Anatomia de um dispositivo confiável

Saiba o que torna os PCs com IA comerciais Dell os mais seguros do mundo[1]

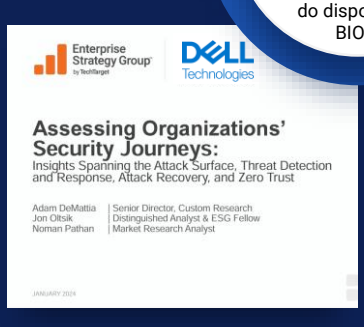
DESAFIOS E AMBIENTE DAS AMEAÇAS

Vetores de ataque emergentes abaixo do sistema operacional criam novos riscos

Os dispositivos endpoint são uma importante porta de entrada para violações. À medida que o trabalho híbrido expandiu a superfície de ataque, a preocupação com a segurança no nível do dispositivo aumentou nos últimos anos. Os invasores cada vez mais atacam a cadeia de suprimentos, bem como rootkits e outras vulnerabilidades de firmware que, na maioria das vezes, não podem ser detectadas apenas pelo software EDR legado.

As ameaças baseadas em dispositivos aumentaram 1,5x desde 2020.[2]

69%
das organizações informam pelo menos UM ataque no nível do dispositivo/ BIOS[2]



Principais critérios de avaliação ao adquirir novos PCs:

- Detecção automatizada de eventos do BIOS[3]
- Lidar com configurações de alto risco[3]

Para combater as ameaças modernas, os dispositivos precisam ser construídos com segurança e ter segurança integrada para ajudar a detectar e afastar ataques.

A SOLUÇÃO

Previna, detecte, responda e recupere-se de ataques de base com os PCs comerciais mais seguros do mundo[1]

A segurança de um parque depende dos PCs individuais. Mas o que torna um dispositivo confiável e seguro? Visibilidade e capacidade de ação. O acesso a mais dados leva à tomada de decisões fundamentadas, ajudando a detectar até mesmo as ameaças emergentes mais sorrateiras. A automação possibilita uma resolução mais rápida de possíveis problemas.

As defesas de hardware e firmware dos PCs comerciais Dell (nas plataformas Intel e AMD) foram desenvolvidas para oferecer visibilidade e capacidade de ação ao seu parque de PCs.

A anatomia de um Dell Trusted Device

Benefícios

- Tenha segurança desde a primeira inicialização com rigorosos controles da cadeia de suprimentos
- Mantenha a integridade do BIOS com visibilidade profunda no nível do firmware
- Proteja a identidade do usuário final contra malware que busca roubar credenciais
- Enriqueça dados no nível do sistema operacional com telemetria "abaixo do sistema operacional" para acelerar a detecção, a resposta e a correção

Aumente a segurança com a telemetria de PCs

Reduza a lacuna de segurança de TI e enriqueça as soluções de software com insights no âmbito do SO. Somente a Dell integra a telemetria de PCs com provedores de software líderes do setor para aperfeiçoar a segurança de todo o parque.[1]
Saiba mais →

Mantenha a integridade do BIOS

Detecte e afaste ameaças com a verificação do BIOS exclusiva da Dell. Avalie um BIOS corrompido, repare-o e obtenha insights que reduzem a exposição a ameaças futuras com a Captura da imagem do BIOS[1].
Saiba mais →

Identifique problemas prestes a acontecer

Indicadores de ataque, um recurso de alerta antecipado que só a Dell oferece, verifica se há ameaças com base no comportamento antes que elas possam causar danos[1].
Saiba mais →

Verifique a integridade do firmware

A verificação de firmware exclusiva da Dell (segurança baseada em hardware encontrada em processadores Intel) oferece proteção contra acessos não autorizados e adulterações de firmware altamente privilegiado. [1]

Detecte vulnerabilidades conhecidas

A detecção de vulnerabilidades e exposições comuns (CVE) exclusiva da Dell monitora falhas de segurança do BIOS relatadas publicamente e recomenda atualizações para reduzir os riscos.[1]
Saiba mais →

Credenciais seguras do usuário final

Verifique o acesso de usuários com o chip de segurança dedicado SafeID, exclusivo da Dell, que mantém as credenciais do usuário ocultas para evitar malware.[1]
Saiba mais →

Tenha segurança durante todo o ciclo de vida do PC

Controles rigorosos e modernos da cadeia de suprimentos e complementos opcionais, como o recurso Secured Component Verification exclusivo da Dell, garantem a integridade do PC, desde a entrega até o fim da vida útil.[1]
Saiba mais →

LIDERANÇA NO SETOR

Nenhum fabricante de PCs oferece a mesma visibilidade no nível do BIOS que a Dell[1].

Saiba o que é necessário para manter a confiança dos dispositivos contra ameaças modernas.[4]

Saiba mais →


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

Explore os Dell Trusted Devices

Notebooks →

Desktops →

Workstations →

Proteja o trabalho em qualquer lugar com o Dell Trusted Workspace

Segurança de hardware integrada e incorporada

Segurança de software incorporada

Visite-nos
dell.com/endpoint-security

Entre em contato conosco
global.security.sales@dell.com

Saiba mais
Endpoint Security Blogs →

Participe da conversa
delltechnologies @delltech

Fontes e isenções de responsabilidade

[1] Com base em uma análise interna da Dell, outubro de 2024 (Intel) e março de 2025 (AMD). Aplicável a PCs com processadores Intel e AMD. Nem todos os recursos estão disponíveis em todos os PCs. Compra adicional necessária para alguns recursos. Validado pela Principled Technologies. A comparison of security features, de abril de 2024.

[2] Fonte: Futurum Group, Endpoint Security Trends, de 2023.

[3] Fonte: Enterprise Strategy Group, uma divisão da TechTarget, pesquisa personalizada encomendada pela Dell Technologies, *Assessing Organizations' Security Journeys*, de novembro de 2023.

[4] Resultados do estudo da Principled Technology disponíveis apenas para dispositivos baseados em Intel.