

NOVELL® ZENWORKS® ENDPOINT SECURITY MANAGEMENT

Chroń najbardziej podatne na zagrożenia zasoby informatyczne za pomocą rozwiązania uwzględniającego lokalizację i opartego na zasadach, które zabezpiecza dane każdego komputera, kontroluje sposób, w jaki punkty końcowe komunikują się między sobą i uzyskują dostęp do informacji, i monitoruje stan punktów końcowych — wszystko z poziomu jednej konsoli.

Przegląd możliwości produktu

Novell® ZENworks® Endpoint Security Management zapewnia precyzyjną, opartą na zasadach kontrolę nad wszystkimi komputerami stacjonarnymi i przenośnymi — w tym możliwość automatycznej zmiany konfiguracji zabezpieczeń w zależności od roli i miejsca pobytu użytkownika. Dzięki możliwości tworzenia zasad i zarządzania nimi w jednym miejscu oprogramowanie Novell ZENworks pozwala wdrażać i egzekwować ściśle kontrolowane i bardzo elastyczne zasady bezpieczeństwa bez konieczności angażowania w te czynności użytkowników końcowych. Novell ZENworks Endpoint Security Management udostępnia również rozbudowane funkcje samoobrony, które uniemożliwiają obchodzenie zasad bezpieczeństwa, a także kompleksowy pakiet narzędzi do monitorowania, ostrzegania, raportowania i audytu.

Kluczowe zalety

Novell ZENworks Endpoint Security Management zapewnia firmom wsparcie w następującym zakresie:

- Kompleksowe, scentralizowane zabezpieczenia najbardziej podatnych na zagrożenia zasobów informatycznych — komputerów przenośnych używanych poza siedzibą firmy.
- Zwiększenie wydajności pracy użytkowników poprzez zwolnienie ich z obowiązku konfigurowania i monitorowania zabezpieczeń w posiadanych urządzeniach.
- Efektywne zarządzanie wszystkimi aspektami zabezpieczeń punktów końcowych — obejmujące wszystkie komputery w firmie — za pomocą jednej konsoli.
- Automatyczna zmiana zasad bezpieczeństwa i ograniczeń dotyczących punktów końcowych w zależności od roli i miejsca pobytu użytkowników, a także używanych przez nich urządzeń.
- Zarządzanie cyklem eksploatacji punktów końcowych i kwestiami bezpieczeństwa w ramach jednego interfejsu, obejmującego zarządzanie konfiguracją, zasobami i poprawkami oraz zapewnianie bezpieczeństwa punktów końcowych — wszystko to w ramach jednej konsoli (z możliwością wdrożenia produktu w postaci maszyny wirtualnej).

- Spokój umysłu, jaki zapewnia świadomość, że kontrolę nad określaniem, wdrażaniem, egzekwowaniem i monitorowaniem zabezpieczeń punktów końcowych przejmują specjaliści ds. zabezpieczeń, a nie niedoświadczeni użytkownicy.

Kluczowe funkcje

Novell ZENworks Endpoint Security Management zawiera kompleksowy, zintegrowany zestaw funkcji zarządzania zabezpieczeniami punktów końcowych i ich egzekwowania w przedsiębiorstwie:

Zabezpieczenia urządzeń USB i pamięci masowych

Novell ZENworks Endpoint Security Management obejmuje rozbudowane funkcje mające na celu określenie dopuszczalnego wykorzystania wymiennych urządzeń pamięci masowej. Rozwiązanie obejmuje następujące funkcje:

- **Ochrona danych przed kradzieżą** — umożliwia włączenie i wyłączenie (oraz ustawienie trybu „tylko do odczytu”) wymiennego urządzenia pamięci masowej — w tym napędów USB, CD/DVD i ZIP, stacji dyskiety, odtwarzaczy MP3, pamięci flash oraz kart SCSI i PCMCIA.
- **Szczegółowe elementy kontroli z użyciem białych list** — pozwalają administratorom kontrolować wykorzystanie urządzeń USB.
- **Zapobieganie niekontrolowanym operacjom** — blokuje lokalne urządzenia pamięci masowej umożliwiające kopiowanie danych bez śladu audytu.
- **Elementy kontroli nagrywarek optycznych (DVD/CD) i stacji dyskiety** — umożliwiają włączenie i wyłączenie napędu lub ustawienie trybu „tylko do odczytu” — w zależności od miejsca pobytu użytkownika i wymogów bezpieczeństwa.
- **Elementy kontroli funkcji automatycznego odtwarzania i uruchamiania** — zapewniają scentralizowane opcje kontroli funkcji automatycznego odtwarzania i uruchamiania w całej firmie.





Skontaktuj się z lokalnym dostawcą rozwiązań lub zadzwoń do firmy Novell:

Niemcy
+49 211 56 31 0

Szwecja
+46 8 477 41 00

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

Austria
+43 1 36 77 444 0

Włochy
+39 02 26 295 1

Szwajcaria
+41 43 299 78 00

Belgia
+32 2 474 46 11

Holandia
+31 10 286 44 44

RPA
+27 11 322 8300

Francja
+33 1 55 62 50 00

Hiszpania
+34 91 640 25 00

Polska
+48 22 537 5000

Szyfrowanie danych

Novell ZENworks Endpoint Security Management pozwala centralnie tworzyć, dystrybuować, egzekwować i kontrolować zasady szyfrowania dotyczące wszystkich punktów końcowych i wymiennych urządzeń pamięci masowej. Rozwiązanie obejmuje następujące funkcje:

- **Szyfrowanie oparte na zasadach i zgodne z programem Safe Harbor** — umożliwia szyfrowanie wszystkich danych zapisanych na dyskach stałych w folderach określonych przez administratora lub użytkownika jako podlegające programowi Safe Harbor.
- **Szyfrowanie wymiennych urządzeń pamięci masowej** — umożliwia szyfrowanie danych skopiowanych na wymienne urządzenia pamięci masowej, a także całej zawartości takiego urządzenia, zaraz po włożeniu (lub podłączeniu) go do komputera.

Zaawansowana zaporą sieciową

W przeciwieństwie do tradycyjnych zapór sieciowych filtrujących w warstwie aplikacji lub wykorzystujących sterownik zapory (tzw. hook driver) Novell ZENworks Endpoint Security Management działa w warstwie NDIS (Network Driver Interface Specification) w przypadku każdej karty sieciowej. Zapewnia to pełne bezpieczeństwo od momentu dotarcia ruchu sieciowego do komputera. Novell ZENworks Endpoint Security Management obejmuje następujące funkcje związane z zaporą sieciową:

- **Zapora sieciowa z monitorowaniem stanu** — urządzenie może odbierać tylko ten ruch sieciowy, którego zażądał użytkownik.
- **Reguły dotyczące portów TCP/UDP i listy kontroli dostępu (ACL)** — ściśle kontrolują działanie zapory (i zarządzają nią) w odniesieniu do określonych urządzeń.
- **Kontrola działania zapory w zależności od lokalizacji** — umożliwia automatyczne stosowanie odrębnych zestawów reguł dotyczących portów i list ACL w zależności od stopnia bezpieczeństwa lokalizacji, w której znajduje się urządzenie.
- **Scentralizowany, oparty na zasadach nadzór nad ustawieniami zapory sieciowej, którego nie mogą wyłączyć ani obejść użytkownicy i nieupoważnieni administratorzy.**
- **Funkcje rzeczywistej kwarantanny** — chronią sieć, gdy zabezpieczenia komputera nie spełniają swojej roli.

Zabezpieczenia sieci bezprzewodowej

Novell ZENworks Endpoint Security Management zapewnia scentralizowany nadzór nad miejscem, czasem i sposobem podłączania użytkowników do sieci bezprzewodowej. Rozwiązanie obejmuje następujące funkcje:

- **Zarządzanie siecią Wi-Fi** — umożliwia tworzenie czarnych i białych list dotyczących bezprzewodowych punktów dostępu i wdrażanie zasad ograniczających, uniemożliwiających lub blokujących łączność Wi-Fi w określonych sytuacjach.

- **Elementy zabezpieczeń sieci Wi-Fi** — pozwalają ograniczyć komunikację Wi-Fi do bezprzewodowych punktów dostępu spełniających standardy szyfrowania.
- **Blokowanie kart Wi-Fi** — sprawia, że punkty końcowe mogą łączyć się z bezprzewodowymi punktami dostępu tylko za pomocą kart Wi-Fi zatwierdzonych przez firmę.

Kontrola portów

Oprócz zabezpieczeń sieci Wi-Fi Novell ZENworks Endpoint Security Management udostępnia kompleksową ochronę wszystkich typów przewodowych i bezprzewodowych portów i urządzeń komunikacyjnych. Obejmuje to porty LAN, USB, 1394 (FireWire), szeregowo, równoległe, a także złącza modemów, Bluetooth i podczerwiieni.

Kontrola aplikacji

Moduł kontrolowania aplikacji w oprogramowaniu Novell ZENworks Endpoint Security Management zapewnia precyzyjną, opartą na zasadach kontrolę nad aplikacjami uruchamianymi w punktach końcowych. Rozwiązanie obejmuje następujące funkcje:

- **Umieszczanie aplikacji na czarnej liście** — pozwala blokować znane złośliwe lub niepożądane aplikacje.
- **Kontrola w oparciu o lokalizację** — administrator może zezwolić na używanie określonych aplikacji, uniemożliwić im dostęp do sieci lub zablokować ich uruchamianie — w oparciu o poziom bezpieczeństwa w miejscu pobytu użytkownika.
- **Sprawdzanie prawidłowości działania oprogramowania antywirusowego i przeciwdziałającego szpiegowaniu** — umożliwia sprawdzanie, czy wszystkie aplikacje zapewniające bezpieczeństwo działają prawidłowo, oraz poddawanie kwarantannie niezgodnych urządzeń (lub usuwanie problemów z tym związanych).
- **Egzekwowanie reguł dotyczących połączeń VPN** — sprawia, że użytkownicy mogą łączyć się tylko za pomocą autoryzowanych połączeń VPN; zapewnia ochronę przed atakami typu „evil twin” i uniemożliwia użytkownikom niebezpieczne praktyki, np. rozdzielenie chronionego i niechronionego ruchu sieciowego (ang. split tunnelling).

Wymagania systemowe

Szczegółowe dane techniczne oraz wymagania systemowe są dostępne pod adresem: www.novell.com/products/zenworks/endpointsecuritymanagement/technical-information