DELL Technologies

Microsoft

Whitepaper

Erweiterter Sicherheitsschutz mit den kombinierten Funktionen von Windows Server 2022 und Dell EMC™ PowerEdge™-Servern der nächsten Generation

Sicherheitsverstärkung von geschäftskritischen Workloads mit sichererer Hardware-, Firmware- und Betriebssystemumgebung

Laut Cybersecurity Ventures wird die globale Cyberkriminalität 2021 voraussichtlich insgesamt 6 Billionen USD kosten. Bis 2025 werden diese Kosten auf 10,5 Billionen USD ansteigen.[1] Allein Ransomwareangriffe sind in sechs Jahren um das 61-Fache auf 20 Milliarden USD im Jahr 2021 gestiegen. Derzeit erfolgt alle 11 Sekunden ein Angriff.[1] Eine IDC-Umfrage aus dem Jahr 2021 ergab, dass es in mehr als einem Drittel der weltweit befragten Unternehmen in den letzten 12 Monaten zu einem Ransomwareangriff oder einer Sicherheitsverletzung gekommen ist (und zwar häufig zu mehr als einen Angriff).[2] IBM schätzt, dass die Kosten einer einzigen Datenschutzverletzung jetzt bei 4,24 Millionen USD liegen.[3] Die tatsächlichen Kosten von Sicherheitsverletzungen können deutlich höher sein: In einigen Fällen mussten Krankenhäuser in den USA NotfallpatientInnen in andere Krankenhäuser verlegen und Krankenwagen aufgrund von Ransomwareangriffen abweisen.[4]

Firmwareangriffe können eine besonders böswillige Bedrohung für Unternehmen sein. Denn bei einem auf die Firmware ausgerichteten Angriff kann Malware sogar vor dem Start des Betriebssystems (BS) – und damit vor der unter dem Betriebssystem ausgeführten Sicherheitssoftware – eingeschleust werden. Doch weniger als die Hälfte der Unternehmen hat Maßnahmen ergriffen, um ihre Systeme vor Firmwareangriffen zu schützen, obwohl sich die Häufigkeit der Angriffe in den letzten fünf Jahren verfünffacht hat.[5] Letztendlich sind Workloads nur so sicher wie die Stacks als Ganzes, auf denen sie ausgeführt werden.

Zur Bewältigung dieses exponentiellen Wachstums der Häufigkeit, Vielfalt und Kosten von Malwarebedrohungen muss die moderne Sicherheit mehrschichtig sein. Denn Malware kann Systeme auf Hardware- und Firmwareebene oder während des Startvorgangs in allen Bereichen gefährden, in denen rein softwaredefinierte Sicherheit machtlos ist. Um dieser Sicherheitslücke entgegenzuwirken, ist moderne Serversicherheit keine eingleisige Strategie. Sie muss in den gesamten Infrastrukturstack integriert sein. Die Kombination aus Dell EMC™ PowerEdge™-Servern der nächsten Generation und Windows Server 2022 erleichtert AdministratorInnen die wichtige Aufgabe, Hardware, Firmware und BS abzustimmen, um geschäftskritische Workloads angemessen zu sichern.

Kombinierte Vorteile von Windows Server 2022-Secured-Core-Servern und PowerEdge-Servern der nächsten Generation

Der Secured-Core-Server ist eine neue Funktion in Windows Server 2022, die Hardware-, Firmware- und BS-Funktionen nutzt, um Schutz vor aktuellen und zukünftigen Bedrohungen zu bieten. Die Kombination der Software für Windows Server 2022-Secured-Core-Server, die auf PowerEdge-Serverhardware der nächsten Generation ausgeführt wird, bietet Unternehmen wie Ihrem drei wesentliche Vorteile:

- Erweiterter Schutz
- Präventive Abwehr
- Vereinfachte Sicherheit

Erweiterter Schutz

Basierend auf Bedrohungsdaten von Microsoft bieten Secured-Core-PCs mehr als doppelt so viel Schutz vor Infizierung wie reguläre PCs. Microsoft bringt jetzt dieselbe Technologie mit Windows Server 2022-Secured-Core-Servern in den Serverbereich.[5] Schutzfunktionen, die durch einen Secured-Core-Server ermöglicht werden, sind darauf ausgerichtet, eine sichere Plattform für kritische Workloads und Daten auf diesem Server zu erzeugen. Insbesondere nutzen Secured-Core-Server die Prozessorunterstützung für die DRTM-Technologie (Dynamic Root of Trust for Measurement), um Firmware in einer hardwarebasierte Sandbox zu platzieren. Diese Isolierung trägt dazu bei, die Auswirkungen von Sicherheitslücken in Millionen von Zeilen hochprivilegierten Firmwarecodes zu begrenzen.

Als Ergänzung zur Firmwareisolierung in Windows Server 2022 isoliert die virtualisierungsbasierte Sicherheit (VBS) wichtige Teile des BS – z. B. den Kernel – vom Rest des Systems. Damit kann sichergestellt werden, dass Server weiterhin kritische Workloads ausführen. Außerdem werden zugehörige Anwendungen und Daten vor Angriffen und Exfiltration geschützt.

Zur weiteren Sicherheitsverstärkung der Firmware in PowerEdge-Servern vor Angriffen trägt Dell Technologies dazu bei, die Lieferkette für PowerEdge-Server zu sichern. So wird sichergestellt, dass niemand den Server während des Transports vom Werk zum Kundenstandort manipuliert hat. (Dies wird im Folgenden unter Zusätzliche Sicherheit durch Lieferkettenintegrität von Dell Technologies ausführlicher erläutert.)

Präventive Abwehr

Die Secured-Core-Funktion sorgt für eine proaktive Abwehr und Unterbrechung vieler der Pfade, die AngreiferInnen möglicherweise für einen Exploit Ihre Systeme nutzen. Die Hypervisor-geschützte Codeintegrität (HVCI) in VBS isoliert die CI-Entscheidungsfindungsfunktion für Codeintegrität vom Rest des Windows-BS. Dadurch wird sichergestellt, dass der Kernelarbeitsspeicher nur durch eine CI-Überprüfung ausführbar werden kann. VBS ermöglicht außerdem die Verwendung von Windows Defender Credential Guard, mit dessen Hilfe Nutzerzugangsdaten und geheime Schlüssel in einem virtuellen Container gespeichert werden, auf den das BS nicht direkt zugreifen kann.

Trusted Platform Module 2.0 (TPM 2.0) ist standardmäßig im Lieferumfang von Secured-Core-Servern enthalten und bietet einen geschützten Speicher für sensible Schlüssel und Daten, z. B. Messgrößen für die Komponenten, die während des Startvorgangs geladen werden. Die Möglichkeit, zu überprüfen, dass während des Startvorgangs ausgeführte Firmware ordnungsgemäß vom erwarteten Autor signiert ist und nicht manipuliert wurde, trägt zur Verbesserung der Sicherheit bei. Diese sog. Root of Trust der Hardware erhöht auch den Schutz durch Funktionen wie die BitLocker-Laufwerkverschlüsselung, die TPM 2.0 verwendet und die Erstellung von bestätigungsbasierten Workflows erleichtert, die in Zero-Trust-Sicherheitsstrategien integriert werden können. Zusammengenommen ermöglichen diese Abwehrmaßnahmen Ihren IT- und SecOps-Teams, in den vielen Sicherheitsbereichen, die ihre Aufmerksamkeit benötigen, ihre Zeit besser zu nutzen.

PowerEdge-Server der nächsten Generation unterstützen den Branchenstandard Unified Extensible Firmware Interface (UEFI) Secure Boot. UEFI Secure Boot prüft die kryptografischen Signaturen von UEFI-Treibern und anderem Code, die vor Ausführung des BS geladen wurden. So wird sichergestellt, dass die Firmware nicht durch Malware manipuliert wurde. Darüber hinaus unterstützen PowerEdge-Server TPM 2.0, um die Sicherheit für Firmware und BS zu erhöhen.

Vereinfachte Sicherheit

Wenn Sie einen PowerEdge-Secured-Core-Server erwerben, haben Sie die Gewissheit, dass Dell Technologies eine Gruppe von Hardware, Firmware und Treibern bereitgestellt hat, die das Versprechen von Secured-Core erfüllen. Microsoft arbeitet eng mit Dell Technologies zusammen, um die Sicherheit auf PowerEdge-Servern zu vereinfachen.

Neue Funktionen in Windows Admin Center erleichtern AdministratorInnen die Konfiguration der BS-Sicherheitsfunktionen von Windows Server 2022-Secured-Core-Servern. Mit der neuen Sicherheitsfunktion von Windows Admin Center können AdministratorInnen per Mausklick erweiterte Sicherheit aktivieren. Windows Admin Center zeigt den Status aller erforderlichen Sicherheitsfunktionen für Windows Server 2022-Secured-Core-Server an, sodass AdministratorInnen Funktionen nach Bedarf von einem einzigen Ort aus aktivieren können.

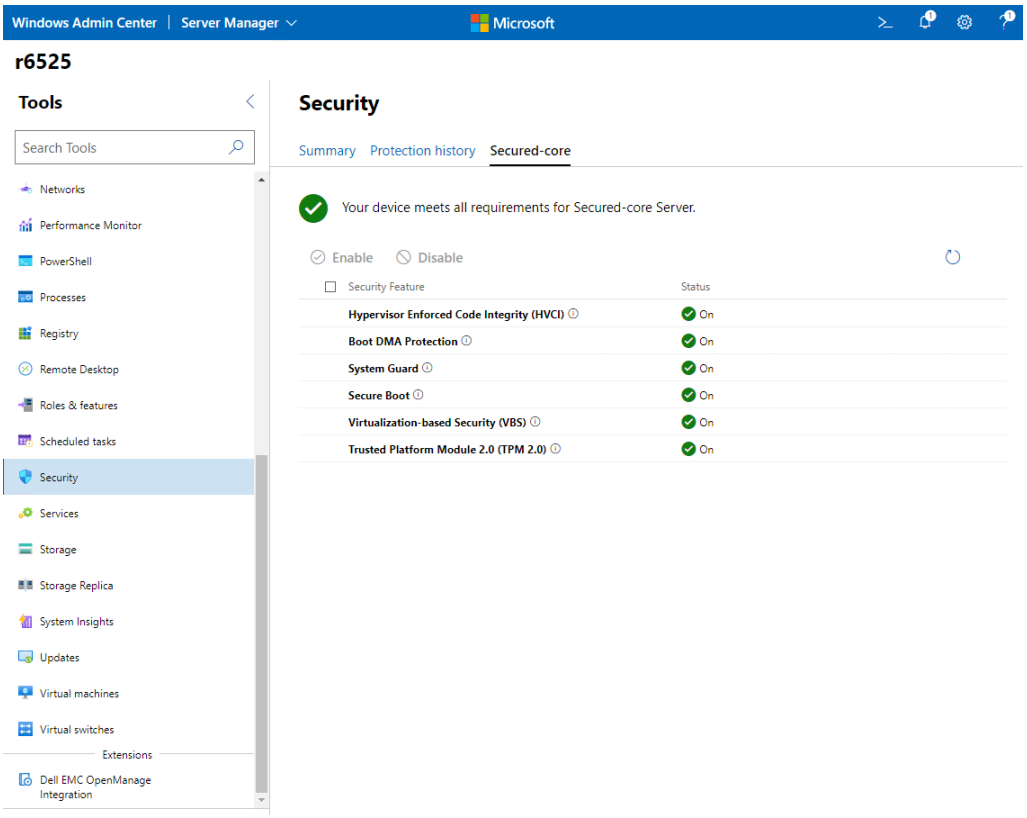


Abbildung 1: Secured-Core-Bestätigungsbildschirm in Windows Admin Center

Dell EMC™ OpenManage™ Integration with Windows Admin Center ist eine Erweiterung für Windows Admin Center, die das Management von Secured-Core-Servern weiter vereinfacht. Unter anderem vereinfacht diese Erweiterung von Windows Admin Center die Sicherheitsaufgaben von IT-AdministratorInnen durch das Remotemanagement von PowerEdge-Servern. Im Kontext von Windows Server 2022 Secured-Core-Servern können Sie mit der Erweiterung OpenManage Integration with Windows Admin Center Ihre Bestandsaufnahme von PowerEdge-Servern innerhalb von Windows Admin Center anzeigen. Sie bietet eine einheitliche Ansicht der Integritäts-, Hardware- und Firmwarebestandsinformationen der PowerEdge-Serverkomponenten.

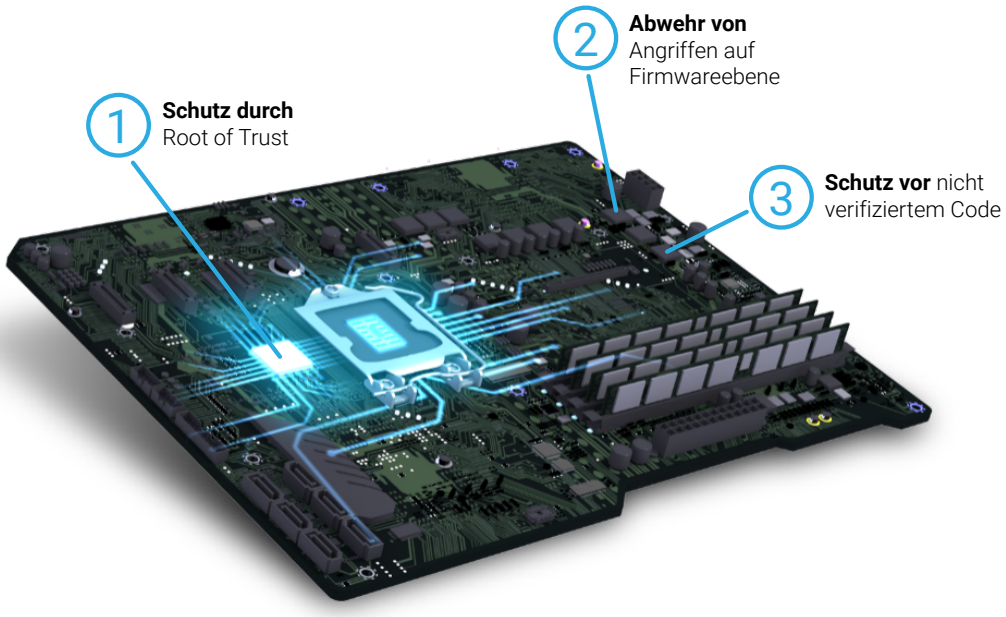
Unterstützung von PowerEdge-Servern für Windows Server 2022-Secured-Core-Server

Aufgrund des mehrschichtigen Charakters der Secured-Core-Serverabwehr ist die Unterstützung von Ihrem Hardware-OEM von entscheidender Bedeutung. PowerEdge-Server werden von Dell Technologies getestet und zertifiziert, um sicherzustellen, dass Hardware und Firmware die Anforderungen der Sicherheitsfunktionen von Windows Server 2022 erfüllen. Darüber hinaus sind die Hardware und Firmware in PowerEdge-Servern so konfiguriert, dass der Windows Server 2022-Secured-Core-Server aktiviert wird. Tabelle 1 stellt dar, wie die Hardware in PowerEdge-Servern die Windows Server 2022-Funktionen verstärkt.

Tabelle 1: Zuordnung der Sicherheitsfunktionen von Windows Server 2022 und der wichtigsten unterstützenden Funktionen auf Dell EMC™ PowerEdge™-Servern der nächsten Generation

	Windows Server 2022	Dell EMC™ PowerEdge™-Server der nächsten Generation
Erweiterter Schutz	Secured-Core-Systeme stellen Firmware in einer hardwarebasierten Sandbox bereit, um die Auswirkungen von firmwarebasierten Sicherheitslücken zu begrenzen. VBS isoliert kritische Teile des BS vor hochentwickelter Malware.	Dell Technologies sichert die Lieferkette für PowerEdge-Server, um sicherzustellen, dass niemand den Server manipuliert oder die Firmware auf dem Werk vom Werk zum Kundenstandort infiziert.
Präventive Abwehr	VBS-Funktionen wie HVCI und Windows Defender Credential Guard verhindern ganze Klassen von Sicherheitslücken und bieten einen besseren Schutz von sensiblen Ressourcen wie Zugangsdaten. TPM 2.0 bietet Root of Trust für Hardware als Fundament für Sicherheit.	PowerEdge-Server unterstützen den Branchenstandard UEFI Secure Boot, um die kryptografischen Signaturen von UEFI-Treibern und anderem Code zu überprüfen, die vor der Ausführung des BS geladen wurden. PowerEdge-Server unterstützen TPM 2.0.
Vereinfachte Sicherheit	Windows Admin Center bietet einfachen Zugriff zum Konfigurieren von Secured-Core-Servern.	Microsoft arbeitet mit Dell Technologies zusammen, um die Sicherheit auf PowerEdge-Servern zu vereinfachen. Windows Admin Center Integration with Dell EMC™ OpenManage™ vereinfacht das Management von Secured-Core-Servern weiter.

Anatomie der erweiterten, mehrschichtigen Sicherheit



1 Schutz durch Root of Trust

Dank der Partnerschaft mit führenden OEMs wie Dell Technologies und Chipanbietern wie Intel und AMD nutzen Secured-Core-Server den Branchenstandard der Root of Trust von Hardware, gepaart mit Sicherheitsfunktionen, die in moderne CPUs von heute integriert sind.

Secured-Core-Server verwenden TPM 2.0 und eine moderne CPU mit DRTM, um Server sicherer zu starten und Firmwaresicherheitslücken zu minimieren.

2 Abwehr von Angriffen auf Firmwareebene

Secured-Core-Server nutzen hardwarebasierte Sicherheit in der modernen CPU, um das System in einem vertrauenswürdigen Zustand zu starten, sodass fortschrittliche Malware das System nicht manipulieren und auf Firmwareebene angreifen kann.

System Guard Secure Launch verwendet die CPU, um das Gerät zu validieren und sicherer zu starten und so ausgefeilte Firmwareangriffe zu verhindern.

3 Schutz vor nicht verifiziertem Code

Innerhalb der vertrauenswürdigen Computing-Basis ausgeführter Code wird mit Integrität ausgeführt und ist keinen Exploits oder Angriffen ausgesetzt.

Ein mit HVCI aktivierter Secured-Core-Server startet nur ausführbare Dateien, die von bekannten und genehmigten Zertifizierungsstellen signiert wurden. Der Hypervisor legt Berechtigungen fest und erzwingt diese, um zu verhindern, dass Malware versucht, den Arbeitsspeicher zu ändern und ausführbar zu machen.

Unterstützung für PowerEdge-Server der nächsten Generation für sichere Konnektivität in Windows Server 2022

PowerEdge-Server der nächsten Generation unterstützen für sicherheitsrelevante Workloads Verschlüsselung vom Typ Server Message Block (SMB) AES-256. Diese Unterstützung bedeutet, dass PowerEdge-Server mit Windows Server 2022 eine End-to-End-Verschlüsselung für Workload-Daten für zusätzliche Sicherheit bieten können. Die 256-Bit-AES-Verschlüsselung, die für SMB in Windows Server 2022 verwendet wird, ist auch stark genug, um selbst gegen Brute-Force-Angriffe durch Quantum-Computer zu schützen, sofern die Sicherheit der verwendeten Kennwörter ausreichend ist.

PowerEdge-Server und Windows Server 2022 weiten die End-to-End-SMB-Verschlüsselung von einzelnen Servern außerdem auf die interne Kommunikation von Clustern mit AES-256-Verschlüsselung für Ost-West-SMB-Datenverkehr aus. Diese zusätzlichen SMB-Verschlüsselungskontrollen verstärken Workload-Sicherheit weiter und verschließen Angriffswege.

Schließlich nutzt Windows Server 2022 Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) in den skalierbaren Intel® Xeon® Prozessoren der 3. Generation sowie die vektorisierte AES-Verschlüsselung für 256-Bit (vAES256) in AMD EPYC™ Zen 3-Prozessoren. Die Instruktionssätze dieser fortschrittlichen Prozessoren steigern die Leistung für die AES-256-Verschlüsselung in PowerEdge-Servern. Durch die Nutzung dieser fortschrittlichen Sicherheitstechnologien sorgen Dell Technologies und Microsoft dafür, dass Sie sich nicht zwischen robuster Sicherheit und Reaktionsgeschwindigkeit für geschäftskritische Workloads entscheiden müssen.

Zusätzliche Sicherheit durch Lieferkettenintegrität von Dell Technologies

Die Lieferkettenintegrität von Dell Technologies schützt Hardware- und Firmwarekomponenten vor einer Infizierung während Fertigung und Versand. Im Bereich der Hardwareintegrität stellt Dell Technologies sicher, dass keine Produktmanipulationen oder ein Einsetzen gefälschter Komponenten vor dem Versand von Produkten an Kunden erfolgen. Zu den Kontrollen von Dell Technologies zählen Lieferantenauswahl, Beschaffung, Produktionsprozesse sowie Governance durch Audits und Tests. Materialprüfungen während der Produktion helfen dabei, Komponenten aufzuspüren, die fehlerhaft sind, von den üblichen Leistungsparametern abweichen oder eine falsche elektronische Kennung aufweisen.

In puncto Softwareintegrität möchte Dell Technologies sicherstellen, dass vor dem Versand eines Produkts an Kunden keine Malware in Firmware- oder Gerätetreiber eingeschleust wird, und Sicherheitslücken bei der Programmierung vermieden werden. Dell Technologies legt an allen globalen Fertigungsstandorten Wert auf ISO 9001-Zertifizierung. Die strikte Einhaltung dieser Prozesse und Kontrollen trägt dazu bei, das Risiko zu minimieren, dass in die Produkte von Dell Technologies™ gefälschte Komponenten gelangen oder dass Malware in Firmware- oder Gerätetreiber eingeschleust werden kann. Darüber hinaus implementiert Dell Technologies diese Maßnahmen als Teil des SDLC-Prozesses (Software Development Lifecycle).

Dell Technologies arbeitet zudem daran, die physische Sicherheit von Fertigungseinrichtungen und Transportketten sicherzustellen. Die Fabriken, in denen Dell Technologies Produkte gefertigt werden, müssen bestimmte FSRs (Facility Security Requirements) der Transported Asset Protection Association (TAPA) erfüllen. Dazu zählen auch Videoüberwachung von wichtigen Bereichen, Zugangskontrollen sowie die ständige Überwachung von Ein- und Ausgängen. Dell Technologies hat im Rahmen eines branchenführenden Logistikprogramms außerdem Schutzmaßnahmen eingeführt, um Produkte vor Diebstahl und Manipulation während des Transports zu schützen. Schließlich können Kunden von Dell Technologies mit Dell Technologies Secured Component Verification (SCV) für PowerEdge-Server überprüfen, ob ein vom Kunden empfangener PowerEdge-Server mit dem übereinstimmt, was im Werk hergestellt wurde.

Schutz Ihrer wichtigsten Workloads mit einer besseren Sicherheitsgrundlage von Windows Server 2022 und Dell EMC PowerEdge-Servern der nächsten Generation

Workloads sind nur so sicher wie die Grundlage, auf der sie ausgeführt werden. Die Bedrohung durch Malware und Datenschutzverletzungen wird in Zukunft weiter zunehmen, insbesondere wenn bösartige Akteure weiterhin Angriffswege erkunden, die gegen herkömmliche, softwarebasierte Sicherheit immun sind. Firmwareangriffe zielen speziell auf Server im Startvorgang ab, bevor die softwarebasierte Sicherheit überhaupt begonnen hat, Systeme zu schützen. Der moderne Serverschutz erfordert eine mehrstufige Sicherheit, die Hardware, Firmware und BS umfasst.

Ein Upgrade auf Windows Server 2022 kann jetzt sinnvoller als je zuvor sein. Mit der Secured-Core-Server-Funktion in Windows Server 2022 können Unternehmen Bedrohungen gegen Firmware und BS abwehren. In Kombination mit den Schutzfunktionen für Hardware- und Softwareintegrität von Dell Technologies bieten unter Windows Server 2022 ausgeführte Dell EMC PowerEdge-Server der nächsten Generation für den gesamten Stack moderne Sicherheit für Hardware, Firmware und BS. Die in Windows Server 2022 integrierten und von PowerEdge-Servern der nächsten Generation unterstützten Funktionen für sichere Konnektivität weiten diese Sicherheit über einzelne Server hinaus auf ganze Cluster in Ihrem Rechenzentrum aus. Darüber hinaus endet im Oktober 2023 die Unterstützung von Windows Server 2012, was bedeutet, dass es an der Zeit ist, Upgradepläne zu erarbeiten.[6]

Weitere Informationen dazu, wie Windows Server 2022 und Dell EMC PowerEdge-Server der nächsten Generation ihre kritischen Workloads und Daten sichern können, finden Sie unter www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. „Cybercrime To Cost The World $10.5 Trillion Annually By 2025“, November 2020. 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“. August 2021,
[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*. August 2021, 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“. März 2021. 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] Zum Zeitpunkt der Verfassung dieses Dokuments. Die neuesten Informationen zum Ende der Unterstützung von Windows Server 2012 finden Sie auf der Seite zum Windows Server 2012-Lebenszyklus: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Modernisierung mit Windows Server 2022.
Das Cloud-fähige Betriebssystem, das On-Premise-Investitionen mit hybriden Funktionen optimiert.