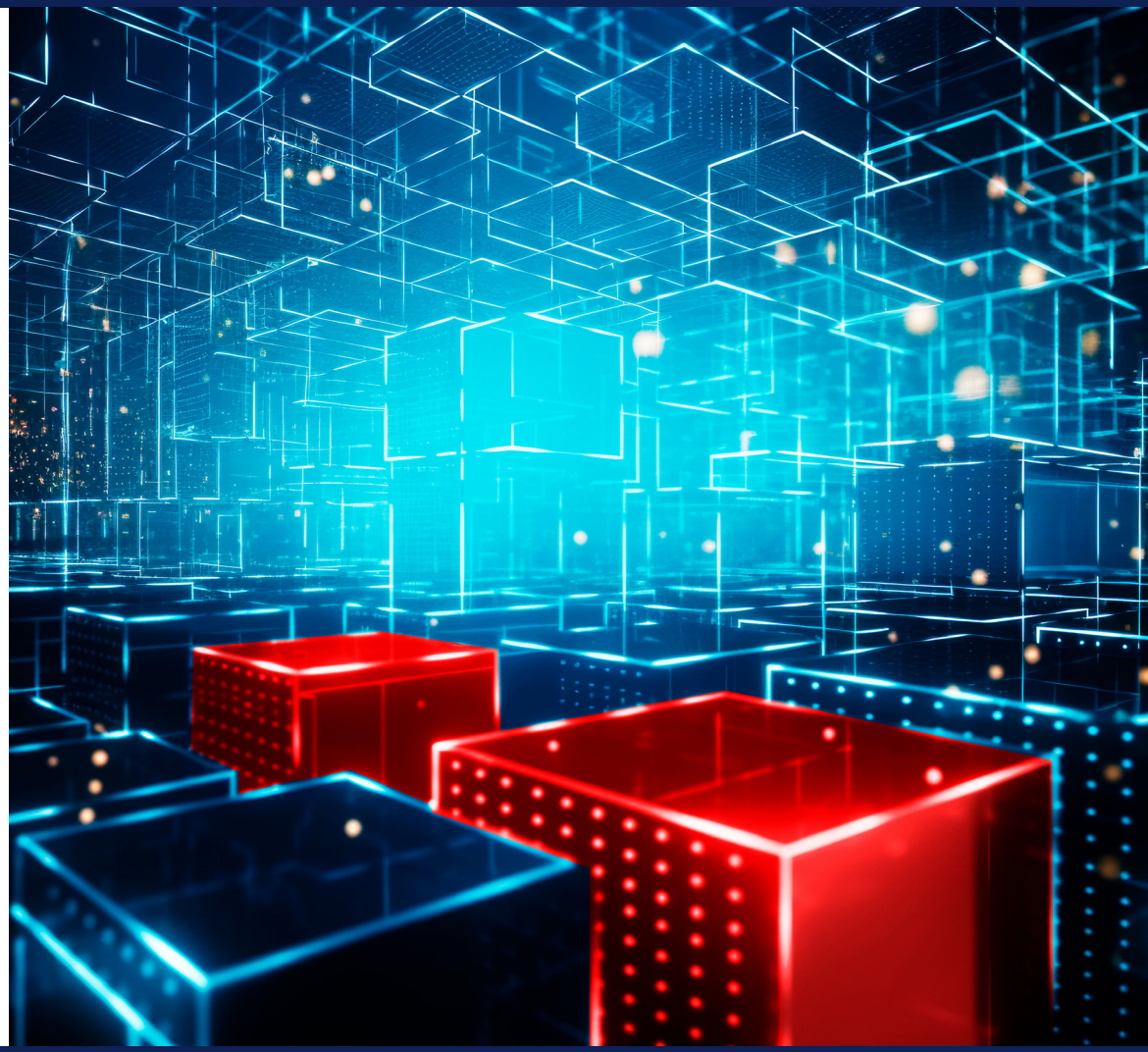
Como proteger o uso da IA no endpoint

Defenda cargas de trabalho de IA no dispositivo com dispositivos seguros e modernos e uma mentalidade adversária.



Resumo executivo

A IA no dispositivo traz inúmeros benefícios, mas também muitos riscos cibernéticos. Neste eBook, analisaremos como posicionar sua organização com segurança para aproveitar as inovações em IA no endpoint.

Sumário

A superfície de ataque da IA no dispositivo

O que pode ser atacado

Todas as tecnologias emergentes apresentam riscos de segurança cibernética por um motivo: é um novo território. Você está lidando com o desconhecido. Vimos isso com a computação em nuvem, com a blockchain e inúmeras outras tecnologias. O mesmo se aplica à IA no dispositivo. A chave para mitigar esse risco, como sempre, é esclarecer o desconhecido.

Antes de podermos falar sobre a segurança de que precisamos para minimizar a superfície de ataque, é útil analisar o que estamos protegendo e por que. Pense nisso como um sistema de tubulações em um prédio comercial que abriga várias empresas. Essas tubulações transportam água, gás etc. por todo o prédio para uma variedade de casos de uso. Se a matéria que flui pelas tubulações estiver contaminada ou for interrompida, ela não cumprirá sua função. Se as tubulações que transportam a matéria estiverem danificadas ou corrompidas, elas não cumprirão sua função. As tubulações e seu conteúdo precisam estar em boas condições de funcionamento para atender às necessidades de seus respectivos casos de uso.►

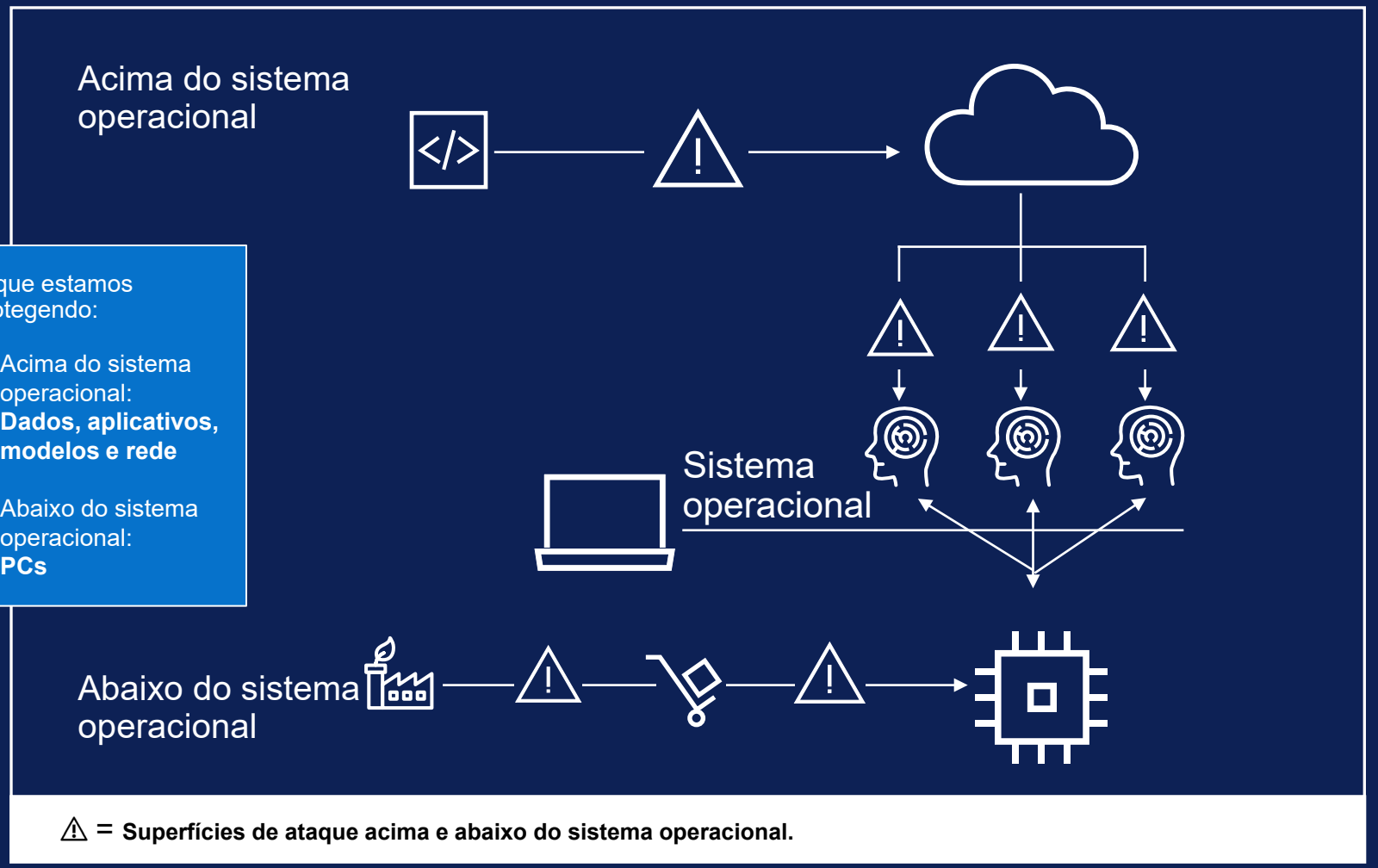
A superfície de ataque da IA no dispositivo, continuação

Possíveis alvos dos ataques, continuação

Voltando à IA no endpoint:

- As tubulações são sua infraestrutura, seus PCs, suas redes corporativas. Como e onde você trabalha.
- O conteúdo que flui pelas tubulações são os dados, aplicativos e modelos que alimentam diversos casos de uso de IA. Os ativos e recursos necessários para realizar seu trabalho.

E você adivinhou. Adversários cibernéticos têm ambos como alvo. Eles podem roubar propriedade intelectual para receber resgate ou contaminar dados ou modelos para afetar as operações. De qualquer forma, as consequências podem ser graves, levando a danos financeiros e de reputação e/ou desencadeando revisões regulamentares.►



Riscos de segurança no endpoint

Táticas que os invasores usam para invadir

Agora, falaremos sobre os métodos que os invasores podem usar para acessar ambos os alvos.

Comprometimento do dispositivo. Como nós vimos no Endpoint Security Market Insights, da Forrester Research, Inc., em março de 2025, os PCs estão entre os principais alvos das ameaças cibernéticas modernas. Esse tipo de ataque pode acontecer antes do início do trabalho da IA no dispositivo, ou seja, um **ataque à cadeia de suprimentos de software ou hardware**. Durante a cadeia de suprimentos, há dezenas, se não centenas, de aspectos em que uma pessoa mal-intencionada pode conseguir adulterar componentes — por exemplo, circuitos e firmware — para introduzir pontos vulneráveis que podem ser explorados posteriormente. Imagine o desastre iminente de uma empresa de investimentos recebendo uma nova remessa de PCs com componentes falsificados.

Comprometimento de credenciais. Violações envolvendo credenciais roubadas ou comprometidas são um dos vetores de ataque que mais crescem. E isso não é nenhuma surpresa. Invasores que utilizam credenciais válidas podem fazer login em um PC, mover-se livremente pela rede corporativa e permanecer na rede sem serem detectados por longos períodos. De acordo com o último relatório sobre o custo de uma violação de dados da IBM, a identificação e contenção dessas violações levaram em média 292 dias, o maior tempo de qualquer vetor de ataque estudado. Esse nível de acesso é valioso demais para ser ignorado por agentes de ameaça. De fato, pesquisas da Zscaler mostram que indivíduos mal-intencionados estão aperfeiçoando suas estratégias de roubo de credenciais para melhorar e dimensionar ataques de phishing utilizando a IA generativa. Esse acesso não autorizado aplicado a dados confidenciais de treinamento ou inferência, ou diretamente a modelos, é categorizado como um **ataque à cadeia de suprimentos de modelos**.

Ameaças internas. Pesquisas recentes mostram que, em comparação com outros vetores de ataque, os **ataques internos mal-intencionados** resultaram em custos mais altos, com uma média de US$ 4,99 milhões. Lembre-se de que ataques internos podem ocorrer na cadeia de suprimentos de hardware, software e de modelos.►

Tempo médio para que um usuário final seja vítima de um e-mail de **phishing**: menos de 60 segundos*

Média de 292 dias para detectar e conter o **comprometimento de credenciais****

Os ataques internos mal-intencionados custam, em média, US$ 4,99 milhões**

*Fonte: Verizon DBIR, 2024
**Fonte: IBM Cost of a Data Breach, 2024

Contramedidas a serem implementadas

O que mitiga o risco

Nenhum desses alvos de ataque é fundamentalmente novo. Nem os objetivos finais dos invasores. Como sempre, queremos nos concentrar em manter seu parque seguro e resiliente. **A sobreposição de contramedidas** pode reduzir a superfície de ataque e esclarecer qualquer comportamento suspeito imediatamente.

Uma **mentalidade Zero Trust** reduzirá os riscos em todo o seu parque. Esses princípios — nunca confiar, sempre verificar e monitorar continuamente — ajudam você a se antecipar aos invasores. É impossível bloquear 100% dos ataques. Para uma postura de segurança sólida, você precisa de **visibilidade e controle** em todo o seu ecossistema de TI.

Com essa estrutura em mente, reavalie sua infraestrutura, especialmente os sistemas e processos que interagem com a IA. Quais contramedidas minimizam o risco de comprometimento do dispositivo, comprometimento de credenciais e ameaça interna?►

Os princípios Zero Trust evitam os riscos e reduzem o raio de ação das atividades cibernéticas

Contramedidas para implementar, continuação

O que reduz os riscos, continuação

Existem duas categorias gerais de contramedidas.

A segurança "abaixo do sistema operacional" protege os dispositivos de IA com os quais você trabalha. Podemos dividir isso em duas partes:

- Defenda seu parque de PCs com dispositivos **construídos com segurança**. Isso significa o uso de AI PCs que sejam seguros por padrão, ou seja, que foram desenvolvidos com princípios de projeto seguro e em uma cadeia de suprimentos segura.
- Defenda seu parque de PCs com dispositivos que têm **segurança integrada**. Os AI PCs seguros incluem camadas de proteção integrada que oferecem visibilidade — até as camadas de BIOS e chip — imediatamente.

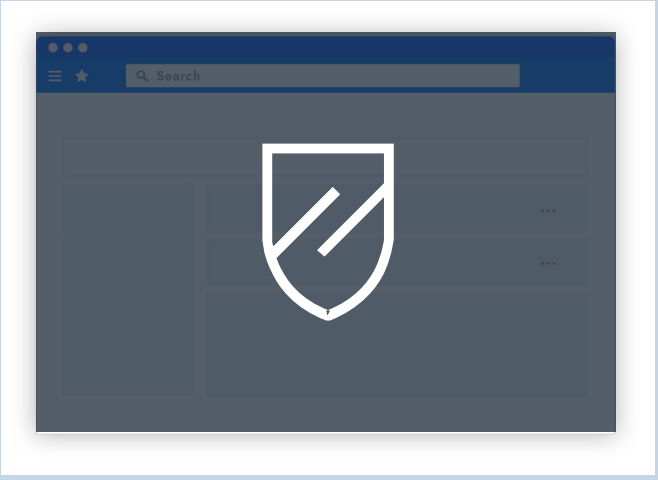
A segurança "acima do sistema operacional" protege o acesso a modelos de IA. Defenda os dados e modelos *com os* quais você trabalha e as redes corporativas em que *trabalha* com **segurança de software**. É essencial proteger as operações de segurança de aprendizado de máquina e monitorar o tráfego de rede de cargas de trabalho de IA implementadas.►

Segurança abaixo do sistema operacional

AI PCs seguros

Segurança de hardware e firmware, segurança da cadeia de suprimentos e do chip principal

Acima da segurança do sistema operacional



Segurança de software

Camada adicional de segurança para endpoints, redes e ambientes de nuvem

Serviços de segurança e conhecimento especializado disponíveis para unir tudo.

Aplicando práticas recomendadas ao seu parque de PCs

Como os AI PCs da Dell trazem segurança básica para seu parque de PCs

É nessa área em que o Dell Trusted Workspace pode ajudar. Nossos tecnólogos desenvolvem e projetam a segurança de nossos AI PCs comerciais com profunda compreensão da mentalidade adversária.

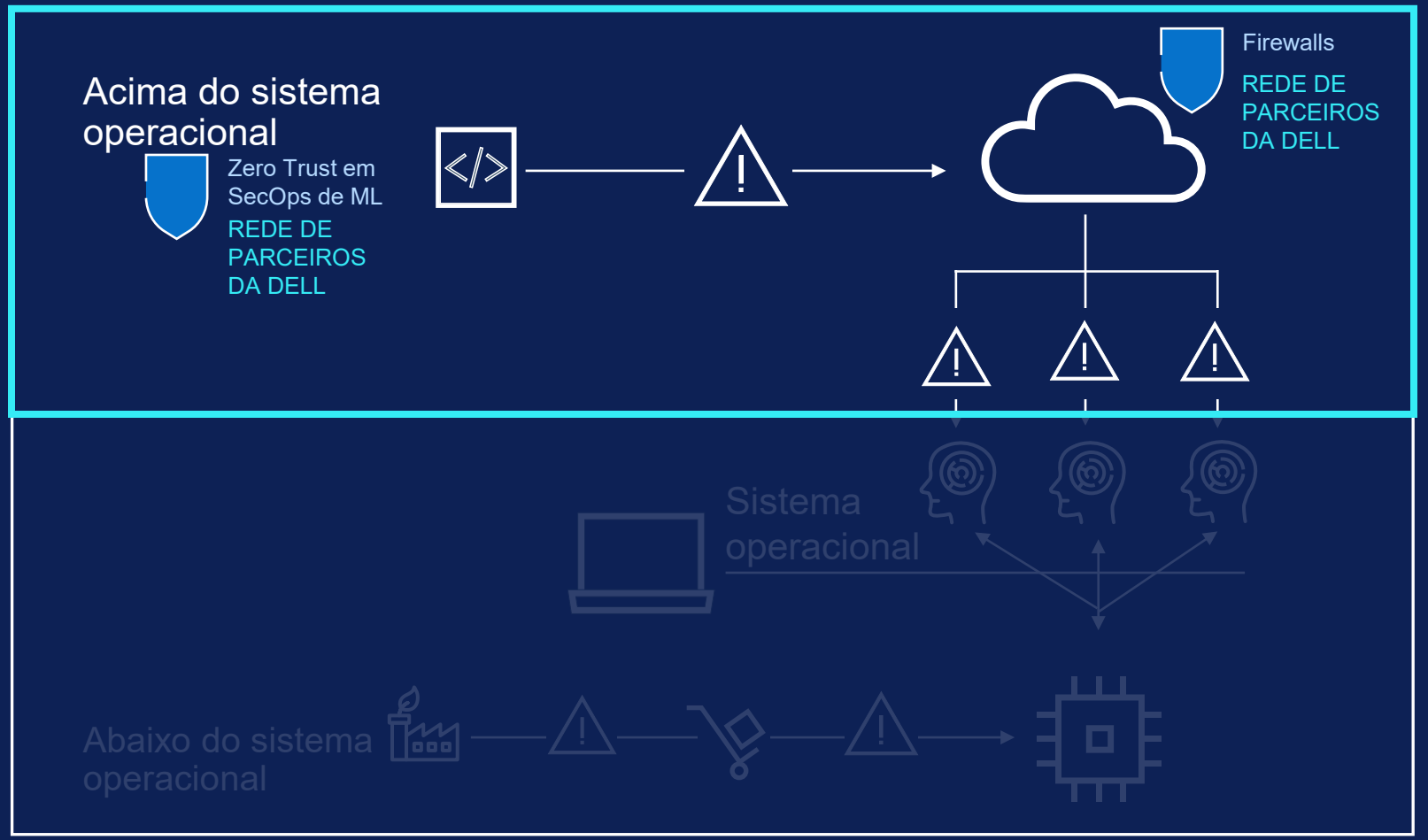
Abaixo do sistema operacional, o design seguro, os sólidos controles da cadeia de suprimentos e a garantia opcional da cadeia de suprimentos garantem que os PCs estejam seguros desde a primeira inicialização.
A segurança integrada de hardware e firmware mantém o PC protegido durante o uso, por exemplo, com detecções exclusivas da Dell* de adulteração no nível do BIOS (Dell SafeBIOS) e segurança de credenciais sem senha (Dell SafeID) para proteger contra acesso não autorizado. Além disso, as tecnologias de chip da Intel® atuam como uma base para proteger vários aspectos da IA, pois são usadas por clients de AI PC. Por exemplo, a Intel ajuda a proteger os dados de IA em repouso no client com aceleração da criptografia de modelos no disco.►

Aplicando práticas recomendadas a seu parque de PCs, continuação

Como os AI PCs da Dell ajudam a levar a segurança básica para seu parque de PCs, continuação

Para complementar essa segurança abaixo do sistema operacional, é possível integrar a tecnologia Absolute Persistence de fábrica para ter maior visibilidade e controle sobre todo o ciclo de vida do PC, permitindo, por exemplo, geolocalização de dispositivos em trânsito e autocorreção de aplicativos essenciais no pior cenário.

De fato, a Dell organizou um ecossistema de soluções de parceiros de software, inclusive CrowdStrike Falcon XDR e Absolute Secure Access, que ativam princípios Zero Trust para proteger sua cadeia de suprimentos modelo para prevenir acessos não autorizados na camada **acima do sistema operacional**. Usando essas soluções, você pode criar e aplicar políticas com controles de acesso granulares (por exemplo, controle de acesso baseado em função ou RBAC) para reduzir o risco de usuários internos mal-intencionados acessarem ou manipularem seus modelos de IA.►



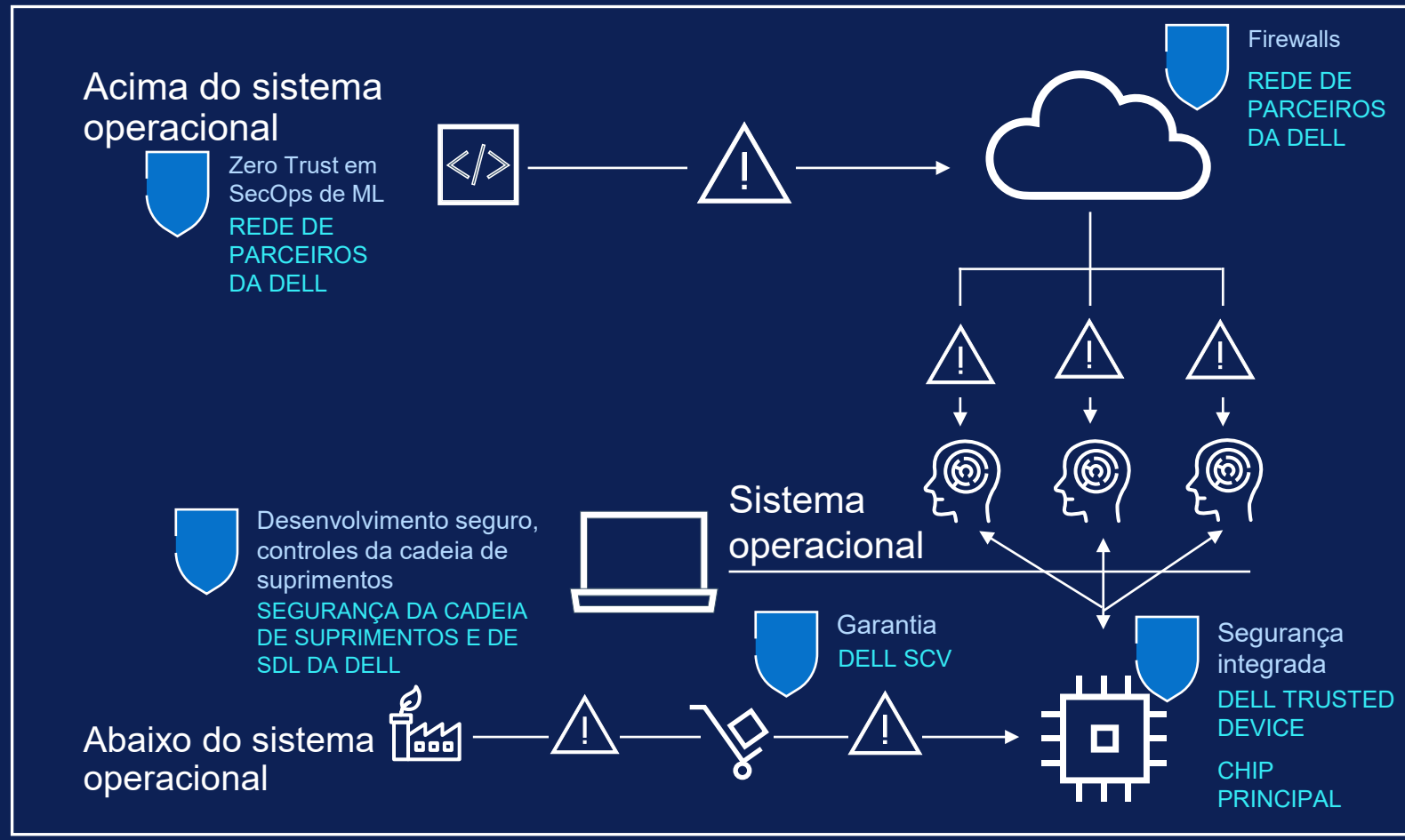
Aplicando práticas recomendadas a seu parque de PCs, continuação

Como os AI PCs da Dell ajudam a levar a segurança básica para seu parque de PCs, continuação

Isso, em conjunto, é a ***segurança para IA***. Esses recursos defendem as cargas de trabalho de IA no dispositivo contra ataques cibernéticos, permitindo que você se concentre na inovação e na conquista de negócios.►

Interrompa ataques avançados ao endpoint com defesas coordenadas de hardware e software

A Dell trabalha com a Intel e a CrowdStrike para integrar as camadas abaixo e acima do sistema operacional com a Segurança assistida por hardware. *Saiba mais >*



Principais conclusões e próximas etapas

Proteja a IA no endpoint com a Dell

As empresas estão entusiasmadas com a IA, mas a prontidão da IA está atrasada, de acordo com uma recente pesquisa de CISOs realizada pela Absolute. Uma análise de milhões de dispositivos revelou uma população de PCs incapaz de absorver novos recursos de IA de forma ampla. **A Dell reúne tudo isso.**

Desenvolva e implemente modelos de IA em uma base segura e moderna. O suporte ao Windows 10 acaba em outubro de 2025. Os PCs não receberão mais atualizações de segurança, atualizações de novos recursos nem suporte ao Windows 10. Os dispositivos mais antigos talvez não atendam aos requisitos do Windows 11 e, portanto, talvez não tenham as melhorias integradas mais recentes de desempenho, segurança e IA. Faça upgrade para o **Dell Pro** ou **Dell Pro Max com base nos processadores Intel® Core™ Ultra com Intel vPro®** para desbloquear os benefícios de segurança e proteger as cargas de trabalho de IA com os **AI PCs comerciais mais seguros do mundo.*** ►

O suporte ao Windows 10 termina em outubro.

Faça upgrade para os AI PCs da Dell mais recentes com Intel para desbloquear benefícios de segurança e aprimoramentos de IA:

Compre o Dell Pro ● Dell Pro Max

*Os AI PCs comerciais mais seguros do mundo**

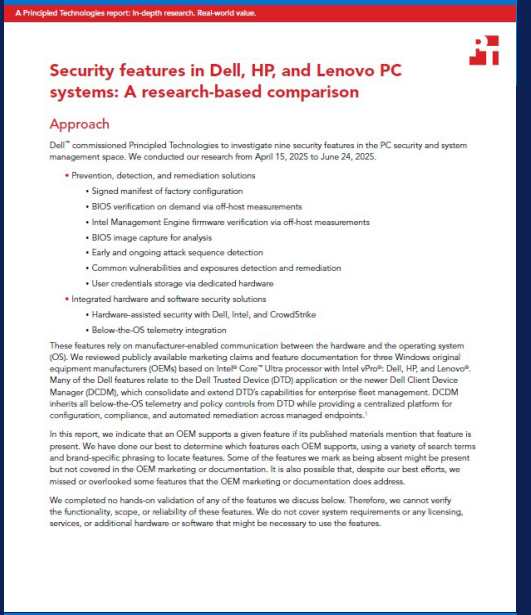
Explore software e serviços de valor agregado para melhorar sua postura de segurança:

Software e integrações

Serviços

LIDERANÇA NO SETOR

A Principled Technologies descobriu que a segurança de AI PCs da Dell e da Intel é superior em comparação com a dos concorrentes


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

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

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) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

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.

Leia a pesquisa

Avisos de isenção de responsabilidade

*Com base em uma análise de terceiros feita pela Principled Technologies, que faz uma comparação entre AI PCs comerciais da Dell com processadores Intel e PCs HP e Lenovo, de julho de 2025. Apoiado pela análise interna da Dell do mercado mundial de PCs, outubro de 2024. Aplicável a PCs com processadores Intel. Nem todos os recursos estão disponíveis em todos os PCs. Compra adicional necessária para alguns recursos.

Para saber mais:

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

Acesse: Dell.com/Endpoint-Security

Siga-nos: LinkedIn @DellTechnologies | X @DellTech

Sobre a segurança de endpoints Dell

A segurança é um tópico assustador para organizações de todos os tamanhos. **Trabalhe com um parceiro experiente de tecnologia e segurança para modernizar a segurança de endpoints**.

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 e aumente a resiliência cibernética 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.