DELL Technologies

Zero Trust
Um caminho para melhorar a segurança cibernética

Faça uma jornada Zero Trust com um parceiro experiente em tecnologia e segurança.

As organizações que avançam a maturidade da segurança cibernética estão criando um roteiro acionável que identifica maneiras de reduzir a superfície de ataque, detectar e responder a ameaças cibernéticas e implementar maneiras de se recuperar de ataques cibernéticos, tudo isso com os recursos possibilitadores do Zero Trust.

Para lidar com ameaças cibernéticas cada vez mais sofisticadas, a Dell utiliza os recursos de segurança integrados em nossas soluções e nossos parceiros para ajudar os clientes a alcançar o Zero Trust que se alinha aos objetivos de negócios de nossos clientes.

O que é Zero Trust?

Imagine sua rede como um castelo. Quando a ponte baixa e alguém entra, eles podem se mover livremente. É hora de atualizar o modelo de segurança de defesa baseado em perímetro para a estrutura Zero Trust mais moderna, mais segura.

O Zero Trust é uma abordagem arquitetônica de segurança em comparação com um produto que você compra. Ele nunca confia e sempre verifica o uso legítimo de negócios antes de conceder a qualquer pessoa ou a qualquer coisa acesso aos recursos. Isso significa que os usuários e dispositivos não são confiáveis por padrão, mesmo que estejam conectados a uma rede com permissão e mesmo se tiverem sido verificados anteriormente.

Nunca confie, sempre verifique.

Conceitos fundamentais para um ecossistema de TI seguro.

A estrutura Zero Trust, conforme definido pelo NIST (National Institute of Standards and Technologies, Instituto Nacional de Padrões e Tecnologias), foi adotada e integrada a uma arquitetura pelo Departamento de Defesa dos EUA (DoD).

Ela inclui sete pilares inter-relacionados que orientam a Dell Technologies em todos os domínios de segurança. Quando combinados, os pilares oferecem uma arquitetura integrada multifacetada para uma abordagem de segurança abrangente que protege os dados e a infraestrutura de sua organização.

A adoção do Zero Trust tem sido desafiadora devido à complexidade da integração de recursos de segurança diversificados e da navegação por opções fragmentadas entre vários provedores de segurança.

NIST

U.S. Department of Defense

DELL Technologies

Aumente a maturidade do Zero Trust.

Não importa onde você está em sua jornada, a Dell tem soluções para ajudar.

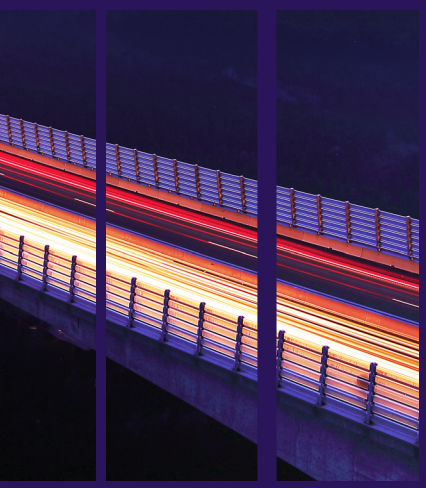
A Dell Technologies oferece opções e flexibilidade para sua organização. Se você quiser aumentar sua maturidade de segurança cibernética, podemos oferecer soluções de segurança com recursos Zero Trust para aprimorar sua capacidade de fortalecer, detectar, defender e se recuperar de atividades cibernéticas mal-intencionadas.

Ative os princípios do Zero Trust.

Possibilite opções e flexibilidade para aumentar a maturidade da segurança cibernética.

A Dell Technologies oferece soluções de segurança e recursos Zero Trust para aprimorar sua capacidade de fortalecer, detectar, defender e se recuperar de atividades cibernéticas mal-intencionadas. Funciona assim:

- Proteções integradas que melhoram a automação, a inteligência de ameaças, a autenticação, a visibilidade e muito mais
- Serviços para desenvolver um roteiro, integrar as principais tecnologias e gerenciar proativamente em suporte do Zero Trust
- Serviços de consultoria profissionais, gerenciados e de segurança
- Ampla rede de parceiros



Simplifique radicalmente a adoção do Zero Trust.

Aposte tudo com uma arquitetura totalmente integrada.

Como o Zero Trust é uma abordagem arquitetônica de segurança, ele não é um produto único e requer uma harmonia cuidadosamente planejada das soluções. A Dell está removendo a carga de integração do Zero Trust. Veja como:

- A Dell está criando a primeira e única arquitetura Zero Trust totalmente integrada projetada, testada e validada pelo Departamento de Defesa dos EUA

DELL Technologies

Ative os princípios do Zero Trust.

Obtenha o Zero Trust de uma forma que se baseia em seu ecossistema de segurança específico.

A Dell ajuda a desenvolver a maturidade da segurança cibernética em suporte a estratégias do Zero Trust, que ajudam a reduzir a superfície de ataque, aprimorar a detecção e acelerar a recuperação de ameaças cibernéticas.

Dentro de cada um dos pilares do Zero Trust retratados estão tecnologias, processos e pessoas alinhados a áreas críticas em que a segurança e as políticas de negócios são necessárias para proteger sua organização. Os serviços Dell Security podem ajudar você com:

- Maturidade da segurança, Zero Trust e avaliações de riscos
- Desenvolvimento de roteiro e estratégia
- Serviços gerenciados dos principais recursos Zero Trust

DELL Technologies

Fundamentos do Zero Trust.

Oferecemos soluções de segurança avançadas e integradas que dão a você uma vantagem sobre seu caminho para o Zero Trust.

Dell Data Protection

Cyber Recovery Vault | PowerProtect Data Manager | CyberSense Transparent Snapshots | Cloud IQ | Bloqueio do sistema | Detecção de desvios | Gerenciamento seguro de chaves empresariais | TLS 1.3 | IPv6 | Autenticação baseada em vários fatores | Sign-on único | Acesso baseado em função | Cloud IQ

Servidores Dell PowerEdge

Lista de materiais de software | Verificação de componentes protegidos | Raiz de confiança do silício | Bloqueio do sistema | Detecção de desvios | Gerenciamento seguro de chaves empresariais | TLS 1.3 | IPv6 | Autenticação baseada em vários fatores | Sign-on único | Acesso baseado em função | Cloud IQ

Plataformas de armazenamento da Dell

Isolamento de dados | Imutabilidade dos dados | Detecção de ameaças | Autenticação de controle de acesso | Criptografia de dados | Fortalecimento de STIG | Raiz de confiança do hardware | Inicialização segura | Firmware assinado digitalmente | Acesso baseado em função | Snapshots seguros

HCI/CI da Dell

Raiz de confiança do hardware | Cadeia de confiança de inicialização segura | Atualizações assinadas digitalmente | Gerenciamento de chaves | Log seguro | Switches virtuais distribuídos | Isolamento de VM | Autenticação e autorização | Conectores do ecossistema | Estados continuamente validados | Integridade do código de software | Matriz de compatibilidade eletrônica

PCs comerciais da Dell

Segurança do BIOS/firmware | Segurança de hardware | Garantia da cadeia de suprimentos | Software de gerenciamento de ameaças (EDR, XDR, VDR) | Software de proteção de dados na nuvem e na rede

Soluções de borda da Dell

Atestado de HW/SW/VM | Integração segura | Cadeia de confiança | Entrega segura de aplicativos/sistema operacional | Gerenciamento de direitos de dados

Dell Network Switches

SmartFabric | Cloud IQ | SD-WAN | Segmentação de VLAN | Enterprise SONiC | Listas de controle de acesso | RADIUS | TACACS+ | Criptografia | Fortalecimento de switch | Microssegmentação | Encaminhamento e roteamento virtuais

DELL Technologies

Nossa abordagem acelerada.

Rápido e completo, o Project Fort Zero integra o Zero Trust em toda a sua organização de maneira holística.

O Project Fort Zero oferece um método validado para maturidade avançada imediata no Zero Trust, reduzindo o tempo de adoção e interrupções e gerenciando custos.

Com base em nosso conhecimento especializado e alcance no setor, o Departamento de Defesa dos EUA pediu para a Dell Technologies ajudar a acelerar a taxa de adoção do Zero Trust. Para ajudar as organizações dos setores público e privado a simplificar a adoção e dimensionar globalmente a arquitetura Zero Trust, a Dell está criando um ecossistema e liderando a integração de mais de 30 empresas líderes em tecnologia e segurança. Estamos liderando o desenvolvimento e o dimensionamento global da arquitetura Zero Trust para organizações públicas e privadas em todo o mundo. Esta é uma prova do compromisso da Dell com os objetivos do DoD dos EUA para alcançar o Zero Trust.

No local

Em data centers para organizações em que a segurança e a conformidade de dados são essenciais.

Remoto ou regional

Em locais como lojas de varejo em que a análise segura e em tempo real dos dados do cliente pode oferecer uma vantagem competitiva.

A borda separável

Em locais como aviões ou veículos com conectividade intermitente em que a implementação temporária é necessária para a continuidade operacional.

DELL Technologies

Ajudaremos você a acelerar a adoção do Zero Trust implementando todas as **152** atividades estabelecidas pelo DoD dos EUA para obter um nível avançado de Zero Trust.

Ativadores de execução

Doutrina | Organização | Treinamento | Material | Liderança e educação | Pessoal | Instalações | Política

Nível de destino Zero Trust

Confiança dos usuários

- Inventário de usuários
- Permissão baseada em aplicativo
- Acesso dinâmico baseado em regras Pt. 1
- MFA/IDP organizacional
- Implemente o sistema e reduza os privilégios de usuários Pt. 1
- Gerenciamento do ciclo de vida de identidade da organização
- Negar usuário por política padrão
- Autenticação única
- Implemente o sistema e reduza os privilégios de usuários Pt. 2
- Gerenciamento do ciclo de vida de identidade empresarial Pt. 1
- Implementar kit de ferramentas UEBA
- Autenticação periódica
- PKI/IDP empresarial Pt. 1

Confiança dos dispositivos

- Ferramenta de ajuda do dispositivo Análise de gap
- Integrar as ferramentas NextGen AV (antivírus de nova geração) ao C2C
- Dispositivo NPE/PKI sob gerenciamento
- Negar dispositivo por política padrão
- Implementar ferramentas UEDM ou equivalentes
- Gerenciamento de dispositivos empresariais Pt. 1
- Implementar ferramentas EDR e integrar ao C2C
- Implementar ferramentas de gerenciamento de ativos, vulnerabilidades e patches
- IDP empresarial Pt. 1
- Implementar a autorização de rede baseada em conformidade/C2C Pt. 1
- Implementar o Controle de aplicativos e ferramentas FIM
- BYOD gerenciado e limitado e suporte a IOT
- Gerenciamento de dispositivos empresariais Pt. 2
- Implementar ferramentas XDR e integrar ao C2C Pt. 1

Aplicativo e carga de trabalho

- Identificação do aplicativo/código
- Autorização de recursos Pt. 1
- Criar software DevSecOps de fábrica Pt. 1
- Binários/código provados
- Programa de gerenciamento de vulnerabilidades Pt. 1
- Autorização de recursos do SDC Pt. 1
- Autorização de recursos Pt. 2
- Criar software DevSecOps de fábrica Pt. 2
- Automatizar aplicativos Correção de segurança e código Pt. 1
- Programa de gerenciamento de vulnerabilidades Pt. 2
- Validação contínua
- Autorização de recursos do SDC Pt. 2

Confiança dos dados

- Análise de dados
- Registro e análise de pontos de imposição do DLP
- Registro e análise de pontos de imposição do DRM
- Definir padrões de marcação de dados
- Implementar ferramentas de marcação e classificação de dados
- Monitoramento de atividade de arquivo Pt. 1
- Implementar o DRM e as ferramentas de proteção Pt. 1
- Implementar pontos de imposição
- Padrões de interoperabilidade
- Desenvolver política de SDS
- Marcação de dados manuais Pt. 1
- Monitoramento de atividade de arquivo Pt. 2
- Implementar o DRM e as ferramentas de proteção Pt. 2
- Imposição de DLP por meio de etiquetas de dados e lógica analítica Pt. 1
- Integrar acesso a DAAS com política de SDS Pt. 1
- Imposição de DRM por meio de etiquetas de dados e lógica analítica Pt. 1
- Integrar as soluções de SDS e política com o IDP empresarial Pt. 1

Rede e ambiente

- Definir regras e políticas de acesso de controle específico Pt. 1
- Definir APIs de SDN
- Definir regras e políticas de acesso de controle específico Pt. 2
- Implementar uma infraestrutura programável de SDN
- Segmentação macro de data center
- Implementar segmentação micro
- O segmento flui em gerenciamento de controle e planos de dados
- Segmentação macro B/C/P/S
- Segmentação micro de aplicativos e dispositivos
- Proteção de dados em movimento

Automação e orquestração

- Inventário e desenvolvimento de políticas
- Análise de automação de tarefas
- Análise de automação de resposta
- Análise de conformidade de ferramentas
- Perfil de acesso da organização
- Implementar ferramentas SOAR
- Chamadas API padronizadas e esquemas Pt. 1
- Enriquecimento do fluxo de trabalho Pt. 1
- Perfil de segurança empresarial Pt. 1
- Integração empresarial e provisionamento de fluxo de trabalho Pt. 1
- Implementar marcação e classificação de dados Ferramentas de ML
- Chamadas API padronizadas e esquemas Pt. 2
- Enriquecimento do fluxo de trabalho Pt. 2

Visibilidade e lógica analítica

- Considerações sobre escala
- Análise de registro
- ID do ativo e correlação de alertas
- Alertas de ameaças Pt.1
- Implementar ferramentas de lógica analítica
- Programa de inteligência de ameaças cibernéticas Pt. 1
- Análise de registro
- Alertas de ameaças Pt. 2
- Linhas de base de usuários/dispositivos
- Estabelecer o comportamento da linha de base do usuário
- Linha de base e Definição de perfis Pt. 1
- Programa de inteligência de ameaças cibernéticas Pt. 2

Total de atividades de destino: 91

Fonte: Publicação da estratégia de Zero Trust do DoD, 07 de novembro de 2022

DELL Technologies

Zero Trust avançado

Confiança dos usuários

- Acesso dinâmico baseado em regras Pt. 2
- Funções e permissões empresariais Pt. 1
- MFA flexível alternativa Pt. 1
- Aprovações em tempo real e lógica analítica de JIT/JEA Pt. 1
- Gerenciamento do ciclo de vida de identidade empresarial Pt. 2
- Monitoramento de atividades do usuário Pt. 1
- Autenticação contínua Pt. 1
- Autenticação contínua Pt. 2
- PKI/IDP empresarial Pt. 3
- Funções e permissões empresariais Pt. 2
- MFA flexível alternativa Pt. 2
- Aprovações em tempo real e lógica analítica de JIT/JEA Pt. 2
- Gerenciamento do ciclo de vida de identidade empresarial Pt. 3
- Monitoramento de atividades do usuário Pt. 2
- PKI/IDP empresarial Pt. 2

Confiança dos dispositivos

- IDP empresarial Pt. 2
- Implementar a autorização de rede baseada em conformidade/C2C Pt. 2
- Monitoramento de atividade da entidade Pt. 1
- Integrar totalmente o slack de segurança do dispositivo ao C2C
- PKI empresarial Pt. 1
- Suporte a BYOD e IOT gerenciado e completo Pt. 1
- Implementar ferramentas XDR e integrar c/ C2C Pt. 2
- Monitoramento de atividade da entidade Pt. 2
- PKI empresarial Pt. 2
- Suporte a BYOD e IOT gerenciado e completo Pt. 2

Aplicativo e carga de trabalho

- Enriquecer atributos para autorização de recursos Pt. 1
- Enriquecer atributos para autorização de recursos Pt. 2
- ATO (Continuous Authorization to Operate, autorização contínua para operar) Pt. 1
- Automatizar aplicativos Correção de segurança e código Pt. 2
- Microssegmentos da API REST
- ATO (Continuous Authorization to Operate, autorização contínua para operar) Pt. 2

Confiança dos dados

- Marcação de dados manuais Pt. 2
- Monitoramento de atividades do banco de dados
- Marcação e suporte de dados automatizados Pt. 1
- Imposição de DRM por meio de etiquetas de dados e lógica analítica Pt. 2
- Imposição de DLP por meio de etiquetas de dados e lógica analítica Pt. 2
- Integrar acesso a DAAS com política de SDS Pt. 2
- Integrar soluções e políticas de SDS com o IDP empresarial Pt. 2
- Integrar a ferramenta SOS e/ou integrar-se à ferramenta DRM Pt. 1
- Marcação de dados automatizados e suporte Pt. 2
- Monitoramento abrangente de atividades de dados
- Imposição de DRM por meio de etiquetas de dados e lógica analítica Pt. 3
- Imposição de DLP por meio de etiquetas de dados e lógica analítica Pt. 3
- Integrar acesso a DAAS com política de SDS Pt. 3
- Integrar ferramenta SDS e/ou integrar-se à ferramenta DRM Pt. 2

Rede e ambiente

- Detecção e otimização de ativos de rede
- Decisões de acesso em tempo real
- Microssegmentação de processo

Automação e orquestração

- Perfil de segurança empresarial Pt. 2
- Integração empresarial e provisionamento de fluxo de trabalho Pt. 2
- Implementar a ferramenta de automação de IA
- Enriquecimento do fluxo de trabalho Pt. 3
- A IA orientada por lógica analítica decide as modificações de A&O
- Implementar guias estratégicos
- Fluxos de trabalho automatizados

Visibilidade e lógica analítica

- Alertas de ameaças Pt. 3
- Linha de base e definição de perfis Pt. 2
- Suporte à linha de base UEBA Pt. 1
- Suporte à linha de base UEBA Pt. 2
- Acesso à rede ativado por IA
- Controle de acesso dinâmico ativado por IA

Total de atividades avançadas: 61

A Dell Technologies pode simplificar a complexidade de alcançar a maturidade do Zero Trust rapidamente.

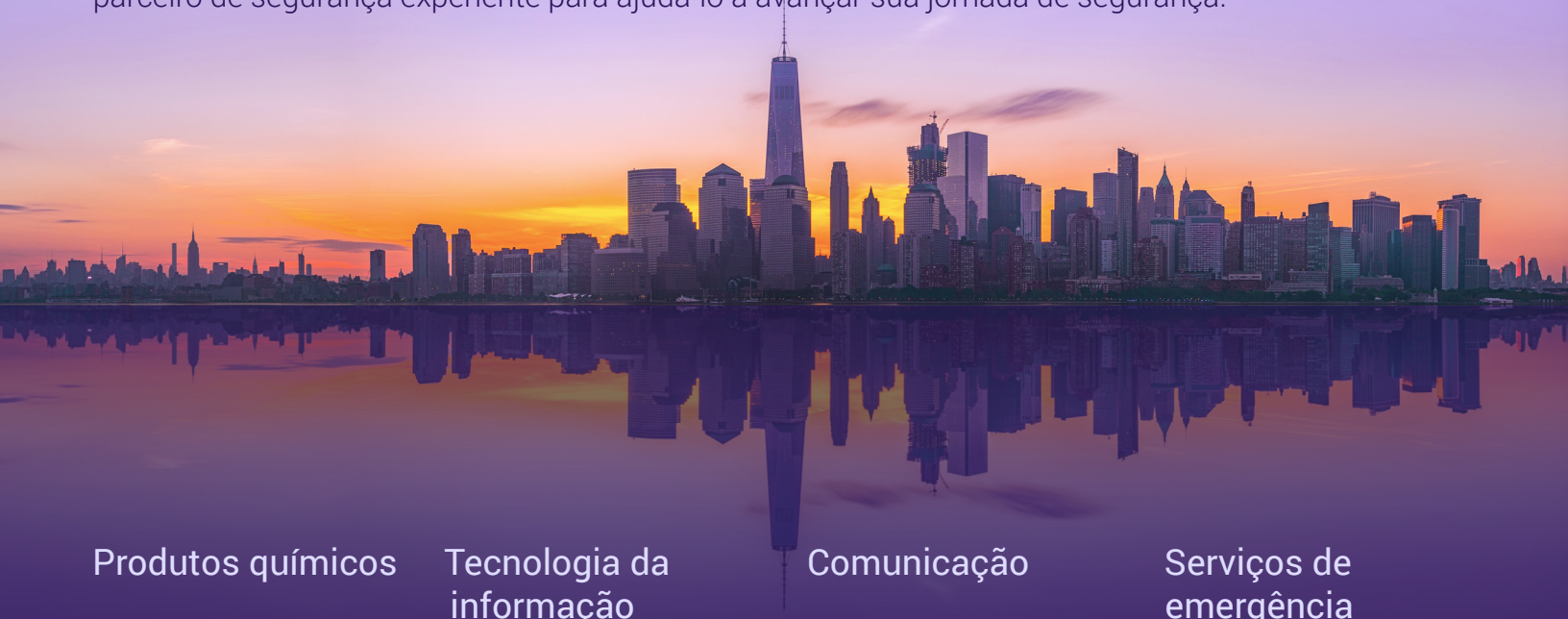
Fonte: Publicação da estratégia de Zero Trust do DoD, 07 de novembro de 2022

DELL Technologies

Atender às necessidades de todas as organizações.

Aumente a maturidade do Zero Trust.

O Zero Trust é uma estrutura definida e um conjunto de princípios que orientam como a segurança deve ser abordada e pode ser implementado usando uma variedade de recursos. Não importa se você está totalmente no Zero Trust ou concentrado ou focado em melhorias direcionadas, alinhada aos princípios do Zero Trust, a Dell é um parceiro de segurança experiente para ajudá-lo a avançar sua jornada de segurança.



Produtos químicos	Tecnologia da informação	Comunicação	Serviços de emergência
Alimentação e agricultura	Defesa	Área da saúde e saúde pública	Produção
Financeira	Reatores nucleares	Comercial	Governo
Energia	Transporte	Água e esgoto	Barragens

DELL Technologies

DELL Technologies

Um parceiro experiente em tecnologia e segurança para a jornada de Zero Trust da sua organização.

Melhore a segurança cibernética em longo prazo implementando o Zero Trust.

Os serviços Dell Security oferecem:

Avaliação especializada da maturidade da segurança e do risco geral.

Desenvolvimento de um roteiro de Zero Trust.

Gerenciamento contínuo de atividades de segurança.

DELL Technologies

Dell.com/SecuritySolutions

Solicitar um retorno

Falar com um consultor de segurança

Ligue para 1-800-433-2393