.04 lub nowszy
- CentOS 7.3 lub nowszy

Komponenty EDR

Główne elementy:

1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.

Wykrywanie podejrzanej aktywności

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

1. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
2. Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
2. Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:

a) Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.

b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.

c) Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

Incydenty

Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

a) Filtrowania zdarzeń
b) Blokowania procesów
c) Dodawanie procesów do czarnej listy
d) Dodawanie procesów do białej listy
e) Izolacja hosta
f) Aktualizacja oprogramowania firm trzecich na hoście(1)
g) Przesłanie pliku do Sandbox
h) Sprawdzenie informacji o pliku w Google
i) Sprawdzenie informacji o pliku w VirusTotal

Filtrowanie zdarzeń odbywa się na podstawie:

a) Ocena zagrożenia od 10 do 100 punktów
b) Data wykrycia
c) Status
d) ID
e) Nazwa punktu końcowego
f) Typ ataku
    a) Ransomware
    b) Potencjalnie niechciana aplikacja
    c) Malware
    d) Exploit
    e) Fileless
    f) Password stealer
    g) Downloader
    h) Inne
    i) Zdefiniowane przez użytkownika

Wyszukiwanie zdarzeń może odbywać się na podstawie:

a) Nazwa alertu
b) IP punktu końcowego
c) Hash MD5
d) Hash SHA256
e) Nazwa użytkownika

Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem.

Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.

Możliwość wyświetlenia zablokowanych hashy plików.

Możliwość dodania własnych hashy MD5 oraz SHA256

Możliwość importu hashy z pliku CSV

Możliwość filtrowania dodanych hashy na podstawie:

a) Typu hashu
b) Wartości hash
c) Źródło dodania
d) Informacje o źródle
e) Nazwa pliku
f) Firma której dotyczy wpis
g) Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.

Przypisy

[1]Add-on jest modułem opcjonalnym, dodatkowo płatnym który należy zakupić oddzielnie

[2]Funkcja dostępna tylko w wersji cloud

[3]Funkcja dostępna tylko w wersji on-premise

Patch management/Zarządzanie łatkami

Wspierane systemy operacyjne Windows:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Wspierane systemy operacyjne Linux (64-bit):

- CentOS 7 – GA+ (7.2003)
- Red Hat Enterprise Linux RHEL 6 – GA+ (6.1-6.10)
- Red Hat Enterprise Linux RHEL 7 – GA+ (7.1-7.9)
- Red Hat Enterprise Linux REL 8 – GA+ (8.4)
- SUSE Linux Enterprise SLES 12 – SP4
- SUSE Linux Enterprise SLES 15 – GA+ (SP3)
- SUSE Linux Enterprise SLED 15 – GA+ (Currently SP3)

1) Możliwość działania w trybie automatycznym
    a) Możliwość oszacowania brakujących łatek
    b) Możliwość zaplanowania oddzielnej automatycznej instalacji w oparciu o kategorię poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami)
    c) Możliwość opóźnienia ponownego uruchomienia, jeśli instalacja łatki tego wymaga
2) Rozwiązanie musi zezwalać na tryb manualny – wykrywanie i instalacje łatek na żądanie

3) Rozwiązanie musi oferować możliwość podejrzenia wszystkich brakujących łatek ze środowiska. Informacje te zostaną zebrane w module zarządzania aktualizacjami.
    a) Rozwiązanie dostarcza możliwość sprawdzenia które punkty końcowe posiadają zainstalowane lub niezainstalowane aktualizacje.
    b) Rozwiązanie przesyła informacje zwrotne w przypadku niepowodzenia instalacji łatki
    c) Rozwiązanie daje użytkownikowi możliwość szybkiej instalacji brakujących łatek na urządzeniu
    d) Użytkownik powinien mieć możliwość dodania do czarnej listy jednej lub wielu łatek
4) Rozwiązanie raportuje brakujące łatki z perspektywy punktu końcowego (zainstalowane/ brakujące na każdym punkcie końcowym)
5) Rozwiązanie będzie okresowo wysyłać powiadomienia jeśli punkty końcowe nie posiadają zainstalowanych łatek.
6) Rozwiązanie zapewni możliwość buforowania, w ten sposób łatki będą pobierane z Internetu tylko przez niektóre przypisane punkty końcowe.
7) System wyświetla pozostały czas do automatycznego ponownego uruchomienia w powiadomieniu zarządzania poprawkami.
8) Funkcja wykrywania i informowania o każdej nowej zainstalowanej aplikacji na punkcie końcowym i dostępnych dla niej aktualizacji.
9) Możliwość automatycznego usuwania aktualizacji które nie mają już zastosowania ponieważ punkt końcowy nie istnieje lub aplikacja została usunięta.
10) Możliwość usunięcia z listy łatek które nie są już dostępne chociaż są obecne na niektórych punktach końcowych.
11) Możliwość wyszukiwania i pobierania aktualizacji dla wspieranych dystrybucji Linux i powiązanych z nimi produktów.