DELL Technologies

A segurança do endpoint é um elemento essencial da sua jornada de Zero Trust

Há três recomendações para se preparar para o Zero Trust

DELL Technologies

Sumário Executivo

Zero Trust é uma jornada de longo prazo. Não é um produto ou uma solução que as organizações implementam: é uma estrutura estratégica para gerenciar a segurança que é criada com o passar do tempo. Este eBook oferece uma orientação prática para os responsáveis pelas decisões de TI que passam por uma transformação de Zero Trust, concentrando-se em específico no papel que a segurança de dispositivos de endpoint desempenha na criação de uma base moderna e realmente segura para nosso mundo onde dá para trabalhar em qualquer lugar.

Sumário

Estado cibernético da união

As ameaças à segurança estão crescendo, impulsionadas por nosso mundo de trabalho cada vez mais remoto/híbrido e na nuvem.

A complexidade em proteger os ativos de dados de uma organização cresceu assustadoramente nos últimos anos. A nuvem tem mudado os planos em relação à produtividade da empresa, uma vez que o uso do trabalho remoto/híbrido está aumentando, mas isso gera um custo. A transição do gerenciamento só da infraestrutura local para a abrangência da nuvem criou uma maior superfície de ataque para os adversários, com grandes consequências. Por exemplo, se um invasor for bem-sucedido, ele pode prejudicar não apenas um cliente, mas potencialmente cada cliente desse serviço em nuvem e os clientes dele em toda a cadeia de suprimentos. A recompensa dos invasores – tanto de Estados-nação como criminosos comuns – pode ser enorme e, por isso, continuarão encontrando novas vulnerabilidades para explorar.

Estima-se que o custo dos danos globais do cibercrime suba para **US$ 10,5 trilhões até 2025**[i]

Houve **5.200** violações de dados confirmadas relatadas pela Verizon em uma pesquisa de 2022 – **1,3 vez maior do que no ano anterior**[ii]

Implicações para nosso mundo que trabalha de qualquer lugar

As organizações devem encontrar um jeito de se antecipar quanto ao ambiente de ameaça em constante evolução.

Então, quais são as implicações do mundo de trabalho cada vez mais remoto? Duas coisas:

Todas as organizações são vulneráveis...

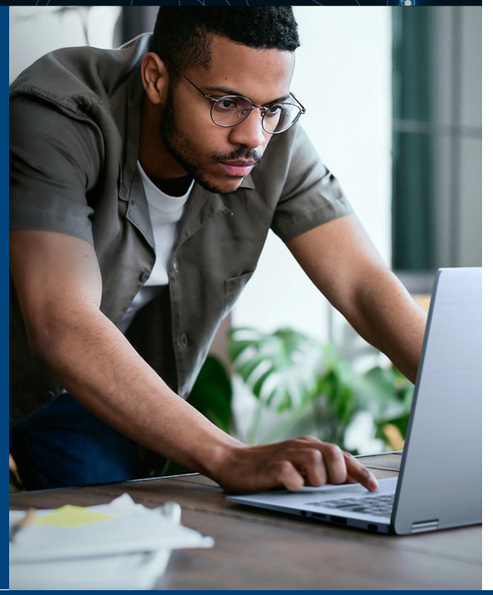
> "[S]e uma entidade focada realmente quiser entrar no sistema, ela terá uma probabilidade realmente alta de conseguir."
>
> — *Almirante Michael Rogers, ex-diretor da Agência de Segurança Nacional e ex-comandante do Comando Cibernético dos EUA*[iii]

...e o custo de dar errado pode ser devastador.

> "Atingindo um ponto máximo, o custo de uma violação de dados teve uma média de USD 4,35 milhões em 2022, [12,7% maior do que em 2020]."[iv]

Os vetores de ataque estão aumentando, as superfícies de ataque estão se expandindo e nenhuma empresa está sempre completamente segura. As organizações devem prever um cenário do pior que pode acontecer e tomar conta de suas defesas para o inevitável ataque.

69% das organizações têm sofrido algum tipo de ataque cibernético por causa de algum ativo voltado para a Internet que tem um gerenciamento insatisfatório.[v]



As estratégias de segurança precisam evoluir

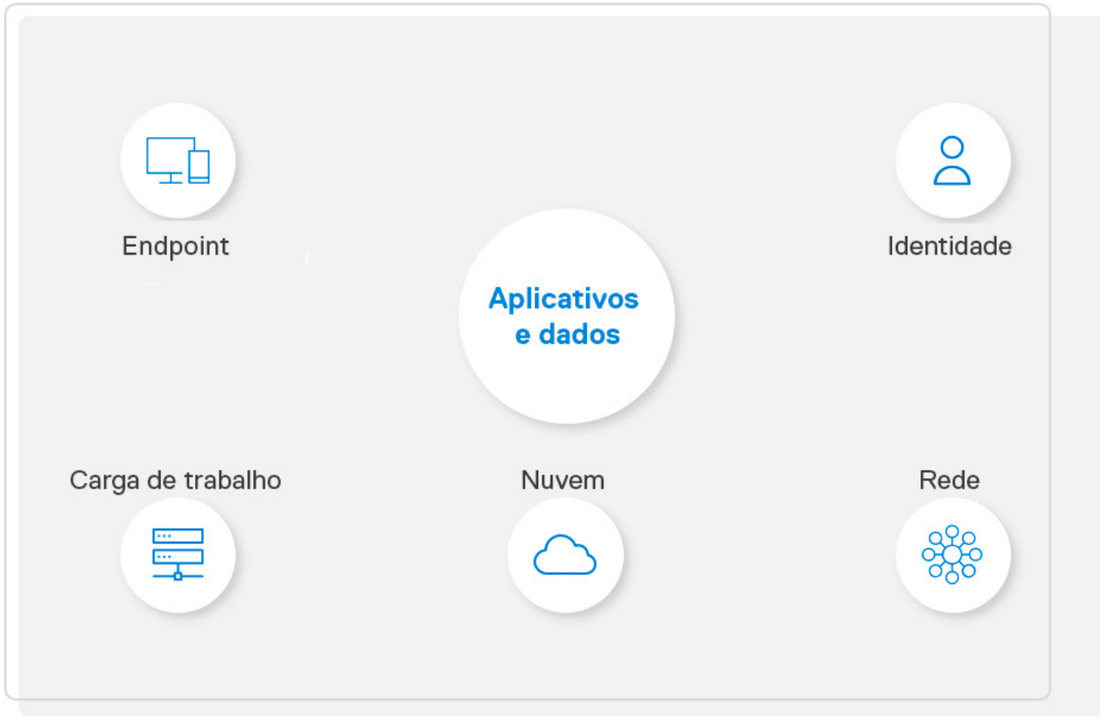
Devemos incluir o ambiente baseado em nuvem. É nesse ponto que entra o Zero Trust.

Os modelos tradicionais de segurança não funcionam mais. Veja os motivos.

Para qualquer organização ter uma postura de segurança efetiva, ela deve contar com cinco pontos de controle: endpoint, carga de trabalho, identidade, rede e nuvem. O objetivo é proteger os aplicativos e os dados.

Abordagens tradicionais frequentemente são em silos, o que torna as organizações que as utilizam mais suscetíveis a ataques.

Avançar...

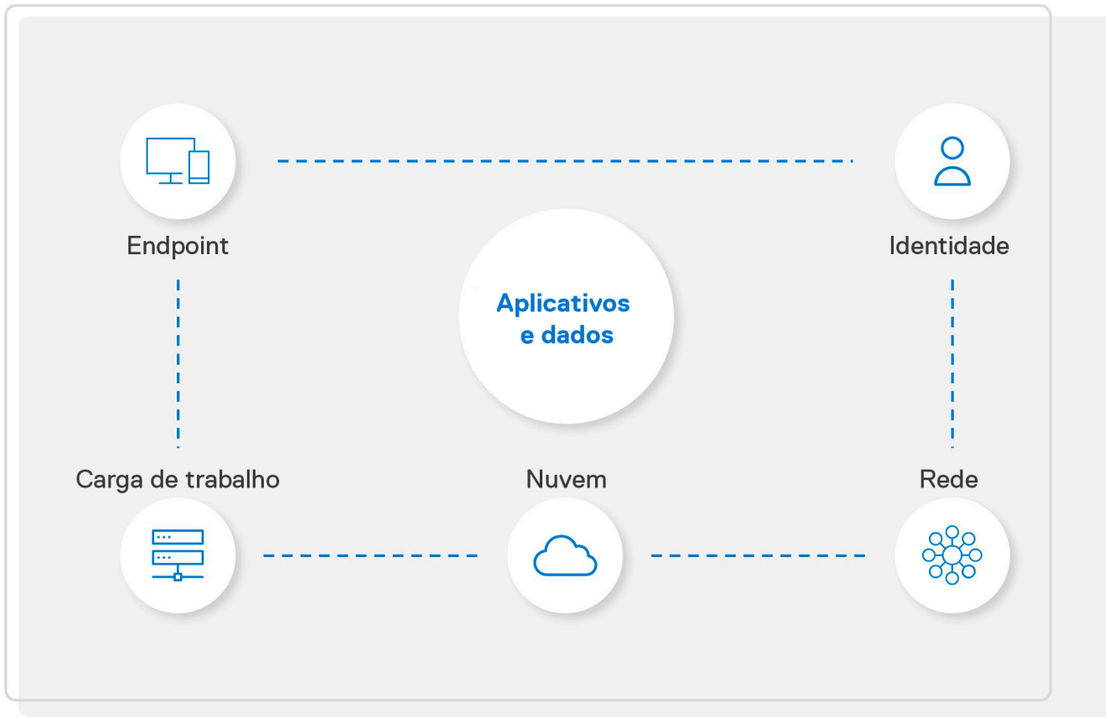


As estratégias de segurança precisam evoluir

Devemos incluir o ambiente baseado em nuvem. É nesse ponto que entra o Zero Trust.

Abordagens modernas têm caminhado para um maior controle, com melhor comunicação entre os pontos de controle. Mas, à medida que adotamos um ambiente de trabalho cada vez mais remoto/híbrido, precisamos reforçar ainda mais o perímetro.

Avançar...

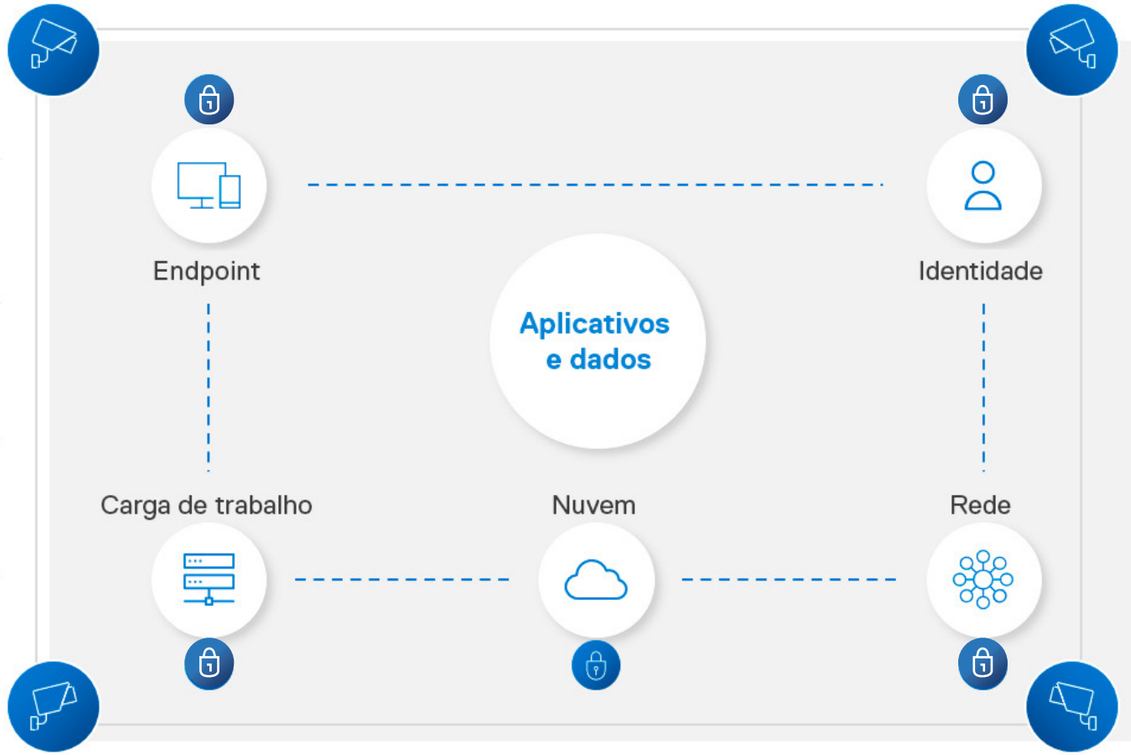


As estratégias de segurança precisam evoluir

Devemos incluir o ambiente baseado em nuvem. É nesse ponto que entra o Zero Trust.

Hoje em dia, os funcionários trabalham de qualquer lugar – de casa, cafés, hotéis – usando com frequência Wi-Fi não seguro limitado a não conectividade de volta aos escritórios e data centers protegidos por firewall. O padrão pode ser conexão direta de seus dispositivos com a Internet em que estão se conectando a servidores de arquivos na nuvem e aplicativos de software "as a service" (SaaS) – e funcionando com dados corporativos.

Com a crescente sofisticação dos ataques e o crescente número de vetores de ataque, as estratégias tradicionais de segurança criadas com confiança implícita não funcionam mais. É nesse ponto que entra o Zero Trust.



Entendendo os conceitos fundamentais do Zero Trust

Zero Trust é uma nova forma de pensar sobre segurança. Ele substitui a confiança *implícita* – ou seja, uma vez autenticados, os usuários circulam livremente pela rede. O Zero Trust inverte o paradigma para dar às organizações um controle explícito do ambiente de TI.

Vamos ilustrar o Zero Trust com um conceito bem conhecido: a criação de protocolos de segurança.

Você trabalha em um escritório corporativo. Quando foi contratado, você recebeu um crachá e aprendeu os protocolos de segurança. Todos os dias, você vai para o prédio. Há câmeras posicionadas em todos os lugares. Você passa o crachá em diversos pontos. Quando se senta à mesa, você desbloqueia o computador com uma senha.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.

Avançar...

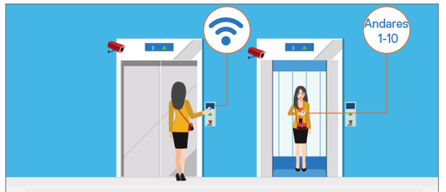
Entendendo os conceitos fundamentais do Zero Trust

Zero Trust é uma nova forma de pensar sobre segurança. Ele substitui a confiança *implícita* – ou seja, uma vez autenticados, os usuários circulam livremente pela rede. O Zero Trust inverte o paradigma para dar às organizações um controle explícito do ambiente de TI.

Vamos ilustrar o Zero Trust com um conceito bem conhecido: a criação de protocolos de segurança.

Você trabalha em um escritório corporativo. Quando foi contratado, você recebeu um crachá e aprendeu os protocolos de segurança. Todos os dias, você vai para o prédio. Há câmeras posicionadas em todos os lugares. Você passa o crachá em diversos pontos. Quando se senta à mesa, você desbloqueia o computador com uma senha.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.



Usa-o para entrar no elevador do andar onde trabalha

Avançar...

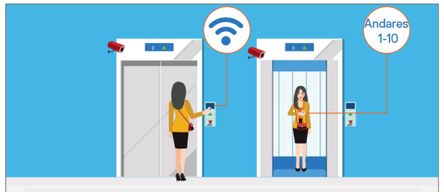
Entendendo os conceitos fundamentais do Zero Trust

Zero Trust é uma nova forma de pensar sobre segurança. Ele substitui a confiança *implícita* – ou seja, uma vez autenticados, os usuários circulam livremente pela rede. O Zero Trust inverte o paradigma para dar às organizações um controle explícito do ambiente de TI.

Vamos ilustrar o Zero Trust com um conceito bem conhecido: a criação de protocolos de segurança.

Você trabalha em um escritório corporativo. Quando foi contratado, você recebeu um crachá e aprendeu os protocolos de segurança. Todos os dias, você vai para o prédio. Há câmeras posicionadas em todos os lugares. Você passa o crachá em diversos pontos. Quando se senta à mesa, você desbloqueia o computador com uma senha.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.



Usa-o para entrar no elevador do andar onde trabalha

Reutiliza o crachá para ativar a seleção do andar no elevador.

Avançar...

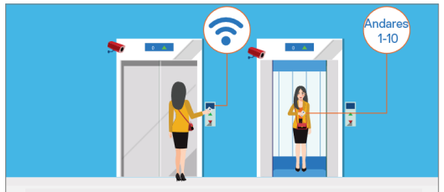
Entendendo os conceitos fundamentais do Zero Trust

Zero Trust é uma nova forma de pensar sobre segurança. Ele substitui a confiança *implícita* – ou seja, uma vez autenticados, os usuários circulam livremente pela rede. O Zero Trust inverte o paradigma para dar às organizações um controle explícito do ambiente de TI.

Vamos ilustrar o Zero Trust com um conceito bem conhecido: a criação de protocolos de segurança.

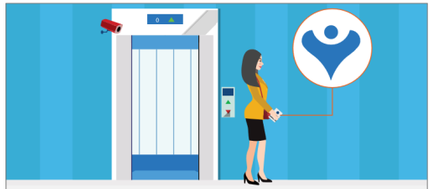
Você trabalha em um escritório corporativo. Quando foi contratado, você recebeu um crachá e aprendeu os protocolos de segurança. Todos os dias, você vai para o prédio. Há câmeras posicionadas em todos os lugares. Você passa o crachá em diversos pontos. Quando se senta à mesa, você desbloqueia o computador com uma senha.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.



Usa-o para entrar no elevador do andar onde trabalha

Reutiliza o crachá para ativar a seleção do andar no elevador.



Ao chegar no andar, caminha rumo à sala do escritório.

Avançar...

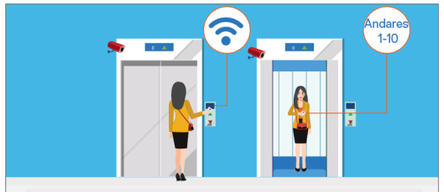
Entendendo os conceitos fundamentais do Zero Trust

Zero Trust é uma nova forma de pensar sobre segurança. Ele substitui a confiança *implícita* – ou seja, uma vez autenticados, os usuários circulam livremente pela rede. O Zero Trust inverte o paradigma para dar às organizações um controle explícito do ambiente de TI.

Vamos ilustrar o Zero Trust com um conceito bem conhecido: a criação de protocolos de segurança.

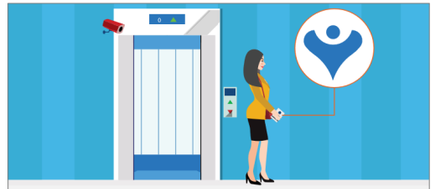
Você trabalha em um escritório corporativo. Quando foi contratado, você recebeu um crachá e aprendeu os protocolos de segurança. Todos os dias, você vai para o prédio. Há câmeras posicionadas em todos os lugares. Você passa o crachá em diversos pontos. Quando se senta à mesa, você desbloqueia o computador com uma senha.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.



Usa-o para entrar no elevador do andar onde trabalha

Reutiliza o crachá para ativar a seleção do andar no elevador.



Ao chegar no andar, caminha rumo à sala do escritório.

Retira o crachá para ter acesso à sala onde trabalha

Avançar...

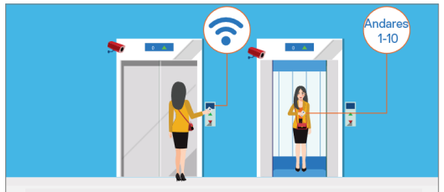
Entendendo os conceitos fundamentais do Zero Trust

Zero Trust é uma nova forma de pensar sobre segurança. Ele substitui a confiança *implícita* – ou seja, uma vez autenticados, os usuários circulam livremente pela rede. O Zero Trust inverte o paradigma para dar às organizações um controle explícito do ambiente de TI.

Vamos ilustrar o Zero Trust com um conceito bem conhecido: a criação de protocolos de segurança.

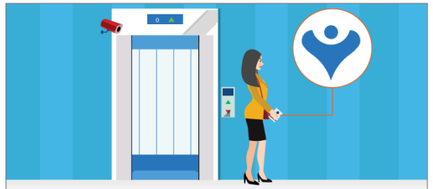
Você trabalha em um escritório corporativo. Quando foi contratado, você recebeu um crachá e aprendeu os protocolos de segurança. Todos os dias, você vai para o prédio. Há câmeras posicionadas em todos os lugares. Você passa o crachá em diversos pontos. Quando se senta à mesa, você desbloqueia o computador com uma senha.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.



Usa-o para entrar no elevador do andar onde trabalha

Reutiliza o crachá para ativar a seleção do andar no elevador.



Ao chegar no andar, caminha rumo à sala do escritório.

Retira o crachá para ter acesso à sala onde trabalha

Chega até a mesa dela e liga o computador com uma senha.

Avançar...

Entendendo os conceitos fundamentais do Zero Trust

O Zero Trust funciona da seguinte maneira.

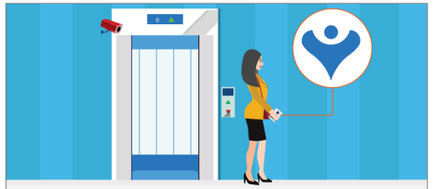
Seu empregador identificou você no primeiro dia. Cada acesso que você solicitou desde então foi verificado para proteger os ativos da organização (usuários, dados etc.). Para um nível a mais de segurança, guardas de segurança viram nos monitores toda a movimentação no prédio. Todo comportamento estranho – por exemplo, a tentativa de acessar uma sala que você não deveria acessar – é investigado.

Hoje, encontramos usuários, dispositivos, aplicativos e dados mais frequentemente fora das redes corporativas do que antes. Como resultado, a identidade do usuário se torna um ponto cego, com o comprometimento da identidade sendo o elemento-chave na maioria das violações. O curso do Zero Trust corrige isso.

Uma funcionária chega ao prédio do escritório e pega o crachá para ter acesso.

Usa-o para entrar no elevador do andar onde trabalha

Reutiliza o crachá para ativar a seleção do andar no elevador.



Ao chegar no andar, caminha rumo à sala do escritório.

Retira o crachá para ter acesso à sala onde trabalha

Chega até a mesa dela e liga o computador com uma senha.

Ativando os princípios do Zero Trust

A segurança do endpoint é uma parte crítica de uma transformação do Zero Trust.

Para ativar efetivamente uma estratégia do Zero Trust, você deve proteger os endpoints.

De acordo com a estrutura do MITRE ATT&CK®, atualmente, há nove “técnicas de acesso inicial” que os adversários usam para conseguir entrar nas redes *(veja a ilustração)*.[vi] Como mostra a pesquisa, nossas defesas mundiais tradicionais baseadas em nuvem não conseguem manter os endpoints seguros. Um invasor precisa apenas de um ponto de entrada. Com os endpoints, os invasores podem explorar dezenas de vulnerabilidades em todo o ciclo de vida de um dispositivo.

À medida que o número de dispositivos em uma rede aumenta, os endpoints se tornam um vetor de ataque cada vez maior.

As políticas de segurança em um modelo do Zero Trust definem o “já conhecido” detalhadamente – tudo o mais é bloqueado. O gerenciamento de ameaças, então, monitora qualquer desvio do já conhecido, sinalizando qualquer comportamento incomum e acionando a ação apropriada para corrigir a possível ameaça.

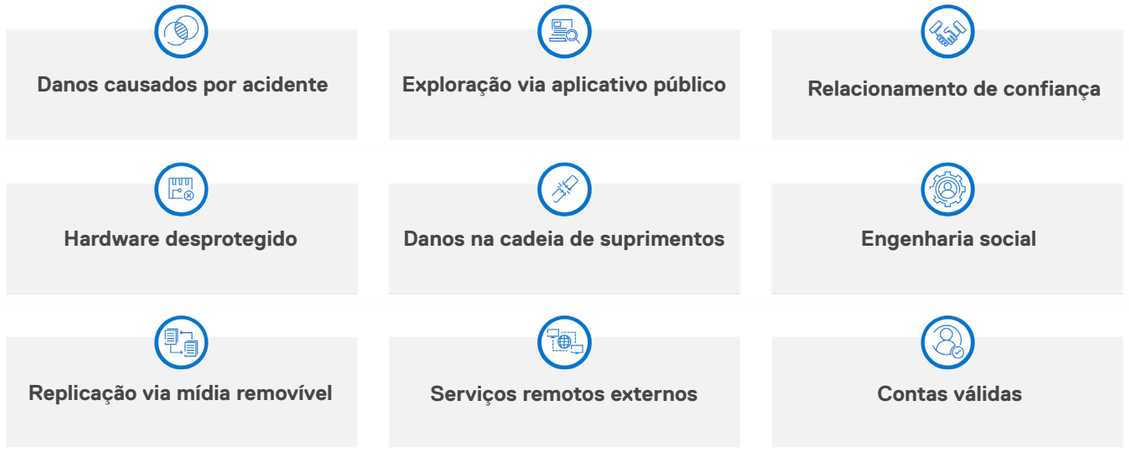


Ilustração 1/3

Ativando os princípios do Zero Trust

A segurança do endpoint é uma parte crítica de uma transformação do Zero Trust.

Para ativar efetivamente uma estratégia do Zero Trust, você deve proteger os endpoints.

De acordo com a estrutura do MITRE ATT&CK®, atualmente, há nove “técnicas de acesso inicial” que os adversários usam para conseguir entrar nas redes *(veja a ilustração)*.[vi] Como mostra a pesquisa, nossas defesas mundiais tradicionais baseadas em nuvem não conseguem manter os endpoints seguros. Um invasor precisa apenas de um ponto de entrada. Com os endpoints, os invasores podem explorar dezenas de vulnerabilidades em todo o ciclo de vida de um dispositivo.

À medida que o número de dispositivos em uma rede aumenta, os endpoints se tornam um vetor de ataque cada vez maior.

As políticas de segurança em um modelo do Zero Trust definem o “já conhecido” detalhadamente – tudo o mais é bloqueado. O gerenciamento de ameaças, então, monitora qualquer desvio do já conhecido, sinalizando qualquer comportamento incomum e acionando a ação apropriada para corrigir a possível ameaça.

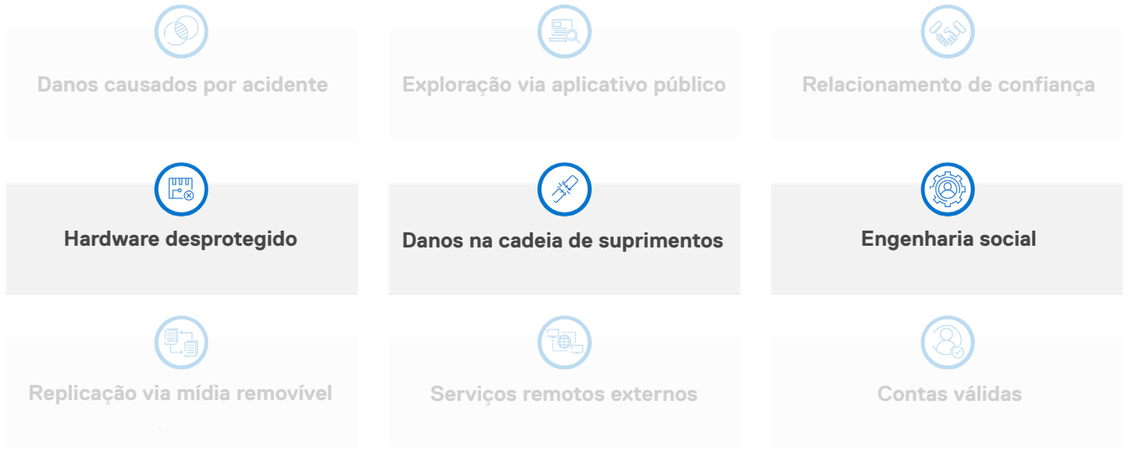


Ilustração 2/3

Ativando os princípios do Zero Trust

A segurança do endpoint é uma parte crítica de uma transformação do Zero Trust.

Para ativar efetivamente uma estratégia do Zero Trust, você deve proteger os endpoints.

De acordo com a estrutura do MITRE ATT&CK®, atualmente, há nove “técnicas de acesso inicial” que os adversários usam para conseguir entrar nas redes *(veja a ilustração)*.[vi] Como mostra a pesquisa, nossas defesas mundiais tradicionais baseadas em nuvem não conseguem manter os endpoints seguros. Um invasor precisa apenas de um ponto de entrada. Com os endpoints, os invasores podem explorar dezenas de vulnerabilidades em todo o ciclo de vida de um dispositivo.

À medida que o número de dispositivos em uma rede aumenta, os endpoints se tornam um vetor de ataque cada vez maior.

As políticas de segurança em um modelo do Zero Trust definem o “já conhecido” detalhadamente – tudo o mais é bloqueado. O gerenciamento de ameaças, então, monitora qualquer desvio do bom conhecido, sinalizando qualquer comportamento incomum e acionando a ação apropriada para corrigir a possível ameaça.

Ilustração 3/3

Há três recomendações para se preparar para o Zero Trust

Posicione sua organização para uma transformação bem-sucedida com o Zero Trust.

1

Estabelecer as políticas e controles certos que oferecem suporte às suas prioridades corporativas.

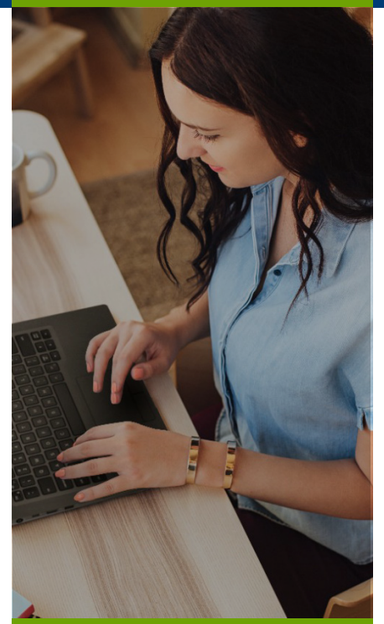
Os mecanismos e o gerenciamento de políticas são essenciais para a implementação efetiva do Zero Trust. No entanto, nenhuma organização tem um orçamento ilimitado para segurança, então, primeiro determine suas prioridades corporativas. Quais são os ativos e IP mais críticos que você está tentando proteger? Pese essa superfície de ataque em relação ao risco permitido de sua organização.

Em seguida, analise as políticas e os controles atualmente em vigor. Os riscos hoje em dia vêm do mundo baseado em nuvem no qual vivemos. Seu mecanismo de política leva isso em consideração?

Com as políticas em vigor que controlam o acesso aos seus ativos mais importantes, você pode expandir seu escopo.

SAIBA MAIS

Para obter mais informações, *assista a este vídeo* em que os especialistas em cibernética da Dell discutem os principais riscos de segurança enfrentados pelas organizações hoje em dia.



Com mais usuários, aplicativos, dados e dispositivos fora de uma rede corporativa do que nunca, **82%** dos responsáveis pelas decisões de segurança de TI dizem que tiveram que reavaliar suas políticas de segurança.[x]

Há três recomendações para se preparar para o Zero Trust

Posicione sua organização para uma transformação bem-sucedida com o Zero Trust.

2 Iniciar com dispositivos seguros.

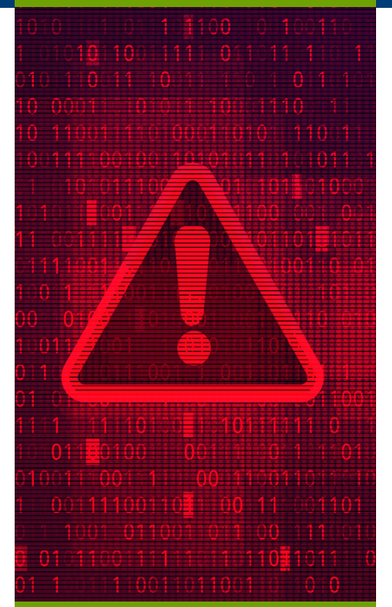
Faça o planejamento do Zero Trust em uma base sólida. Reforce suas defesas com dispositivos projetados e desenvolvidos com a segurança em mente. Isso inclui:

A. **Proteções baseadas em hardware e firmware** que protegem o pacote do endpoint e permitem visibilidade (por exemplo, detectam se um BIOS foi comprometido e alertam a TI). Equipe sua organização com tecnologias que verificam a identidade em cada nova solicitação de acesso – com o menor impacto possível sobre a produtividade do funcionário.

B. **Proteções da cadeia de suprimentos e controles de integridade** que protegem cada passo do ciclo de vida do PC. Como vimos nos últimos anos, os ataques a cadeias de suprimentos podem ser devastadores. Para uma arquitetura real do Zero Trust, a autenticação, a verificação e o monitoramento começam na cadeia de suprimentos. Trabalhe com fornecedores que 1) empregam práticas seguras e 2) permitem que você valide a integridade de seus dispositivos, da compra à produção e à entrega.

SAIBA MAIS

Para obter mais informações sobre as práticas recomendadas em segurança de dispositivos, leia o white paper da Dell e da Intel, Achieving Pervasive Security Above and Below the OS.



Em **2021**, uma empresa de gerenciamento de TI espalhou um ataque de ransomware a pelo menos **1.500** clientes.[xi]

Há três recomendações para se preparar para o Zero Trust

Posicione sua organização para uma transformação bem-sucedida com o Zero Trust.

3

Lutar pela integração e interoperabilidade contínuas em seu ecossistema.

Para alcançar uma postura eficaz de segurança, em alto nível, três coisas são essenciais:

A. Integração de todas as defesas no ecossistema de TI,

B. Visibilidade em tempo real e

C. Capacidade de agir quando necessário.

Em nosso mundo baseado em nuvem, no qual até mesmo a menor vulnerabilidade que fica sem verificação é um possível pesadelo, é importante que todos os sistemas reconheçam possíveis ataques *e* sejam configurados para que as ações necessárias sejam tomadas.

Seus sistemas são integrados ou eles operam em silos? Seu mecanismo de política pode acionar um fluxo de trabalho específico quando um administrador de TI é alertado sobre um BIOS corrompido na rede? Em um ambiente integrado, as automações devem colocar imediatamente em quarentena qualquer BIOS em questão, limitar qualquer acesso adicional e executar um exercício de correção.

Você tem visibilidade de todos os seus endpoints? De preferência, você tem um fluxo de telemetria rico em qualquer nível, da cadeia de suprimentos (por exemplo, dock station de carregamento) ao firmware (por exemplo, alertas de falsificação no nível do BIOS).

Mas essa telemetria é só tão boa quanto suas integrações. Você pode medir seus dados? É importante que você tenha os recursos certos – por exemplo, talentos qualificados de segurança cibernética – em vigor para fazer sentido com os fluxos de trabalho de dados e de programa que lidam com os problemas.

41% das organizações estão implantando o Zero Trust[xii]

DELL Technologies

Principais conclusões

O futuro da segurança é o Zero Trust.

- Os vetores de ataque se multiplicaram, pois nós aceitamos o futuro do trabalho.
- Uma violação é inevitável. Minimize a superfície de ataque com defesas que preparam para o pior cenário.
- O Zero Trust é uma nova maneira de pensar sobre segurança que oferece às organizações o controle explícito do ambiente de TI.
- As proteções do endpoint que ativam os princípios do Zero Trust são essenciais para manter uma base moderna e segura.
- Identifique seus ativos mais essenciais para priorizar a expansão de sua arquitetura com Zero Trust.
- Compre dispositivos de fornecedores que oferecem proteções integradas e investem muito nos controles da cadeia de suprimentos.
- Avalie a segurança e a interoperabilidade da TI. Continue a integrar fluxos de trabalho para fortalecer sua postura de segurança.

Dê o próximo passo

A segurança é um tópico assustador para organizações de todos os tamanhos. Engaje um parceiro experiente de tecnologia e segurança para ajudar a simplificar sua transformação do Zero Trust.

O Dell Trusted Workspace ajuda a proteger os endpoints para 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.

Fale conosco: EndpointSecurity@Dell.com
Visite nosso site: Dell.com/Endpoint-Security
Siga-nos: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum, Four Keys to Navigating the Hardware Security Journey, 2020 https://futurumresearch.com/research-reports/four-keys-to-navigating-the-hardware-security-journey/

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by--REvil-attacks

[xii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach