DELL Technologies

Microsoft

Opracowanie

Uzyskaj zaawansowaną ochronę bezpieczeństwa dzięki połączeniu możliwości systemu Windows Server 2022 i serwerów Dell EMC™ PowerEdge™ nowej generacji

Stabilizowanie obciążeń roboczych o znaczeniu krytycznym dla firm dzięki bezpieczniejszemu sprzętowi, oprogramowaniu wewnętrznemu i środowisku systemu operacyjnego

Według Cybersecurity Ventures oczekuje się, że globalna cyberprzestępczość będzie kosztować łącznie 6 bilionów dolarów w 2021 roku i koszty te wzrosną do 10,5 biliona dolarów w 2025 roku[1]. Koszty samych ataków ransomware wzrosły 61-krotnie w ciągu sześciu lat do 20 miliardów dolarów w 2021 r., przy czym obecnie ataki mają miejsce co 11 sekund[1]. Badanie IDC z 2021 r. wykazało, że ponad jedna trzecia ankietowanych organizacji na całym świecie padła ofiarą ataku lub naruszenia zabezpieczeń typu ransomware w ciągu ostatnich 12 miesięcy (i często więcej niż jednego ataku)[2]. I chociaż IBM szacuje, że koszt pojedynczego naruszenia danych wynosi obecnie 4,24 miliona dolarów[3], to prawdziwy koszt naruszeń może być znacznie wyższy: miały miejsce przypadki, w których szpitale w Stanach Zjednoczonych musiały przekierowywać pacjentów z akcji ratunkowych do innych szpitali i zawracać karetki pogotowia z powodu ataków ransomware[4].

Ataki na oprogramowanie wewnętrzne mogą być szczególnie szkodliwym zagrożeniem dla organizacji. Dzieje się tak, ponieważ atak ukierunkowany na oprogramowanie wewnętrzne może wszczepić złośliwe oprogramowanie, zanim uruchomiony zostanie system operacyjny, a tym samym zabezpieczenia oparte na oprogramowaniu działające w tym systemie operacyjnym. Jednak mniej niż połowa organizacji podjęła kroki w celu zabezpieczenia swoich systemów przed atakami na oprogramowanie układowe, mimo że liczba takich ataków wzrosła pięciokrotnie w ciągu ostatnich pięciu lat[5]. W ostatecznym rozrachunku obciążenia robocze są tak bezpieczne, jak całe stosy, na których działają.

Aby sprostać temu wykładniczemu wzrostowi częstotliwości, różnorodności i kosztów zagrożeń ze strony złośliwego oprogramowania, nowoczesne zabezpieczenia muszą być wielowarstwowe. Dzieje się tak, ponieważ złośliwe oprogramowanie może zagrozić systemom na poziomie sprzętu i oprogramowania wewnętrznego lub podczas rozruchu, czyli we wszystkich obszarach, w których bezskuteczne są zabezpieczenia zdefiniowane wyłącznie programowo. Aby przeciwdziałać tej luce, nowoczesne zabezpieczenia serwerów nie projektowane jednotorowo. Muszą być wbudowane w cały stos infrastruktury. Połączenie serwerów Dell EMC™ PowerEdge™ nowej generacji i systemu Windows Server 2022 upraszcza administratorom ważne zadanie dostosowania sprzętu, oprogramowania wewnętrznego i systemu operacyjnego w celu odpowiedniego zabezpieczenia obciążeń roboczych o znaczeniu krytycznym.

Połączone zalety systemu Windows Server 2022 Secured-Core Server i serwerów PowerEdge nowej generacji

Serwer z zabezpieczonym rdzeniem to nowa funkcja w systemie Windows Server 2022, która wykorzystuje możliwości sprzętu, oprogramowania wewnętrznego i systemu operacyjnego w celu zapewnienia ochrony przed obecnymi i przyszłymi zagrożeniami. Połączenie oprogramowania Windows Server 2022 Secured-Core Server ze sprzętem serwerowym PowerEdge nowej generacji zapewnia organizacjom takim jak Twoja trzy istotne korzyści:

- Zaawansowana ochrona
- Obrona prewencyjna
- Prostsze zabezpieczenia

Zaawansowana ochrona

Na podstawie danych firmy Microsoft dotyczących analizy zagrożeń Threat Intelligence można stwierdzić, że komputery z zabezpieczonymi rdzeniami zapewniają ponad dwukrotnie lepszą ochronę przed infekcją niż zwykłe komputery; firma Microsoft wprowadza obecnie tę technologię do przestrzeni serwerowej dzięki systemom Windows Server 2022 Secured-Core Server[5]. Zabezpieczenia wprowadzone w serwerze z zabezpieczonymi rdzeniami mają na celu stworzenie bezpiecznej platformy dla krytycznych obciążeń roboczych i danych znajdujących się na danym serwerze. W szczególności serwery z zabezpieczonymi rdzeniami wykorzystują obsługę procesora dla technologii DRTM (Dynamic Root of Trust for Measurement) w celu umieszczenia oprogramowania wewnętrznego w piaskownicy sprzętowej. Ta izolacja pomaga ograniczyć wpływ luk w zabezpieczeniach w milionach wierszy wysoce uprzywilejowanego kodu oprogramowania wewnętrznego.

Uzupełniając izolację oprogramowania wewnętrznego w systemie Windows Server 2022, zabezpieczenia oparte na wirtualizacji (VBS) izolują krytyczne części systemu operacyjnego, takie jak jądro, od reszty systemu. Pomaga to zapewnić, że serwery pozostają przeznaczone do uruchamiania krytycznych obciążeń roboczych, a także pomaga chronić powiązane aplikacje i dane przed atakami i eksfiltracją.

Aby jeszcze bardziej zabezpieczyć oprogramowanie wewnętrzne serwerów PowerEdge przed atakami, firma Dell Technologies pomaga zabezpieczyć łańcuch dostaw serwerów PowerEdge, aby nikt nie dopuścił się ingerencji w serwer podczas transportu z fabryki do siedziby klienta (bardziej szczegółowo zostanie to wyjaśnione w poniższym punkcie Dodatkowe zabezpieczenia dzięki integralności łańcucha dostaw firmy Dell Technologies).

Obrona prewencyjna

Funkcje zabezpieczonego rdzenia umożliwiają aktywną obronę i zakłócenie działania wielu ścieżek, które atakujący mogą wykorzystać do ingerencji w systemy. Integralność kodu chroniona przez monitor maszyny wirtualnej (HVCI) w VBS izoluje funkcję podejmowania decyzji dotyczących integralności kodu od reszty systemu operacyjnego Windows, co pomaga zapewnić, że jedynym sposobem, w jaki pamięć jądra może stać się wykonywalna, jest weryfikacja integralności kodu. VBS umożliwia również korzystanie z funkcji Windows Defender Credential Guard, w której poświadczenia użytkownika i wpisy tajne są przechowywane w kontenerze wirtualnym, do którego system operacyjny nie ma bezpośredniego dostępu.

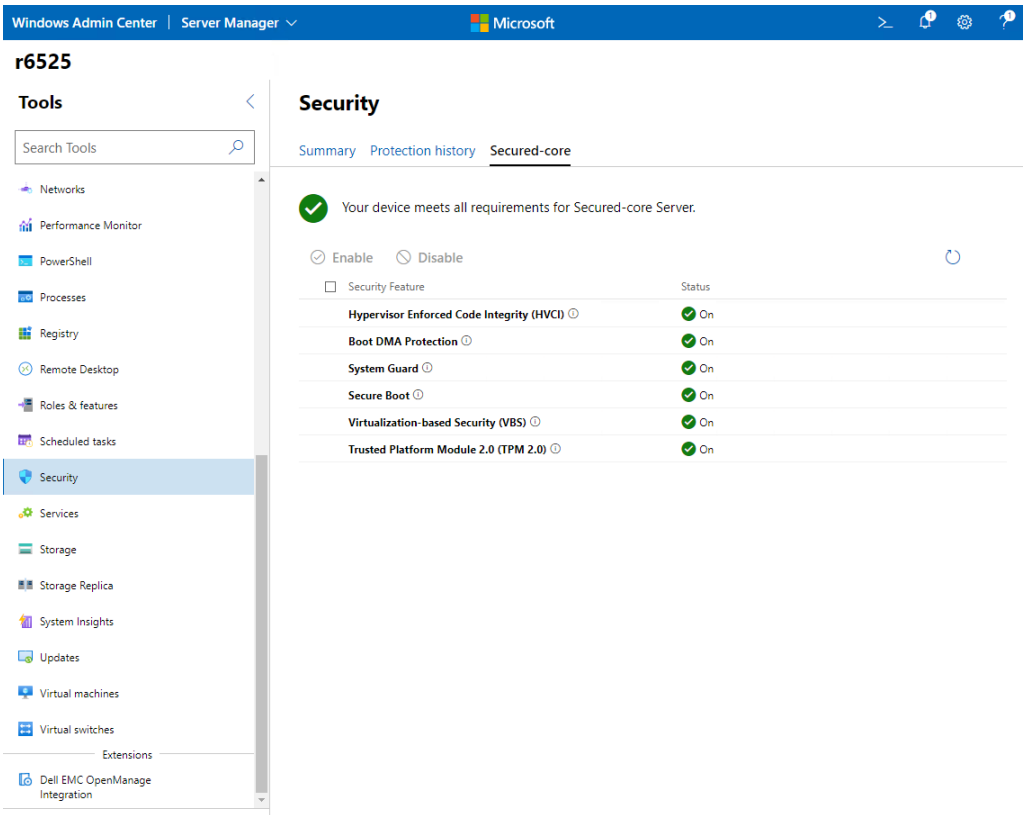
Moduł Trusted Platform Module 2.0 (TPM 2.0) jest standardowo dostarczany w przypadku serwerów z zabezpieczonym rdzeniem i zapewnia chroniony magazyn poufnych kluczy i danych, takich jak pomiary komponentów ładowanych podczas rozruchu. W podwyższeniu poziomu bezpieczeństwa pomaga możliwość sprawdzenia, czy oprogramowanie wewnętrzne uruchamiane podczas rozruchu jest prawidłowo podpisane przez oczekiwanego autora i czy nie zostało naruszone. To sprzętowe źródło zaufania podnosi również poziom ochrony zapewnianej przez takie funkcje, jak szyfrowanie dysków funkcją BitLocker, które korzysta z modułu TPM 2.0 i ułatwia tworzenie przepływów pracy opartych na poświadczaniach, które można włączyć do strategii bezpieczeństwa w modelu „zero trust”. Podsumowując, zabezpieczenia te umożliwiają zespołom IT i zespołom SecOps lepsze wykorzystanie czasu w wielu obszarach zabezpieczeń, które wymagają ich uwagi.

Serwery PowerEdge nowej generacji obsługują standard branżowy bezpiecznego rozruchu UEFI (Unified Extensible Firmware Interface) Secure Boot. Funkcja bezpiecznego rozruchu UEFI Secure Boot sprawdza podpisy kryptograficzne sterowników UEFI i innego kodu wczytanego przed uruchomieniem systemu operacyjnego, aby upewnić się, że złośliwe oprogramowanie nie naruszyło oprogramowania wewnętrznego. Ponadto serwery PowerEdge obsługują moduł TPM 2.0 w celu zwiększenia bezpieczeństwa oprogramowania wewnętrznego i systemu operacyjnego.

Prostsze zabezpieczenia

Kupując serwer PowerEdge z zabezpieczonym rdzeniem, mamy pewność, że firma Dell Technologies dostarczyła zestaw sprzętu, oprogramowania wewnętrznego i sterowników, które spełniają obietnicę zabezpieczonego rdzenia. Firma Microsoft ściśle współpracuje z firmą Dell Technologies w celu uproszczenia zabezpieczeń serwerów PowerEdge.

Nowe funkcje w systemie Windows Admin Center ułatwiają administratorom konfigurowanie funkcji zabezpieczeń systemu operacyjnego Windows Server 2022 Secured-Core Server. Nowa funkcja zabezpieczeń Windows Admin Center umożliwia administratorom włączanie zaawansowanych zabezpieczeń jednym kliknięciem na przycisk. Windows Admin Center przedstawia stan wszystkich wymaganych funkcji zabezpieczeń systemu Windows Server 2022 Secured-Core Server i umożliwia administratorom włączanie funkcji w razie potrzeby z jednej lokalizacji.



Rysunek 1. Ekran potwierdzenia zabezpieczonego rdzenia w Windows Admin Center

Integracja Dell EMC™ OpenManage™ z Windows Admin Center stanowi rozszerzenie programu Windows Admin Center, które jeszcze bardziej upraszcza zarządzanie serwerami z zabezpieczonymi rdzeniami. To rozszerzenie Windows Admin Center upraszcza zadania (między innymi) administratorów IT związane z zabezpieczeniami poprzez zdalne zarządzanie serwerami PowerEdge. W kontekście systemu Windows Server 2022 Secured-Core Server integracja OpenManage z Windows Admin Center umożliwia wyświetlanie spisu serwerów PowerEdge z poziomu Windows Admin Center oraz zapewnia ujednolicony widok informacji o kondycji, sprzęcie i oprogramowaniu wewnętrznym elementów serwera PowerEdge.

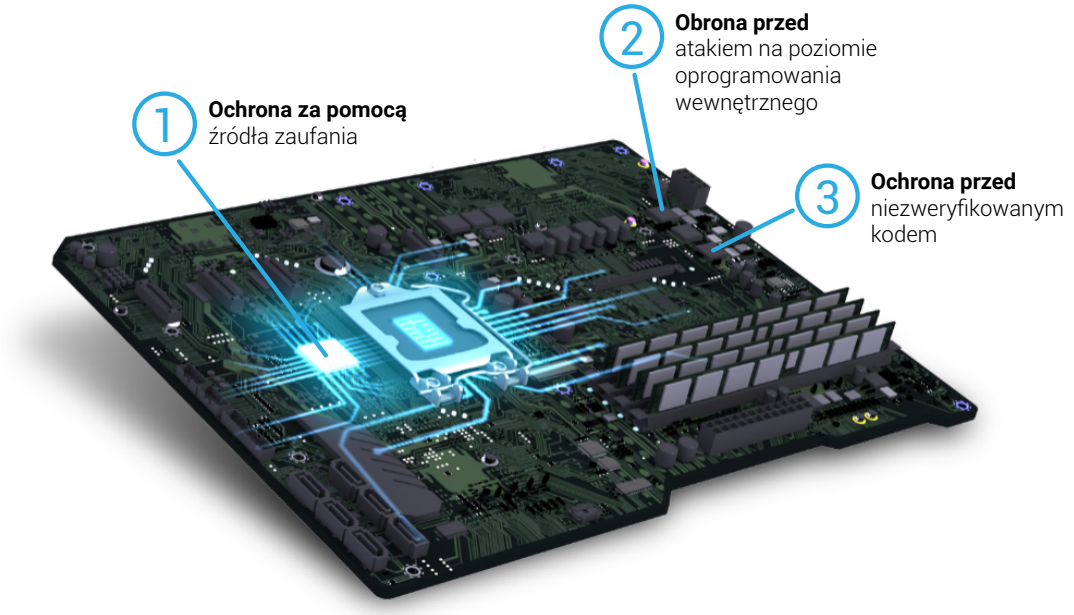
Obsługa serwerów PowerEdge pod kątem systemu Windows Server 2022 Secure-Core Server

Ze względu na wielowarstwowy charakter zabezpieczeń serwerów z zabezpieczonym rdzeniem wsparcie ze strony producenta OEM sprzętu ma kluczowe znaczenie. Serwery PowerEdge są testowane i certyfikowane przez firmę Dell Technologies w celu zapewnienia, że sprzęt i oprogramowanie wewnętrzne spełniają wymagania funkcji zabezpieczeń systemu Windows Server 2022. Ponadto sprzęt i oprogramowanie wewnętrzne w serwerach PowerEdge są skonfigurowane tak, aby umożliwić działanie systemu Windows Server 2022 Secure-Core Server. W tabeli 1 przedstawiono szczegółowe informacje na temat sposobu w jaki sprzęt serwerów PowerEdge wspiera funkcje systemu Windows Server 2022.

Tabela 1. Mapowanie funkcji zabezpieczeń systemu Windows Server 2022 i najważniejszych funkcji pomocniczych w serwerach Dell EMC™ PowerEdge™ nowej generacji

	Windows Server 2022	Serwery Dell EMC™ PowerEdge™ nowej generacji
Zaawansowana ochrona	Systemy z zabezpieczonymi rdzeniami umieszczają oprogramowanie wewnętrzne w piaskownicach sprzętowych, co pomaga ograniczyć wpływ luk w zabezpieczeniach związanych z oprogramowaniem wewnętrznym. Zabezpieczenia VBS izolują krytyczne części systemu operacyjnego od zaawansowanego złośliwego oprogramowania.	Firma Dell Technologies pomaga zabezpieczyć łańcuch dostaw serwerów PowerEdge, aby nikt nie mógł dopuścić się ingerencji w serwer ani naruszenia integralności oprogramowania wewnętrznego podczas transportu z fabryki do lokalizacji klienta.
Obrona prewencyjna	Funkcje VBS, takie jak HVCI i Windows Defender Credential Guard, zapobiegają powstawaniu całych klas luk w zabezpieczeniach i lepiej chronią wrażliwe zasoby, takie jak poświadczenia. Moduł TPM 2.0 zapewnia sprzętowe źródło zaufania używane jako bezpieczny fundament.	Serwery PowerEdge obsługują standardową w branży funkcję bezpiecznego rozruchu UEFI Secure Boot w celu sprawdzania podpisów kryptograficznych sterowników UEFI i innego kodu załadowanego przed uruchomieniem systemu operacyjnego. Serwery PowerEdge obsługują moduł TPM 2.0.
Prostsze zabezpieczenia	Windows Admin Center zapewnia łatwy dostęp do konfiguracji serwerów z zabezpieczonymi rdzeniami.	Firma Microsoft współpracuje z firmą Dell Technologies w celu uproszczenia zabezpieczeń serwerów PowerEdge. Integracja Windows Admin Center z Dell EMC™ OpenManage™ jeszcze bardziej upraszcza zarządzanie serwerami z zabezpieczonymi rdzeniami.

Anatomia zaawansowanych zabezpieczeń wielowarstwowych



1 Ochrona za pomocą źródła zaufania

Dzięki współpracy z czołowymi producentami OEM, takimi jak Dell Technologies, oraz dostawcami układów scalonych, takimi jak Intel i AMD, serwery z zabezpieczonymi rdzeniami wykorzystują zgodne ze standardami branżowymi sprzętowe źródło zaufania w połączeniu z funkcjami zabezpieczeń wbudowanymi we współczesne procesory.

Serwery z zabezpieczonymi rdzeniami korzystają z modułu TPM 2.0 i nowoczesnego procesora z DRTM, aby bezpieczniej uruchamiać serwery i minimalizować luki w zabezpieczeniach oprogramowania wewnętrznego.

2 Obrona przed atakiem na poziomie oprogramowania wewnętrznego

Serwery z zabezpieczonymi rdzeniami wykorzystują zabezpieczenia sprzętowe nowoczesnego procesora, aby uruchamiać system w stanie zaufanym, zapobiegając ingerencjom zaawansowanego złośliwego oprogramowania w system i atakom na poziomie oprogramowania wewnętrznego.

Funkcja System Guard Secure Launch używa procesora do weryfikacji urządzenia pod kątem bezpieczniejszego rozruchu, co pomaga zapobiegać zaawansowanym atakom na oprogramowanie wewnętrzne.

3 Ochrona przed niezweryfikowanym kodem

Kod uruchomiony w zaufanej bazie obliczeniowej działa w sposób integralny i nie jest narażony na zagrożenia ani ataki.

Dzięki funkcji HVCI serwer z zabezpieczonymi rdzeniami uruchamia tylko pliki wykonywalne podpisane przez znane i zatwierdzone urzędy. Monitor maszyny wirtualnej ustawia i wymusza uprawnienia, aby zapobiec próbom modyfikacji pamięci i uczynienia jej wykonywalną przez złośliwe oprogramowanie.

Obsługa serwerów PowerEdge nowej generacji w celu zapewnienia bezpiecznej łączności w systemie Windows Server 2022

Serwery PowerEdge nowej generacji obsługują szyfrowanie AES-256 bloków SMB (Server Message Block) w celu obsługi wymagających zabezpieczenia obciążeń roboczych. Ta obsługa oznacza, że serwery PowerEdge z systemem Windows Server 2022 mogą zapewnić kompleksowe szyfrowanie danych obciążeń roboczych w celu zapewnienia dodatkowego bezpieczeństwa. 256-bitowe szyfrowanie AES używane do SMB w systemie Windows Server 2022 jest również wystarczająco niezawodne, aby było odporne nawet na ataki brute-force ze strony komputerów kwantowych, jeśli używane są wystarczająco silne hasła.

Serwery PowerEdge i system Windows Server 2022 dodatkowo rozszerzają kompleksowe szyfrowanie SMB z poziomu poszczególnych serwerów na komunikację wewnętrzną klastrów za pomocą szyfrowania AES-256 dla ruchu danych SMB wschód-zachód. Te dodatkowe mechanizmy kontroli szyfrowania SMB jeszcze bardziej uodporniają obciążenia robocze i zamykają drogi ataku.

Ponadto system Windows Server 2022 korzysta z instrukcji Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) zawartych w skalowalnych procesorach Intel® Xeon® trzeciej generacji oraz wektorowego szyfrowania AES dla 256-bitów (vAES256) zawartego w procesorach AMD EPYC™ Zen 3. Zestawy instrukcji tych zaawansowanych procesorów zwiększają wydajność szyfrowania AES-256 w serwerach PowerEdge. Korzystając z tych zaawansowanych technologii zabezpieczeń, firmy Dell Technologies i Microsoft sprawiają, że nie musisz wybierać między solidnymi zabezpieczeniami a responsywnością w przypadku obciążeń roboczych o znaczeniu krytycznym.

Dodatkowe zabezpieczenia dzięki integralności łańcucha dostaw firmy Dell Technologies

Integralność łańcucha dostaw firmy Dell Technologies chroni elementy sprzętowe i oprogramowania wewnętrznego przed atakami podczas produkcji i transportu. W trosce o integralność sprzętu firma Dell Technologies dba o to, aby przed wysyłką produktów do klientów nie dochodziło do ingerencji w produkt ani umieszczania w nim podrobionych podzespołów. Mechanizmy kontroli stosowane przez firmę Dell Technologies obejmują wybór dostawców, zaopatrzenie, procesy produkcyjne i zarządzanie nimi, a także audyty i testy. Kontrole materiałów podczas produkcji pomagają zidentyfikować komponenty, które są błędnie oznaczone, odbiegają od normalnych parametrów wydajności lub zawierają nieprawidłowy identyfikator elektroniczny.

W trosce o integralność oprogramowania firma Dell Technologies stara się przed wysyłką produktu zapewnić ochronę przed umieszczeniem złośliwego oprogramowania w oprogramowaniu wewnętrznym lub sterownikach urządzeń, a także zapobiegać wszelkim lukom w zabezpieczeniach kodowania. Firma Dell Technologies utrzymuje certyfikat ISO 9001 dla wszystkich zakładów produkcyjnych na całym świecie. Ścisłe przestrzeganie tych procesów i środków kontroli pomaga zminimalizować ryzyko wprowadzania podrobionych komponentów w produktach Dell Technologies™ oraz złośliwego oprogramowania w oprogramowaniu wewnętrznym lub sterownikach urządzeń. Ponadto firma Dell Technologies wdraża te środki w ramach procesu cyklu życia tworzenia oprogramowania SDLC (Software Development Lifecycle).

Firma Dell Technologies pracuje również nad zapewnieniem fizycznego bezpieczeństwa zakładów produkcyjnych i łańcuchów transportowych. Firma Dell Technologies wymaga, aby niektóre fabryki, w których produkowane są produkty Dell Technologies, spełniały określone wymagania organizacji TAPA (Transportation Asset Protection Association) dotyczące bezpieczeństwa, w tym wymogi dotyczące stosowania monitorowanych kamer przemysłowych w kluczowych obszarach, kontroli dostępu oraz stale strzeżonych wejść i wyjść. Firma Dell Technologies wdrożyła również środki ochrony produktów przed kradzieżą i naruszeniem podczas transportu w ramach wiodącego w branży programu logistycznego. Wreszcie narzędzie Secured Component Verification (SCV) firmy Dell Technologies dla serwerów PowerEdge umożliwia klientom firmy Dell Technologies sprawdzenie, czy serwer PowerEdge otrzymany przez klienta odpowiada serwerowi wyprodukowanemu w fabryce.

Chroń najważniejsze obciążenia robocze dzięki lepszej platformie zabezpieczeń systemu Windows Server 2022 i serwerów Dell EMC PowerEdge nowej generacji

Obciążenia robocze są tak bezpieczne, jak bezpieczny jest fundament, na którym działają. Zagrożenie ze strony złośliwego oprogramowania i naruszeń danych będzie nadal rosło w przyszłości, zwłaszcza że cyberprzestępcy stale badają możliwości ataku odporne na tradycyjne zabezpieczenia oparte na oprogramowaniu. Ataki na oprogramowanie wewnętrzne są wymierzone w serwery podczas procesu rozruchu, zanim jeszcze zabezpieczenia oparte na oprogramowaniu zaczną chronić systemy. Nowoczesna ochrona serwerów wymaga wielotorowych zabezpieczeń obejmujących sprzęt, oprogramowanie wewnętrzne i system operacyjny.

Uaktualnienie do systemu Windows Server 2022 może być obecnie bardziej uzasadnione niż kiedykolwiek. Funkcja serwera z zabezpieczonymi rdzeniami w systemie Windows Server 2022 pomaga organizacjom przeciwdziałać zagrożeniom zarówno dla oprogramowania wewnętrznego, jak i systemu operacyjnego. W połączeniu z zabezpieczeniami integralności sprzętu i oprogramowania firmy Dell Technologies serwery Dell EMC PowerEdge nowej generacji z systemem Windows Server 2022 mogą zapewnić nowoczesne zabezpieczenia dla całego stosu sprzętu, oprogramowania wewnętrznego i systemu operacyjnego. Funkcje bezpiecznej łączności dostępne w systemie Windows Server 2022 i obsługiwane przez serwery PowerEdge nowej generacji rozszerzają te zabezpieczenia poza pojedyncze serwery i obejmują całe klastry w centrum danych. Oprócz tego wsparcie dla systemu Windows Server 2012 kończy się w październiku 2023 r., co oznacza, że nadszedł czas, aby zacząć planować aktualizację[6].

Aby dowiedzieć się więcej o tym, w jaki sposób system Windows Server 2022 i serwery Dell EMC PowerEdge nowej generacji mogą pomóc w zabezpieczeniu krytycznych obciążeń roboczych i danych, odwiedź stronę www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. „Cybercrime To Cost The World $10.5 Trillion Annually By 2025”. Listopad 2020 r. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[2] IDC. „IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach”. Sierpień 2021 r.
[3] IBM. „How much does a data breach cost?” 2021. www.ibm.com/security/data-breach.
[4] Dan Goodin. „Hospitals hamstrung by ransomware are turning away patients”. *Ars Technica.* Sierpień 2021 r. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. „New Security Signals study shows firmware attacks on the rise; here’s how Microsoft is working to help eliminate this entire class of threats”. Marzec 2021 r. www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/.
[6] W momencie pracy nad tym artykułem. Aby uzyskać najnowsze informacje na temat zakończenia świadczenia pomocy technicznej dla systemu Windows Server 2012, odwiedź stronę cyklu życia systemu Windows Server 2012: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Przeprowadź modernizację z użyciem systemu Windows Server 2022. Gotowy do pracy w chmurze system operacyjny, który zwiększa wartość inwestycji lokalnych dzięki możliwościom hybrydowym.