DELL Technologies

5 Recomendações para atender às suas necessidades de Zero Trust

1	2	3	4	5
Planeje a mudança de paradigma para "nunca confie, sempre verifique"	**Determine o caminho desejado**	**A organização impulsiona o ambiente de Zero Trust e não o contrário**	**Concentre-se nos dados**	**Implemente o modelo "nunca confie, sempre verifique" em todo o ecossistema de TI**
Determine a compensação aceitável entre a redução de riscos e o impacto nos negócios	Aprimoramento de segurança incremental	Crie controles de acordo com as necessidades dos negócios	Certifique-se de que todas as atividades da rede, do dispositivo e do usuário sejam registradas continuamente	As atividades de Zero Trust, como autenticação baseada em vários fatores e gerenciamento de identidade, devem ser aplicadas universalmente para evitar lacunas críticas
Considere o custo, o impacto para as operações e as partes interessadas e os requisitos regulamentares e de conformidade	Hiperescaladores	Documente processos, funções, responsabilidades e classificações de dados	Utilize IA e ML para analisar dados e identificar anomalias que possam indicar ameaças	Inclua cadeias de suprimentos físicas e digitais de terceiros na estrutura de Zero Trust
Evolua da segurança baseada em perímetro para um modelo microssegmentado e centrado em dados	Ambiente dedicado	A experiência do usuário continua sendo essencial	Lembre-se de que proteger dados e aplicativos é a principal função de uma arquitetura Zero Trust	
Utilize ajuda externa, se necessário	A identidade é o novo perímetro	Aprimoramentos de segurança, como o Zero Trust, não podem ser feitos às custas da usabilidade		
		Metas organizacionais, como crescimento e inovação, continuam sendo essenciais		

O Zero Trust é amplamente considerado a prática recomendada para a arquitetura de segurança.

Os dados mostram que a maioria das organizações começou a considerar ou está no processo de implementação do Zero Trust[1]. Embora a mudança para o Zero Trust seja importante, existem algumas considerações práticas que ajudarão a orientar a jornada.

Os especialistas da Dell Technologies, Tracy Emmersen, Diretora de adoção de soluções do Project Fort Zero, e Justin Vogt, Engenheiro principal de segurança, compartilharam recomendações e insights com Ash Lakshmanan, Gerente de produtos de serviços de segurança. As principais sugestões estão resumidas abaixo ou você pode assistir à conversa inteira em dell.com/cybersecuritymonth.

> "Quando analisamos o Zero Trust de um ponto de vista holística, quando recuamos um pouco, vemos que tudo se resume aos dados."
>
> ***Tracy Emmersen***
> *Diretora de adoção de soluções para Project Fort Zero, Dell Technologies*

Planeje a (grande) mudança de paradigma para nunca "confie, sempre verifique"

Em seu aspecto mais fundamental, adotar um ambiente Zero Trust representa uma grande mudança dos modelos de segurança históricos para um que se baseia nos princípios de "nunca confie, sempre verifique" e acesso com privilégios mínimos. "Precisamos olhar para nossa postura de segurança de forma diferente de como fizemos no passado, fugindo das soluções tradicionais de segurança de rede baseadas em perímetro e indo mais para uma arquitetura microssegmentada e centrada em dados", observa Emmersen.

Determine o caminho desejado

Emmersen explicou três caminhos distintos para alcançar os benefícios do Zero Trust:

- **Incremental:** uma abordagem iterativa que apresenta os principais princípios de Zero Trust para o ambiente atual
- **Hiperescalador:** aproveitando os recursos Zero Trust dos principais provedores de serviços em nuvem
- **Ambiente dedicado e em total conformidade:** ambiente privado, no local, desenvolvido desde o início, estritamente aderente aos padrões Zero Trust

Além desses três caminhos, empresas virtualizadas, de pequeno e médio porte também podem adotar uma abordagem denominada "Identidade é o novo perímetro". Essa metodologia se concentra no gerenciamento de identidade e acesso e aproveita ferramentas SaaS para obter proteção baseada em Zero Trust. Um componente essencial desse método é a implementação da autenticação baseada em vários fatores (MFA) em todos os lugares, ilustrando o impacto desse único recurso Zero Trust.

As abordagens de hiperescalador e identidade geralmente têm um custo menor, enquanto os ambientes incrementais e dedicados exigem maior investimento.

A organização impulsiona a adoção do Zero Trust e não o contrário

Em sua forma mais fundamental, uma arquitetura Zero Trust foi projetada para administrar e proteger os fluxos de trabalho, as funções de usuário e os privilégios, dispositivos, dados, aplicativos e redes relacionados de uma organização. A primeira parte de uma implementação requer uma documentação robusta desses aspectos e, em seguida, o plano de controle e a infraestrutura são projetados para aplicar as políticas que os regem.

Se o ambiente de Zero Trust inibir ou alterar significativamente as operações de negócios em detrimento da organização, qualquer segurança aprimorada alcançada provavelmente não valerá a pena. Como aponta Vogt, "se [a segurança]... atrapalha a missão central da organização... na verdade, não somos melhores do que os adversários que estamos tentando impedir. Apenas fornecemos nossa própria negação de serviço."

Concentre-se nos dados

Como Emmersen observa: "Quando olhamos para o Zero Trust de um ponto de vista holístico, quando recuamos um pouco, vemos que tudo se resume aos dados." Proteger os dados da organização é um dos benefícios mais valiosos de uma mudança para o Zero Trust, e princípios como verificação e segmentação contínuas protegem dados e aplicativos, evitando que ameaças se movam lateralmente dentro da rede.

O registro e o monitoramento contínuo são componentes essenciais do Zero Trust, e os dados e a telemetria são analisados para identificar anomalias que possam indicar um risco ou ameaça. Por exemplo, uma alteração nos padrões de uso de dados pode identificar uma possível exfiltração ou um ataque de ransomware.

1. De um estudo encomendado pela Dell pelo Enterprise Strategy Group, "Avaliando as jornadas de segurança das organizações: insights sobre superfície de ataque, detecção e resposta a ameaças, recuperação de ataques e Zero Trust", novembro de 2023

DELL Technologies

Dada a enorme quantidade de dados gerados pelo registro de todas as atividades, as ferramentas modernas de análise devem usar IA e aprendizado de máquina para serem eficazes.

"Nunca confie, sempre verifique" deve ser aplicado em todas as situações

Embora grande parte do foco em dados, aplicativos, usuários e dispositivos seja interna, o escrutínio inerente a uma arquitetura Zero Trust deve ser aplicado durante todo o ciclo de vida da TI. Se isso não for feito, poderá deixar brechas críticas de segurança.

A cadeia de suprimentos é um bom exemplo, e Vogt sugere fazer perguntas importantes sobre hardware e software de terceiros:

- "Quem mais teve acesso a isso?
- Do que é feito?
- O que mais está correndo abaixo da superfície?
- Como podemos adotar esses princípios de não confiar [e] ter algum tipo de processo de verificação e algum tipo de postura de privilégio mínimo em relação à tecnologia que estamos consumindo? Mesmo que seja no início da cadeia de suprimentos de tecnologia?"

Adotar uma arquitetura Zero Trust ou implementar seus princípios representa a prática recomendada atual para aumentar a maturidade da segurança cibernética. Vários caminhos representam diferentes compensações entre custo, risco e o nível de aprimoramento da segurança. A primeira etapa deve ser determinar a posição exclusiva da organização e deixar que isso guie as decisões tecnológicas.

Saiba como lidar com alguns dos principais desafios de segurança cibernética atuais em **dell.com/cybersecuritymonth**

DELL Technologies