DELL Technologies

Como combater as ameaças cibernéticas modernas

com segurança de endpoint integrada e capacidade de gerenciamento

CROWDSTRIKE intel ABSOLUTE®

Sumário Executivo

Os vetores de ataque emergentes estão criando novos riscos. Mantenha-se à frente das ameaças modernas aos endpoints com várias camadas de defesa que funcionam em conjunto. Saiba como a telemetria de hardware pode se integrar ao software para melhorar a segurança e a capacidade de gerenciamento de todo o parque. Interrompa ataques com mais rapidez, aplique os princípios de Zero Trust e inove com segurança usando dispositivos e soluções simples de gerenciar.

Sumário

O ambiente de ameaças

Estudo de caso

Em 2023, a Eclypsium descobriu uma falha no firmware das placas-mãe vendidas por um fabricante de Taiwan. Com a intenção de apenas manter o firmware atualizado, os pesquisadores descobriram que a implementação do código não foi segura, o que permitia que o mecanismo fosse sequestrado e usado para instalar malware.

Alguns motivos que tornam essa descoberta particularmente alarmante

- Os clientes foram expostos por uma vulnerabilidade de firmware.
- A vulnerabilidade existia em uma área do dispositivo em que, tradicionalmente, é difícil detectar ameaças.
- Ele pode ser usado para iniciar um ataque remoto que ignora as verificações de credenciais.

Extraído das manchetes...

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Código oculto em centenas de modelos de placas-mãe faz download de programas de modo invisível e sem segurança, um recurso propício para abuso, dizem os pesquisadores.

O ambiente de ameaças

Implicações

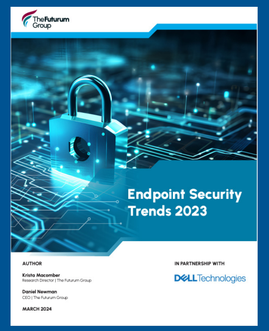
Este é um fator-chave que preocupa muito as equipes de TI e segurança:

Ataques com base em dispositivos.

Esses ataques sofisticados e mal-intencionados permitem que os adversários obtenham acesso privilegiado. Além disso, muitos deles podem desativar proteções tradicionais somente de software, como antivírus, sem serem detectados.

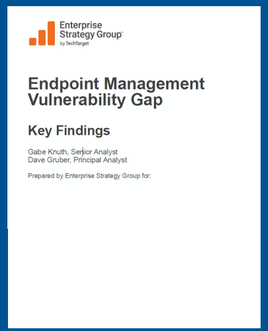
De acordo com uma recente pesquisa global com profissionais de TI e segurança[1], entre os principais critérios de avaliação das organizações quando adquirem novo hardware, estão:

Detecção automática de eventos de firmware do BIOS



69% das organizações relataram pelo menos UM ataque no nível do dispositivo nos últimos 12 meses. Isso representa um aumento de 1,5 vezes em relação ao estudo de 2020![2]

Configurações de alto risco



Mais de 75% das organizações relatam que sofreram pelo menos um ataque cibernético causado por um dispositivo de endpoint desconhecido, não gerenciado ou mal gerenciado.[3]

Desafios

Então, o que torna um dispositivo um alvo fácil?

Visibilidade

É difícil identificar esses ataques, executados em uma parte do dispositivo que tradicionalmente não tem visibilidade nem observabilidade.

Capacidade de ação

Muitas vezes, as organizações têm dezenas de ferramentas instaladas que operam em silos. Então, se um ataque for detectado, a resposta e correção rápidas serão um grande desafio com muito trabalho manual.

Solução

Visibilidade | Capacidade de ação

Como uma das maiores empresas provedoras de tecnologia do mundo, a Dell pensa muito na segurança. É por isso que **criamos nossos PCs comerciais para priorizar a visibilidade e a capacidade de ação desde o início**. Isso coloca o poder nas mãos das operações de TI e de segurança.

Nossos PCs comerciais são enviados com **recursos de segurança integrados exclusivos**, como Verificação do BIOS[4] e Indicadores de ataque[4], que ajudam a detectar ameaças antes que elas causem danos. Tornamos essas detecções visíveis com a **telemetria de dispositivo exclusiva da Dell**[4]. Quando um PC comercial da Dell no Intel vPro® detecta uma possível ameaça no nível do dispositivo, ele pode enviá-la ao sistema operacional para investigação e resposta mais rápidas e eficazes

Liderança no setor

A Dell oferece os PCs comerciais mais seguros do mundo[4]

Saiba o que é necessário para manter a confiança dos dispositivos contra ameaças modernas.

Leia o estudo da Principled Technologies sobre segurança de dispositivos →


Principled Technologies®

A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Solução

Combata ameaças com segurança e capacidade de gerenciamento trabalhando em conjunto

A Dell e nossa rede de parceiros conectados estão trabalhando para trazer visibilidade e capacidade de ação ao espaço de trabalho. Isso inclui:

- Segurança da cadeia de suprimentos e defesas integradas de hardware e firmware da Dell
- Proteções do núcleo de silício e "abaixo do sistema operacional" da Intel
- Capacidade de gerenciamento por meio de consoles unificados de gerenciamento de endpoint e da Dell
- Proteção avançada contra ameaças que abrange endpoints, redes e a nuvem de parceiros, incluindo CrowdStrike e Absolute

O ecossistema usa a telemetria do PC como conector, ajudando a eliminar a lacuna entre as soluções de TI e de segurança, onde podem ocorrer as ameaças. Além de ajudar a evitar ataques, essa abordagem também pode detectar, responder, recuperar-se e corrigi-los.

Casos de uso e contramedidas

Para demonstrar como a segurança e a capacidade de gerenciamento integradas funcionam para melhorar a resiliência cibernética, analisaremos dois casos de uso incluindo cenários de ataque e contramedidas.

Primeiro, um ataque ao firmware do BIOS. Aqui, conferimos como a cadeia de ataque cibernético[5] de um ataque de downgrade do BIOS pode se desenrolar.

Ataque de downgrade do BIOS

Acesso inicial: Replicação por mídia removível + phishing

Etapa 1a

Um invasor mal-intencionado explora uma vulnerabilidade existente do BIOS para roubar remotamente as credenciais do sistema operacional. Ele invade o dispositivo e faz downgrade do BIOS.

Etapa 1b

O invasor inicia um ataque de spear phishing e rouba um token de sessão quando um administrador faz autenticação por engano em um site mal-intencionado.

Etapa 2

Acesso às credenciais

O invasor alcança a persistência criando contas de administrador adicionais e começa a se movimentar pela rede.

Etapa 3

Movimento lateral

O invasor mapeia a rede e localiza os servidores de gerenciamento do sistema.

Etapa 4

Exfiltração

O invasor exfiltra dados por meio de um serviço Web.

Casos de uso e contramedidas

Contramedidas de downgrade do BIOS

Os adversários estão invadindo a rede mais rápido do que nunca. Na verdade, de acordo com o Global Threat Report da CrowdStrike, o tempo médio de invasão do crime eletrônico (o tempo necessário para invadir um sistema e se movimentar lateralmente) diminuiu de 84 minutos em 2022 para 62 minutos em 2023. O tempo de invasão mais rápido observado foi de apenas 2 minutos e 7 segundos![6]

Confira como a Dell e nossas parceiras Intel® e CrowdStrike ajudam a detectar e afastar um ataque de downgrade do BIOS ao longo da cadeia de ataque com segurança assistida por hardware.

Prevenção | **Detectar e responder** | **Recuperar e corrigir**

Cadeia de suprimentos segura: Controles rigorosos protegem os PCs desde o projeto e desenvolvimento, passando pela aquisição, montagem e entrega. A Dell e a Intel trabalham incansavelmente para garantir que os produtos sejam desenvolvidos com redução no risco de vulnerabilidades e adulteração de produtos durante todo o ciclo de vida.

Security	Integrity	Quality	Resilience
• Secure development lifecycle • Software partners securely onboarded • Information exchange with partners securely • Quality Process Audit • Separation of Duties • Least Privilege Access	• Supplier accountability • Supplier due diligence • Piece-Part Identification • SAFECode • US Exec Order 14028 SBOM -SPDX	• Counterfeit prevention & detection • Enhanced manufacturing security program • Enterprise code signing • Secured Component Verification • Freight Tracking	• Silicon Root of Trust • Platform Firmware Resiliency Guidelines • BIOS Protection Guidelines • Built-in Supplier Redundancy

Casos de uso e contramedidas

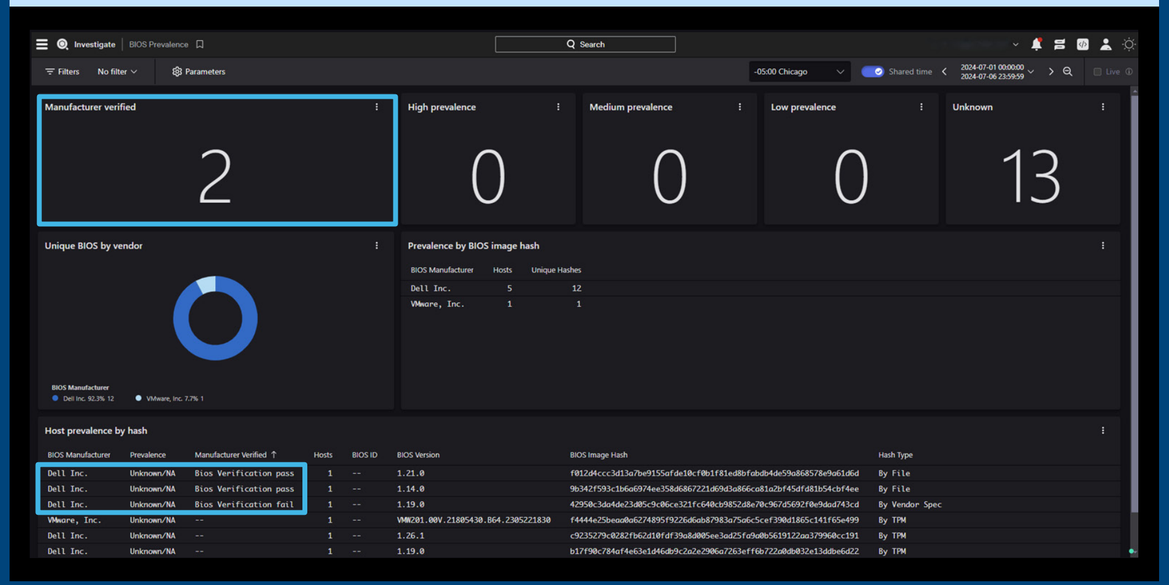
Contramedidas de downgrade do BIOS

Os adversários estão invadindo a rede mais rápido do que nunca. Na verdade, de acordo com o Global Threat Report da CrowdStrike, o tempo médio de invasão do crime eletrônico (o tempo necessário para invadir um sistema e se movimentar lateralmente) diminuiu de 84 minutos em 2022 para 62 minutos em 2023. O tempo de invasão mais rápido observado foi de apenas 2 minutos e 7 segundos![6]

Confira como a Dell e nossas parceiras Intel® e CrowdStrike ajudam a detectar e afastar um ataque de downgrade do BIOS ao longo da cadeia de ataque com segurança assistida por hardware.

Prevenção | **Detectar e responder** | **Recuperar e corrigir**

Detectar certificação do BIOS na plataforma CrowdStrike Falcon: Com a telemetria de dispositivo da Dell ativada, um administrador pode visualizar remotamente notificações de recursos de segurança integrados, como a Verificação do BIOS, no CrowdStrike Falcon, acelerando a detecção de atividades suspeitas antes que ocorram danos duradouros.



Casos de uso e contramedidas

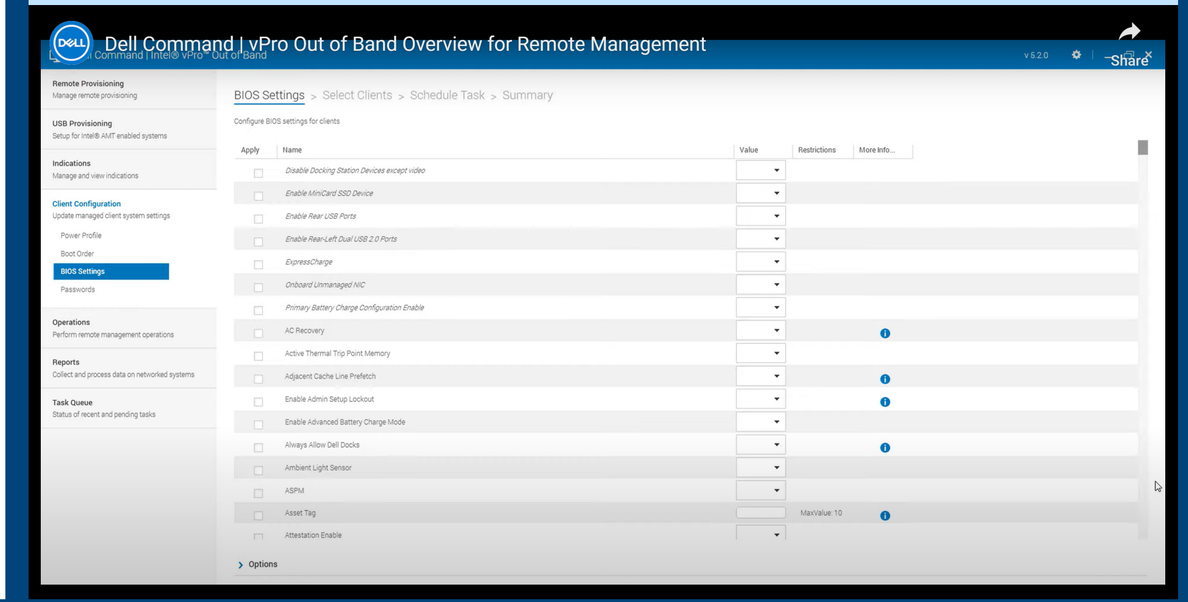
Contramedidas de downgrade do BIOS

Os adversários estão invadindo a rede mais rápido do que nunca. Na verdade, de acordo com o Global Threat Report da CrowdStrike, o tempo médio de invasão do crime eletrônico (o tempo necessário para invadir um sistema e se movimentar lateralmente) diminuiu de 84 minutos em 2022 para 62 minutos em 2023. O tempo de invasão mais rápido observado foi de apenas 2 minutos e 7 segundos![6]

Confira como a Dell e nossas parceiras Intel® e CrowdStrike ajudam a detectar e afastar um ataque de downgrade do BIOS ao longo da cadeia de ataque com segurança assistida por hardware.

Prevenção | **Detectar e responder** | **Recuperar e corrigir**

Corrigir o downgrade do BIOS: Ajuda a evitar ameaças futuras para sistemas fora de banda. O Dell Client Command Suite com Intel vPro possibilita a correção remota.



Casos de uso e contramedidas

Neste segundo caso de uso, é assim que a etapa na cadeia de ataque à cadeia de suprimentos de software pode se desenrolar.

Ataque à cadeia de suprimentos de software

Etapa 1

Acesso inicial: Comprometimento da cadeia de suprimentos

O invasor injeta código mal-intencionado em um utilitário de software (BIOS/firmware).

Etapa 2

Persistência

Os clientes fazem download do código mal-intencionado quando vão atualizar seus dispositivos.

O invasor instala um malware.

Etapa 3

Movimento lateral

O invasor se faz passar por um usuário que acabou de ser atacado e envia um link mal-intencionado a outro usuário. Esse usuário clica no link, e o invasor rouba as credenciais dele.

Etapa 4

Exfiltração

O invasor exfiltra os dados.

Casos de uso e contramedidas

A cadeia de suprimentos se tornou um dos principais alvos dos invasores. Embora esses ataques sejam menos comuns, os resultados de um ataque bem-sucedido podem ser devastadores porque as organizações ainda estão aprendendo a reforçar suas defesas contra eles.

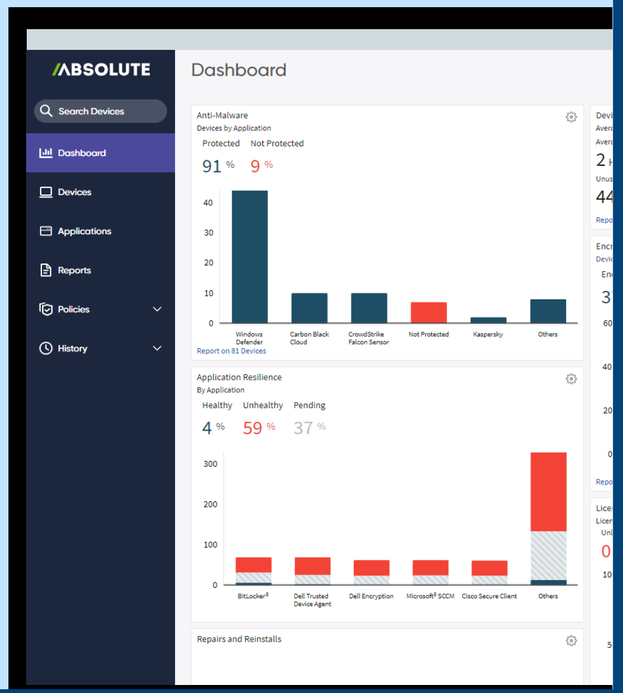
Uma das principais responsabilidades de todos os provedores de tecnologia é garantir a venda de produtos que não apresentem riscos acidentais aos usuários por meio de vulnerabilidades.

Para ajudar a evitar ataques e fornecer resiliência à pilha de segurança, a Dell e a Intel® seguem o processo e os protocolos rigorosos do nosso ciclo de desenvolvimento seguro[7]. A garantia adicional da cadeia de suprimentos, como a verificação de componentes protegidos da Dell[8], além da segurança no nível do firmware da Absolute (mostrada à direita), oferecem confiança aos clientes durante toda a vida útil do PC.

Prevenção | **Detectar e responder** | **Recuperar e corrigir**

Visibilidade de endpoints de fábrica: Acesse todos os dispositivos dentro e fora da rede com o Absolute incorporado nas fábricas gerenciadas pela Dell. O Absolute Custom Factory Install (CFI) remove uma etapa na implementação e protege os dispositivos que podem ser enviados para armazéns e vários locais de usuário final. Reduza os riscos com uma visão completa do parque usando um painel de indicadores baseado na nuvem.

- Encontre e mantenha facilmente um inventário completo de seus ativos e aplicativos de TI
- Localize e mapeie toda a sua frota
- Otimize o uso de ativos e monitore a postura de segurança
- Suporte a várias plataformas (Windows, Mac e Chrome)
- Incorporado no BIOS de 27 OEMs líderes de PC



Casos de uso e contramedidas

A cadeia de suprimentos se tornou um dos principais alvos dos invasores. Embora esses ataques sejam menos comuns, os resultados de um ataque bem-sucedido podem ser devastadores porque as organizações ainda estão aprendendo a reforçar suas defesas contra eles.

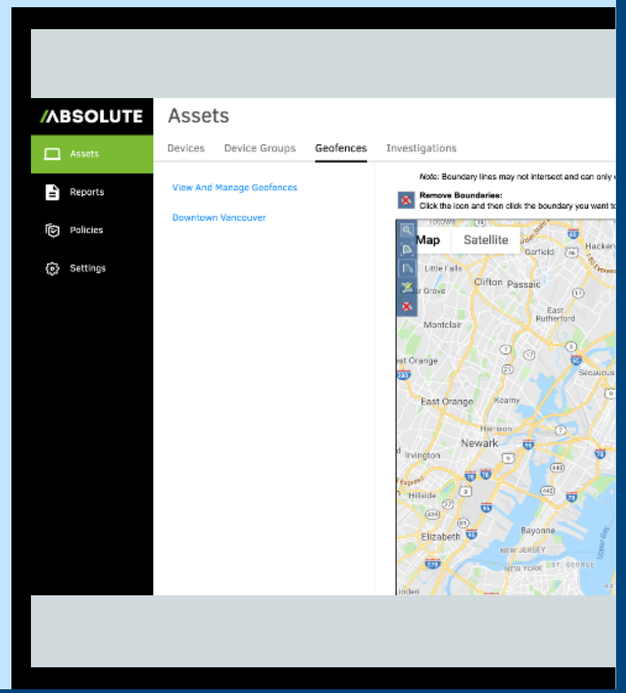
Uma das principais responsabilidades de todos os provedores de tecnologia é garantir a venda de produtos que não apresentem riscos acidentais aos usuários por meio de vulnerabilidades.

Para ajudar a evitar ataques e fornecer resiliência à pilha de segurança, a Dell e a Intel® seguem o processo e os protocolos rigorosos do nosso ciclo de desenvolvimento seguro[7]. A garantia adicional da cadeia de suprimentos, como a verificação de componentes protegidos da Dell[8], além da segurança no nível do firmware da Absolute (mostrada à direita), oferecem confiança aos clientes durante toda a vida útil do PC.

Prevenção | **Detectar e responder** | **Recuperar e corrigir**

Controlar endpoints: Com o Absolute, detecte quando os endpoints estão comprometidos (por exemplo, um aplicativo essencial é corrompido por malware ou um PC desaparece em trânsito). Tome medidas remotas para corrigir ameaças imediatamente, tornando os dispositivos inúteis e/ou excluindo os dados neles.

- Proteja os dispositivos quando eles se moverem além dos limites definidos
- Proteja e higienize dados essenciais remotamente
- Realize a limpeza de dados no fim da vida útil com certificados de conformidade
- Bloqueie dispositivos para proteger ativos críticos sob demanda
- Ativar proteção de firmware remoto



Casos de uso e contramedidas

A cadeia de suprimentos se tornou um dos principais alvos dos invasores. Embora esses ataques sejam menos comuns, os resultados de um ataque bem-sucedido podem ser devastadores porque as organizações ainda estão aprendendo a reforçar suas defesas contra eles.

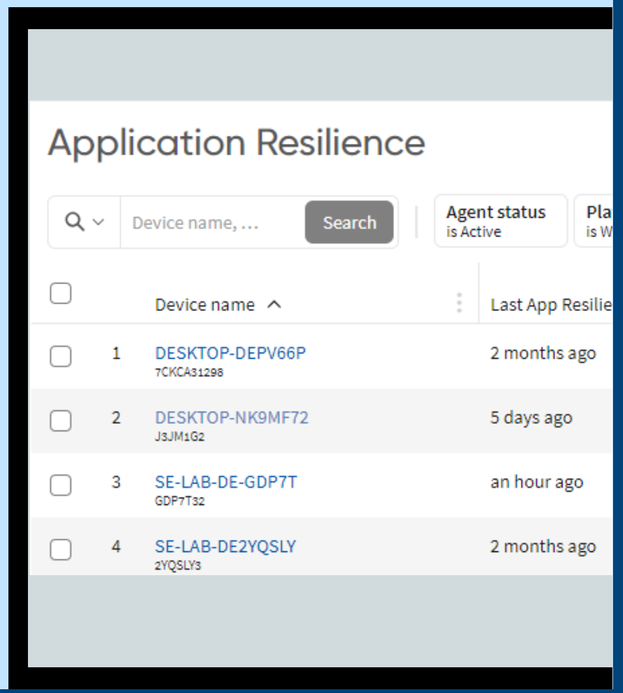
Uma das principais responsabilidades de todos os provedores de tecnologia é garantir a venda de produtos que não apresentem riscos acidentais aos usuários por meio de vulnerabilidades.

Para ajudar a evitar ataques e fornecer resiliência à pilha de segurança, a Dell e a Intel® seguem o processo e os protocolos rigorosos do nosso ciclo de desenvolvimento seguro[7]. A garantia adicional da cadeia de suprimentos, como a verificação de componentes protegidos da Dell[8], além da segurança no nível do firmware da Absolute (mostrada à direita), oferecem confiança aos clientes durante toda a vida útil do PC.

Prevenção | **Detectar e responder** | **Recuperar e corrigir**

Autocorreção: Com o Absolute Persistence incorporado ao firmware do BIOS da Dell, volte ao estado original quando a adulteração for detectada. O Absolute pode se autocorrigir, ou persistir, em qualquer endpoint comprometido ou aplicativo compatível no catálogo de resiliência de aplicativos (+ de 80 aplicativos), incluindo uma biblioteca de outras contramedidas em vigor, como o aplicativo Dell Trusted Device, Zscaler.

- Encontre e exclua com facilidade dados confidenciais em endpoints
- Tome medidas corretivas em todos os dispositivos por meio de uma biblioteca de scripts personalizados
- Aplicativos de monitoramento e autocorreção
- Catálogo de resiliência de aplicativos de controles de endpoints de terceiros grande e aumentando
- Investigue e localize dispositivos perdidos ou roubados com a equipe de investigações da Absolute



Principais conclusões

A segurança de um parque depende dos PCs individuais.

Para combater as ameaças modernas, os dispositivos precisam ser construídos com segurança e ter segurança integrada.

Detecte, afaste e recupere-se de ataques garantindo que a segurança do endpoint e a capacidade de gerenciamento trabalhem em conjunto.

A segurança é um esporte em equipe. Use tanto hardware quanto software para ter a melhor defesa.

Para saber mais:

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

Acesse: Dell.com/Endpoint-Security

Siga-nos: LinkedIn @DellTechnologies | X @DellTech

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.

1. Fonte: Enterprise Strategy Group, uma divisão da TechTarget, pesquisa personalizada encomendada pela Dell Technologies, *Assessing Organizations' Security Journeys*, de novembro de 2023.
2. Fonte: Futurum Group, Endpoint Security Trends, 2023.
3. Fonte: Enterprise Strategy Group, uma divisão da TechTarget, relatório de pesquisa *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, de maio de 2023.
4. Com base em análise interna da Dell, de outubro de 2024. Aplicável a PCs com processadores Intel. Nem todos os recursos estão disponíveis em todos os PCs. Alguns recursos exigem compra separada. Validado pela Principled Technologies. A comparison of security features, de abril de 2024.
5. Fonte: What is the Cyber Kill Chain? Introduction Guide – CrowdStrike.
6. Fonte: CrowdStrike 2024 Global Threat Report.
7. Fonte: Três considerações para estabelecer a confiança do dispositivo | Dell EUA.
8. Fonte: Como manter a confiança do dispositivo em segredo | Dell EUA.