DELL Technologies

Microsoft

백서

Windows Server 2022 및 차세대 Dell EMC™ PowerEdge™ 서버의 통합 기능을 통한 고급 보안 보호 기능

더욱 안전한 하드웨어, 펌웨어, 운영 체제 환경을 통한 비즈니스 크리티컬 워크로드 강화

Cybersecurity Ventures에 따르면 2021년에는 전 세계 사이버 범죄로 인해 총 6조 달러의 비용이 들 것으로 예상되며, 2025년에는 10조 5,000억 달러로 증가할 것으로 예상됩니다.[1] 랜섬웨어 공격에 든 비용만 해도 6년 사이 61배 증가하여 2021년에는 200억 달러에 달했으며, 현재 11초마다 한 번씩 공격이 발생하고 있습니다.[1] 2021년 IDC 설문조사에 따르면 전 세계 설문조사 대상 기업 중 3분의 1 이상이 지난 12개월 동안 랜섬웨어 공격 또는 보안 침해를 경험한 적이 있는 것으로 나타났습니다(2회 이상인 경우가 많음).[2] IBM에서는 한 번의 데이터 침해로 인한 비용이 미화 424만 달러에 달하는 것으로 추정하고 있으며,[3] 실제 데이터 침해로 인한 비용은 훨씬 더 높을 수 있습니다. 미국 병원에서는 랜섬웨어 공격으로 인해 응급환자를 다른 병원으로 이송하고 구급차를 돌려보낸 일도 있습니다.[4]

펌웨어 공격은 조직에 특히 커다란 위협이 될 수 있습니다. 펌웨어 벡터가 적용된 공격은 OS(Operating System) 시작 후 실행되는 소프트웨어 기반 보안이 작동하기 전기 전에 멀웨어를 이식할 수 있기 때문입니다. 지난 5년 동안 이러한 공격의 빈도가 5배 넘게 증가했지만, 펌웨어 공격에 대비하여 시스템을 강화하기 위한 조치를 취한 조직은 절반도 채 되지 않습니다.[5] 결국 워크로드의 보안은 워크로드가 실행되는 전체 스택의 보안에 달려 있습니다.

기하급수적으로 증가하는 멀웨어 위협의 빈도, 다양성, 비용에 대처하려면 최신 보안 시스템을 다층적으로 구성해야 합니다. 이는 멀웨어가 하드웨어 및 펌웨어 수준에서 시스템을 훼손하거나 부팅 중에 소프트웨어 정의로만 보호되는 모든 영역의 보안이 취약하기 때문입니다. 이러한 취약성을 해결하려면 최신 서버 보안은 한 가지 전략만으로 구성되어서는 안 됩니다. 서버 보안 전략은 전체 인프라스트럭처 스택에 구축되어야 합니다. 차세대 Dell EMC™ PowerEdge™ 서버와 Windows Server 2022를 함께 사용하면 하드웨어, 펌웨어, OS를 조정하는 등 중요한 관리자의 작업을 간소화하여 비즈니스에 중요한 워크로드를 적절하게 보호할 수 있습니다.

Windows Server 2022 보안 코어 서버와 차세대 PowerEdge 서버의 이점 통합

보안 코어 서버(Secured-core server)는 Windows Server 2022의 새로운 기능으로 하드웨어, 펌웨어 및 OS 기능을 사용하여 현재와 미래의 위협에 대한 보호를 제공합니다. Windows Server 2022 보안 코어 서버 소프트웨어의 조합은 차세대 PowerEdge 서버 하드웨어에서 실행되며 귀사와 같은 조직에 세 가지 실질적인 이점을 제공합니다.

- 고급 보호
- 예방적 방어
- 간소화된 보안

고급 보호

Microsoft의 위협 인텔리전스 데이터를 기반으로 하는 보안 코어 PC는 일반 PC보다 2배 이상 높은 감염 방지 기능을 제공합니다. Microsoft는 Windows Server 2022 보안 코어 서버를 통해 이 기술을 서버 공간에 적용하고 있습니다.[5] 보안 코어 서버를 사용하는 보호 기능은 해당 서버의 중요한 워크로드 및 데이터를 위한 보안 플랫폼을 구축하는 것을 목표로 합니다. 특히 보안 코어 서버는 DRTM(Dynamic Root of Trust for Measurement) 기술용 프로세서 지원을 사용하여 펌웨어를 하드웨어 기반 샌드박스에 적용합니다. 이러한 격리를 통해 권한이 높은 펌웨어 코드의 수백만 줄에 취약성이 미치는 영향을 제한할 수 있습니다.

Windows Server 2022의 펌웨어 격리를 보완하는 VBS(Virtualization Based Security)는 커널 등 OS의 중요한 부분을 시스템의 나머지 부분에서 분리합니다. 이렇게 하면 서버가 중요한 워크로드를 실행하는 데 전념할 수 있고, 관련 애플리케이션과 데이터를 공격 및 유출로부터 보호할 수 있습니다.

PowerEdge 서버의 펌웨어를 공격으로부터 더욱 강력하게 보호하기 위해 Dell Technologies는 PowerEdge 서버의 공급망을 보호하여 공장에서 고객 사이트로 운송되는 동안 아무도 서버를 조작하지 못하도록 합니다(자세한 내용은 Dell Technologies 공급망 무결성을 통한 추가 보안 참조).

예방적 방어

보안 코어 기능은 공격자가 시스템을 악용하는 데 사용할 수 있는 많은 경로를 사전 예방적으로 방어하고 차단하는 데 도움이 됩니다. VBS의 HVCI(Hypervisor-protected Code Integrity)는 Windows OS의 나머지 부분으로부터 CI(Code Integrity) 의사 결정 기능을 격리하므로, CI 검증을 통해서만 커널 메모리를 실행할 수 있습니다. 또한 VBS를 통해 Windows Defender Credential Guard를 사용할 수 있으며 Windows Defender Credential Guard에서는 OS가 직접 액세스할 수 없는 가상 컨테이너에 사용자 자격 증명과 비밀번호가 저장됩니다.

TPM 2.0(Trusted Platform Module 2.0)에는 보안 코어 서버가 표준으로 제공되며, 부팅 시 로드되는 구성 요소 측정과 같은 중요한 키와 데이터를 위한 보호 저장소를 제공합니다. 부팅 시 실행되는 펌웨어의 예상 작성자 서명이 유효하고, 해당 펌웨어가 변조되지 않았는지 확인할 수 있어 보안 향상에 도움이 됩니다. 또한 이러한 하드웨어 RoT(Root of Trust)는 TPM 2.0을 사용하는 BitLocker 드라이브 암호화와 같은 기능을 통해 제공되는 보호 기능을 강화하고, 제로 트러스트(Zero Trust) 보안 전략에 통합될 수 있는 증명 기반 워크플로를 쉽게 만들 수 있도록 합니다. 이러한 방어 체계를 함께 사용하면 IT 및 SecOps 팀이 주의를 기울여야 하는 다양한 보안 영역에서 시간을 더욱 효율적으로 사용할 수 있습니다.

차세대 PowerEdge 서버는 업계 표준 UEFI(Unified Extensible Firmware Interface) 보안 부팅을 지원합니다. UEFI 보안 부팅은 OS를 실행하기 전에 로드된 UEFI 드라이버 및 기타 코드의 암호화 서명을 확인하여 멀웨어가 펌웨어를 훼손하지 않았는지 확인합니다. 또한 PowerEdge 서버는 펌웨어 및 OS의 보안을 강화하기 위해 TPM 2.0을 지원합니다.

간소화된 보안

보안 코어 PowerEdge 서버를 사용하면 Dell Technologies에서 보안 코어의 약속을 충족하는 하드웨어, 펌웨어, 드라이버 세트가 제공됩니다. Microsoft는 Dell Technologies와 긴밀하게 협력하여 PowerEdge 서버의 보안 지원을 간소화합니다.

관리자는 Windows Admin Center의 새로운 기능을 사용하여 Windows Server 2022 보안 코어 서버의 OS 보안 기능을 쉽게 구성할 수 있습니다. 관리자는 새로운 Windows Admin Center 보안 기능을 사용하면 한 번의 버튼 클릭으로 고급 보안을 활성화할 수 있습니다. Windows Admin Center는 Windows Server 2022 보안 코어 서버에 필요한 모든 보안 기능의 상태를 보여 주며, 관리자는 한곳에서 필요한 기능을 사용 설정할 수 있습니다.

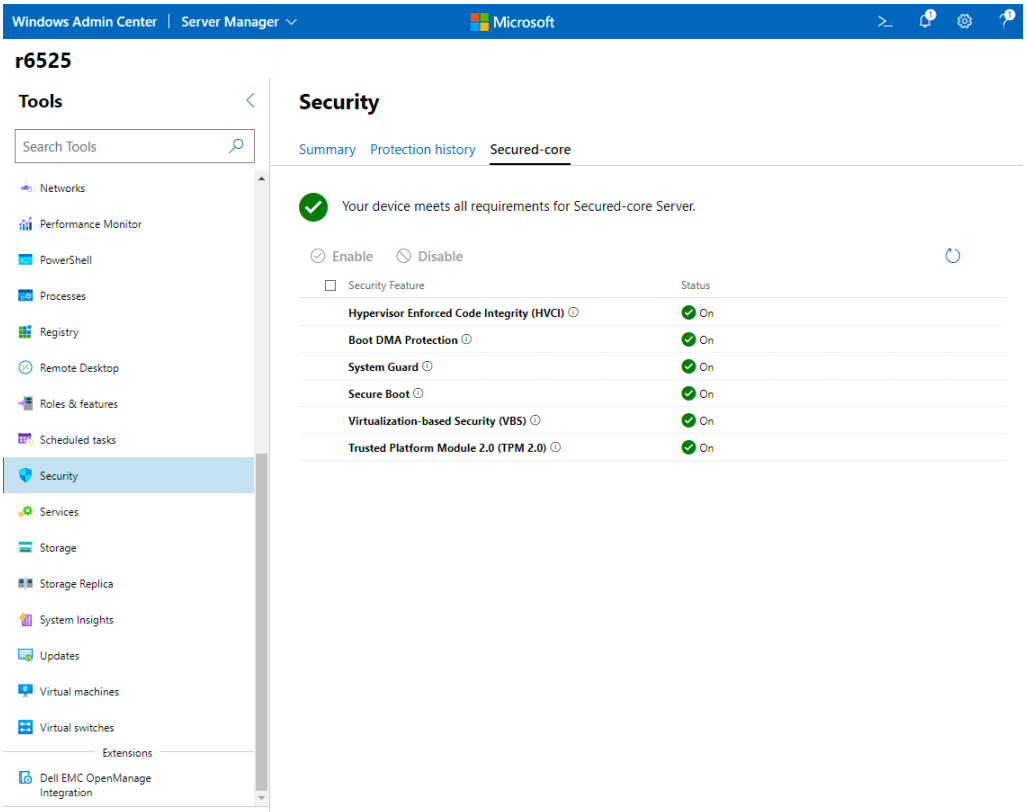


그림 1 Windows Admin Center의 보안 코어 확인 화면(영문)

Windows Admin Center와 Dell EMC™ OpenManage™의 통합은 보안 코어 서버의 관리를 더욱 간소화하는 Windows Admin Center의 확장 기능입니다. 이 Windows Admin Center 확장 기능으로 PowerEdge 서버를 원격으로 관리하여 IT 관리자의 보안 작업 등 다양한 작업을 간소화할 수 있습니다. Windows Server 2022 보안 코어 서버의 맥락에서 OpenManage Integration with Windows Admin Center 확장 기능을 사용하면 Windows Admin Center 내에서 PowerEdge 서버의 인벤토리를 볼 수 있으며 PowerEdge 서버 구성 요소의 상태, 하드웨어 및 펌웨어 인벤토리 정보를 한눈에 볼 수 있습니다.

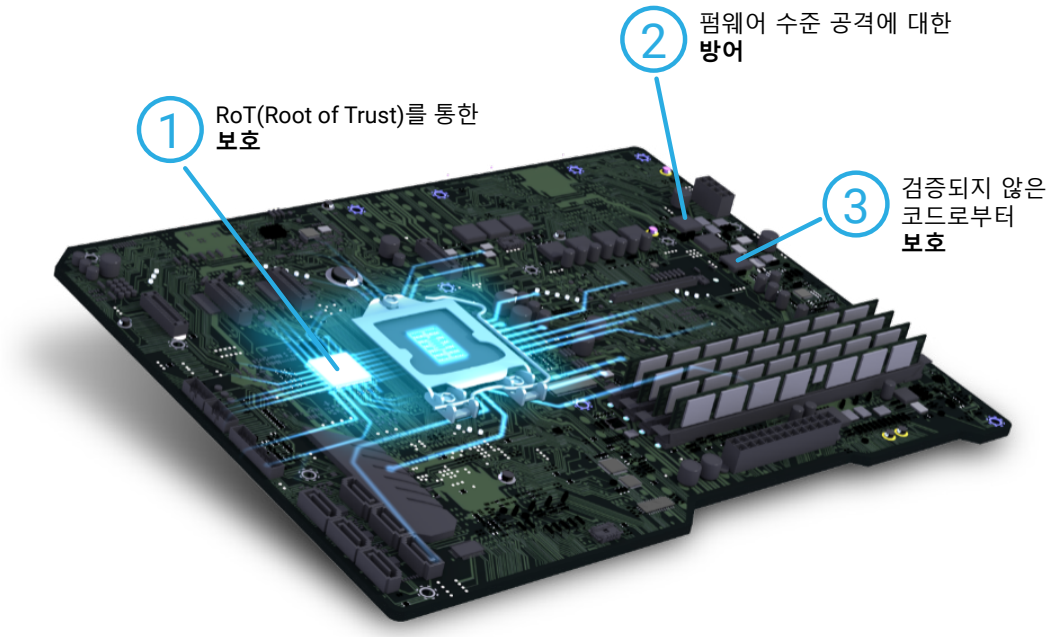
Windows Server 2022 보안 코어 서버에 대한 PowerEdge 서버 지원

보안 코어 서버 방어는 다중 계층적 특성이 있어 하드웨어 OEM의 지원이 매우 중요합니다. PowerEdge 서버는 하드웨어 및 펌웨어가 Windows Server 2022 보안 기능의 요구 사항을 충족하도록 Dell Technologies의 테스트와 인증을 거칩니다. 또한 PowerEdge 서버의 하드웨어 및 펌웨어는 Windows Server 2022 보안 코어 서버를 사용하도록 구성되어 있습니다. 표 1은 PowerEdge 서버의 하드웨어가 Windows Server 2022 기능을 어떻게 지원하는지 자세히 설명합니다.

표 1. 차세대 Dell EMC™ PowerEdge™ 서버의 Windows Server 2022 보안 기능 및 주요 지원 기능 매핑

	Windows Server 2022	차세대 Dell EMC™ PowerEdge™ 서버
고급 보호	보안 코어 시스템은 펌웨어를 하드웨어 기반 샌드박스에 적용하여 펌웨어 기반 취약성의 영향을 제한합니다. VBS는 고급 멀웨어로부터 OS의 중요한 부분을 격리합니다.	Dell Technologies는 PowerEdge 서버의 공급망을 보호하여 공장에서 고객 사이트로 운송하는 동안 아무도 서버를 조작하거나 펌웨어를 훼손하지 못하도록 합니다.
예방적 방어	HVCI 및 Windows Defender Credential Guard와 같은 VBS 기능은 전체 취약성 등급을 방지하고 자격 증명과 같은 중요한 자산을 더욱 효과적으로 보호합니다. TPM 2.0은 보안 기반으로 사용되는 하드웨어 RoT(Root of Trust)를 제공합니다.	PowerEdge 서버는 업계 표준 UEFI 보안 부팅을 지원하여 OS를 실행하기 전에 로드되는 UEFI 드라이버 및 기타 코드의 암호화 서명을 확인합니다. PowerEdge 서버는 TPM 2.0을 지원합니다.
간소화된 보안	Windows Admin Center를 통해 보안 코어 서버를 쉽게 구성할 수 있습니다.	Microsoft는 Dell Technologies와 협력하여 PowerEdge 서버에 대한 보안 지원을 간소화합니다. Windows Admin Center를 Dell EMC™ OpenManage™와 통합하면 보안 코어 서버의 관리가 더욱 간소화됩니다.

고급 다중 계층 보안의 구조



1 RoT(Root of Trust)를 통한 보호

Dell Technologies와 같은 대표적인 OEM과 인텔 및 AMD와 같은 칩 공급업체와의 제휴를 통해 보안 코어 서버는 오늘날의 최신 CPU에 내장된 보안 기능과 함께 업계 표준 하드웨어 RoT(Root of Trust)를 사용합니다.

보안 코어 서버는 TPM 2.0과 DRTM이 포함된 최신 CPU를 사용하여 서버를 더 안전하게 부팅하고 펌웨어 취약성을 최소화합니다.

2 펌웨어 수준 공격에 대한 방어

보안 코어 서버는 최신 CPU에 하드웨어 기반 보안을 사용하여 시스템을 신뢰할 수 있는 상태로 실행하여 고급 멀웨어가 시스템을 변조하고 펌웨어 수준에서 공격하는 것을 방지합니다.

System Guard Secure Launch는 CPU를 사용하여 디바이스가 더욱 안전하게 부팅되는지 검증하므로 고급 펌웨어 공격을 방지할 수 있습니다.

3 검증되지 않은 코드로부터 보호

신뢰할 수 있는 컴퓨팅 기반 내에서 실행되는 코드는 무결성을 갖춘 상태에서 실행되며 악용이나 공격의 대상이 아닙니다.

HVCI를 사용할 경우 보안 코어 서버는 알려진 승인 기관에서 서명한 실행 파일만 시작합니다. 하이퍼바이저는 멀웨어가 메모리 수정 및 이를 실행하려는 시도를 방지하는 권한을 설정하고 적용합니다.

Windows Server 2022의 보안 연결을 위한 차세대 PowerEdge 서버 지원

차세대 PowerEdge 서버는 보안에 민감한 워크로드에 대해 SMB(Server Message Block) AES-256 암호화를 지원합니다. 이러한 지원을 통해 Windows Server 2022를 실행하는 PowerEdge 서버가 추가적인 보안을 위해 워크로드 데이터에 대한 포괄적인 암호화를 제공할 수 있습니다. Windows Server 2022에서 SMB에 사용되는 256비트 AES 암호화 역시 강력한 비밀번호를 사용할 경우 양자 컴퓨터의 무차별 대입 공격에도 충분히 견딜 수 있을 만큼 강력합니다.

PowerEdge 서버 및 Windows Server 2022는 East-West SMB 데이터 트래픽을 위한 AES-256 암호화를 통해 개별 서버에서 클러스터의 내부 통신까지 포괄적인 SMB 암호화를 추가로 확장합니다. 이러한 추가적인 SMB 암호화 제어는 워크로드를 더욱 강화하고 공격 경로를 차단합니다.

마지막으로, Windows Server 2022는 3세대 인텔® 제온® 스케일러블 프로세서에 포함된 인텔® AES-NI(인텔® Advanced Encryption Standard New Instructions)와 AMD EPYC™ Zen 3 프로세서에 포함된 vAES256(vectorized AES encryption for 256-bit)을 사용합니다. 이러한 고급 프로세서의 명령 세트는 PowerEdge 서버의 AES-256 암호화 성능을 향상합니다. Dell Technologies와 Microsoft는 이러한 고급 보안 기술을 활용하여 비즈니스에 중요한 워크로드에 대해 강력한 보안과 반응성 중 하나만 선택할 필요가 없도록 지원합니다.

Dell Technologies 공급망 무결성을 통한 추가 보안

Dell Technologies의 공급망 무결성은 제조 및 배송 과정에서 하드웨어 및 펌웨어 구성 요소가 손상되지 않도록 보호합니다. 하드웨어 무결성과 관련하여, Dell Technologies는 고객에게 제품을 배송하기 전에 제품 변조 방지, 위조된 구성 요소의 유입 차단을 위해 노력하고 있습니다. 공급업체 선택, 조달, 생산 프로세스, 감사 및 테스트를 통한 거버넌스에 모두 Dell Technologies의 품질 관리가 적용됩니다. 생산 중 자재 검수를 통해 표시가 잘못되었거나 정상 성능 매개변수를 이탈했거나 잘못된 전자 식별자가 포함된 구성 요소를 식별합니다.

소프트웨어 무결성을 위해 코딩 취약성을 방지하는 것 외에도, Dell Technologies는 고객에게 제품을 배송하기 전에 펌웨어나 디바이스 드라이버에 멀웨어가 삽입되지 않도록 합니다. Dell Technologies는 전 세계 모든 제조 사이트에서 ISO 9001 인증을 유지하고 있습니다. 이러한 프로세스 및 관리 조치를 엄격하게 준수함으로써 위조된 구성 요소가 Dell Technologies™ 제품에 유입되거나 멀웨어가 펌웨어 또는 디바이스 드라이버에 삽입될 위험이 최소화됩니다. 또한 Dell Technologies는 이러한 조치를 SDLC(Software Development Lifecycle) 프로세스의 일부로 구현합니다.

또한 Dell Technologies는 제조 시설 및 운송망의 물리적 보안을 보장하기 위해 노력하고 있습니다. Dell Technologies에서는 주요 구역에 모니터링되는 폐쇄 회로 카메라를 사용하고, 액세스 제어를 적용하며, 24시간 출입구 경비를 수행하는 것을 비롯하여 Dell Technologies 제품을 제작하는 특정 공장들에 지정된 TAPA(Transported Asset Protection Association) 시설 보안 요건을 준수하도록 요구하고 있습니다. 또한 Dell Technologies에서는 업계를 선도하는 물류 프로그램의 일환으로 운송 중 도난 및 변조를 방지하기 위해 제품 보호 조치를 시행하고 있습니다. 마지막으로, Dell Technologies의 PowerEdge 서버용 SCV(Secured Component Verification)를 통해 Dell Technologies 고객은 고객이 받은 PowerEdge 서버가 공장에서 제조된 것과 일치하는지 확인할 수 있습니다.

Windows Server 2022 및 차세대 Dell EMC PowerEdge 서버의 강화된 보안 기반을 통해 중요한 워크로드 보호

워크로드의 보안은 워크로드가 실행되는 기반의 보안에 달려 있습니다. 악의적인 공격자들이 기존 소프트웨어 기반 보안에 영향을 받지 않는 공격 경로를 계속 모색하는 상황에서 멀웨어와 데이터 침해로 인한 위협은 앞으로도 계속 증가할 것입니다. 펌웨어 공격은 부팅 프로세스 중 소프트웨어 기반 보안이 시스템 보호를 시작하기 전 단계에 있는 서버를 목표로 이루어집니다. 최신 서버 보호를 위해서는 하드웨어, 펌웨어, OS를 아우르는 다각적인 보안이 필요합니다.

지금이야말로 Windows Server 2022로 업그레이드할 적기입니다. Windows Server 2022의 보안 코어 서버 기능은 조직이 펌웨어와 OS 모두에 대한 위협에 대응하는 데 도움이 됩니다. Dell Technologies의 하드웨어 및 소프트웨어 무결성 보호와 함께 Windows Server 2022를 실행하는 차세대 Dell EMC PowerEdge 서버는 하드웨어, 펌웨어, OS에 대한 전체 스택에 최신 보안을 제공할 수 있습니다. 또한 차세대 PowerEdge 서버에서 지원되기도 하는 Windows Server 2022의 보안 연결 기능은 개별 서버를 넘어 데이터 센터 내의 전체 클러스터로 보안을 확장합니다. 또한 Windows Server 2012에 대한 지원은 2023년 10월에 종료되므로 이제 업그레이드 계획을 수립해야 합니다.[6]

Windows Server 2022 및 차세대 Dell EMC PowerEdge 서버를 통해 중요한 워크로드 및 데이터를 보호하는 방법에 대해 자세히 알아보려면 www.delltechnologies.com/en-us/solutions/microsoft-oem/을 참조하십시오.

[1] Cybersecurity Ventures. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." 2020년 11월. 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." 2021년 8월.
[3] IBM. "How much does a data breach cost?" 2021년. www.ibm.com/security/data-breach.
[4] Dan Goodin. "Hospitals hamstrung by ransomware are turning away patients." *Ars Technica*. 2021년 8월. 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." 2021년 3월. 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] 문서 작성 시 기준. Windows Server 2012 지원 종료에 대한 최신 정보는 Windows Server 2012 수명주기 페이지를 참조하십시오. https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Windows Server 2022로 현대화
하이브리드 기능으로 온프레미스 투자 수익을 향상하는 클라우드 지원 운영 체제