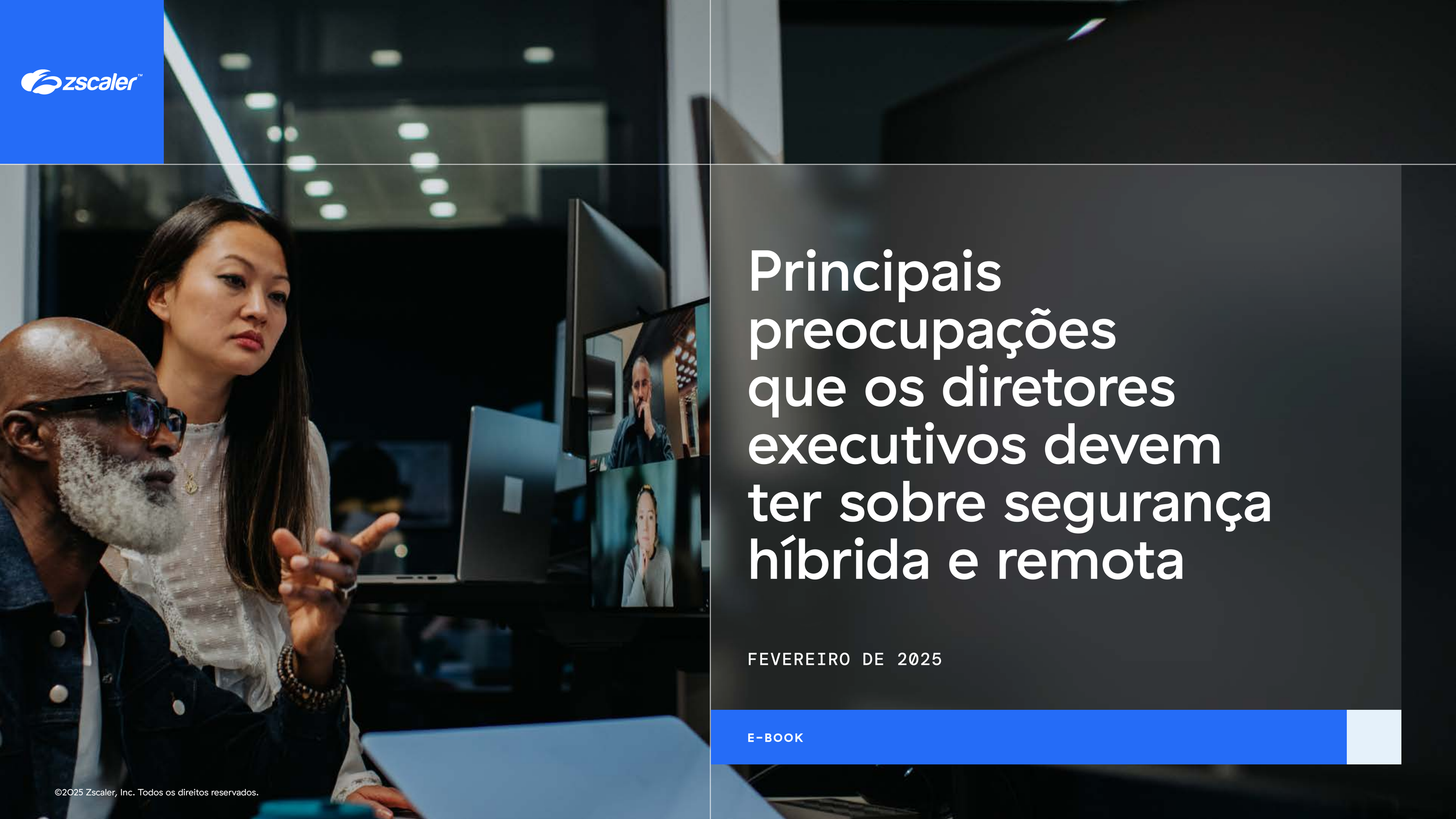


Principais preocupações que os diretores executivos devem ter sobre segurança híbrida e remota

FEVEREIRO DE 2025

E-BOOK

©2025 Zscaler, Inc. Todos os direitos reservados.

Índice

©2025 Zscaler, Inc. Todos os direitos reservados.

Introdução

Os ataques cibernéticos cresceram impressionantes 30% ano a ano[1] globalmente no segundo trimestre de 2024. A adoção crescente do trabalho remoto expandiu a superfície de ataque e deixou as organizações vulneráveis a uma ampla gama de ameaças. De acordo com o Relatório de ataques criptografados da Zscaler ThreatLabz, a nuvem da Zscaler bloqueou 32,1 bilhões de ataques sem precedentes incorporados no tráfego em TLS/SSL, com ameaças criptografadas respondendo por 87,2% de todos os ataques bloqueados; um aumento de 10,3% em relação ao ano anterior.[2] Esses dados destacam o crescente uso de criptografia por criminosos para ocultar suas atividades maliciosas.

Tecnologias legadas como firewalls e redes privadas virtuais (VPNs) não são mais suficientes para proteger dados, aplicativos e redes da empresa, dando aos tomadores de decisão e aos que estão no topo uma longa lista de preocupações quando se trata de proteger ambientes de trabalho remoto. Os líderes estão sob pressão constante para minimizar os riscos de violações, garantir a conformidade com regulamentações e padrões do setor e evitar o roubo de dados valiosos, como propriedade intelectual ou segredos comerciais.

A boa notícia é que as soluções zero trust baseadas na nuvem são projetadas para proteger as redes de organizações com equipes de trabalho remotas e híbridas. Com a tecnologia certa, os executivos podem eliminar essas principais preocupações.

Visão geral de problemas críticos de segurança de rede e remota

As operações de trabalho remoto podem enfraquecer o controle das empresas sobre os dados e a integridade de sua arquitetura de segurança. Funcionários podem usar dispositivos não gerenciados, que podem não ter software de segurança instalado ou ser monitorados ativamente, para acessar recursos da empresa, incluindo aplicativos críticos.

Além disso, os profissionais de segurança não têm visibilidade completa sobre como os funcionários remotos lidam com dados sigilosos e se eles os excluem após o uso. Os funcionários podem armazenar dados em seus dispositivos pessoais, tornando-os vulneráveis a ataques de ransomware, violações de dados e outras ameaças.

A mudança para aplicativos baseados na nuvem expande ainda mais a superfície de ataque, complicando a segurança da sua infraestrutura digital.

©2025 Zscaler, Inc. Todos os direitos reservados.

O cenário de segurança digital em evolução

No mundo pré-pandemia, firewalls e VPNs podem ter sido suficientes para proteger as redes e os dados sigilosos de uma empresa. No entanto, o trabalho remoto e híbrido promoveu a necessidade de uma transformação completa na forma como as organizações protegem seus ambientes digitais hoje.

Últimas tendências em segurança digital e trabalho remoto

Funcionários remotos inevitavelmente precisam de recursos da empresa para fazer seu trabalho, independentemente de sua localização, e muitas organizações adotaram aplicativos de software como serviço (SaaS) baseados na nuvem para dar suporte ao trabalho remoto e melhorar a produtividade. A implantação de SaaS em uma rede de funcionários dispersa resulta em uma superfície de ataque mais ampla e aumenta o risco de acessos não autorizados e violações de segurança.

Os criminosos cibernéticos também desenvolveram táticas mais sofisticadas, incluindo ataques de preenchimento de credenciais e de dia zero, aumentando a aposta para a alta gerência quando se trata de segurança cibernética. Na verdade, os Estados Unidos continuam sendo o principal alvo de ransomware, sofrendo 49,95% dos ataques em geral, seguidos pelo Reino Unido, Alemanha, Canadá e França.[3] Além de corroer a reputação da marca e a confiança dos clientes, esses ataques colocam sua empresa em risco de não conformidade com as regulamentações de privacidade e segurança de dados, além do perigo financeiro.

À luz dessas tendências, diretores executivos e líderes de segurança estão adotando novas medidas de segurança, como:

- **Arquitetura zero trust**, que funciona com o princípio de "nunca confie, sempre verifique". Todos os usuários e dispositivos, incluindo dispositivos pessoais (BYOD), devem ser verificados.
- **Detecção de ameaças com inteligência artificial (IA) e aprendizado de máquina (ML)**, que ajuda a identificar e mitigar proativamente ataques cibernéticos sofisticados.
- **Segmentação de aplicativos**, que impede a movimentação lateral de ameaças.
- **Segurança de terminais**, que foca na proteção dos dispositivos usados por funcionários remotos. Soluções com tecnologia de IA podem detectar e bloquear ameaças antes que elas afetem os terminais, garantindo melhor proteção para equipes de trabalho distribuídas.

©2025 Zscaler, Inc. Todos os direitos reservados.

Principais preocupações de segurança organizacional para líderes

Com a prevalência do trabalho remoto e híbrido e a crescente dependência de soluções baseadas na nuvem, os líderes empresariais e CISOs devem pensar além da segurança baseada em perímetro.

Proteção de dados sigilosos

Quando os funcionários acessam dados comerciais por meio de redes desprotegidas e os salvam em dispositivos pessoais, isso aumenta o risco de acessos não autorizados e manuseio incorreto de dados. A proteção de dados sigilosos em ambientes de trabalho remoto envolve:

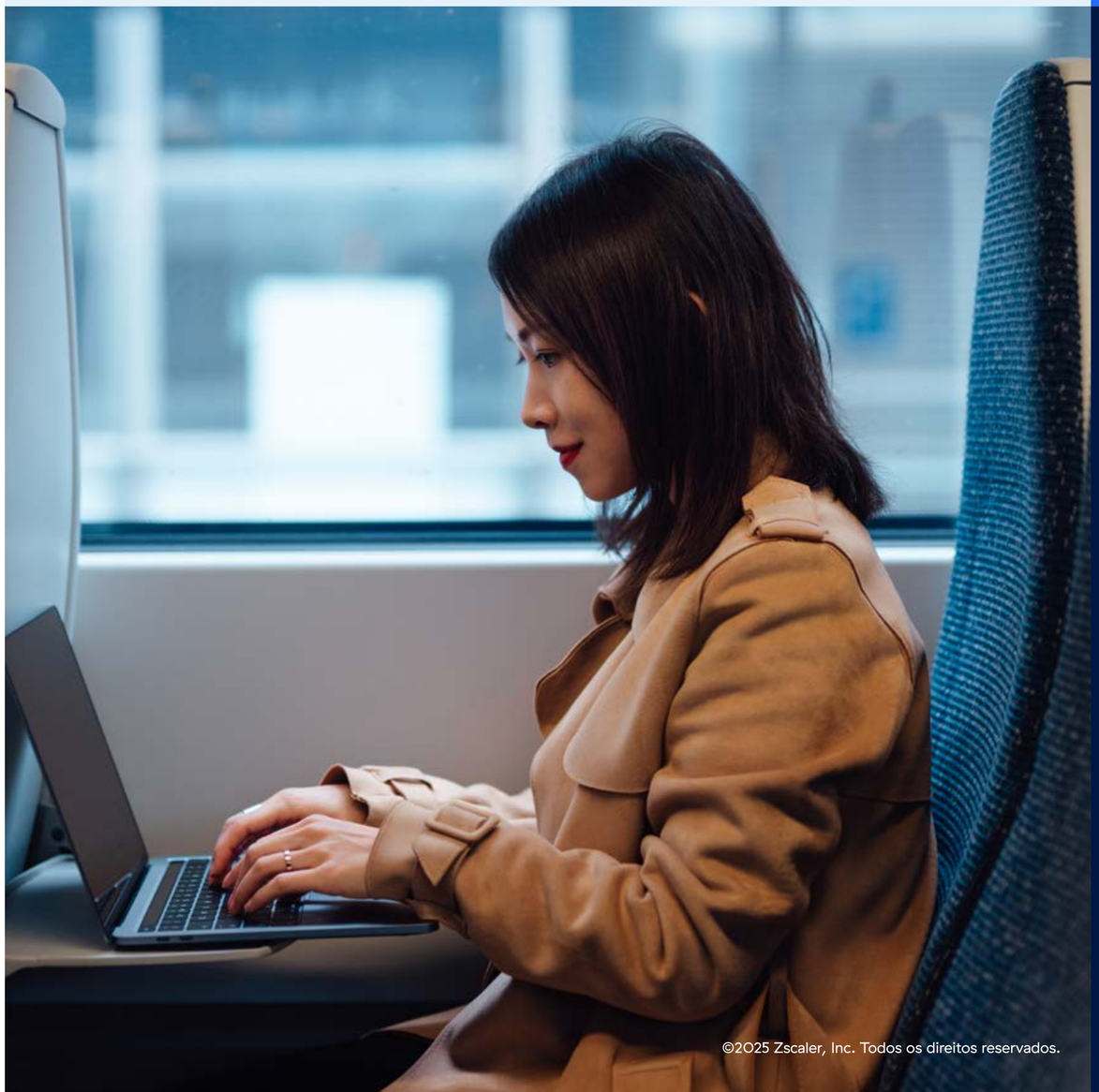
- **Criptografia de ponta a ponta** para proteger dados em repouso e em trânsito, principalmente quando transferidos por canais não seguros.
- **Gerenciamento de identidade e acesso** para garantir que somente funcionários autorizados possam acessar e usar os dados necessários.
- **Técnicas de prevenção contra perda de dados** para mitigar a exposição acidental de dados e violações.

Gerenciamento de ameaças internas

Ações acidentais e intencionais de funcionários locais e remotos podem comprometer a segurança do sistema. Por exemplo, um novo funcionário pode ser vítima de um golpe de phishing, ou um funcionário insatisfeito pode usar indevidamente dados confidenciais da empresa. Controle de acesso baseado em funções, políticas de acesso de privilégio mínimo e análises comportamentais podem ajudar a minimizar os riscos de ameaças internas.

Garantia de cumprimento dos regulamentos

Dezenas de governos implementaram leis de proteção de dados e privacidade para proteger as informações pessoais dos consumidores, como o Regulamento Geral de Proteção de Dados (GDPR) e a Lei de Privacidade do Consumidor da Califórnia (CCPA). Além disso, existem regulamentações específicas do setor, como a Lei de Portabilidade e Responsabilidade de Seguro Saúde (HIPAA). Em ambientes de trabalho remoto, manter a conformidade com esses requisitos regulatórios envolve estratégias de governança completas.



©2025 Zscaler, Inc. Todos os direitos reservados.

Estratégias para abordar preocupações da liderança

Várias estratégias podem ser adotadas por diretores executivos para lidar com os complexos desafios de segurança do ambiente de trabalho moderno.

Implementação de gerenciamento robusto de identidade e acesso

O gerenciamento de identidade e acesso (IAM) é um método eficaz de impedir acessos não autorizados à rede e aos sistemas da sua organização. Ele garante que somente as pessoas certas tenham acesso aos aplicativos e dados necessários para realizar seu trabalho.

O IAM minimiza a superfície de ataque, reduzindo a exposição desnecessária a dados sigilosos. Ao contrário dos métodos de segurança baseados em perímetro, o IAM envolve controles de acesso mais rigorosos, independentemente do dispositivo e da localização do usuário. Os líderes devem considerar a implementação de uma plataforma que ofereça suporte a soluções e integração de IAM flexíveis.

Melhoria das capacidades de detecção e resposta a ameaças

À medida que os cibercriminosos evoluem suas estratégias, os líderes de segurança também devem atualizá-las para impedir ataques com detecção e resposta avançadas a ameaças. Implemente soluções que usem modelos de IA e ML para monitorar o tráfego de rede e o comportamento dos usuários para detectar desvios automaticamente.

IA e ML também ampliam soluções zero trust que isolam dispositivos e arquivos comprometidos em tempo real, permitindo respostas rápidas a ameaças e apoiando uma abordagem de segurança cibernética mais proativa. Os algoritmos de ML também podem destacar vulnerabilidades potenciais ao mesmo tempo em que identificam e bloqueiam ameaças emergentes.

Treinamentos de segurança frequentes e programas de conscientização

As políticas e ferramentas de segurança são tão boas quanto as pessoas que as usam.

Um exemplo: 80% dos CISOs acreditam que a negligência dos funcionários e o risco humano serão as principais preocupações de segurança cibernética até 2026[4]. Os funcionários em ambientes de trabalho remotos são particularmente vulneráveis porque nem sempre podem entrar em contato com profissionais de segurança pessoalmente para obter ajuda, causando atrasos e danos irreversíveis.

Para atenuar esses cenários, as organizações podem implementar programas contínuos de treinamento de segurança que familiarizem os funcionários com ameaças existentes, emergentes e em evolução, além de práticas recomendadas que os capacitem a permanecer vigilantes contra um cenário de ameaças em constante mudança. Instrua sua equipe sobre as práticas recomendadas de trabalho remoto, higiene de senhas e manuseio seguro de dados. Além disso, realize sessões de treinamento com frequência para atualizar os funcionários sobre os protocolos de segurança cibernética de toda a empresa e os recursos prontamente disponíveis sobre o que fazer se seus dispositivos, dados e acesso a aplicativos forem comprometidos.

©2025 Zscaler, Inc. Todos os direitos reservados.

Como aproveitar as soluções da Zscaler para segurança no escritório, híbrida e remota

As soluções de zero trust baseadas na nuvem da Zscaler são projetadas para ajudar líderes empresariais a proteger qualquer ambiente de trabalho hoje e no futuro, conforme as ameaças evoluem. A Zscaler Zero Trust Exchange™ inclui as seguintes soluções essenciais para garantir que as equipes tenham segurança abrangente:

Zscaler Internet Access (ZIA)

O Zscaler Internet Access é uma solução nativa da nuvem, alimentada por IA e zero trust que ajuda a reforçar a segurança digital de equipes de trabalho remotas. Usando uma arquitetura de proxy zero trust que inspeciona 100% do tráfego em TLS/SSL em larga escala, com conexões diretas de usuário para aplicativo baseadas em identidade, contexto e políticas de negócios, o ZIA garante acesso contínuo e seguro a aplicativos SaaS e baseados na web com os seguintes recursos principais:

- **O Secure Web Gateway (SWG) nativo da nuvem** oferece uma experiência web segura e rápida, ao mesmo tempo em que detecta e previne ataques avançados com análise em tempo real, baseada em IA e filtragem de URL.
- **A prevenção contra ameaças avançadas baseada em IA/ML** bloqueia ameaças avançadas como botnets, ransomware, comando e controle, compartilhamento de risco, conteúdo ativo malicioso, cross-site scripting, sites fraudulentos e mais.
- **A filtragem de URL baseada em IA** garante sessões de navegação seguras em aplicativos web para seus usuários interrompendo ameaças avançadas, como phishing e ransomware, e aplicando uma política de uso aceitável.
- **O agente de segurança de acesso à nuvem (CASB)** protege aplicativos na nuvem, dados, bloqueia ameaças e garante a conformidade em seus ambientes de SaaS e IaaS com proteção integrada.
- **A prevenção contra perda de dados (DLP)** protege os dados em trânsito com uma inspeção integrada completa, que inclui correspondência exata de dados (EDM), correspondência de documentos indexados (IDM) e aprendizado de máquina.
- **As políticas dinâmicas e baseadas em risco** impedem ataques ativos e preparam suas defesas para o futuro com a análise contínua de riscos de usuários, dispositivos, aplicativos e conteúdo, alimentando controles de acesso dinâmicos.
- **O firewall zero trust** oferece conexões rápidas e seguras dentro e fora da rede e desvios locais da internet para o tráfego de usuários em todas as portas e protocolos, sem nenhum hardware ou software para gerenciar.
- **O isolamento do navegador com tecnologia de IA** renderiza sessões web apenas como pixels no navegador do usuário, proporcionando uma experiência web quase nativa sem o risco de perda de dados ou infecção do dispositivo.
- **A segurança de DNS** filtra domínios de risco e maliciosos e interrompe o uso do tunelamento de DNS para transferência de cargas maliciosas e dados sigilosos.

©2025 Zscaler, Inc. Todos os direitos reservados.

Zscaler Private Access (ZPA)

O Zscaler Private Access é a primeira solução de acesso à rede de zero trust (ZTNA) com tecnologia de IA do setor e é uma oferta nativa da nuvem que fornece acesso zero trust para todos os usuários. Ao oferecer conectividade direta a aplicativos privados enquanto minimiza a superfície de ataque, o ZPA elimina a movimentação lateral de ameaças usando segmentação de usuário para aplicativo com tecnologia de IA e protege contra ataques sofisticados com inspeção de tráfego integrada e proteção de aplicativos e dados. Alguns dos principais recursos do ZPA que podem proteger as equipes de trabalho híbridas incluem:

- **A segmentação de aplicativos com tecnologia de IA** descobre aplicativos automaticamente e fornece recomendações geradas por IA sobre segmentos e políticas de aplicativos para reduzir sua superfície de ataque e evitar a movimentação lateral.
- **A segmentação de carga de trabalho para carga de trabalho** protege as comunicações de cargas de trabalho na nuvem em ambientes híbridos e multinuvem, como AWS e Azure.
- **O acesso remoto privilegiado** fornece aos trabalhadores remotos e terceiros acesso remoto sem cliente a sistemas de produção de RDP, SSH e VNC sigilosos.
- **A borda de serviço privado** leva o ZTNA para usuários locais com acesso direto dos usuários aos aplicativos e acesso de privilégio mínimo a aplicativos privados.
- **A continuidade de negócios** garante acesso ininterrupto e com aplicação de políticas a aplicativos essenciais durante interrupções de conectividade e eventos inesperados.
- **O suporte a aplicativos de extranet** oferece acesso zero trust a aplicativos de parceiros de negócios e fornecedores hospedados em suas redes.
- **O monitoramento da experiência digital** otimiza suas experiências digitais para manter os usuários produtivos, detectando e resolvendo rapidamente problemas de aplicativos, rede e dispositivos.

Recursos avançados de segurança

A Zscaler oferece vários recursos avançados, incluindo:

- **Inspeção de SSL/TLS** em larga escala para proteção completa de dados e inspeção de usuários a aplicativos.
- **Detecção de ameaças em linha com tecnologia de IA** para bloquear vetores de ataque antes que eles atinjam seu alvo.
- **Risk360™** para visualizações intuitivas de riscos, fatores, detalhes e relatórios para que você possa tomar medidas imediatas para mitigar riscos.

©2025 Zscaler, Inc. Todos os direitos reservados.

Como proteger sua equipe com a Zscaler

Se você deseja fortalecer a segurança do seu ambiente de trabalho remoto, deve considerar abandonar as soluções de segurança cibernética legadas. A plataforma zero trust da Zscaler oferece diversas maneiras de facilitar a transição.

Transformação de firewalls para zero trust

Firewalls e VPNs são ineficazes no ambiente empresarial moderno porque expandem sua rede corporativa, dando aos invasores mais caminhos de entrada. Em contraste, a Zscaler Zero Trust Exchange™ atua como uma central telefônica inteligente, inspecionando o tráfego de entrada e saída de dispositivos de usuários para detectar e bloquear ameaças, ao mesmo tempo em que intermedia conexões seguras com aplicativos e recursos de nuvem.

Uma abordagem zero trust abrangente

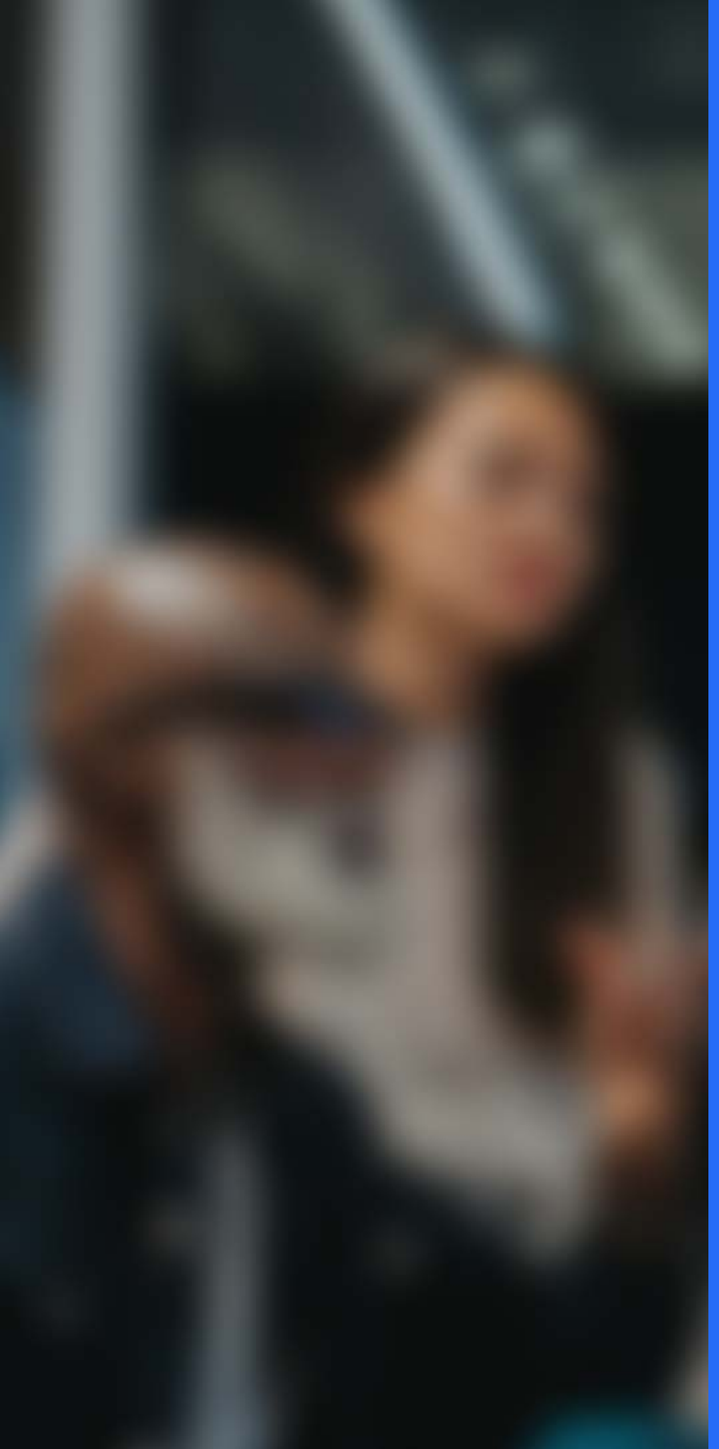
Uma verdadeira abordagem zero trust para segurança requer políticas de acesso centradas na identidade e sensíveis ao contexto, adaptadas a cada usuário, dispositivo e aplicativo. O objetivo é garantir que somente usuários confiáveis possam acessar recursos específicos, e esses usuários e recursos sejam designados pelos controles estabelecidos pela sua empresa. Você pode definir regras em sua estrutura de segurança zero trust para conceder acesso aos usuários com base na localização, identidade, hora/data e mais, e a Zscaler orienta você nesse processo para que sua organização comece com o pé direito com esses controles.

Descubra mais sobre como a Zscaler pode ajudar você a transformar sua postura de segurança para proteger suas equipes de trabalho dispersas solicitando uma demonstração.

FONTES:

1. CISO inteligente, Check Point Research revela tendências de ataques cibernéticos no segundo trimestre de 2024, destacando aumentos globais e nos Emirados Árabes Unidos, 29 de julho de 2024.
2. Zscaler, Relatório de ataques criptografados de 2024 da ThreatLabz, 2024.
3. Zscaler, Relatório de ransomware de 2024 da ThreatLabz, 2024.
4. Revista Infosecurity, 70% dos CISOs esperam ataques cibernéticos no próximo ano, revela relatório, 21 de maio de 2024.

©2025 Zscaler, Inc. Todos os direitos reservados.



zscaler™ | Experience your world, secured.™

©2025 Zscaler, Inc. Todos os direitos reservados. Zscaler™ e outras marcas registradas listadas em zscaler.com/br/legal/trademarks são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.