CrowdStrike, Okta e Zscaler: unificando a segurança com a proteção entre domínios para aumentar a resiliência cibernética na era da IA

Desafios

Os adversários estão se movendo mais rápido do que nunca, com o tempo médio observado para a propagação de crimes cibernéticos caindo para uma baixa histórica de 48 minutos em 2024, e o mais rápido ocorrendo em apenas 51 segundos[1]. Ao mesmo tempo, 79% dos ataques não foram malwares, aproveitando a exploração de identidade, engenharia social e configurações incorretas na nuvem para evitar a detecção[1]. As estratégias de segurança tradicionais e reativas não podem mais conter as táticas em evolução dos adversários modernos. Os criminosos utilizam métodos cada vez mais sofisticados, incluindo automação orientada por IA e táticas furtivas, para se infiltrar e se mover sem serem detectados em ambientes. Para superar esses desafios, as organizações devem ir além de soluções de segurança fragmentadas e pontuais, uma abordagem que aumenta a complexidade, atrasa a resposta e, em última análise, enfraquece a segurança geral.

Do que você precisa

É hora de reimaginar a forma como abordamos a segurança e usar o poder da IA para fornecer velocidade e escala. As organizações precisam de plataformas de segurança avançadas que funcionem perfeitamente em conjunto para fornecer proteção em camadas, reduzindo a complexidade e promovendo a eficiência operacional.

Solução

Para lidar com as ameaças em evolução intensificadas pela IA, CrowdStrike, Okta e Zscaler fornecem uma solução de segurança totalmente integrada e multidomínio, projetada para eliminar pontos cegos, aumentar a visibilidade e acelerar os tempos de resposta para uma mitigação robusta de ameaças. Essa abordagem combinada protege e autentica identidades, oferece controles de acesso zero trust dinâmicos e sensíveis ao contexto e protege terminais distribuídos, ao mesmo tempo em que aproveita o SIEM de última geração para detecção e resposta a ameaças em tempo real.

Ao correlacionar sinais de risco em camadas de identidade, terminais, nuvem, rede e além, as equipes de segurança obtêm uma visão unificada da movimentação de adversários, permitindo que elas detectem, contenham e neutralizem as ameaças antes que causem danos. Com automação orientada por IA, compartilhamento bidirecional de inteligência sobre ameaças e ações de resposta coordenadas, a solução conjunta não apenas detecta ameaças, mas também as interrompe antes que elas se agravem.

As equipes de segurança podem antecipar táticas adversárias, automatizar ações de resposta e se mover na velocidade da máquina para conter ataques antes que os adversários se propaguem.

À medida que as ameaças cibernéticas se tornam mais rápidas e sofisticadas, as organizações devem adotar uma defesa proativa, alimentada por IA, que opere na velocidade dos adversários, garantindo que as ameaças sejam neutralizadas antes que afetem os negócios.

Segurança que funciona como uma só: proteção unificada para uma nova era

Para organizações que estão iniciando uma jornada zero trust ou projetando uma solução zero trust que maximize os investimentos atuais, as sólidas parcerias e integrações comprovadas dos líderes de mercado CrowdStrike, Okta

1. Relatório de ameaças globais de 2025 da CrowdStrike, https://www.crowdstrike.com/en-us/global-threat-report/"

e Zscaler fornecem um modelo para uma solução zero trust de ponta a ponta, desde usuários até terminais e aplicativos.Essas integrações fornecem aos administradores visibilidade em tempo real do cenário de ameaças e da postura de segurança de terminais e aplicativos.

O acesso a aplicativos críticos pode ser alterado com base nas políticas de usuário, terminais e acesso. Se ocorrer um ataque, a remediação multiplataforma será acionada rapidamente. As defesas são ainda mais fortalecidas com políticas de prevenção aplicadas entre as integrações para impedir ataques semelhantes no futuro.

O resultado é uma excelente solução de zero trust dinâmica, nativa da nuvem e orientada por contexto, que ajuda as equipes a ficarem à frente das ameaças modernas alimentadas por IA com risco reduzido e implantação simplificada, eliminando a complexidade das abordagens do tipo \"faça você mesmo"\.

Destaques da solução

Acesso adaptativo zero trust:

a Zscaler aplica acesso de privilégio mínimo com base na identidade do usuário, postura do dispositivo e contexto de risco, com a Zscaler Zero Trust Exchange (ZTE) integrando a Identity Threat Protection com as pontuações da Okta AI (ITP) e CrowdStrike Falcon® ZTA para implantar políticas de acesso baseadas em risco em tempo real.

Gerenciamento automatizado do ciclo de vida da identidade:

a Okta simplifica o provisionamento e o desprovisionamento de usuários por meio da integração do Okta SCIM, oferecendo atualizações baseadas em funções em tempo real e reduzindo a carga de trabalho manual.

Detecção de ameaças de identidade e terminais:

a CrowdStrike detecta e atenua ameaças direcionadas a usuários e terminais compartilhando sinais do Zscaler Deception com o Okta ITP para oferecer respostas adaptativas, enquanto a telemetria da CrowdStrike fornece contexto detalhado para aumentar a detecção de ameaças.

Autenticação contínua e acesso baseado em risco:

a Zscaler aplica políticas de acesso dinâmicas com a Okta acionando autenticação por etapas com base em comportamento anômalo detectado pela Zscaler ou CrowdStrike.

Visibilidade de risco unificada:

o Zscaler Risk360 e o Data Fabric assimilam logs de identidade da Okta e sinais de terminais da CrowdStrike.

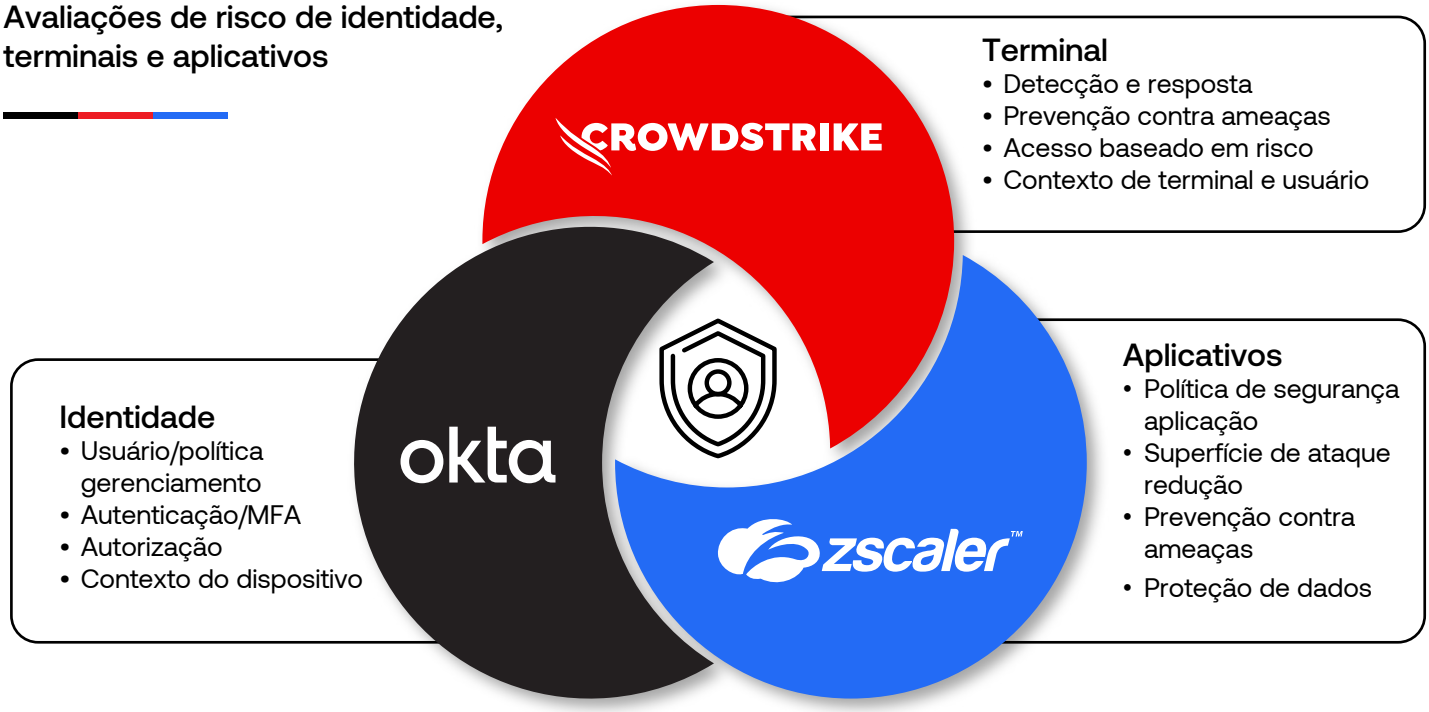
Compartilhamento de inteligência sobre ameaças entre plataformas:

a Zscaler compartilha telemetria unificada para acelerar a detecção e a resposta, com a CrowdStrike aprimorando as listas de bloqueio personalizadas da Zscaler para oferecer proteção proativa.

Detecção e resposta unificadas a ameaças entre domínios:

a CrowdStrike oferece visibilidade abrangente e respostas coordenadas e automatizadas em terminais, identidades e aplicativos por meio das integrações do CrowdStrike Falcon® Next-Gen SIEM e CrowdStrike Falcon® Fusion SOAR com a Okta e a Zscaler para ver e interromper rapidamente ameaças entre domínios, evitando a movimentação lateral.

Avaliações de risco de identidade, terminais e aplicativos



Telemetria compartilhada e inteligência de ameaças

Os benefícios das sinergias combinadas para uma resiliência cibernética de nível superior

1. Acesso zero trust aumentado:
O acesso zero trust impede a movimentação lateral de ameaças com a aplicação de políticas de acesso adaptáveis, com base na identidade do usuário, na postura do dispositivo e no contexto da ameaça em tempo real.

2. Detecção e remediação automatizadas de ameaças:
A detecção em tempo real e a inteligência sobre ameaças acionam respostas imediatas e coordenadas, incluindo a aplicação de políticas e o logout universal.

3. Visibilidade unificada de riscos:
O Zscaler Risk360 integra-se aos logs da CrowdStrike e da Okta para fornecer telemetria contextualizada e insights abrangentes sobre riscos, acelerando a investigação e a remediação.

4. Investigação e resposta rápidas:
Investigação e resposta aceleradas por meio da integração com o SIEM de última geração CrowdStrike Falcon, que fornece visibilidade unificada, detecção com tecnologia de IA e fluxos de trabalho automatizados para conter rapidamente ameaças entre domínios.

5. Gerenciamento de identidade eficiente:
O provisionamento baseado em SCIM da Okta garante provisionamento e desprovisionamento de usuários seguros e automatizados, permitindo somente acesso autorizado.

6. Experiência de usuário aprimorada:
O acesso contínuo habilitado pelo Okta SSO, MFA e políticas adaptáveis da Zscaler aumenta a produtividade sem comprometer a segurança.

Conclusão

A CrowdStrike, a Okta e a Zscaler oferecem soluções de segurança integradas e simplificadas que aumentam a proteção, reduzem a complexidade e garantem a capacidade de dimensionamento para os ecossistemas digitais em evolução atuais.

Juntas, elas capacitam organizações com uma defesa zero trust que simplifica o acesso baseado em identidade e fortalece a detecção de ameaças entre domínios. Essa parceria poderosa ajuda as organizações a fortalecer proativamente sua postura de cibersegurança e a construir resiliência para a era da IA.

Sobre a CrowdStrike

A CrowdStrike (NASDAQ: CRWD), líder global em cibersegurança, redefiniu a segurança moderna com a plataforma nativa da nuvem mais avançada do mundo para proteger áreas críticas de risco empresarial: terminais e cargas de trabalho na nuvem, identidade e dados. Desenvolvida especificamente na nuvem com uma única arquitetura de agente leve, a plataforma Falcon oferece implantação rápida e dimensionável, proteção e desempenho superiores, complexidade reduzida e tempo de retorno imediato.

Sobre a Okta

A Okta, Inc. é referência mundial em identidade. Nós protegemos a identidade para que todos tenham liberdade para usar qualquer tecnologia com segurança. Nossas soluções para clientes e equipes de trabalho capacitam empresas e desenvolvedores a usar o poder da identidade para promover segurança, eficiência e sucesso, enquanto protegem seus usuários, funcionários e parceiros. Saiba por que as principais marcas do mundo confiam na Okta para autenticação, autorização e muito mais em okta.com.

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que os clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança em linha na nuvem do mundo. Saiba mais em zscaler.com ou siga-nos no Twitter @zscaler.

Saiba mais sobre nossas soluções em okta.com, crowdstrike.com e zscaler.com.br |