Documento técnico do modelo de maturidade zero trust da CISA

WHITE PAPER

Resumo executivo

No atual cenário em rápida evolução da cibersegurança, as organizações enfrentam uma gama crescente de ameaças sofisticadas. Os modelos tradicionais de segurança baseados em perímetro são cada vez mais ineficazes na proteção de redes, à medida que a transformação digital acelera e o trabalho em qualquer lugar se torna a norma. A cibersegurança deve evoluir para proteger dados e sistemas, independentemente de onde os usuários ou dispositivos estejam localizados. Em resposta a esses desafios, a Agência de Segurança Cibernética e de Infraestrutura (CISA) desenvolveu um modelo de maturidade zero trust para orientar as organizações na adoção e implementação eficaz dos princípios de zero trust.

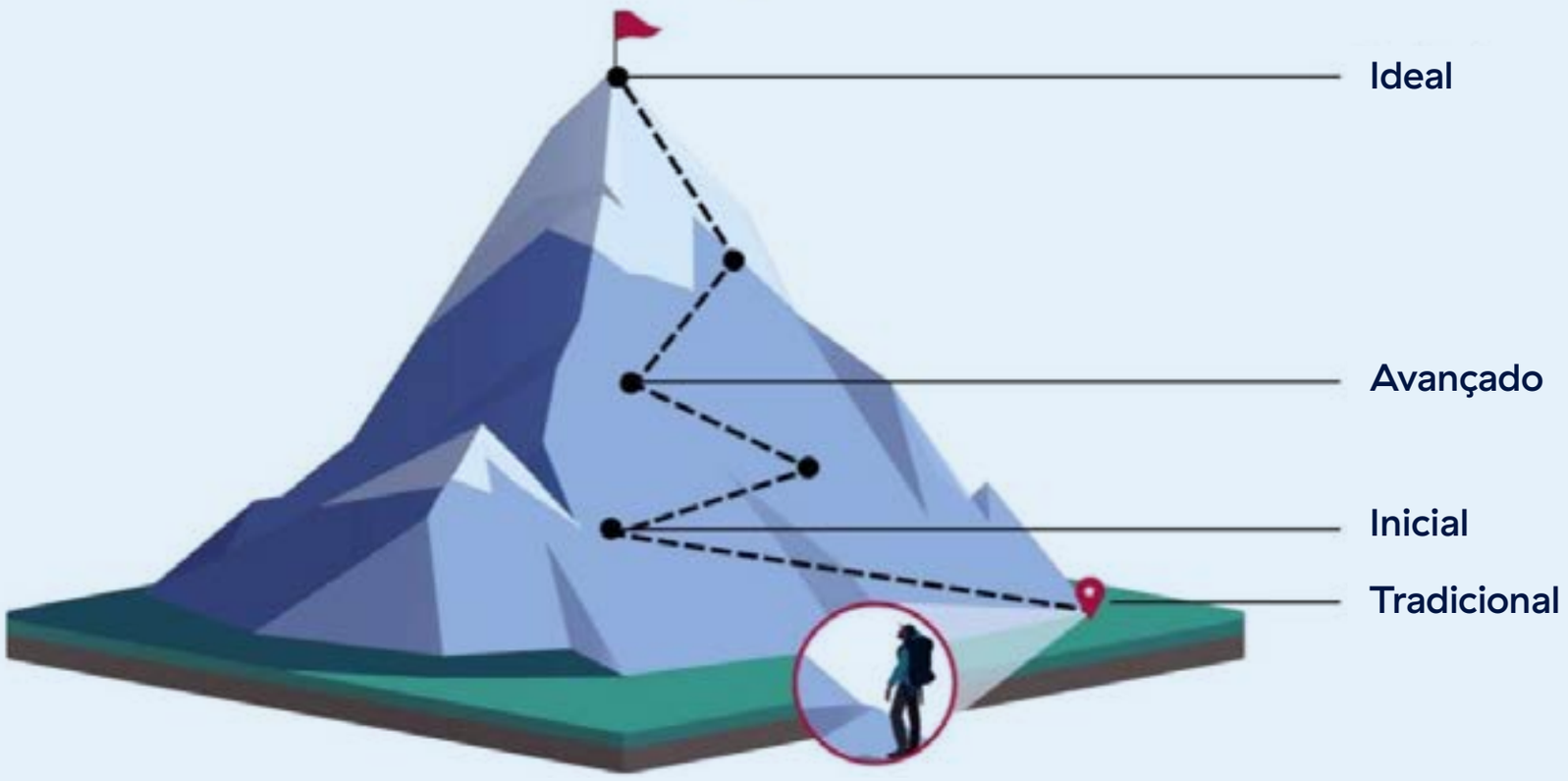
O que é Zero Trust?

Zero trust é um modelo de segurança que opera sob a premissa de que as ameaças podem ser internas ou externas e, portanto, nenhum usuário ou dispositivo deve ser considerado confiável por padrão. Cada solicitação de acesso, seja de dentro ou de fora da rede, é rigorosamente autenticada, autorizada e monitorada continuamente. A estrutura zero trust busca garantir que a segurança seja mantida em toda a infraestrutura de uma organização, com grande ênfase em identidade, gerenciamento de acesso e monitoramento em tempo real.

O que é o modelo de maturidade zero trust da CISA?

O modelo de maturidade zero trust da CISA fornece às organizações uma estrutura para adotar e amadurecer progressivamente os princípios de zero trust. Esse modelo descreve uma abordagem em fases para implementar zero trust em uma organização, desde a conscientização e o planejamento iniciais até operações de segurança totalmente maduras e integradas. Ele fornece um método estruturado para entender onde uma organização está em sua jornada zero trust e quais etapas ela deve seguir para melhorar a segurança.

Jornada de maturidade zero trust



Fonte: CISA

O modelo da CISA divide o zero trust em várias áreas principais, incluindo gerenciamento de identidade e acesso, segurança de dispositivos, segurança de rede, segurança de dados, segurança de aplicativos, visibilidade e análise. O modelo de maturidade ajuda as organizações a avaliar suas capacidades atuais em cada uma dessas áreas e a definir um caminho claro para fortalecer sua postura de segurança. As organizações são avaliadas em quatro estágios de maturidade (tradicional, inicial, avançado e ótimo), com cada estágio exigindo um nível maior de proteção, com crescimento exponencial em esforços e benefícios.

O modelo de maturidade zero trust da CISA está sendo cada vez mais utilizado como referência global para implementação do modelo zero trust. Governos internacionais, incluindo o Reino Unido e a Austrália, alinharam suas estratégias de cibersegurança com o modelo de maturidade, reconhecendo sua abordagem estruturada para avançar os recursos de zero trust. Além dos governos, a Cloud Security Alliance também mapeou seu Zero Trust Advancement Center para o modelo de maturidade, reforçando ainda mais seu papel como uma estrutura comum para organizações no mundo todo. À medida que a adoção do zero trust cresce, o modelo de maturidade fornece uma linguagem compartilhada e um roteiro de maturidade, ajudando entidades dos setores público e privado a avaliar seu progresso e refinar suas estratégias de segurança.

PRINCIPAIS COMPONENTES DO MODELO

1. **Gerenciamento de identidade e acesso (IAM):** estabelece mecanismos de autenticação robustos, como autenticação multifator (MFA), para verificar as identidades dos usuários antes de conceder acesso.

2. **Segurança de dispositivo:** garante que os dispositivos estejam seguros, gerenciados e em conformidade com as políticas de segurança antes de acessar recursos organizacionais.

3. **Segurança de rede:** implementa segmentação e monitoramento para restringir a movimentação lateral e detectar atividades suspeitas dentro da rede.

4. **Segurança de dados:** protege dados sigilosos aplicando criptografia, controles de acesso rigorosos e monitorando o uso de dados.

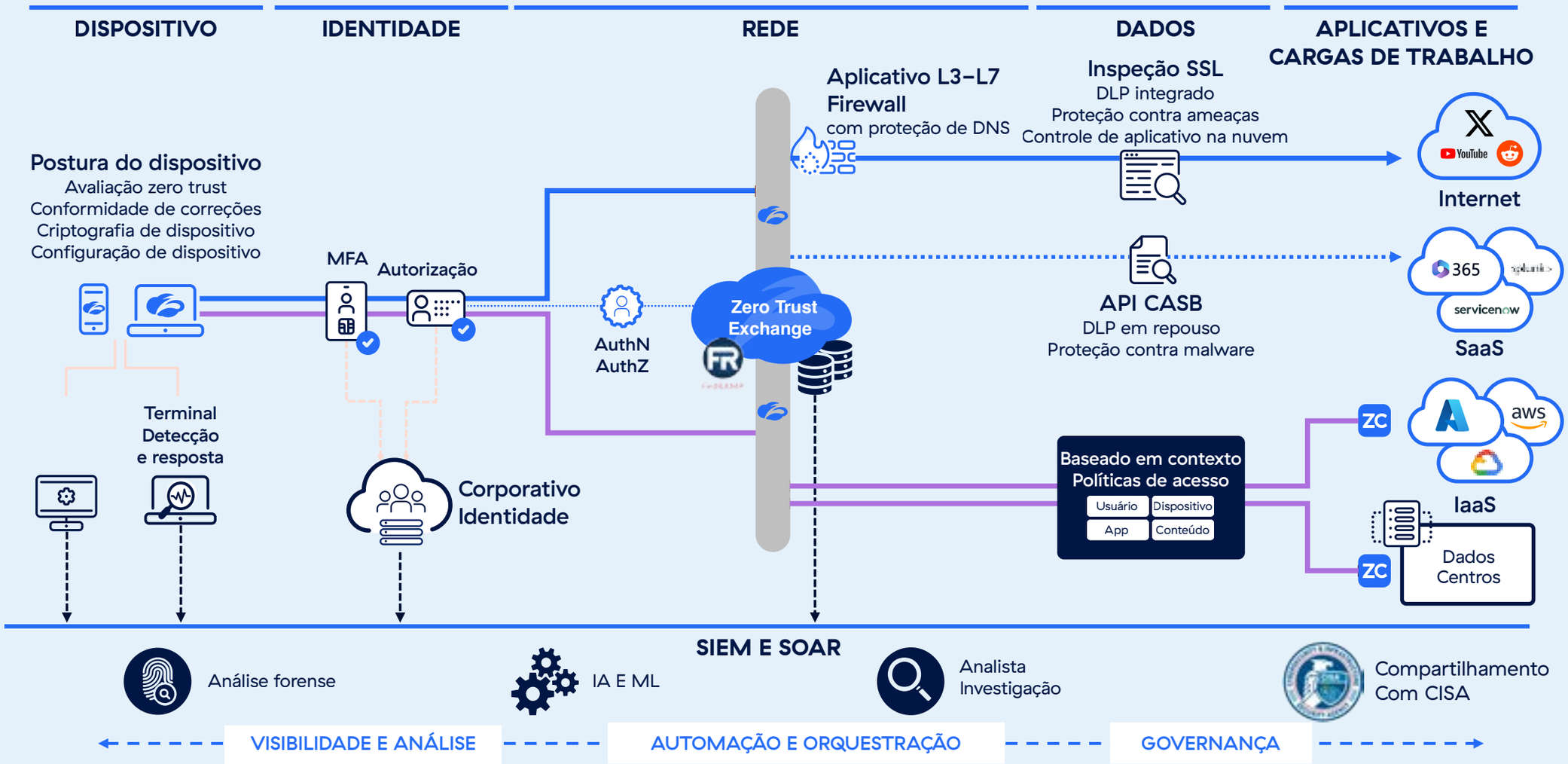
5. **Segurança de aplicativos:** garante que os aplicativos sejam seguros implementando práticas de desenvolvimento seguras, monitoramento contínuo e gerenciamento de vulnerabilidades.

6. **Visibilidade e análise:** melhora a percepção situacional monitorando continuamente todo o tráfego e eventos, identificando comportamentos anômalos e fornecendo alertas em tempo real.

7. **Automação e orquestração:** integra e automatiza sistemas para melhorar a eficácia e a eficiência dos sistemas cibernéticos.

8. **Governança:** estabelece políticas, procedimentos e mecanismos de supervisão para garantir a implementação eficaz.

Modelo de maturidade zero trust 2.0



Implementação do modelo de maturidade zero trust da CISA com a Zscaler

A implementação da Zscaler ZTE aprimora imediatamente sua postura de segurança, migrando da segurança tradicional baseada em perímetro para uma defesa em camadas mais abrangente. Ao verificar continuamente usuários, dispositivos e dados, as organizações podem reduzir os riscos de violações de dados, ameaças internas e ataques externos. Essa abordagem minimiza a superfície de ataque e impede a movimentação lateral dos invasores. A Zscaler também permite que as organizações avancem em sua estratégia de modelo de maturidade zero trust da CISA, fornecendo produtos e recursos robustos que dão suporte às principais áreas, incluindo gerenciamento de identidade e acesso, segurança de dispositivos, segurança de rede, segurança de dados, segurança de aplicativos, visibilidade e análise.

IDENTIDADE

- **Acesso de privilégio mínimo:** a Zscaler minimiza contas com permissões excessivas ao aplicar controles de acesso granulares baseados em funções (RBAC) e políticas contextuais (por exemplo, localização do usuário, postura do dispositivo).

- **Logon único (SSO) e autenticação multifator (MFA):** as políticas de zero trust são reforçadas com integração de SSO/MFA, garantindo uma autenticação robusta e reduzindo o risco de comprometimento de credenciais.

- **Monitoramento contínuo dos usuários:** a ZTE garante que os usuários sejam autenticados continuamente e que seu comportamento seja monitorado para mitigar riscos.

- **Integração com provedores de identidade (IdPs):** a Zscaler integra-se perfeitamente com os principais provedores de identidade, como Okta, Microsoft Azure AD e Ping Identity, para aplicar políticas robustas de autenticação e autorização de usuários.

DISPOSITIVOS

- **Verificações de postura do dispositivo:** a Zscaler usa integrações com ferramentas de detecção e resposta de terminais (EDR) para realizar verificações de postura e garantir que somente dispositivos seguros e gerenciados possam acessar recursos sigilosos.

- **Aplicação baseada em agentes:** o agente de software leve Zscaler Client Connector (ZCC) da Zscaler garante que todo o tráfego de usuário seja roteado pela nuvem de segurança da Zscaler, oferecendo visibilidade e aplicação consistente de políticas de segurança.

- **Zero trust para dispositivos de IoT/ não gerenciados:** as soluções da Zscaler incluem recursos para controlar o acesso por dispositivos não gerenciados, incluindo IoT, usando políticas comportamentais e controles de acesso granulares.

REDE

- **Acesso à rede zero trust (ZTNA):** o Zscaler Private Access (ZPA) substitui as VPNs tradicionais pelo ZTNA. Os usuários recebem acesso de "privilégio mínimo" a aplicativos específicos, não à rede inteira.

- **Secure Access Service Edge (SASE):** a Zscaler atende aos requisitos de arquitetura SASE ao fornecer serviços de segurança dimensionáveis, como Secure Web Gateways (SWG) e firewall na nuvem, em ambientes distribuídos.

- **Microssegmentação:** a Zscaler garante que usuários e cargas de trabalho sejam segmentados no nível do aplicativo, minimizando a movimentação lateral em caso de violação.

- **Monitoramento de criptografia de ponta a ponta:** a Zscaler inspeciona o tráfego de internet criptografado por meio da interceptação de SSL/ TLS sem comprometer o desempenho ou a privacidade.

APLICATIVOS E CARGAS DE TRABALHO

- **Segmentação de aplicativos:** o Zscaler ZPA fornece segmentação baseada em aplicativos em vez da segmentação de rede tradicional, oferecendo conexões diretas e seguras entre usuários e aplicativos.

- **Segurança de cargas de trabalho:** a Zscaler Workload Segmentation (ZWS) protege as comunicações entre cargas de trabalho em ambientes de nuvem pública e privada, garantindo a "microssegmentação baseada em identidade".

- **Monitoramento contínuo:** o monitoramento no nível do aplicativo rastreia a atividade dos usuários e os padrões de acesso em busca de anomalias, garantindo que contas comprometidas não possam aumentar os privilégios.

- **Segurança de SaaS:** o agente de segurança de acesso à nuvem (CASB) da Zscaler controla o acesso a aplicativos SaaS sancionados e não sancionados, impedindo o acesso e uso não autorizado de dados.

DADOS

- **Prevenção contra perda de dados (DLP):** o DLP baseado na nuvem da Zscaler ajuda a proteger dados sigilosos em e-mails, web, SaaS e aplicativos privados. Ele identifica e previne a exfiltração de propriedade intelectual (PI) e informações de identificação pessoal (PII).

- **Gerenciamento da postura de segurança na nuvem (CSPM):** a Zscaler fornece insights e correções para configurações incorretas em sistemas de armazenamento de dados na nuvem, reduzindo os riscos de exposição.

- **Controle de criptografia:** a Zscaler aplica protocolos de criptografia rigorosos para dados em trânsito e em repouso, garantindo que as informações sigilosas sejam protegidas de ponta a ponta.

- **Descoberta de TI invisível:** o CASB da Zscaler identifica e limita o uso de aplicativos/serviços não aprovados ou de alto risco, protegendo dados contra vazamentos acidentais ou uso indevido malicioso.

GOVERNANÇA, VISIBILIDADE, ANÁLISE, AUTOMAÇÃO E ORQUESTRAÇÃO

- **Gerenciamento de segurança centralizado:** a Zscaler Zero Trust Exchange oferece uma visão única do tráfego, das políticas e dos incidentes de segurança.

- **Análise de segurança integrada:** a Zscaler fornece visibilidade em tempo real das atividades de usuários e aplicativos por meio de painéis e logs avançados, integrando-se com plataformas de SIEM/SOAR para uma resposta simplificada a incidentes.

- **Inteligência sobre ameaças:** a Zscaler utiliza inteligência global de ameaças e análise de comportamento para detectar e responder proativamente a ameaças em toda a estrutura zero trust.

- **Aplicação de políticas:** a Zscaler automatiza alterações de políticas e verificações de conformidade, garantindo governança consistente entre usuários, aplicativos e dados.

A abordagem de implementação zero trust da Zscaler e o modelo de maturidade zero trust da CISA são muito semelhantes e se alinham em diversas áreas importantes, não apenas nos pilares do zero trust. A arquitetura da Zscaler oferece suporte a funções essenciais do modelo de maturidade zero trust, como aplicação dinâmica de políticas, visibilidade centralizada e controles de acesso adaptativos baseados em risco; elementos essenciais para o amadurecimento de uma estratégia zero trust. Ao aproveitar uma abordagem nativa da nuvem e em linha, a Zscaler ajuda as organizações a avançar seus níveis de maturidade descritos no modelo da CISA, reduzindo as superfícies de ataque e, ao mesmo tempo, simplificando o acesso seguro.

Roteiro estratégico para adoção do zero trust

Tanto a implementação da Zscaler quanto o modelo de maturidade zero trust da CISA oferecem um roteiro estratégico para as organizações seguirem ao adotar os princípios do zero trust. Dividimos o processo de implementação em etapas gerenciáveis, o que permite que as organizações definam metas e cronogramas realistas para cada fase. Este roteiro garante que as organizações adotem uma abordagem estruturada para a implementação do zero trust, reduzindo o risco de falhas ou erros.

Implementação incremental

A implementação incremental permite que as organizações melhorem gradualmente seus recursos de zero trust ao longo do tempo. Essa abordagem em fases facilita a implementação do zero trust sem sobrecarregar os sistemas ou recursos existentes. Ela também permite que as organizações monitorem o progresso e ajustem as estratégias conforme necessário. Isso permite que a Zscaler lance continuamente novos produtos para melhorar a postura de segurança de nossos clientes, e também permitirá que a CISA, no futuro, ajuste seus critérios. O que é considerado "ótimo" hoje pode ser "avançado" no futuro.

Nenhuma organização é igual

As necessidades de cibersegurança e a infraestrutura de cada organização são únicas. A implementação da Zscaler ZTE e o modelo de maturidade zero trust da CISA são flexíveis o suficiente para serem personalizados e alinhados às metas, desafios e recursos específicos de uma organização. Não importa se uma organização adotou totalmente o zero trust ou se está apenas começando a jornada, o modelo fornece a orientação necessária para adaptar a estrutura zero trust às suas necessidades.

Medição de progresso e sucesso

O modelo de maturidade inclui métricas e critérios de avaliação claros, o que permite que as organizações monitorem seu progresso ao longo do tempo. Ao medir o sucesso em relação a estágios predefinidos, as organizações podem identificar áreas de melhoria e garantir que estão caminhando na direção certa para alcançar um ambiente zero trust maduro.

Conclusão

O modelo de maturidade zero trust 2.0 da CISA fornece às organizações uma estrutura clara e estruturada para adotar e promover os princípios de zero trust. Ao implementar esse modelo, as organizações podem melhorar significativamente sua postura de cibersegurança, mitigar riscos e garantir a conformidade com os requisitos regulatórios.

À medida que o cenário de ameaças continua a evoluir, a importância do zero trust só aumentará, tornando o modelo da CISA uma ferramenta crucial para organizações que buscam proteger seus ambientes digitais contra as ameaças avançadas atuais. Por meio de implementação estratégica e incremental, as organizações podem adotar o zero trust de uma forma que se alinhe às suas necessidades e capacidades específicas, garantindo o sucesso a longo prazo em sua jornada de cibersegurança.

+1 408.533.0288 **Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/br**

zscaler™

Zero Trust Everywhere