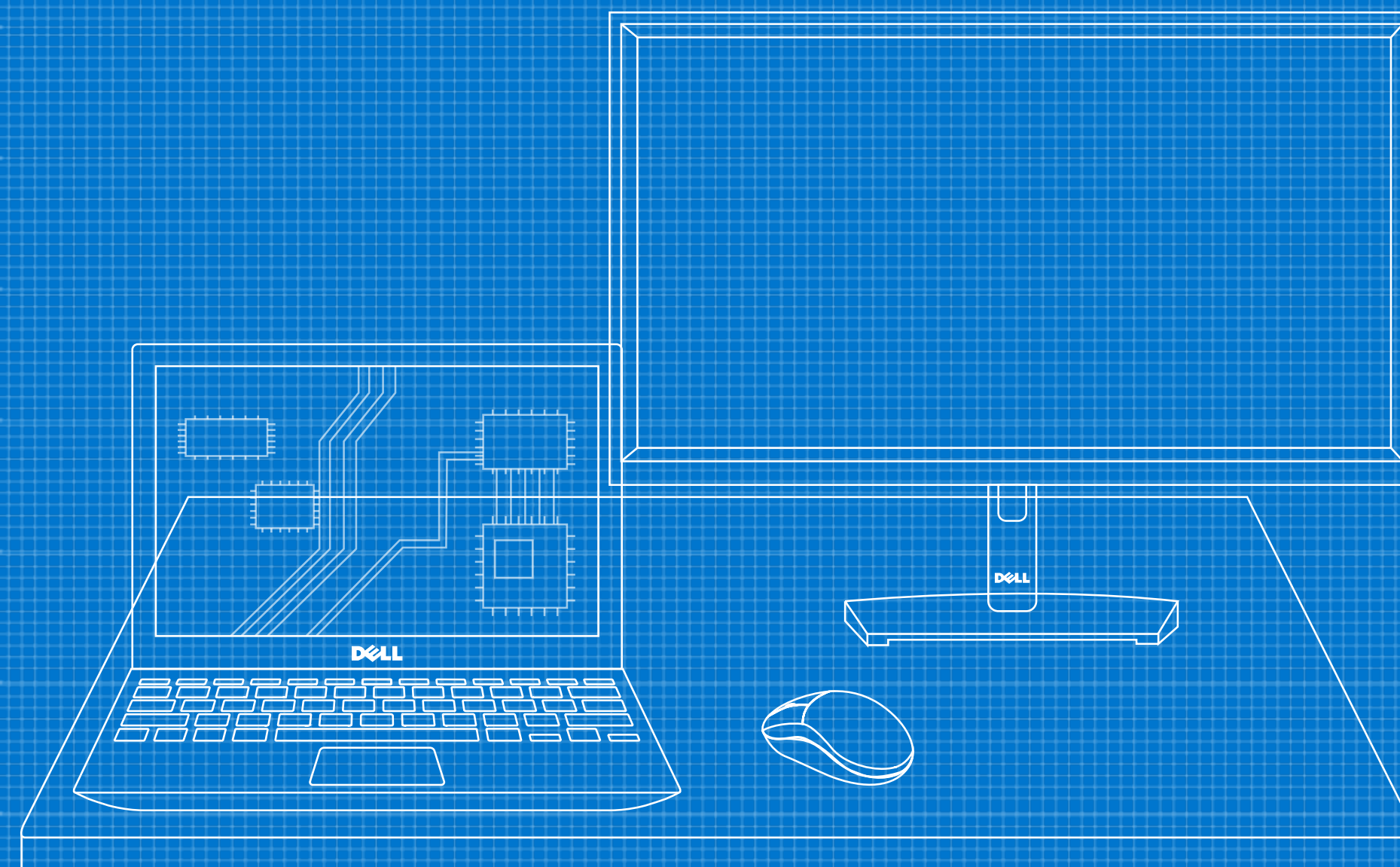


A anatomia de um espaço de trabalho confiável

Melhore a segurança de seu parque com várias camadas de defesa



Sumário Executivo

Os ataques cibernéticos são inevitáveis, e seu volume e sofisticação vêm crescendo. Os dispositivos de endpoint, redes e ambientes de nuvem se tornaram alvos-chave.

Este eBook oferece a quem toma decisão nos setores de TI e segurança orientação sobre os elementos necessários para tornar o endpoint mais eficiente nesse cenário de ameaças em evolução.



Índice

- 1 [0 ambiente de ameaças](#)
- 2 [Desafios](#)
- 3 [Proteger o espaço de trabalho moderno](#)
- 4 [A anatomia de um espaço de trabalho confiável](#)
- 5 [Abordagem da Dell](#)
- 6 [Combinando todos os recursos](#)
- 7 [Lições a serem aprendidas e Call-to-action](#)



O ambiente de ameaças

A mudança para o trabalho híbrido trouxe novas complexidades e vetores de ataque – e **endpoints, redes e nuvens estão expandindo as superfícies de ataque.**

Além disso, os criminosos agora empregam técnicas sofisticadas que visam a diferentes camadas da pilha de computação, misturando-se com processos válidos nos sistemas. Alguns métodos permitem até que os criminosos tenham acesso privilegiado e desabilitem proteções de software *sem serem detectados.*

Várias organizações embarcaram em uma jornada em direção ao Zero Trust para combater essas ameaças. No entanto, para ativar princípios de Zero Trust, você deve conseguir manter a confiança no dispositivo.

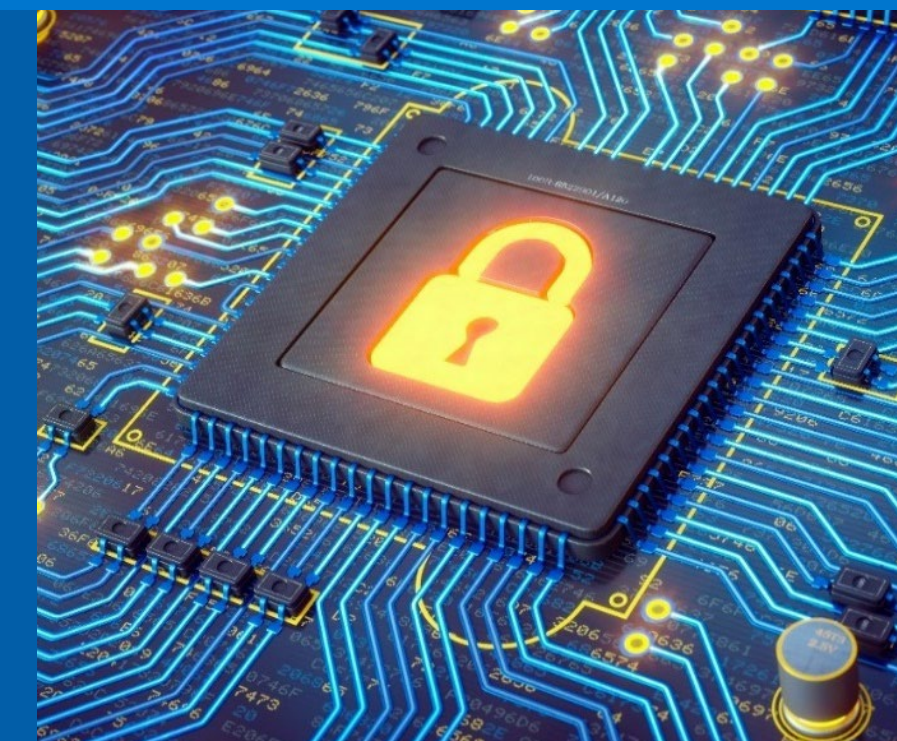
Como manter a confiança no dispositivo à medida que os ataques se tornam mais frequentes e tecnologias avançadas criam novos vetores de ataque?

¹[CrowdStrike Global Threat Report, 2023.](#)

²[Dell Innovation Index, 2023.](#)

Você sabia que:

71% dos ataques em 2022 não foram baseados em malware, um aumento de 9% em comparação com o ano anterior¹



Somente 41% das organizações pesquisadas podem afirmar, com total confiança, que a segurança está incorporada em sua tecnologia e seus aplicativos²

Explorar o Zero Trust para promover a maturidade da segurança virtual? Confira nosso eBook: [Endpoint security is an essential element of your Zero Trust journey.](#)

Desafios

Para segurança efetiva de endpoint, é importante entender seu adversário e como ele trabalha.

Devido a potencial recompensa decorrente de uma violação, **os criminosos muitas vezes fazem várias tentativas de violar a mesma organização, empregando diferentes métodos e pontos de entrada para aumentar suas chances.** Por exemplo, ao longo do ciclo de vida de um único dispositivo, os criminosos podem tentar tirar vantagem das vulnerabilidades por meio de dezenas de vetores.

As defesas preexistentes não estão fazendo o suficiente para manter os endpoints seguros. À medida que as organizações fortalecem uma superfície de ataque, os agentes da ameaça simplesmente passam para alvos mais fáceis. Com o mundo se tornando cada vez mais híbrido, os agentes de ameaças identificaram novos vetores de ataque a endpoints que levaram a consequências devastadoras.

Veja à direita exemplos de ataques

Ataque à cadeia de suprimentos: visa fornecedores para ganhar acesso aos sistemas, dados e/ou redes e, por extensão, aos clientes. **EXEMPLO:** Um ataque à cadeia de suprimentos de hardware, iniciado por falsificação de componentes:

Os criminosos interceptam um carregamento de PCs e trocam discos rígidos.



A TI implementa os dispositivos comprometidos em toda a empresa.



O criminoso instala o malware para extrair credenciais assim que os usuários fazem login.



Ataque de engenharia social: Engana os usuários finais para que forneçam informações confidenciais que podem ser usadas para obter acesso a dispositivos e à rede. **EXEMPLO:** Um ataque de spoofing iniciado por um e-mail de phishing:

O usuário final se deixa enganar pelo e-mail de phishing e entrega as credenciais em uma página da web falsa.



O criminoso usa as credenciais válidas para acessar remotamente a rede.



O criminoso extrai os dados em um serviço da web, criptografa dados roubados e os retém em troca de resgate.



Proteger o espaço de trabalho moderno

Quando se trata de proteção de endpoint, você precisa de prevenção, detecção e resposta, além de recuperação e remediação em vários estados ao longo de todo o ciclo de vida de um dispositivo – desde a aquisição e fabricação de PCs até o envio e implantação, durante o uso e até a desativação. Imagine o tamanho dessa superfície de ataque combinada!

Os planos estratégicos de segurança cibernética mais eficazes para a pior situação. Isso pressupõe que uma violação é possível e incorpora diversas camadas de proteção para interromper o ataque o mais rápido e com a maior frequência possível. Também inclui recursos de remediação para minimizar o risco de uma ocorrência repetida.

³Dell Innovation Index, 2023.

PREVENÇÃO

Torne-se um alvo menor com defesas projetadas para bloquear ataques.

DETECÇÃO E RESPOSTA

Sempre assuma que pode haver uma violação e fique vigilante.

RECUPERAÇÃO E REMEDIAÇÃO

Mitigue o impacto de um ataque e volte ao normal.

Você sabia que:

Apenas 33%

das organizações empregam uma estratégia de segurança abrangente e completa que integra proteções baseadas em hardware e software.³



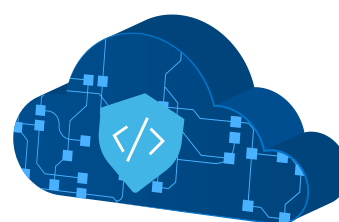
A anatomia de um espaço de trabalho confiável

Descompactando as múltiplas camadas de segurança

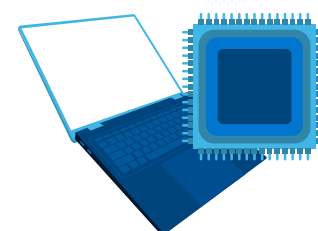
(Exemplos representativos de medidas de segurança listadas)

A segurança moderna de endpoint requer três itens:

1 Segurança de software: Hoje mais do que nunca, encontramos usuários, dispositivos e dados fora das redes corporativas. A segurança do software não apenas protege os dispositivos, mas também estende a proteção aos ambientes de rede e nuvem, onde muitas vezes se originam atividades maliciosas.



2 Segurança de hardware: Os dispositivos devem incluir recursos de segurança integrados. Isso está relacionado à segurança de hardware e firmware que protege o dispositivo em uso. Para defender o espaço de trabalho, você deve ter funcionalidades integradas que proporcionem visibilidade e controle sobre o dispositivo.



3 Segurança da cadeia de suprimentos: Os dispositivos devem ser construídos de modo seguro. Isso significa trabalhar com fornecedores que a) entendam a situação de ameaças e b) possam colocar esse conhecimento em uso à medida que o cenário evolui. O design, o desenvolvimento e os testes seguros de PC minimizam o risco de vulnerabilidades do produto, enquanto os controles da cadeia de suprimentos atenuam o risco de adulteração do produto.



Segurança de software

- Antivírus de última geração (NGAV)
- Detecção e resposta de endpoints (EDR)
- Detecção e resposta estendidas (XDR)
- Proteção de dados em nuvem
- Proteção de rede
- Autocorreção automatizada

Segurança de hardware e firmware

- Verificação do tempo de inicialização
- Verificação do tempo de execução
- Autenticação do usuário
- Notificações e alertas de segurança/telemetria

Segurança da cadeia de suprimentos

- Práticas seguras de desenvolvimento
- Práticas seguras na cadeia de suprimentos
- Verificação de componentes
- Embalagem que evidencia a violação

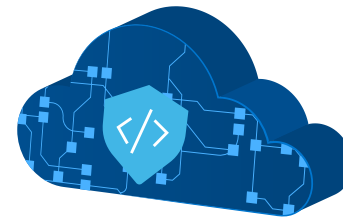
Nossa abordagem: Dell Trusted Workspace

A Dell é um parceiro de segurança e TI para organizações em todo o mundo. Ao contrário das soluções pontuais, a Dell concentra-se nos resultados gerais de segurança, criando um conjunto de soluções que interrompem as abordagens de kill chain e aumentam a resiliência a ataques cibernéticos.

O Dell Trusted Workspace inclui:

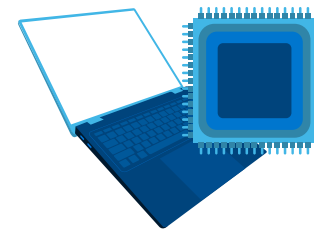
- **Proteções exclusivas de hardware e firmware** que tornam os PCs comerciais da Dell os mais seguros do setor.⁴ (*Segurança projetada e integrada*)
- Uma rede de parceiros de **software líderes do setor** oferece proteção avançada contra ameaças, tanto para o dispositivo quanto para a rede e a nuvem. (*Segurança construída*)

⁴ Com base em uma análise interna da Dell, de setembro de 2023. Aplicável a PCs com processadores Intel. Nem todos os recursos estão disponíveis para todos os PCs. Compra adicional necessária para alguns recursos.



Software de Segurança baseado na rede de parceiros

- **Dell SafeGuard and Respond:** CrowdStrike, VMware Carbon Black e Secureworks fornecem detecção, resposta e correção de ameaças.
- **Dell SafeData:** Netskope oferece visibilidade, monitoramento e prevenção contra perda de dados para aplicativos baseados em nuvem. Absolute permite a autocorreção de aplicativos e redes.



Segurança de hardware e firmware integrada pelos PCs comerciais mais seguros do setor⁴

Exemplo de recursos que protegem o dispositivo em uso:

- BIOS Verification fora do host **Dell SafeBIOS*** e Indicadores de Ataque* ajudam a capturar atividades mal-intencionadas antes que comprometam o PC.
- **Dell SafeID:** protege as credenciais do usuário em um chip dedicado.*
- **Verificação de firmware fora do host** protege a integridade de firmware altamente privilegiado.*
- Com o **software Dell Trusted Device**, a Dell integra telemetria dos dispositivos com software líder do setor para melhorar a segurança em todo o parque.*



Integração projetada com a segurança da cadeia de suprimentos ajuda a garantir que os PCs são seguros desde a primeira inicialização

- Suplementos **Dell SafeSupply Chain** como Dell Secured Component Verification oferecem garantia adicional de integridade do produto.

* Exclusivo da Dell

A Dell combina vários recursos

Com contramedidas de hardware e software implementadas, reduza a superfície de ataque com defesas que ajudam a prevenir ataques comuns.

Os recursos de detecção e resposta abordam ataques furtivos que podem passar despercebidos.

No caso do Ataque à cadeia de suprimentos debatido na página 4, ao trabalhar com a Dell, medidas preventivas, como **práticas seguras na cadeia de suprimentos**, podem impedir um ataque logo no início da kill chain. Se um ataque passar, outras contramedidas – como **SCV** – também serão implementadas.

No caso do Ataque de engenharia social, mesmo se um criminoso conseguir enganar um usuário a entregar credenciais válidas, **verificações de usuário baseadas em hardware como SafeID** podem impedir o criminoso e podem negar demais acessos. Um software de segurança como um **gateway da web seguro de última geração** oferece outra camada de proteção de monitoramento.

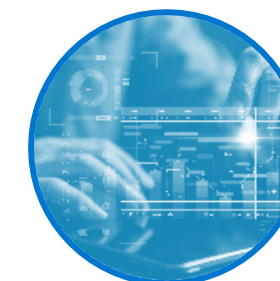
Combate ao ataque de cadeia de suprimentos de hardware iniciado por falsificação de componentes.

Os criminosos interceptam um carregamento de PCs e trocam os discos rígidos.



- **Práticas seguras na cadeia de suprimentos**
- Embalagem que evidencia a violação
- Travas de porta

A TI implementa os dispositivos comprometidos em toda a empresa.



- Secured Component Verification (SCV)
- Verificação do tempo de execução

O criminoso instala o malware para extrair credenciais assim que os usuários entram.



- Agente de segurança com acesso à nuvem
- Gateway da Web seguro de última geração

Como combater um ataque de engenharia social iniciado por um e-mail de phishing.

O usuário final se deixa enganar pelo e-mail de phishing e entrega as credenciais em uma página da web falsa.



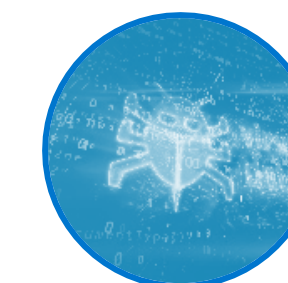
- NGAV
- EDR
- XDR

O criminoso usa as credenciais válidas para acessar remotamente a rede.



- **Autenticação baseada em vários fatores com SafeID**
- Acesso à rede com Zero Trust

O criminoso extrai os dados em um serviço da web, criptografa dados roubados e os retém em troca de resgate.



- Gateway da Web seguro de última geração e lógica analítica de comportamento de entidade do usuário



Principais conclusões

As violações são inevitáveis.

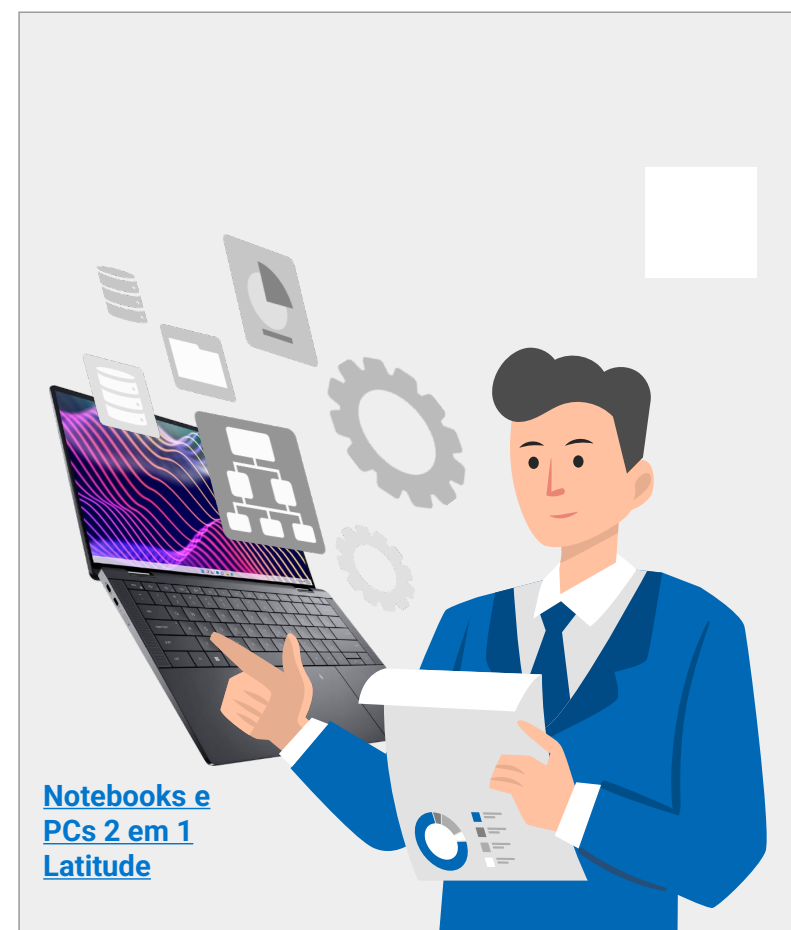
A segurança efetiva do endpoint pressupõe a pior situação sempre e se concentra em evitar kill chains sempre que ocorrerem, do dispositivo para a rede para a nuvem.

Nenhuma solução bloqueia

100% dos ataques. Combine contramedidas de hardware e software para conseguir a melhor defesa.

Você terá o mesmo nível de segurança

de seus fornecedores. Desafie seus fornecedores a apresentar as medidas de segurança.



Dê o próximo passo

A segurança é um tópico assustador para organizações de todos os tamanhos. **Envolva-se com um parceiro de tecnologia e segurança experiente para modernizar a segurança do endpoint.**

O Dell Trusted Workspace ajuda a proteger os endpoints de um ambiente de TI moderno, pronto para o Zero Trust. Reduza a superfície de ataque com um portfólio abrangente de proteções de hardware e software exclusivas da Dell. Nossa abordagem altamente coordenada e baseada em defesa neutraliza as ameaças combinando proteções integradas com vigilância contínua. Os usuários finais continuam produtivos e a TI fica confiante com as soluções de segurança criadas para o mundo baseado em nuvem de hoje em dia.

Para saber mais:

Fale conosco: Global.Security.Sales@Dell.com

Acesse: Dell.com/Endpoint-Security

Siga-nos: LinkedIn [@DellTechnologies](https://www.linkedin.com/company/delltechnologies) | X [@DellTech](https://twitter.com/DellTech)

