Práticas de segurança de dispositivos na Dell

Três considerações para estabelecer a confiança do dispositivo

Os especialistas cibernéticos da Dell explicam o papel essencial que as práticas de segurança de dispositivos desempenham na resiliência de longo prazo do seu ecossistema de TI.

Autores
Rick Martinez
Associado e vice-presidente da Dell

Eric Baize
Vice-presidente, segurança de produtos e aplicativos

Introdução

No atual mercado cibernético já tão saturado, provavelmente você se depara com inúmeras opções de produtos e soluções de segurança. Mas e se eu lhe dissesse que a parte mais importante da sua estratégia de segurança não são os seus produtos de segurança?

Como uma importante fabricante de PCs, a Dell pensa muito em segurança. E o que ficou claro nos últimos anos, enquanto observamos as consequências devastadoras dos ataques de ransomware e a expansão do malware baseado em firmware, é que os dispositivos de endpoint são um alvo crescente. Infelizmente, as soluções de ponto único, por mais inovadoras que sejam, não conseguem manter usuários e dados completamente seguros.

Ao reavaliar a segurança do seu ecossistema existente e explorar produtos para uma atualização, considere como o fabricante do seu PC aborda a segurança e o que comprar. Por quê? Você pode até pensar que isso serve para avaliar o produto, mas também serve para avaliar o fornecedor. Um fornecedor de PC seguro, confiável e experiente, que entenda o cenário de ameaças, poderá usar esse conhecimento para ajudar você a proteger sua organização à medida que esse cenário evolui. Com esse parceiro, você construirá um ecossistema de segurança que mitiga de forma inteligente o ataque inevitável e impulsiona a resiliência cibernética a longo prazo.

A segurança começa antes do que você pode imaginar

Os tomadores de decisão de TI e os usuários finais normalmente interagem com uma combinação de equipe de vendas, dispositivos e suporte ao produto. Mas isso é apenas a ponta do iceberg quando se trata de segurança. Por quê? É semelhante à segurança alimentar. Você não pode julgar a segurança alimentar com base apenas em suas interações com um garçom em um restaurante, porque a segurança alimentar começa na cozinha. Da mesma forma, o que torna os dispositivos seguros deve ser implementado mesmo antes da fabricação dos produtos — e, por isso, essa segurança geralmente passa despercebida. A Dell dedicou inúmeras horas de engenharia e

esforço intelectual para proteger o ambiente de trabalho de TI do cliente desde o início, os complexos processos e protocolos que regem o projeto, o desenvolvimento e a entrega de cada dispositivo. O trabalho que ninguém vê e que forma a base estável sob a superfície para fabricar o dispositivo mais seguro possível. O trabalho que ajuda a proteger o ambiente de trabalho de TI do cliente, seja você um cliente federal, uma grande corporação ou uma pequena e média empresa. A Dell acredita em possibilitar a segurança moderna para todas as empresas, grandes e pequenas, e estamos comprometidos em fornecer soluções que mantenham sua organização segura e, por extensão, seus clientes.

Nossas práticas de segurança de dispositivos

Quando nós avaliamos as proteções de dispositivos comerciais, pensamos nos resultados de segurança — ou seja, como o dispositivo contribui para a integridade geral da segurança de uma organização. Como o dispositivo ajuda a evitar ataques? O que o mantém seguro durante um ataque? E como ele permanece seguro ao longo de sua vida útil?

Como é de se esperar, nós temos dezenas de práticas em vigor para desenvolver PCs comerciais seguros que se alinham aos padrões do setor e oferecem suporte a uma abordagem de segurança Zero Trust. Hoje, vou destacar três temas principais: cadeia de suprimentos segura, código seguro e segurança no uso.

1. Protegemos nossa cadeia de suprimentos de dispositivos. Isso significa controles rigorosos em nossas cadeias de suprimentos, tanto para hardware quanto para software, também conhecidas como cadeias de suprimentos físicas e digitais. Esses controles ajudam a manter a integridade de nossos produtos durante os processos de fabricação, montagem, entrega e implementação. Isso garante que nossos clientes recebam exatamente o que compraram, nada mais, nada menos. Além disso, transmitimos esses requisitos rigorosos a todos os nossos fornecedores. Dito isso, no verdadeiro estilo Zero Trust de presumir uma violação, nós incluímos verificações durante todas as etapas desse processo.

Essas verificações incluem tecnologias avançadas, como Secured Component Verification,* para identificar trocas de componentes e verificação do SafeBIOS fora do host, a fim de identificar e alertar sobre qualquer adulteração do firmware mais privilegiado no sistema. Esses e muitos outros recursos estão integrados ao Dell Trusted Device, parte do nosso portfólio da Dell Trusted Workspace. Mas também os utilizamos em toda a nossa cadeia de suprimentos para manter todos os elos da cadeia intactos. Isso nos permite identificar desvios antes que eles cheguem à próxima etapa da cadeia de suprimentos. (*Recurso adicional opcional disponível para compra. A disponibilidade varia de acordo com a região.)

Isso é o que significa ter foco em resultados. Esses recursos foram desenvolvidos não por uma questão de inovação, mas porque resolvem ativamente preocupações reais que nossos clientes têm em relação à segurança da cadeia de suprimentos e ao gerenciamento do parque de PCs. Nunca confie, sempre verifique.

Relacionando isso à avaliação do fornecedor, lembre-se de que a cadeia de suprimentos do seu OEM é a sua cadeia de suprimentos, portanto, certifique-se de verificar as práticas que eles implementam. (Para obter mais informações sobre o que é necessário para proteger a cadeia de suprimentos, consulte nossa perspectiva no white paper sobre cadeia de suprimentos.)

2. Projetamos e desenvolvemos dispositivos seguros. É aqui onde você vê a interseção de práticas e recursos. É assim que desenvolvemos hardware e firmware eficientes e inovadores.

Agora, os recursos de segurança fazem parte da nossa oferta voltada para o mercado, mas isso é apenas parte do quebra-cabeça. Nossos produtos não seriam seguros se seu design, desenvolvimento e testes não fossem regidos pelo nosso Ciclo de vida de desenvolvimento de segurança (SDL) prescritivo. 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 nossa pilha de software de segurança, realizamos uma modelagem rigorosa de ameaças durante o processo de desenvolvimento de software, identificando riscos em relação a suposições de adversários muito sofisticadas e até mesmo aplicando essa metodologia a hardware crítico.

Nós testamos e verificamos essas premissas de modelos de ameaças durante todo o processo de desenvolvimento, trabalhando com alguns dos melhores consultores em testes de invasão e pesquisadores terceirizados, dando a eles sistemas Dell para tentar violar. Da mesma forma, também oferecemos um programa público de detecção de bugs para submeter a segurança de nossos PCs comerciais a um teste de resistência. Usamos o resultado desses relatórios e os enviamos de volta à engenharia para desenvolver mitigações. Repita as mesmas etapas. Por que fazemos isso? Para operar com eficiência, os ambientes de nossos clientes exigem dispositivos reforçados e confiáveis.

3. Trabalhamos para garantir que os dispositivos estejam seguros durante o uso. A segurança é uma tarefa coletiva. E hoje, a verdadeira segurança inclui proteção em nível de hardware e firmware, bem como de software. É por isso que a Dell se esforça muito para criar uma rede dos melhores parceiros cuidadosamente selecionados que oferecem proteção contra ameaças avançadas. Muitos estão diretamente integrados aos nossos PCs comerciais. Dito isso, os hackers estão constantemente inovando em novas maneiras de invadir softwares. Por esse motivo, nossas práticas de SDL são projetadas para estender a proteção após o lançamento, incluindo a capacidade de identificar e corrigir vulnerabilidades de forma rápida e fácil. A Dell também relata proativamente as próximas atualizações de segurança e políticas claras de suporte de segurança para facilitar aos clientes a compreensão de como seus produtos permanecem protegidos ao longo de sua vida útil. Para ajudar os clientes a encontrar rapidamente informações sobre vulnerabilidades e aplicabilidade em versões de produtos, nós consolidamos todos as orientações e avisos de segurança em um só lugar. Combinar isso com uma política de resposta a vulnerabilidades bem documentada nos permite trabalhar em estreita colaboração com os pesquisadores, conforme novas vulnerabilidades são relatadas. Isso encurta o ciclo e garante que informações precisas estejam sempre disponíveis para permitir que os clientes avaliem e corrijam os riscos em seus ambientes.

Um parceiro de segurança combinando todos os recursos

A Dell se esforça para conquistar confiança e criar um mundo seguro e conectado. Nós trabalhamos incansavelmente para manter os dados, a rede, a organização e a segurança dos clientes em primeiro lugar, e a segurança é cuidadosamente integrada a todas as nossas soluções. Para saber mais sobre nossas práticas de segurança, visite a Central de segurança e confiabilidade da Dell. E, como sempre, entre em contato com seu representante Dell em caso de dúvidas ou fale com nossos especialistas em segurança através do e-mail global.security.sales@dell.com

Saiba mais sobre Segurança de endpoints da Dell

Entre em contato com um especialista da Dell Technologies

Veja mais recursos

Participe da conversa com #HashTag