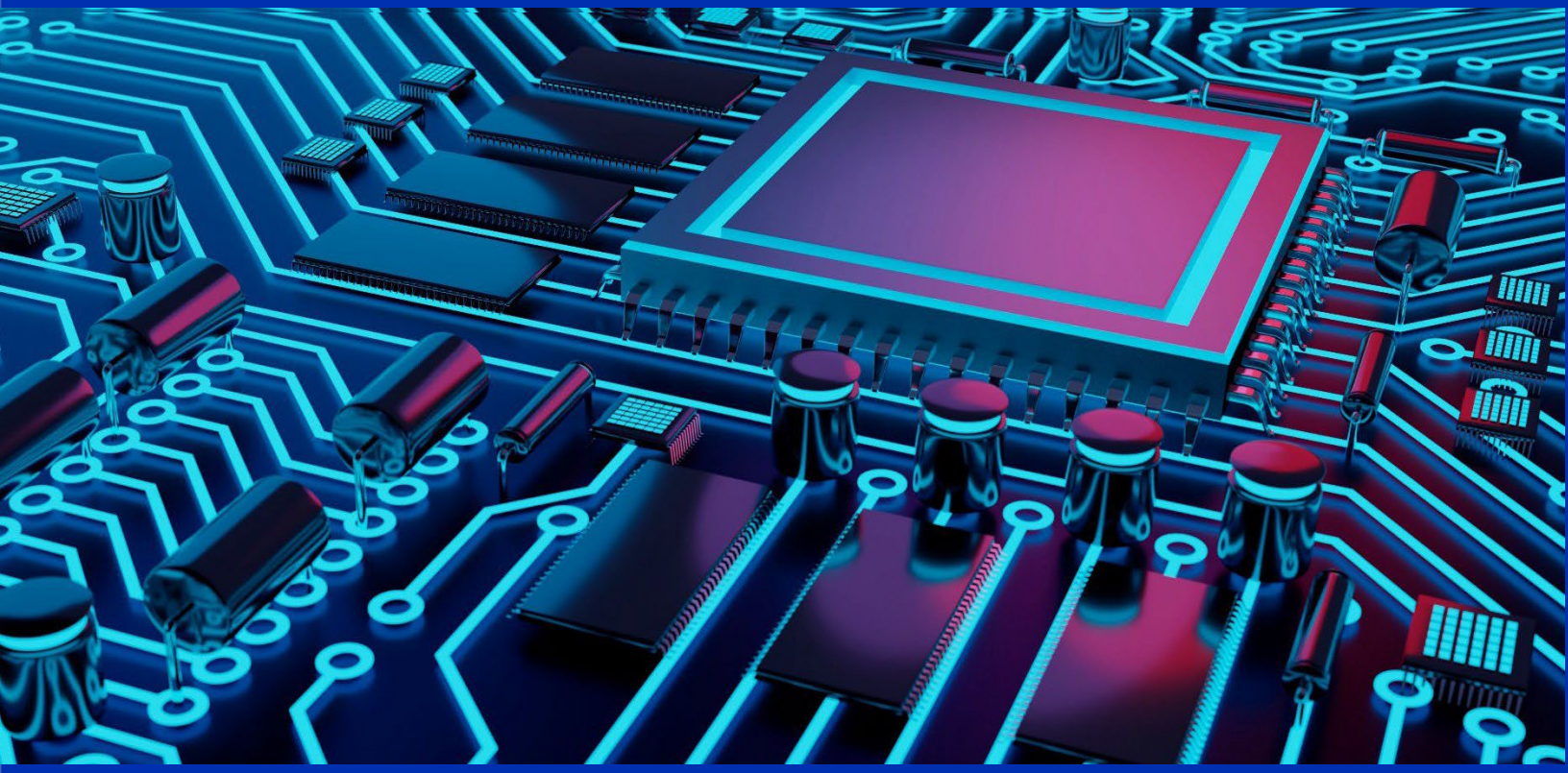
DELL Technologies intel

Conquista da segurança abrangente acima e abaixo do sistema operacional

Os AI PCs* comerciais mais seguros do mundo são fornecidos pela Dell e Intel®. Prepare seu parque de PCs para o futuro e fique à frente dos adversários cibernéticos com múltiplas camadas de defesa.

Julho de 2025



Sumário Executivo

- Manter os dados de negócios seguros é uma tarefa desafiadora, com a complicação da proliferação de endpoints que operam fora da rede organizacional e pela constante evolução dos vetores de ameaças.
- A IA chegou aos dispositivos, expandindo a inovação e também a superfície de ataque. Com centenas de modelos e recursos de IA agora combinados, os dados confidenciais estão em risco de exposição a aplicativos, como os de IA generativa.
- A Dell e a Intel estão comprometidas em manter as redes comerciais de clientes seguras com várias camadas de defesa.
- A Dell combina a segurança integrada de hardware e firmware com as proteções baseadas em chip da Intel para defender os níveis mais profundos de um dispositivo contra ataques básicos.
- Nós reforçamos essas defesas "abaixo do SO" com software inteligente da nossa rede de parceiros para a proteção avançada contra ameaças.
- Além dessa abordagem, a Dell e a Intel investiram em práticas e políticas para ajudar continuamente a proteger as plataformas assim que elas são disponibilizadas no mercado e estão sujeitas a ataques de agentes mal-intencionados.

Tópicos abordados neste documento

Base de segurança

Ciclo de vida de desenvolvimento seguro A Dell e a Intel projetam seus produtos com a segurança como elemento principal e os testam rigorosamente antes do lançamento.

Segurança da cadeia de suprimentos As proteções são implementadas ao longo da cadeia de suprimentos para ajudar a garantir que os dispositivos permaneçam seguros após saírem da fábrica.

Estrutura de defesa abrangente

Segurança integrada: Controles rigorosos da cadeia de suprimentos e garantia opcional ajudam a garantir a segurança dos clientes desde a primeira inicialização.

Segurança integrada:

- Os recursos de segurança baseados em hardware e firmware ajudam a proteger os dispositivos contra ameaças que visam suas camadas básicas, como o BIOS.
- As proteções baseadas em chip proporcionam uma camada fundamental que sustenta a confiabilidade e a credibilidade do AI PC.

Segurança integrada: A segurança baseada em software oferece proteção avançada para endpoints, redes e ambientes de nuvem — fundamental para a segurança moderna de dispositivos.

Suporte contínuo: A Dell e a Intel trabalham para garantir que nossos produtos permaneçam seguros, corrijam vulnerabilidades e atualizem a segurança baseada em chip no sistema operacional.

Principais tendências de segurança

1. No estudo Endpoint Security Market Insights, Forrester Research, Inc., março de 2025, a empresa explica que "Endpoints estão entre os principais alvos de ataques externos de empresas que enfrentaram uma violação nos últimos 12 meses".

2. De acordo com o 2025 Global Threat Report da CrowdStrike, os ataques de malware sem arquivos, o que significa ataques à memória, que são mais difíceis de detectar, agora representam 79% dos ataques.

3. De acordo com um relatório de pesquisa da Enterprise Strategy Group de maio de 2023, 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.

Introdução

Sua rede é tão segura quanto seu endpoint mais fraco

A segurança começa bem antes do que você imagina. Parece que, a cada poucos meses, outra marca global proeminente sofre uma grande violação de segurança e a exposição pública negativa causa grandes danos à sua reputação. Isso já é suficiente para manter proprietários de empresas e profissionais de segurança preocupados, pois eles também podem estar expostos, seja por meio de uma vulnerabilidade ignorada incorporada em seus dispositivos ou por uma fraqueza desconhecida e explorável em seu software. Você pode confiar em sua equipe de TI para proteger suas redes e implementar práticas de segurança de dados, mas como você pode confiar em todos os endpoints e aplicativos que usa para fazer negócios, se não supervisionou a fabricação ou o desenvolvimento deles?

Não basta proteger apenas o software. Uma abordagem comum, porém com falhas, para lidar com a integridade de dispositivos, é tentar criar uma falsa sensação de segurança por meio de soluções somente de software, sem abordar as vulnerabilidades subjacentes baseadas em hardware. É importante que os líderes empresariais entendam as limitações dessa estratégia: ao confiar apenas em software para proteger seus negócios, eles deixam o hardware no qual o software está sendo executado potencialmente vulnerável a ataques. Em essência, se o hardware não for seguro, as tecnologias e os aplicativos de segurança executados nele também não podem ser seguros.

Outros provedores tentam criar um "jardim murado" para proteger dispositivos, onde limitações são incorporadas aos aplicativos e serviços que restringem a flexibilidade do usuário. Embora isso possa fazer sentido no contexto do consumidor, isso tem o custo da liberdade de aproveitar totalmente os dispositivos, um desafio que só é agravado no contexto comercial. Essa abordagem também pode levar os invasores a visar e quebrar cada vez mais esses sistemas para expor vulnerabilidades em configurações comuns.

Em termos simples, o que funciona para dispositivos diretos ao consumidor geralmente falha quando aplicado em um ambiente comercial que representa um alvo mais atraente para os invasores. É por isso que a Dell e a Intel adotam uma abordagem diferente e holística para a segurança. A Dell e a Intel sabem que a única maneira de proteger de forma confiável dispositivos e redes comerciais é por meio da harmonização das tecnologias de segurança de hardware e software funcionando em conjunto. Embora nossas equipes tenham trabalhado juntas para criar uma armadura com recursos de segurança de hardware e software estreitamente integrados, outros provedores podem não ter feito esse investimento.

Segurança baseada em hardware para AI PCs comerciais

Todos os PCs serão AI PCs. O analista de mercado de tecnologia da Canalys prevê que os AI PCs dominarão todo o mercado de PCs nos próximos seis anos. Isso significa que PCs sem recursos de IA integrados não serão mais vendidos até 2030. Essencialmente, para preparar seu negócio para o futuro, você precisa começar agora. A boa notícia: a Dell e a Intel estão ajudando os clientes a navegarem pelo cenário em desenvolvimento de TI e segurança com AI PCs comerciais que contam com proteção, velocidade e eficiência integradas, fundamentais e necessárias para combater as ameaças modernas.

Mas essa não é uma tarefa fácil. As complexidades e preocupações de proteger dispositivos e redes são suficientes para deixar você atordoado. Além disso, as tecnologias emergentes de IA tornaram essa área ainda mais complexa. É por isso que nossa missão é disponibilizar aos clientes dispositivos projetados com a segurança em mente, a fim de permitir que eles se concentrem no que realmente importa: fazer negócios. A relação de engenharia conjunta da Dell e da Intel se estende por várias décadas e sempre se concentrou em manter os dados de nossos clientes seguros, especialmente no mercado business-to-business. Por meio de sua parceria com a Intel, a Dell estabeleceu uma reputação como principal provedor de dispositivos de funcionários para empresas de todos os portes e em todos os mercados. O que compõe um dispositivo de IA comercial da Dell? É mais do que um conjunto desordenado de recursos, a Intel e a Dell desenvolvem tecnologias, ferramentas e políticas ao longo do ciclo de vida do PC comercial para ajudar a fornecer segurança completa para os clientes e seus negócios.

Segurança por padrão

A Intel e a Dell olham além das ameaças atuais ao projetar os sistemas do futuro para minimizar a superfície de ataque e ajudar a garantir que os dispositivos comerciais permaneçam seguros.

Proteção em trânsito

Temos tecnologias e políticas em vigor para ajudar a proteger a integridade dos dispositivos antes que eles cheguem às suas mãos, ajudando a manter a segurança durante o fornecimento, a montagem e a entrega de componentes.

Defesa contra as ameaças em evolução

Empregamos segurança baseada em hardware por meio dos Dell Trusted Devices e dos recursos de segurança Intel vPro® para fortalecer os dispositivos que lidam com casos de uso primários de segurança cibernética para prevenção, detecção, resposta, recuperação e correção. Além disso, a Dell e a Intel têm equipes de segurança dedicadas para sondar os próprios produtos e encontrar novas vulnerabilidades antes dos invasores, lançando patches rapidamente para ajudar a manter você e sua equipe protegidos.

Neste white paper, exploraremos como a Dell e a Intel trabalharam juntas para produzir plataformas de AI PCs comerciais com segurança integrada nos níveis mais profundos, ajudando a proteger os dispositivos durante todo o ciclo de vida, na próxima renovação e assim por diante.

Segurança cibernética e IA generativa, uma faca de dois gumes

Assim como os defensores cibernéticos usam a IA generativa para o bem, os criminosos cibernéticos recorrem à essa tecnologia para promover os próprios objetivos mal-intencionados, lançando ataques mais sofisticados com grande rapidez e em escala.

Embora os casos de uso da IA generativa ainda estejam em sua fase inicial e se expandindo diariamente, é importante manter alguns conceitos-chave em mente. Primeiro, há uma série de ameaças que a IA generativa pode representar para as organizações incluindo:

- Problemas de integridade e privacidade de dados
- Problemas de conformidade
- E violação de propriedade intelectual

Além disso, vemos várias maneiras pelas quais a IA generativa poderá ajudar na luta pela segurança, incluindo, entre outras:

- Detecção de ameaças avançadas
- Treinamento especializado e focado para funcionários e
- Automação

A Dell e a Intel estão trabalhando ativamente para permitir uma melhor modelagem de ameaças específica para IA generativa. Isso pode incluir prevenção contra perda de dados, gerenciamento de direitos de dados, phishing avançado, adulteração de modelos, regulamentação e conformidade, tudo com a aplicação dos controles apropriados.

A Dell também pode ajudar você a testar seu cenário da IA generativa em termos de segurança com programas de testes de penetração e gerenciamento de vulnerabilidades para acompanhar o cenário de ameaças em constante evolução.

Base de segurança

Ciclo de vida de desenvolvimento seguro

A proteção de nossas plataformas começa no quadro branco

Planejamento, avaliação e análise

Antes de as plataformas e os chipsets mais recentes serem desenvolvidos, os especialistas da Dell e da Intel, respectivamente, definem parâmetros rígidos para o que uma plataforma segura precisa incluir para atender às necessidades futuras de segurança e cumprir as normas obrigatórias de segurança. Esse processo começa com uma determinação em mesa redonda dos prováveis riscos futuros de segurança e privacidade e as atividades necessárias para resolvê-los. Essa avaliação é usada para definir os objetivos de segurança com os quais analisaremos nossas arquiteturas. Com essas informações, as equipes de segurança da Dell e da Intel desenvolvem modelos de ameaças com uma abordagem antagônica dessa arquitetura conceitual, fazendo uma sondagem em busca de possíveis vulnerabilidades e explorações que precisarão ser mitigadas. Este exercício provou dar grande melhorias para encontrar e mitigar possíveis vulnerabilidades no BIOS, firmware e design de hardware.

Design centrado na segurança

Depois que as avaliações de ameaças são concluídas e os modelos são criados para definir qual é a superfície da ameaça e onde os testes devem ser focados, os engenheiros começam a desenvolver o código do produto. Os objetivos de segurança definidos na etapa anterior fornecem orientação durante esta fase de desenvolvimento e servem como critérios para determinar se o produto está no caminho certo para atender às necessidades de nossos clientes.

Verificação e teste

Depois que o código é refinado a ponto de satisfazer os objetivos de segurança estabelecidos no início do ciclo de vida de desenvolvimento, o produto segue para um rigoroso processo de teste. Esses testes geralmente começam com revisões seguras de código e análise estática de código, um processo automatizado que usa ferramentas especiais para encontrar e corrigir defeitos. Alguns produtos com código mais complexo exigem um processo de revisão manual, no qual especialistas em segurança realizam revisões linha por linha do código do produto para encontrar erros até então desconhecidos e ajudar a garantir que ele tenha sido projetado de forma segura. Por fim, as equipes de hackers especialistas são orientadas a realizar testes de penetração e outras atividades de "red team" para encontrar possíveis vulnerabilidades que não foram observadas nas fases anteriores. Esses resultados são mitigados novamente com base no risco, para que qualquer exposição adicional identificada seja documentada e corrigida.

Lançamento e pós-lançamento

Depois que o produto é rigorosamente testado e atende ou excede os objetivos de segurança definidos no início, ele está pronto para lançamento no mercado. No entanto, essas fases representam apenas uma parte do ciclo de vida de desenvolvimento seguro. Para a Dell e a Intel, manter a segurança de nossas plataformas é um esforço contínuo. Nossas equipes trabalham para descobrir vulnerabilidades antes que elas possam ser exploradas por invasores e, em seguida, desenvolvem e lançam atualizações de segurança para corrigi-las. Um exemplo do compromisso da Dell e da Intel com a segurança de ponta a ponta é o investimento em uma cadeia de suprimentos segura entre a montagem e a entrega de um dispositivo, um dos vetores de ataque que mais crescem para agentes mal-intencionados. Na próxima seção, examinaremos como a Dell e a Intel mitigam os riscos ao longo das próprias cadeias de suprimentos para ajudar a garantir que o dispositivo entregue para você esteja seguro desde a primeira inicialização.

Segurança da cadeia de suprimentos

A garantia da cadeia de suprimentos é fundamental para a segurança dos dispositivos

Muita coisa pode acontecer entre o momento em que um componente ou dispositivo sai da fábrica e chega ao seu destino. Cada etapa da cadeia de suprimentos representa um novo vetor que expõe seus funcionários, sua empresa e seus clientes a possíveis ataques. A Dell e a Intel desenvolveram ferramentas, tecnologias e processos para ajudar a garantir a segurança dos produtos antes que eles cheguem ao cliente e permitir a verificação automática da autenticidade do dispositivo antes de serem implementados para os funcionários.

Source
A Dell emprega um rigoroso processo de triagem de parceiros para ajudar a garantir a qualidade e a segurança dos dispositivos e seus componentes. Esses parceiros também passam por auditorias de rotina para garantir a conformidade com o conjunto abrangente de Padrões de segurança da cadeia de suprimentos da Dell.

Fabricação
Além de aderir aos Padrões de segurança da cadeia de suprimentos da Dell, os fabricantes de dispositivos Dell também testam peças com frequência durante a fabricação para garantir que produtos falsificados não entrem na cadeia de suprimentos. Para mitigar ainda mais esse risco, etiquetas com números exclusivos de identificação de peça (PPID) são afixadas em componentes específicos de alto risco, contendo informações sobre o fornecedor, o número de peça, o país de origem e a data de fabricação para que a Dell possa identificar, autenticar, rastrear e, por fim, validar esses componentes, garantindo que o cliente receba exatamente o que foi enviado.

Entrega
As cargas da Dell são protegidas durante o transporte por camadas de segurança física, desde lacres invioláveis e mecanismos de travamento de portas até uma variedade de dispositivos de rastreamento, desenvolvidos para detectar se os dispositivos Dell foram adulterados durante o transporte.

Os próprios dispositivos Dell também oferecem tecnologias de detecção de violação. As soluções Dell SafeSupply Chain abrangem controles de segurança e integridade da cadeia de suprimentos, como lacres invioláveis e limpezas de disco rígido no nível NIST, para ajudar a garantir que você tenha uma placa limpa para poder adicionar sua imagem corporativa.

Verificação
Os dispositivos comerciais de IA Dell são enviados com certificados de plataforma autenticados por criptografia que registram atributos de snapshot das plataformas durante a fabricação, a montagem, os testes e a integração. Esses atributos de plataforma são então vinculados por criptografia ao dispositivo específico usando o Trusted Platform Module (TPM) como a raiz de confiança do hardware.

Saiba mais sobre os esforços conjuntos da Dell e da Intel para proteger a cadeia de suprimentos. Assista à entrevista ***com a SiliconANGLE***

A Dell implementou certificados de plataforma do Trusted Computing Group (TCG) na solução Dell Secured Component Verification (SCV) para AI PCs comerciais com processadores Intel (certificado disponível no dispositivo para organizações federais e na nuvem para clientes comerciais). A SCV fornece certificados de inventário assinados criptograficamente para a TI para dispositivos Dell compatíveis. Com ferramentas seguras de verificação automática, a solução SCV* exclusiva da Dell ajuda a garantir a integridade total do hardware durante o transporte para ambientes de TI e permite que os clientes verifiquem se os AI PCs comerciais e os principais componentes da Dell chegaram conforme foram solicitados e fabricados.

Estrutura de defesa abrangente

Segurança abaixo do SO

As tecnologias de segurança integradas ajudam a prevenir, detectar, responder e se recuperar de ameaças

Segurança holística significa ir além do modelo legado de software que protege o software para acompanhar novas categorias de ameaças contra segurança, proteção e privacidade digitais. Combinando esse componente com a tecnologia de segurança "abaixo do SO" baseada em hardware, é possível proteger cada camada da pilha de computação trabalhando para prevenir e detectar ataques básicos, incluindo variantes de ameaças que ocorrem com mais frequência ao longo da cadeia de suprimentos. A relação de engenharia conjunta da Dell e da Intel tem se concentrado em cobrir essa superfície de ataque com uma complexa trama de tecnologias, tanto no nível de componentes quanto de plataforma.

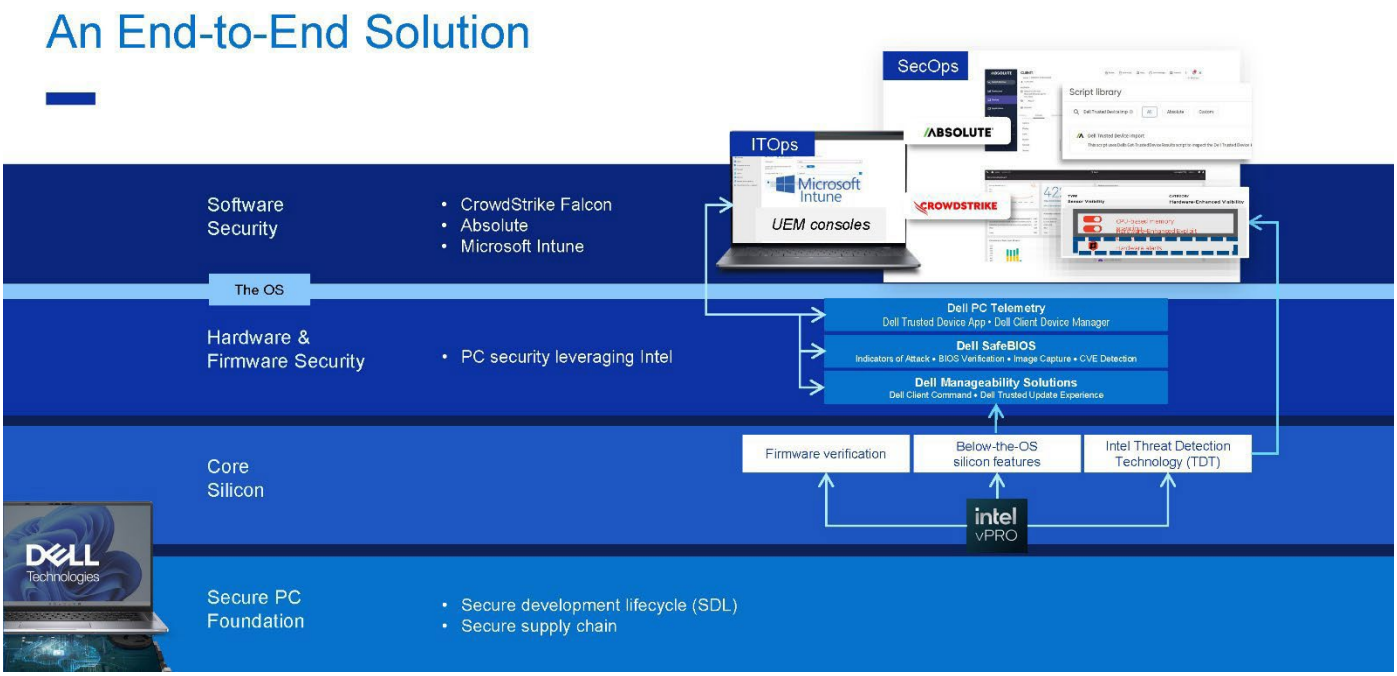


Figura 1: Hoje, uma segurança eficaz requer várias camadas de contramedidas para ataques. A Dell e a Intel trabalham com parceiros de software para fornecer defesa em profundidade.

Abordamos a cadeia de suprimentos e a base de segurança em AI PCs que a Dell e a Intel oferecem. Agora, vamos analisar as camadas intermediárias.

Intel vPro® Security

O Intel vPro Security está incluído em todos os dispositivos comerciais Dell executados na plataforma Intel vPro® e oferece recursos de segurança aprimorados por hardware que ajudam a proteger todas as camadas da pilha de computação. Esse conjunto de tecnologias de segurança ajuda a proteger os dispositivos contra ameaças modernas, em cada uma das camadas: hardware, BIOS/firmware, hipervisor, VMs, SO e aplicativos.

Segurança integrada de hardware e firmware Dell

A proteção do Sistema Básico de Entrada/Saída (BIOS) é fundamental para a segurança dos dispositivos. Se um invasor conseguir corromper o BIOS de um dispositivo, ele poderá obter o controle de todo o dispositivo devido à posição única e privilegiada do BIOS dentro da arquitetura do dispositivo. Para proteger essa camada crítica, os dispositivos comerciais de IA Dell são enviados com o SafeBIOS, um conjunto de segurança em camadas no nível do firmware. Os recursos subjacentes que constituem o SafeBIOS aprimoram a proteção, a detecção e a recuperação no nível do BIOS.

Figura 2: De acordo com a Principled Technologies, a Dell e a Intel oferecem os AI PCs comerciais mais seguros do mundo.*

Também é importante observar que uma segurança eficaz inclui visibilidade da postura de segurança atual. A Dell torna esses eventos abaixo do SO no SafeBIOS visíveis no nível do SO para que os administradores e usuários finais possa visualizá-los e tomar as devidas decisões com o aplicativo Dell Trusted Device (aplicativo DTD).
O aplicativo DTD detecta se o BIOS foi comprometido comparando as medições da imagem do BIOS em execução com a cópia definitiva protegida no ambiente Dell, garantindo nossa verificação diferenciada do BIOS fora do host. Além disso, a verificação de firmware do Intel Management Engine (ME), disponível exclusivamente em PCs comerciais da Dell, protege contra acesso não autorizado e adulteração de firmware altamente privilegiado.

Essa telemetria de PC exclusiva da Dell (disponível por meio do Dell Client Device Manager (DCDM) para ambientes de TI gerenciados ou do console do aplicativo DTD para ambientes não gerenciados) é segredo na equação de segurança. Essa telemetria permite a integração com consoles de terceiros, como CrowdStrike e Absolute para segurança e Microsoft Intune para gerenciamento (consulte a Figura 1). De fato, a Dell é a única fabricante de PCs a fornecer integração e visibilidade de detecção de ameaças em nível de firmware por meio de consoles de segurança de terceiros*

A Dell também reduz o risco crescente de comprometimento de identidade e acesso não autorizado a cargas de trabalho confidenciais. Os dispositivos comerciais selecionados da Dell incluem o Dell SafeID com ControlVault 3+, um chip de segurança com certificação FIPS 140-3 exclusivo de nível 3* que armazena as credenciais do usuário final, isolando-as do sistema operacional e tornando-as muito menos vulneráveis a ataques.

A segurança abaixo do sistema operacional é apenas uma parte da abordagem holística que a Dell adota para proteger dispositivos

Para proteger mais completamente os dispositivos comerciais de IA Dell, a Dell e a Intel também investiram pesado na verificação e na seleção de um ecossistema de soluções de segurança de software líderes do setor. Esses recursos fornecem proteção contra ameaças avançadas representadas por invasores sofisticados, oferecendo uma camada adicional de segurança na camada de dados e aplicativos.

Mais uma vez, a Dell e a Intel podem enriquecer as tecnologias de software com telemetria de PC abaixo do SO para melhorar a detecção de ameaças e as respectivas respostas.

Acima da segurança do sistema operacional

A segurança de software integrada oferece proteção contra ameaças avançada

Devido ao possível retorno financeiro de apenas uma violação bem-sucedida, os invasores virtuais são altamente motivados, muitas vezes fazendo dezenas de tentativas em um único dispositivo ao longo da vida útil dele. Agravado pelo parque de PCs de uma organização, isso representa uma séria preocupação. Você acha que existe a chance de um ataque conseguir escapar da detecção? Neste ponto, uma coisa é certa: nenhuma solução pode bloquear 100% dos ataques. Isso se refere aos endpoints do seu parque de PCs, bem como às redes e ambientes de nuvem em que operam.
As soluções de software inteligentes podem ajudar a prevenir, detectar, responder e se recuperar de ameaças onde quer que elas ocorram. Para isso, o portfólio de segurança de endpoints do Dell Trusted Workspace inclui software líder do setor para simplificar a aquisição e fornecer aos líderes de negócios tudo o que eles precisam para defender seus endpoints. Os recursos incluem:

- Prevenção, detecção, resposta e remediação em ambientes de endpoint, rede e nuvem, aproveitando a IA e o aprendizado de máquina
- Geolocalização de endpoints, geofencing, limpeza remota de dados, bem como autocorreção de aplicativos críticos, dentro ou fora da rede
- Soluções Security Service Edge para uma abordagem centrada em dados para segurança e acesso à nuvem, protegendo dados e usuários em todos os lugares

Os recursos de segurança da Intel, integrados no chip, como o Intel Control-flow Enforcement Technology, protegem os dispositivos contra ataques direcionados ao SO, enquanto outros recursos do Intel vPro® Security ajudam a fazer a segurança abaixo do SO, resguardar aplicativos e dados e oferecer proteções avançadas contra ameaças.

Segurança assistida por hardware

Segurança integrada

Os invasores estão cada vez mais direcionando seus esforços para toda a pilha de computação da organização, que tradicionalmente não tem visibilidade nem controle. Essas ameaças em evolução estão contornando as legadas ferramentas de segurança de software de resposta e detecção de endpoint (EDR). Por isso, a segurança do PC é tão importante. Para ficar à frente das ameaças modernas e em rápida evolução, é preciso uma profunda colaboração no ecossistema para conectar adequadamente as proteções de superfície de ataque entre fornecedores em uma solução coesa.

No entanto, esse trabalho de integração de back-end é complexo e consome muito tempo e recursos. Para ajudar a resolver isso, a Dell e a Intel aproveitaram nosso profundo conhecimento dos pontos problemáticos do adversário e do cliente para trabalhar com parceiros para desenvolver uma solução integrada de hardware e software chamada "Segurança assistida por hardware". Além de a Dell oferecer AI PCs seguros e firmar parceria com os principais fornecedores de software, a telemetria exclusiva de dispositivos* da empresa enriquece todo o ecossistema de segurança, proporcionando maior visibilidade no nível do BIOS para seu parque de PCs. Essa capacidade de integração é fundamental para fechar a lacuna de segurança de TI com a qual tantas organizações enfrentam atualmente. Com a Dell, a Intel e nossa rede de parceiros, o hardware e o software se comunicam, melhorando a segurança e a capacidade de gerenciamento de toda o parque de PCs.

Figura 3: As ameaças cibernéticas em evolução contornam defesas baseadas apenas em software. Ajude a reduzir a superfície de ataque de endpoints com segurança assistida por hardware.

Destaque para a segurança assistida por hardware com a Dell, a Intel e a CrowdStrike

A Dell, a Intel e a CrowdStrike projetaram em conjunto recursos de detecção e respostas a ameaças que combinam o poder dos Dell Trusted Devices, os AI PCs comerciais mais seguros do mundo,* com os recursos de chip da Intel e as plataformas da CrowdStrike, protagonistas no Quadrante Mágico da Gartner 2024. Trabalhando juntas, a CrowdStrike, a Dell e a Intel desenvolveram uma solução em camadas que reinventa a segurança de endpoints para sua empresa, indo além das proteções de software para incorporar segurança assistida por hardware.

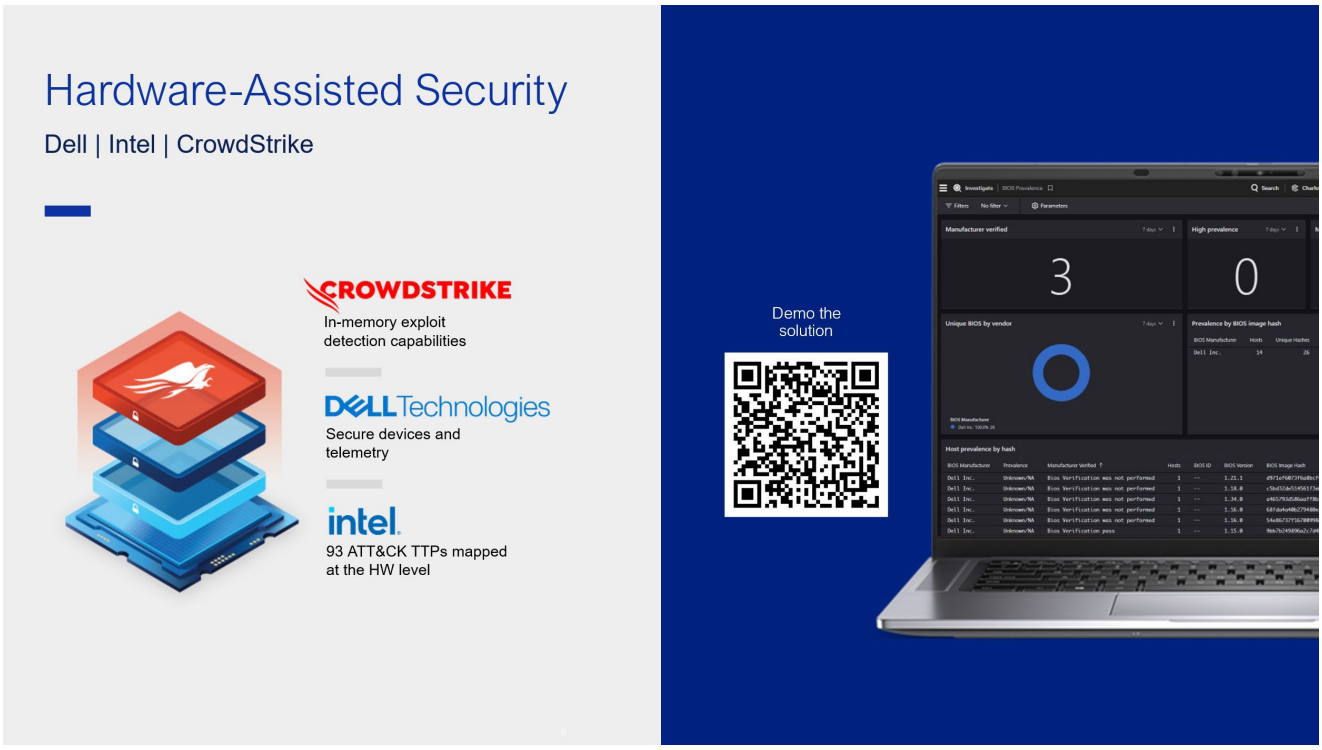


Figura 4: Segurança multicamadas em AI PCs comerciais Dell, com integração com a CrowdStrike e a Intel.

Valor adicional da integração entre a Intel e a CrowdStrike em AI PCs Dell

Aprimoramento da segurança de endpoints por meio da aceleração de NPU/GPU e IA: As ameaças cibernéticas estão ficando cada vez mais avançadas. Dessa forma, os AI PCs foram desenvolvidos para ficarem à frente usando IA no dispositivo para detectar ameaças em tempo real com mais rapidez e, ao mesmo tempo, reduzir a dependência dos serviços em nuvem. Ferramentas como a CrowdStrike podem redirecionar a detecção de malware para as unidades de processamento neural (NPUs) integradas, detectando ameaças mais rapidamente com impacto mínimo no desempenho da CPU. Com processamento de dados locais e recursos avançados antiphishing em AI PCs baseados em Intel, as informações confidenciais permanecem seguras, reduzindo a exposição a riscos externos.

Alguns exemplos do trabalho da Intel e da CrowdStrike (está em fase de prova de conceito no momento, mas estará disponível publicamente nos próximos meses) para promover a segurança de endpoints por meio da aceleração de NPU e IA:

- Detecção de exploração aprimorada por hardware (HEED): usa a telemetria de CPU Intel para acompanhar o fluxo de controle de aplicativos e identificar ataques à memória.
- Verificação de memória acelerada (AMS): usa o Intel Threat Detection Technology para redirecionar a verificação intensiva de memória de computação para a GPU integrada Intel, com capacidade de verificação de memória sete vezes maior.

Com esses dois recursos, a Intel é fundamental para alimentar indicadores de capacidade de ataque baseados em IA da CrowdStrike, presentes no endpoint e na nuvem de segurança da CrowdStrike. Esses recursos também oferecem uma nova perspectiva sob a camada de memória, permitindo que a CrowdStrike incorpore novos modelos de detecção por varredura no futuro, aprimorando a segurança ao longo do tempo.

Defesa validada pelo setor da segurança de AI PCs: Uma nova pesquisa da MITRE comprova que sua escolha de hardware de PC desempenha um papel fundamental na habilitação de software de segurança e recursos de SO para proteger seus ativos de forma eficaz.

As equipes de operações de segurança (SecOps) implementam agentes poderosos em parques de PCs de endpoint para inspecionar sinais de malware em todos os processos. Os fornecedores de software de segurança mapearam seus recursos para a estrutura MITRE ATT&CK para mostrar onde eles fornecem soluções. Os provedores de segurança gerenciados ajudam as empresas na triagem de alertas diários em ferramentas de segurança XDR, SIEM e Co-pilot. Bastante sofisticação, mas a aplicabilidade da segurança de hardware para ataques reais, nos PCs que você já possui, tem sido um mistério... até agora.

No final de 2024, o Center for Informed Defense* (CTID) da MITRE colaborou com mais de trinta especialistas da Intel, Microsoft, CrowdStrike e ATTACK IQ para mapear e classificar o significado dos recursos de software de segurança otimizados por hardware com relação a táticas e (sub) técnicas da estrutura MITRE ATTACK. Em conjunto, o grupo mapeou os recursos do Intel vPro® Security com 150 táticas, (sub) técnicas e procedimentos (TTPs) de ameaças exclusivas e cumulativas, em que o hardware do PC oferece proteções integradas com software de segurança otimizado.

Para a validação de teste de mapeamento e emulação, a MITRE utilizou um Dell Pro com um processador Intel Core Ultra (incluindo o conjunto completo de proteções de segurança Intel vPro habilitado em uma pilha típica de software de segurança de classe empresarial), o que enriquece as defesas integradas, exclusivas e abaixo do sistema operacional da Dell.

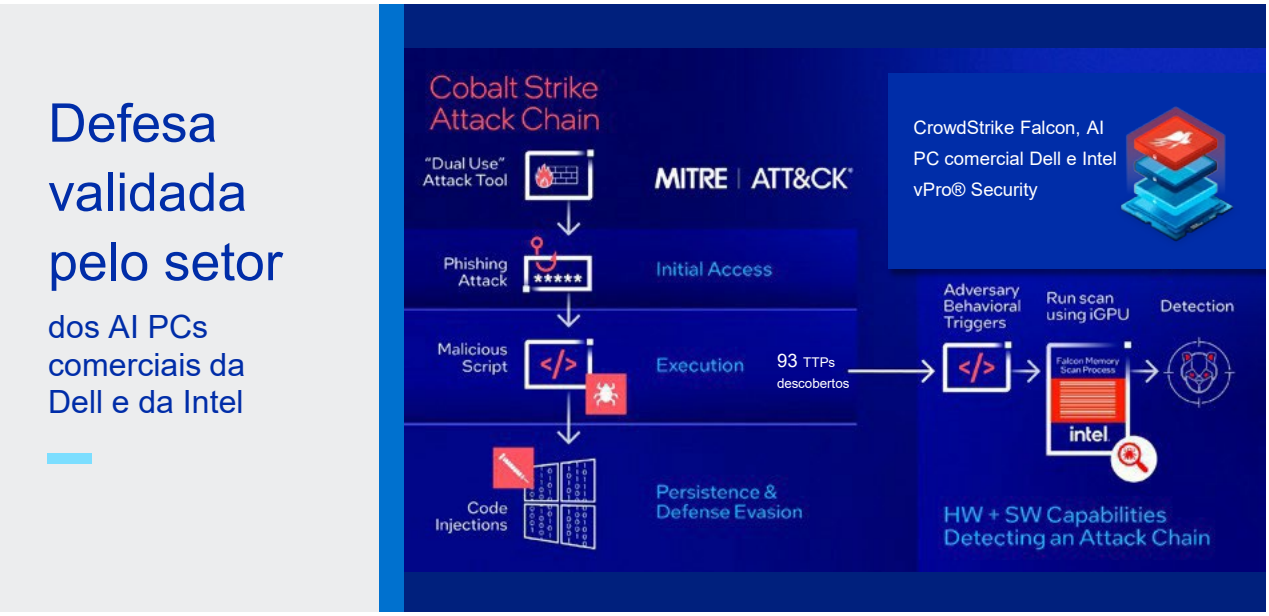


Figura 5: A segurança assistida por hardware funciona.

No cenário de exemplo (cenário de cadeia de ataques do Cobalt Strike), mostramos um ataque sem arquivos do Cobalt Strike à memória e como o CrowdStrike Falcon possibilita mitigações usando hardware. Como mencionado anteriormente, os ataques de malware sem arquivos se tornaram populares entre os adversários. Quase 75% de todos os tipos de ataque abusam de processos válidos do sistema, como a execução na memória, para poderem escapar das defesas tradicionais do EDR. Esta é uma ilustração clara de como o hardware do seu PC ajuda a fornecer o poder de computação incremental necessário para verificar a memória sem interromper a experiência de computação do usuário. **Para a CrowdStrike, que utiliza os algoritmos de verificação de memória acelerada da Intel Threat Detection Technology (Intel TDT) e sua capacidade de redirecionar o processamento para o processador de placa gráfica integrada da tecnologia de placas gráficas Intel, isso resulta em uma aceleração de desempenho de até 7x, o que ajuda a garantir uma boa experiência do usuário, ao mesmo tempo em que oferece a capacidade de verificação mais profunda e descoberta de mais de 93 TTPs.** (Nota: O recurso de verificação de memória da CrowdStrike, desenvolvido em seu software, funciona apenas em PCs Intel vPro.)

Ter insights sobre medidas de segurança baseadas em software e hardware pode ajudar as empresas a liberar todo o potencial disponível em AI PCs modernos. Os resultados comprovam que a escolha do hardware do PC tem um impacto significativo na capacidade do software de segurança e dos recursos do sistema operacional de combater ameaças específicas e proteger os ativos corporativos contra adversários cibernéticos avançados.

As estruturas de segurança acima e abaixo do SO da Dell e da Intel oferecem uma abordagem holística para proteger dispositivos comerciais. No entanto, como especialistas em segurança, sabemos que nenhum dispositivo está totalmente seguro. É por isso que somos líderes do setor em investimentos em segurança pós-lançamento para ajudar a garantir que nossos dispositivos permaneçam seguros por anos após o lançamento.

Suporte contínuo

A Dell e a Intel investem na segurança contínua de suas plataformas após o lançamento

A Dell e a Intel fizeram investimentos significativos e sustentados para ajudar a garantir a segurança durante todo o ciclo de vida de um produto. Assim que um dispositivo ou plataforma é lançado no mercado, as equipes da Dell e da Intel continuam a examinar ativamente seus produtos em busca de vulnerabilidades. Para a Intel, esse processo inclui trabalhar em conjunto com pesquisadores e universidades para encontrar possíveis explorações antes que os agentes mal-intencionados o façam, corrigir rapidamente quaisquer vulnerabilidades encontradas e denunciá-las depois que a brecha de segurança for fechada.

A garantia proativa de segurança do produto inclui esforços para encontrar vulnerabilidades internamente e por meio de incentivos à comunidade externa de pesquisa de segurança por meio de programas Bug Bounty. Em 2024, o investimento da Intel em garantia proativa de segurança do produto foi responsável por 96% das vulnerabilidades descobertas e mitigadas. As vulnerabilidades restantes de 4% abordadas pela Intel não foram enviadas pelo programa Intel Bug Bounty ou foram enviadas por parceiros ou outras organizações que não buscam pagamentos de recompensa. Em todos os casos, a Intel trabalhou com pesquisadores para coordenar a divulgação pública desses problemas, o que significa que as mitigações estavam disponíveis para os clientes na data da divulgação pública.

Para lidar com vulnerabilidades e exposições comuns (CVEs) encontradas por meio de seus extensos programas, a Intel distribui regularmente as atualizações da plataforma Intel para todos os sistemas executados em seus produtos. Esse processo trimestral consiste em atualizações de segurança, de funções e de recursos em microcódigo, firmware e BIOS do sistema. Atualizações regulares permitem que os parceiros da Intel validem e integrem atualizações de hardware e firmware em suas plataformas em um cronograma trimestral previsível, levando à divulgação pública coordenada em todo o ecossistema.

A coordenação da divulgação e da resposta às vulnerabilidades identificadas do produto é realizada pelas equipes dedicadas da Dell e da Intel de resposta a incidentes de segurança de produtos. Juntos, eles trabalham para ajudar a garantir que vulnerabilidades e exposições comuns sejam tratadas com rapidez e segurança, mitigando efetivamente quaisquer riscos que possam representar.

A Dell e a Intel fizeram esses investimentos para oferecer suporte contínuo aos nossos clientes e aliviar a carga de suas equipes de TI. Contratamos pesquisadores, arquitetos de segurança e analistas forenses cibernéticos para ajudar a manter seus negócios seguros e permitir que suas equipes se concentrem em equipar seus funcionários para fazer o melhor trabalho possível.

Contas de investimentos da Intel para 96% das vulnerabilidades abordadas em 2024

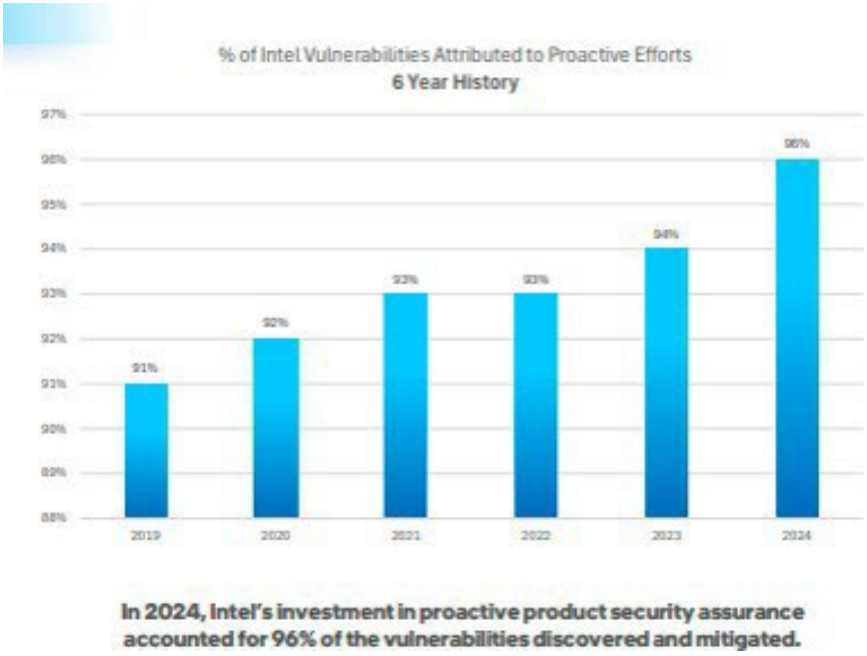
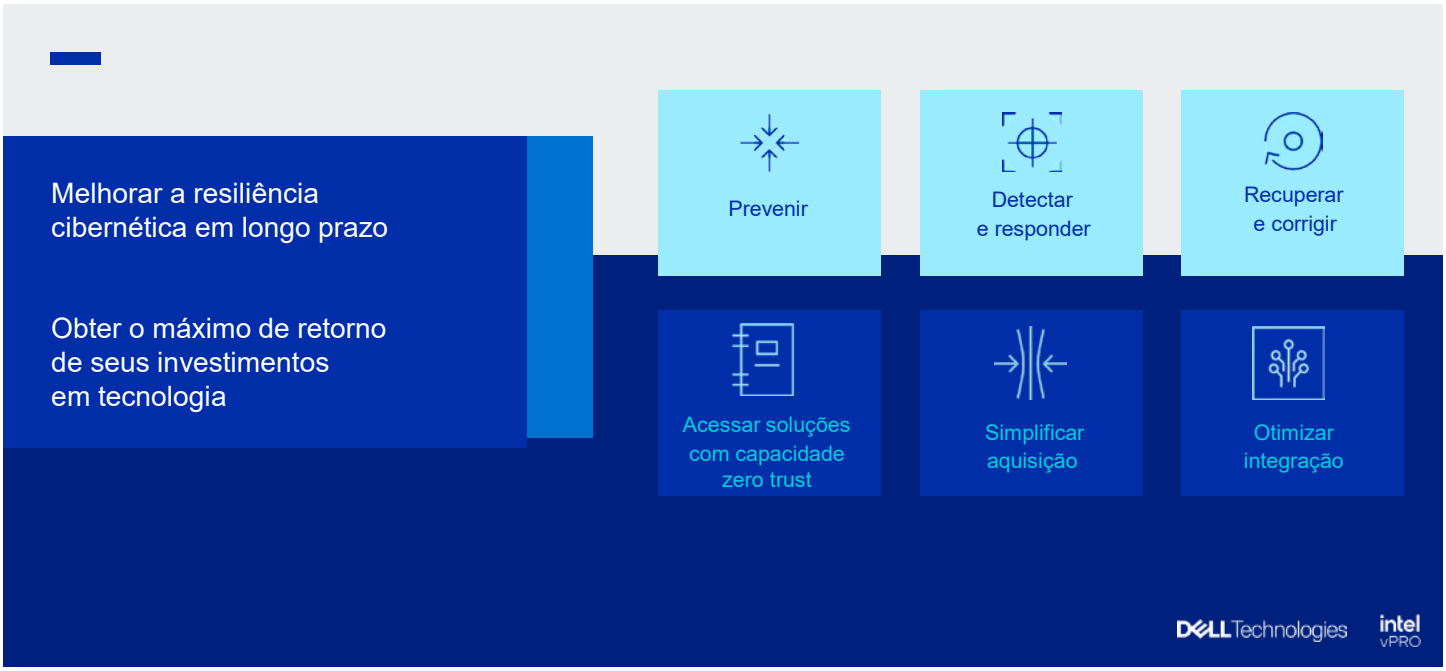


Figura 6: % de vulnerabilidades da Intel atribuídas a esforços proativos (fonte: Relatório de segurança do produto Intel de 2024)

Conclusão

Os resultados de trabalhar com a Dell e a Intel



A Dell e a Intel estão concentradas em resultados de segurança e no desenvolvimento de soluções baseadas na mentalidade adversária. Um objetivo final fundamental para adversários cibernéticos: dinheiro, que eles ganham roubando dados e vendendo-os ou mantendo-os reféns. Portanto, embora o método de entrada varie, (a estrutura MITRE ATT&CK® rastreia nove métodos gerais de acesso inicial), as cadeias de ataque cibernético seguem padrões muito semelhantes: reconhecimento, acesso inicial (explorando qualquer vulnerabilidade, fraqueza, exposição ou erro que encontrarem), infiltração em uma rede, movimentação lateral/obtenção de acesso privilegiado e espionagem do ambiente para aprender mais e extrair dados.

Podemos ajudá-lo a proteger qualquer carga de trabalho com produtos, soluções e serviços inteligentes projetados com o adversário em mente. Em vez de tentar bloquear 100% dos ataques (o que é impossível), deixamos nosso ego de lado, assumimos que um ataque é inevitável e estruturamos camadas de defesa para o pior cenário possível. Enfatizamos a visibilidade e a capacidade de ação em todo o parque de PCs. Isso ajuda nossos clientes a se manterem à frente dos vetores de ataque emergentes.

Com as soluções de segurança de endpoint da Dell e da Intel implementadas, as organizações **alcançam resultados de segurança importantes**:

- **Melhorar a resiliência cibernética em longo prazo**
- **Obter o máximo de retorno de seus investimentos em tecnologia**

Atenda aos dois casos de uso de segurança cibernética...:

- **Reduzir a superfície de ataque** — Diminuir os riscos de um ataque escapar e minimizar as vulnerabilidades e pontos de entrada que podem ser explorados para comprometer o ambiente.
- **Melhorar a detecção e resposta a ameaças** — Identificar e resolver ativamente possíveis incidentes de segurança e atividades mal-intencionadas com camadas de defesa integradas que aceleram a detecção e a resposta.
- **Permitir a recuperação e correção** — Analisar os dados de violação para proteção contra ameaças futuras e restaurar os endpoints a um estado anterior, seguro e operacional após um incidente de segurança.

...além de aliviar a carga operacional da segurança:

- Mantenha a confiança do dispositivo e da identidade com **ofertas compatíveis com Zero Trust**
- **Simplifique a aquisição** consolidando provedores e obtendo acesso a hardware, software e serviços, tudo em um só lugar
- Economize tempo e recursos com uma **integração simplificada**

A batalha da segurança cibernética é vencida ou perdida com base na sua capacidade de coletar, analisar e responder à inteligência contra ameaças. Os invasores atuais são inovadores. Sabendo que a maioria das soluções de segurança se concentra somente acima do SO, os adversários estão mirando superfícies de ataque mais vulneráveis, ou seja, camadas abaixo do SO e cadeia de suprimentos. Para ficar à frente desses agentes mal-intencionados e manter os negócios protegidos, os líderes atuais precisam considerar como essenciais as tecnologias de segurança integradas e baseadas em hardware e incorporadas no chip ao implementarem dispositivos comerciais para seus funcionários.

Veja quais são as soluções certas para você

AI PCs comerciais

PERGUNTE SOBRE:

Segurança de hardware e firmware • Segurança da cadeia de suprimentos • Capacidade de gerenciamento • Otimizações de IA e de núcleo de silício

Software e integrações

PERGUNTE SOBRE:

Licenças disponíveis para compra com PCs da Dell • Licenças independentes • Integrações de telemetria

Serviços

PERGUNTE SOBRE:

Managed Detection & Response (MDR) • Recuperação de incidentes

Com segurança de cadeia de suprimentos de classe mundial, proteções baseadas em hardware, software para proteção contra ameaças avançadas, serviços gerenciados e suporte contínuo, a Dell e a Intel estão prontas para oferecer a você e à sua empresa dispositivos comerciais corporativos que entregam resultados e que foram desenvolvidos para ajudar a manter os dados da sua empresa fora da dark web.

Os AI PCs comerciais mais seguros: com base em uma análise de terceiros, realizada pela Principled Technologies, que faz uma comparação entre os AI PCs comerciais Dell com processadores Intel e os respectivos dispositivos da HP e da Lenovo, em 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.

Saiba mais
sobre as soluções Dell

Entre em contato
com um especialista
da Dell Technologies

Veja mais recursos

Participe da conversa