



Nadzór z jednego miejsca nad bezpieczeństwem punktów końcowych

Pełne zabezpieczenie urządzenia końcowego z zachowaniem funkcji centralnego sterowania rozwiązaniami informatycznymi

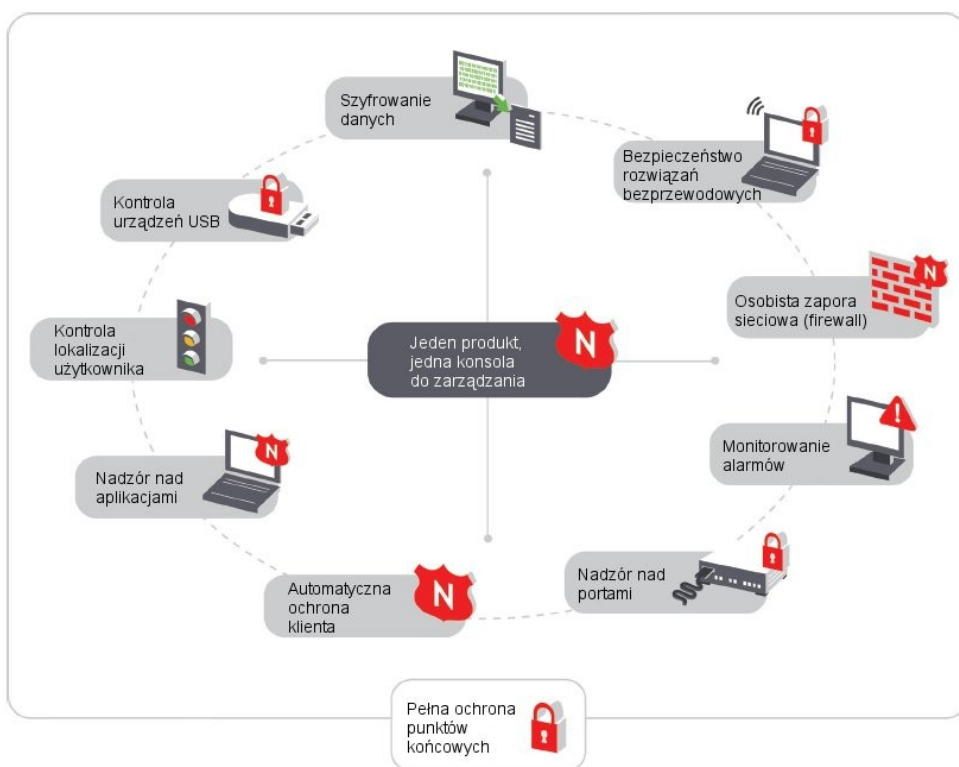
■ **Rozwiązanie**
Endpoint Security Management

■ **Produkty**
Novell ZENworks Endpoint Security Management



„Wielu producentów nadal próbuje na siłę łączyć różne technologie, starając się zapewnić ochronę punktów końcowych w heterogenicznym środowisku informatycznym, obejmującym użytkowników mobilnych i urządzenia bezprzewodowe. Natomiast Novell wprowadza na rynek innowacyjną architekturę, zapewniającą wszechstronne, zautomatyzowane zarządzanie regułami bezpieczeństwa i wdrażanie ich na wszystkich urządzeniach użytkowników.”

Charles Kolodgy
Dyrektor ds. badań
IDC, czerwiec 2007 r.



Rysunek 1. Za pomocą jednej konsoli w Novell ZENworks Endpoint Security Management można zabezpieczyć wszystkie punkty końcowe w sieci.

Prosta, scentralizowana i pełna ochrona dla wszystkich punktów końcowych w sieci — przewodowych i bezprzewodowych

Bezpieczeństwo punktów końcowych to kwestia nazbyt ważna, by pozostawiać ją pieczy samych użytkowników. Zbyt wiele firm powierza pojedynczym pracownikom obowiązek skonfigurowania zapory sieciowej (*firewall*), stosowania skanerów antywirusowych, uruchamiania własnych

klientów VPN, gdy przebywają poza biurem itd. Jednak zwykli użytkownicy nie mają zwykle odpowiednich kwalifikacji do podejmowania decyzji związanych z bezpieczeństwem i nie można na nich polegać w tym zakresie. Użytkownik może znać na wylot swoje aplikacje biurowe, ale nie musi zdawać sobie sprawy, co się dzieje po kliknięciu OK w aplikacji zabezpieczającej. Tylko specjaliści ds. bezpieczeństwa mają pełną wiedzę



np. o tym, jakie będą konsekwencje nadania konkretnej aplikacji dostępu do sieci albo zezwolenia konkretnemu portowi na odbiór przychodzącego ruchu. Pozostawienie takich decyzji pracownikom to prosta droga do chaosu w sieci korporacyjnej.

Novell® ZENworks® Endpoint Security Management przekazuje całą kontrolę nad bezpieczeństwem sprzętu biurowego we właściwe ręce — informatyków, specjalistów ds. zabezpieczeń IT. System zapewnia wszechstronny zestaw opartych na regułach rozwiązań, które obsługują wszystkie aspekty bezpieczeństwa punktów. Zarządza się nimi z jednej konsoli. Rozwiązania te można wdrażać indywidualnie, stosownie do konkretnych potrzeb, albo w formie zintegrowanego pakietu, zapewniającego pełną ochronę punktów końcowych.

Osobista zapora sieciowa

Novell oferuje najlepszą zaporę sieciową na świecie, chroniącą przed hakerami, destrukcyjnym oprogramowaniem, atakami z użyciem różnych protokołów i wieloma innymi zagrożeniami — a przy tym całkowicie niewidoczną dla użytkowników.

W przeciwieństwie do typowych osobistych zapór sieciowych, które działają tylko w warstwie aplikacji lub w formie sterownika punktu zaczepienia zapory, rozwiązanie oferowane przez firmę Novell jest zintegrowane ze sterownikiem NDIS każdej karty sieciowej. Umożliwia to optymalizację wydajności oraz zapewnia blokowanie niepożądanego ruchu w momencie, w którym próbuje on wejść do komputera użytkownika.

Technologia adaptacyjnego blokowania portów (ang. *Adaptive Port Blocking*) zapewnia niezrównaną ochronę przed atakami wykorzystującymi protokoły, takimi jak nieuprawnione skanowanie portów, zalew pakietów z flagą synchronizacji (ang. *SYN flood*), ataki w protokole NetBIOS i ataki typu DDOS (odmowa usługi). Administrator może skonfigurować zaufane i obce hosty według adresów IP lub adresów MAC, według ich położenia, a także według obsługujących je struktur sieciowych, które używają konkretnych technologii rozsyłania, np. multicastingu IP, ARP, ICMP i 802.1x.

Użytkownicy mają spokojnie wykonywać swoją pracę. Odpowiedzialność za ochronę punktów końcowych spoczywa na administratorach systemów informatycznych. Novell oferuje oparte na regułach rozwiązania obsługujące wszystkie aspekty bezpieczeństwa komputerów biurowych i mobilnych — od brzegu do rdzenia sieci — a przy tym są wyposażone w łatwą w obsłudze konsolę do zarządzania.

Bezprzewodowo i bezpiecznie

Rozwiązanie do kontroli rozwiązań bezprzewodowych zapewnia centralny nadzór nad tym, gdzie, kiedy i jak użytkownicy mogą łączyć się z siecią. Można dzięki temu ograniczyć łączność bezprzewodową tylko do uprawnionych punktów dostępowych, określić minimalną siłę szyfrowania lub nawet całkowicie wyłączyć obsługę Wi-Fi*. Oprócz tego automatycznie wymusza się przestrzeganie stosowania wirtualnych sieci prywatnych przez wprowadzenie wymogu, że oprogramowanie VPN musi być uruchomione w momencie połączenia urządzenia z obcymi sieciami, np. w hotelach, lotniskach czy kawiarniach. Funkcja wykrywania nieuprawnionych punktów dostępowych ułatwia ochronę sieci bezprzewodowej w biurze i w jego otoczeniu.

Wszystkie te funkcje zapewniają kompleksową kontrolę nad łącznością Wi-Fi i ochronę przed hakerami niezależnie od użytych przez nich sztuczek. Użytkownicy mogą pracować w dogodnym dla nich miejscu i czasie, nie musząc samodzielnie podejmować decyzji związanych z bezpieczeństwem czy ręcznie wprowadzać kluczy zabezpieczeń.

Kontrola portów

Oprócz ochrony środowiska Wi-Fi, ZENworks Endpoint Security Management zabezpiecza wszystkie porty i karty komunikacyjne na urządzeniach końcowych, takie jak:

- porty sieci lokalnej
- porty modemowe
- porty Bluetooth*
- porty podczerwieni
- port 1394 (Firewire*)
- porty szeregowo i równoległe

Przeprowadzone przez Ponemon Institute badanie „Koszt złamania zabezpieczeń danych” z 2006 r. wykazało, że firmy poświęcają przeciętnie 5 mln USD na odzyskanie skradzionych danych. Przeciętny koszt na jeden rekord klienta, którego poufność została naruszona, to 182 USD. W 49% przypadków do utraty danych doszło w wyniku kradzieży laptopa, komputera biurowego, asystenta cyfrowego (PDA) lub napędu USB.

Szyfrowanie danych

Moduł Encryption szyfruje dane we wszystkich miejscach, do których one trafiają. Umożliwia to scentralizowane tworzenie, dystrybucję, narzucanie i kontrolowanie reguł szyfrowania we wszystkich punktach końcowych i wymowalnych urządzeniach pamięci masowej (np. pamięć USB). Sterowanie szyfrowaniem odbywa się w rozbiciu na poszczególne typy plików, lokalizacje, typy urządzeń i inne kryteria. Nie wymaga się przy tym od użytkowników samodzielnego zarządzania ustawieniami i kluczami bezpieczeństwa.

Bezpieczeństwo urządzeń USB

Przy braku odpowiedniego zarządzania, wymowalne urządzenia pamięci masowej mogą stanowić poważne zagrożenie dla bezpieczeństwa i uniemożliwić zachowanie zgodności z przepisami i regulacjami. Użytkownicy o złych zamiarach mogą skopiować na te urządzenia wielkie ilości danych nie pozostawiając po sobie żadnego śladu. Urządzenia zawierające poufne informacje łatwo jest też ukraść czy zgubić. Co więcej, przez urządzenia USB bez żadnych przeszkód może wkroczyć do firmy destrukcyjne oprogramowanie i zainfekować całą sieć. Niekontrolowane przenoszenie niezasyfrowanych danych poza firmę czy instytucję naraża jej zarząd na poważne kłopoty ze strony audytorów kontrolujących zgodność z przepisami ustawy o ochronie danych, **normą ISO:27001**, regulacjami SOX, czy europejską Basel II.

Rozwiązanie USB Security egzekwuje przestrzeganie reguł bezpieczeństwa dla urządzeń pamięci masowej. Reguły można swobodnie dostosowywać. Są one bezustannie i automatycznie rozsyłane do urządzeń bez udziału użytkownika. Dzięki USB Security administratorzy uzyskują rozbudowaną, szczegółową kontrolę nad:

- *dyskami CD i DVD*
- *napędami USB*
- *pamięcią Flash*
- *kartami PCMCIA SCSI*
- *dyskietkami*
- *dyskami ZIP*
- *odtwarzaczami muzyki, inteligentnymi telefonami i innymi urządzeniami osobistymi*

Zgodność z wewnętrznymi regulaminami firmy i przepisami prawa można zapewnić dopuszczając, blokując lub ograniczając dostęp do lokalnych urządzeń pamięci masowej, które umożliwiają kopiowanie danych bez pozostawiania śladów. Skonfigurowane uprawnienia można w elastyczny sposób egzekwować za pomocą zautomatyzowanych reguł działania, uwzględniających położenie użytkownika czy nawet numer seryjny urządzenia. Jeżeli np. dopuści się możliwość zapisywania na urządzeniu wymowalnym, to można też automatycznie generować szczegółowe alarmy i raporty dotyczące wszystkich plików skopiowanych na dane urządzenie.

W przeciwieństwie do innych rozwiązań, system firmy Novell zapewnia kontrolę na poziomie urządzenia pamięci masowej i systemu plików. Dzięki temu urządzenia niestanowiące zagrożenia — np. mysz czy klawiatura USB — mogą pozostać włączone i zwyczajnie działać. Co istotne, można zarządzać osobno wieloma urządzeniami wspólnie korzystającymi z jednego portu USB.

Nadzór nad aplikacjami

Świadome czy nieświadome uruchamianie niedozwolonych aplikacji na komputerach w firmie jest źródłem wielu zagrożeń — od infekcji destrukcyjnym kodem po dotkliwe kary finansowe za używanie nielicencjonowanego oprogramowania. Rozwiązanie Application Control zapewnia szczegółową kontrolę nad aplikacjami, oferując następujące funkcje:

- *Czarne listy aplikacji, które umożliwiają blokowanie znanych, szkodliwych aplikacji.*
- *Kontrola aplikacji według ich położenia, w tym możliwość zezwalania na uruchomienie aplikacji, zezwalania, ale bez dostępu do sieci, i blokowania. Reguły egzekwowania przestrzegania zabezpieczeń umożliwiają automatyczną zmianę uprawnień stosownie do położenia użytkownika. Zablokowane incydenty są rejestrowane i zgłaszane na serwer.*
- *Kontrola spójności oprogramowania antywirusowego i antyspieszającego sprawdza, czy takie aplikacje mają aktualne wersje i czy są uruchomione. Urządzenia niespełniające wymogów zgodności można*

Pełny nadzór
z jednego miejsca
nad bezpieczeństwem
punktów końcowych

www.novell.pl

Zachowanie spójnego profilu bezpieczeństwa

Rozwiązanie może monitorować każdy punkt końcowy w czasie rzeczywistym, sprawdzając jego zgodność ze standardami spójności definiowanymi przez administratorów ds. bezpieczeństwa. Kontrola spójności pozwala np. wyegzekwować uruchamianie funkcji antywirusowych, obsługi kopii zapasowych, audytu i innych procesów zgodnie z ustalonymi regułami. Jeśli punkt końcowy okaże się niezgodny, nawet przy braku połączenia z jakąkolwiek siecią, to można go skorygować; służy do tego wiele opcji, od kwarantanny i blokady po zaawansowane mechanizmy raportowania i audytu.

Centralny nadzór nad wszystkimi punktami końcowymi — w pracy, w domu i w podróży

www.novell.pl

poddać kwarantannie i skorygować za pomocą ustalonych reguł, nawet jeśli urządzenie próbujące nawiązać łączność znajduje się z dala od biura.

■ **Narzucanie stosowania wirtualnej sieci prywatnej** zapewnia, że użytkownik łączy się przez sieć VPN np. wtedy, gdy korzysta z publicznych punktów dostępowych. Funkcja ta nie tylko wymusza korzystanie z bezpiecznego połączenia i szyfrowanie danych, ale też chroni przed atakami typu Evil Twin (podszywaniem się pod punkt dostępowy) oraz zapobiega niebezpiecznym zachowaniom użytkowników, takim jak wydzielanie pobocznych tras dostępu (ang. split tunnelling).

■ **Zaawansowana obsługa skryptów** umożliwia automatyczne porównywanie programów korygujących z serwisem aktualizacji firmy Microsoft lub wewnętrznym serwerem WSUS, wymuszanie instalowania brakujących poprawek, ciągłą kontrolę aktualności sygnatur wirusów itd. Nie wymaga to ani interwencji użytkownika, ani pomocy informatyków.

Automatyczna ochrona klienta

Zabezpieczenia działają tylko wtedy, jeśli się je odpowiednio zainstaluje, skonfiguruje i uruchomi. Rozwiązanie Client Self-defense chroni punkt końcowy dbając też o to, by nie można było zmodyfikować, zaatakować ani odinstalować klienta zabezpieczeń. Analizując położenie punktu końcowego w danym momencie, klient zabezpieczeń:

- stosuje oparte na regułach filtry ruchu przychodzącego i wychodzącego
- sprawdza reguły nadzorujące używany sprzęt — np. bezprzewodowe punkty dostępowe, wymowalne nośniki i karty sieciowe

- gromadzi dane do raportów
- uruchamia aplikacje zabezpieczające, niezbędne w konkretnych sytuacjach określonych regułami.

Aby uniemożliwić odinstalowanie, zmianę czy wyłączenie tych funkcji, co mogłoby pozwolić nieupoważnionym użytkownikom na dostęp do poufnych danych, rozwiązanie Client Self-defense stosuje następujące mechanizmy:

- do odinstalowania klienta wymagane jest hasło lub użycie pakietu instalacyjnego wysłanego przez administratora
- do wstrzymania lub zatrzymania usługi wymagane jest hasło (zgodnie z ustawieniami obowiązującej reguły)
- nie można zatrzymywać procesów bezpieczeństwa za pomocą Menedżera zadań Windows*
- najważniejsze pliki, klucze i wartości rejestru są monitorowane w poszukiwaniu nieprawidłowych zmian
- rozwiązanie wymusza powiązanie filtra NDSI z kartą sieciową.

Monitorowanie alarmów

Funkcja Alerts Monitoring nadzoruje i zgłasza do konsoli administracyjnej wszystkie próby naruszenia firmowych reguł bezpieczeństwa, co pozwala administratorom szybko skorygować problem. Konsola rozwiązania Alerts umożliwia swobodną konfigurację i zapewnia precyzyjną kontrolę nad sposobem oraz częstotliwością wyzwalania alarmów. Administrator ma do dyspozycji pełny pakiet narzędzi raportowo-kontrolnych, za pomocą których można narzucić użytkownikom przestrzeganie wewnętrznych reguł bezpieczeństwa i dokumentować zgodność zabezpieczeń punktów końcowych z normami ISO ustawami typu SOX, HIPAA i innymi przepisami o kontroli i ochronie danych.



Więcej informacji można znaleźć w Internecie na stronie www.novell.com/zenworks lub kontaktując się autoryzowanymi partnerami firmy Novell w Polsce.

Aktualna lista dostępna jest na stronie www.novell.pl/partner

Bezpłatna infolinia

0-800-22-NOVL
(0-800 226685)
infolinia@novell.pl

Novell Polska

ul. Wspólna 47/49
00-684 Warszawa
Tel. (22) 537 5000
Faks (22) 537 5098
www.novell.pl