DELL Technologies

Microsoft

White paper

Obtenha proteção avançada de segurança com os recursos combinados do Windows Server 2022 e dos servidores Dell EMC™ PowerEdge de™ última geração

Fortaleça as cargas de trabalho essenciais aos negócios com um ambiente mais seguro de hardware, firmware e sistema operacional

Estima-se que o crime cibernético global custará um total de US$ 6 trilhões em 2021 e crescerá para US$ 10,5 trilhões em 2025, de acordo com a Cybersecurity Ventures.[1] Os ataques de ransomware aumentaram 61 vezes em seis anos para US$ 20 bilhões em 2021 e, atualmente, ocorre um ataque a cada 11 segundos.[1] Uma pesquisa da IDC de 2021 descobriu que mais de um terço das organizações entrevistas no mundo todo sofreu um ataque ou uma violação de ransomware nos últimos 12 meses (e, muitas vezes, mais de um ataque).[2] E, embora a IBM estime que o custo de uma só violação de dados agora seja de US$ 4,24 milhões[3], o custo real das violações pode ser muito maior: em alguns casos, hospitais nos Estados Unidos tiveram que redirecionar pacientes de emergência para outros hospitais e recusar ambulâncias devido a ataques de ransomware.[4]

Os ataques de firmware podem ser uma ameaça particularmente prejudicial para as organizações. Isso ocorre porque um ataque vetorizado no firmware pode implementar um malware antes que o sistema operacional (SO) — e, portanto, a segurança baseada em software em execução nesse sistema operacional — tenha começado. No entanto, menos da metade das organizações adotaram medidas para fortalecer seus sistemas contra ataques de firmware, mesmo que esses ataques tenham aumentado cinco vezes mais nos últimos cinco anos.[5] No fim das contas, as cargas de trabalho são tão seguras quanto todas as pilhas nas quais são executadas.

Para atender a esse crescimento exponencial à frequência, variedade e custo elevado das ameaças de malware, a segurança moderna deve ser multicamada. Isso ocorre porque o malware pode comprometer os sistemas nos níveis de hardware e firmware ou durante a inicialização, áreas em que apenas a segurança definida por software é impotente. Para combater essa vulnerabilidade, a segurança do servidor moderno não é uma estratégia única. Ela deve ser integrada a toda a pilha de infraestrutura. A combinação de servidores Dell EMC™ PowerEdge™ de última geração com o Windows Server 2022 simplifica para os administradores a importante tarefa de alinhar hardware, firmware e SO para proteger adequadamente as cargas de trabalho essenciais aos negócios.

Os benefícios combinados do servidor de núcleo seguro do Windows Server 2022 e dos servidores PowerEdge de última geração

O servidor de núcleo seguro é um novo recurso do Windows Server 2022 que usa recursos de hardware, firmware e SO para oferecer proteção contra ameaças atuais e futuras. A combinação do software de servidor de núcleo seguro do Windows Server 2022 em execução no hardware de servidor PowerEdge de última geração oferece três benefícios substanciais para organizações como a sua:

- Proteção avançada
- Defesa preventiva
- Segurança simplificada

Proteção avançada

Com base nos dados de inteligência contra ameaças da Microsoft, os PCs de núcleo seguro oferecem mais do que o dobro da proteção contra infecções do que PCs regulares; a Microsoft agora está trazendo essa mesma tecnologia para o espaço de servidor com os servidores de núcleo seguro do Windows Server 2022.[5] As proteções habilitadas por um servidor de núcleo seguro visam criar uma plataforma segura para cargas de trabalho e dados essenciais nesse servidor. Especificamente, os servidores de núcleo seguro usam suporte a processador da tecnologia Dynamic Root of Trust for Measurement (DRTM) para colocar o firmware em uma área restrita baseada em hardware. Esse isolamento ajuda a limitar o impacto das vulnerabilidades em milhões de linhas de código de firmware altamente privilegiado.

Complementando o isolamento de firmware no Windows Server 2022, a segurança baseada em virtualização (VBS) isola partes essenciais do sistema operacional, como o kernel, do restante do sistema. Isso ajuda a garantir que os servidores permaneçam dedicados à execução de cargas de trabalho críticas e ajude a proteger os aplicativos e dados relacionados contra ataques e exfiltração.

Para fortalecer ainda mais o firmware nos servidores PowerEdge contra ataques, a Dell Technologies ajuda a proteger a cadeia de suprimentos dos servidores PowerEdge para ajudar a garantir que ninguém tenha adulterado o servidor durante o transporte da fábrica para o local do cliente (explicado em mais detalhes em Segurança adicional por meio da integridade da cadeia de suprimentos da Dell Technologies abaixo).

Defesa preventiva

A funcionalidade de núcleo seguro ajuda a defender proativamente e a interromper muitos dos caminhos que os invasores podem usar para explorar seus sistemas. A integridade de código protegida por hypervisor (HVCI) no VBS isola a função de tomada de decisões de integridade do código (CI) do restante do sistema operacional Windows, o que ajuda a garantir que a única maneira de a memória kernel se tornar executável seja por meio de uma verificação de CI. O VBS também permite o uso do Windows Defender Credential Guard, no qual segredos e credenciais do usuário são armazenados em um contêiner virtual que o SO não pode acessar diretamente.

O Trusted Platform Module 2.0 (TPM 2.0) vem por padrão com servidores de núcleo seguro e fornece um armazenamento protegido para chaves e dados confidenciais, como medições dos componentes carregados durante a inicialização. A capacidade de verificar se o firmware executado durante a inicialização foi assinado validamente pelo autor esperado e não foi adulterado ajuda a melhorar a segurança. Essa raiz de confiança de hardware também eleva a proteção fornecida por recursos como a criptografia de unidade do BitLocker, que usa o TPM 2.0 e facilita a criação de fluxos de trabalho baseados em atestado que podem ser incorporados em estratégias de segurança Zero Trust. Juntas, essas defesas permitem que suas equipes de TI e SecOps usem melhor o tempo nas várias áreas de segurança que precisam de atenção.

Os servidores PowerEdge de última geração são compatíveis com a Unified Extensible Firmware Interface (UEFI) Secure Boot padrão do setor. A UEFI Secure Boot verifica as assinaturas criptográficas dos drivers da UEFI e outros códigos carregados antes da execução do SO para ajudar a garantir que o malware não tenha adulterado o firmware. Além disso, os servidores PowerEdge são compatíveis com o TPM 2.0 para aumentar a segurança do firmware e do SO.

Segurança simplificada

Quando você adquire um servidor PowerEdge de núcleo seguro, você tem a garantia de que a Dell Technologies forneceu um conjunto de hardware, firmware e drivers que cumprem a promessa de núcleo seguro. A Microsoft colabora estreitamente com a Dell Technologies para simplificar a ativação da segurança nos servidores PowerEdge.

A nova funcionalidade do Windows Admin Center facilita aos administradores a configuração dos recursos de segurança do SO nos servidores de núcleo seguro do Windows Server 2022. A nova funcionalidade de segurança do Windows Admin Center permite que os administradores habilitem a segurança avançada com o clique de um botão. O Windows Admin Center apresenta o status de todos os recursos de segurança necessários para os servidores de núcleo seguro do Windows Server 2022 e permite que os administradores ativem os recursos conforme necessário, de um único local.

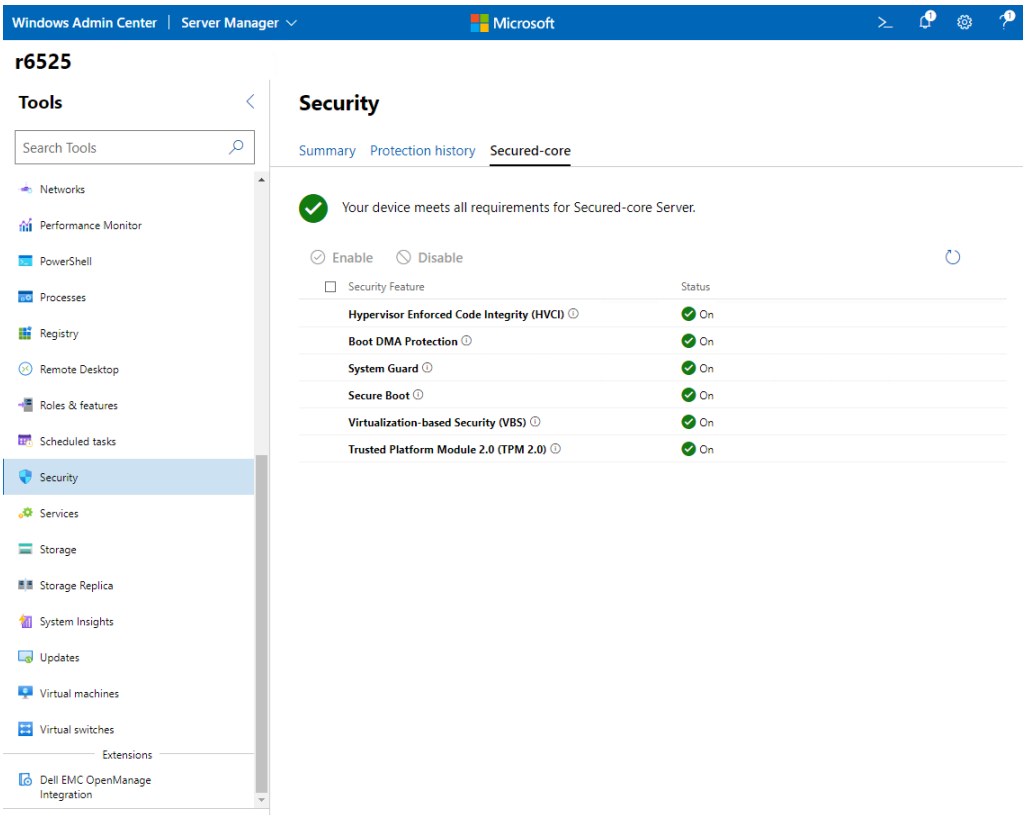


Figura 1. Tela de confirmação do núcleo seguro no Windows Admin Center

A integração do Dell EMC™ OpenManage™ com o Windows Admin Center é uma extensão do Windows Admin Center que simplifica ainda mais o gerenciamento de servidores de núcleo seguro. Essa extensão do Windows Admin Center simplifica as tarefas de segurança (entre outros) dos administradores de TI gerenciando remotamente os servidores PowerEdge. No contexto dos servidores de núcleo seguro do Windows Server 2022, a integração do OpenManage com a extensão do Windows Admin Center permite que você visualize seu inventário de servidores PowerEdge no Windows Admin Center e fornece uma visão unificada das informações de inventário de integridade, hardware e firmware dos componentes do servidor PowerEdge.

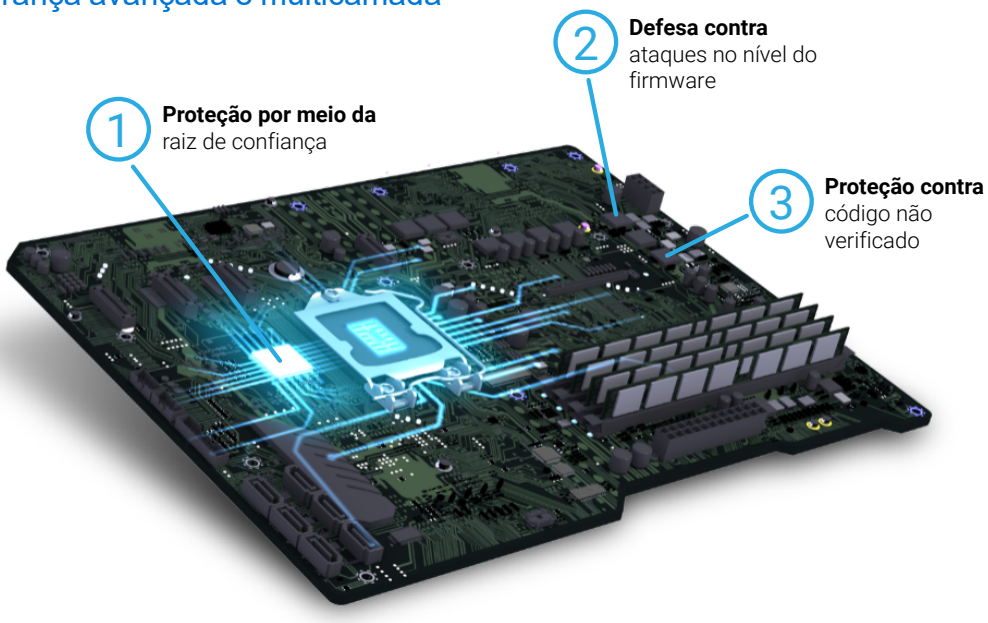
Suporte do servidor PowerEdge para servidores de núcleo seguro com Windows Server 2022

Devido à natureza de várias camadas das defesas de servidor de núcleo seguro, o suporte de OEM de hardware é fundamental. Os servidores PowerEdge são testados e certificados pela Dell Technologies para garantir que o hardware e o firmware atendam aos requisitos dos recursos de segurança do Windows Server 2022. Além disso, o hardware e o firmware nos servidores PowerEdge estão configurados para habilitar o servidor de núcleo seguro do Windows Server 2022. A Tabela 1 detalha como o hardware nos servidores PowerEdge fortalece os recursos do Windows Server 2022.

Tabela 1. Mapeamento de recursos de segurança do Windows Server 2022 e principais recursos de suporte dos servidores Dell EMC™ PowerEdge™ de última geração

	Windows Server 2022	Servidores Dell EMC™ PowerEdge™ de última geração
Proteção avançada	Os sistemas de núcleo seguro colocam o firmware em uma área restrita baseada em hardware ajudando a limitar o impacto das vulnerabilidades baseadas em firmware. A VBS isola partes essenciais do sistema operacional contra malware avançado.	A Dell Technologies ajuda a proteger a cadeia de suprimentos dos servidores PowerEdge para ajudar a garantir que ninguém tenha adulterado o servidor ou comprometido o firmware durante o transporte da fábrica para o local do cliente.
Defesa preventiva	Recursos de VBS, como HVCI e Windows Defender Credential Guard, impedem classes inteiras de vulnerabilidades e protegem melhor os ativos confidenciais, como credenciais. O TPM 2.0 fornece raiz de confiança de hardware usada como uma base segura.	Os servidores PowerEdge oferecem suporte a UEFI Secure Boot padrão do setor que verifica as assinaturas criptográficas dos drivers UEFI e outros códigos carregados antes da execução do SO. Os servidores PowerEdge são compatíveis com o TPM 2.0.
Segurança simplificada	O Windows Admin Center oferece acesso fácil para configurar servidores de núcleo seguro.	A Microsoft colabora com a Dell Technologies para simplificar a ativação da segurança nos servidores PowerEdge. A integração do Windows Admin Center com o Dell EMC™ OpenManage™ simplifica ainda mais o gerenciamento de servidores de núcleo seguro.

Anatomia da segurança avançada e multicamada



1 Proteção por meio de Raiz de confiança

Em parceria com os principais OEMs, como a Dell Technologies e fornecedores de silício, como a Intel e a AMD, os servidores de núcleo seguro usam raiz de confiança de hardware padrão do setor, juntamente com recursos de segurança integrados às CPUs modernas de hoje.

Os servidores de núcleo seguro usam o TPM 2.0 e uma CPU moderna com DRTM para inicializar servidores com mais segurança e minimizar as vulnerabilidades de firmware.

2 Defesa contra ataques no nível do firmware

Os servidores de núcleo seguro usam a segurança baseada em hardware da CPU moderna para iniciar o sistema em um estado confiável, impedindo que malware avançado adultere o sistema e ataque no nível do firmware.

O System Guard Secure Launch usa a CPU para validar o dispositivo para inicializar com mais segurança, ajudando a evitar ataques avançados de firmware.

3 Proteção contra código não verificado

O código em execução na base de computação confiável é executado com integridade e não está sujeito a ataques ou explorações.

Habilitado com HVCI, um servidor de núcleo seguro só inicia executáveis assinados por autoridades conhecidas e aprovadas. O hypervisor define e impõe permissões para impedir que o malware tentar modificar a memória e torná-la executável.

Suporte ao servidor PowerEdge de última geração para conectividade segura no Windows Server 2022

Os servidores PowerEdge de última geração são compatíveis com a criptografia AES-256 do Server Message Block (SMB) para cargas de trabalho em que a segurança é essencial. Esse suporte significa que os servidores PowerEdge que executam o Windows Server 2022 podem fornecer criptografia completa aos dados da carga de trabalho para segurança extra. A criptografia AES de 256 bits usada pelo SMB no Windows Server 2022 também é robusta o suficiente para ser resistente até mesmo a ataques de força bruta por computadores quânticos, caso senhas fortes o suficiente sejam usadas.

Os servidores PowerEdge e o Windows Server 2022 estendem ainda mais a criptografia completa do SMB de servidores individuais para as comunicações internas de clusters com criptografia AES-256 para tráfego de dados horizontal do SMB. Esses controles adicionais de criptografia de SMB fortalecem ainda mais as cargas de trabalho e fecham as vias de ataque.

Por fim, o Windows Server 2022 usa a Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) incluídas nos processadores escaláveis Intel® Xeon® de 3ª geração e criptografia vetorizada AES para 256 bits (vAES256) incluída nos processadores AMD EPYC™ Zen 3. Esses conjuntos de instruções dos processadores avançados aumentam o desempenho da criptografia AES-256 nos servidores PowerEdge. Ao usar essas tecnologias avançadas de segurança, a Dell Technologies e a Microsoft ajudam a garantir que você não tenha que escolher entre segurança robusta e capacidade de resposta para cargas de trabalho essenciais aos negócios.

Segurança adicional por meio da integridade da cadeia de suprimentos da Dell Technologies

A integridade da cadeia de suprimentos da Dell Technologies protege os componentes de hardware e firmware contra comprometimento durante a fabricação e o envio. No domínio da integridade do hardware, a Dell Technologies trabalha para garantir que não haja adulteração ou inserção de componentes falsificados antes de enviar produtos aos clientes. Os controles que a Dell Technologies tem em vigor cobrem a seleção de fornecedores, suprimento, processos de produção e governança por meio de auditorias e testes. As fiscalizações de materiais durante a produção ajudam a identificar componentes com defeitos, que se desviam dos parâmetros de desempenho normais ou que contêm um identificador eletrônico incorreto.

No que diz respeito à integridade do software, a Dell Technologies busca garantir que nenhum malware seja inserido no firmware ou nos drivers de dispositivo antes de enviar um produto aos clientes, além de evitar quaisquer vulnerabilidades de codificação. A Dell Technologies mantém a certificação ISO 9001 para todos os locais de produção globais. Seguir esses processos e controles rigorosamente ajuda a minimizar o risco de componentes falsificados serem incorporados aos produtos da Dell Technologies™ e de malware ser inserido em firmware ou drivers de dispositivos. Além disso, a Dell Technologies implementa essas medidas como parte do processo de ciclo de vida de desenvolvimento de software (SDLC).

A Dell Technologies também trabalha para ajudar a garantir a segurança física das instalações de produção e das cadeias de transporte. A Dell Technologies exige que determinadas fábricas em que seus produtos são produzidos atendam a requisitos específicos de segurança de instalações da Transported Asset Protection Association (TAPA), incluindo o uso de câmeras com circuito fechado monitorado nas áreas principais, controles de acesso e entradas e saídas vigiadas a todo momento. A Dell Technologies também colocou em vigor medidas de proteção para proteger os produtos contra roubo e adulteração durante o transporte como parte de um programa de logística líder do setor. Por fim, a verificação de componentes protegidos (SCV) da Dell Technologies para servidores PowerEdge permite que os clientes da Dell Technologies verifiquem se um servidor PowerEdge recebido pelo cliente corresponde ao que foi produzido na fábrica.

Proteja suas cargas de trabalho essenciais com uma base de segurança melhor do Windows Server 2022 e dos servidores Dell EMC PowerEdge de última geração

As cargas de trabalho são tão seguras quanto a base em que são executadas. A ameaça de malware e violações de dados só continuará a crescer no futuro, especialmente à medida que os agentes mal-intencionados continuarem a explorar as vias de ataque imunes à segurança tradicional baseada em software. Os ataques de firmware visam especificamente os servidores durante o processo de inicialização, antes mesmo que a segurança baseada em software tenha começado a proteger os sistemas. A proteção do servidor moderno requer segurança múltipla que abranja hardware, firmware e sistema operacional.

O upgrade para o Windows Server 2022 pode fazer mais sentido agora do que nunca. O recurso de servidor de núcleo seguro do Windows Server 2022 ajuda as organizações a combater ameaças ao firmware e ao sistema operacional. Quando combinados com as proteções de integridade de hardware e software da Dell Technologies, os servidores Dell EMC PowerEdge de última geração que executam o Windows Server 2022 podem fornecer segurança moderna para toda a pilha de hardware, firmware e sistema operacional. E os recursos de conectividade segura do Windows Server 2022 e compatíveis com os servidores PowerEdge de última geração estendem essa segurança além dos servidores individuais para clusters inteiros em seu data center. Além disso, o suporte ao Windows Server 2012 termina em outubro de 2023, o que significa que é hora de começar a fazer planos de upgrade.[6]

Para saber mais sobre como o Windows Server 2022 e os servidores Dell EMC PowerEdge de última geração podem ajudar a proteger suas cargas de trabalho e dados essenciais, visite www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Novembro de 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." Agosto de 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.* Agosto de 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." Março de 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] A partir da escrita deste artigo. Para obter as informações mais recentes sobre o fim do suporte para o Windows Server 2012, visite a página do ciclo de vida do Windows Server 2012: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Modernize com o Windows Server 2022.
O sistema operacional pronto para a nuvem que impulsiona os investimentos locais com recursos híbridos.