Zscaler e CrowdStrike

Estendendo zero trust para modernizar o centro de operações de segurança (SOC)

Resumo da solução

Principais destaques

- A Zscaler coleta e analisa sinais ativos de incidentes de segurança que ocorrem no terminal a partir da plataforma CrowdStrike Falcon, adicionando uma camada de contexto detalhada ao seu mecanismo de política de controle de acesso adaptável e tornando o controle de acesso zero trust orientado pela postura do dispositivo ainda mais robusto.
- O serviço Zscaler Risk360 integra-se à CrowdStrike para fornecer insights sobre fatores que contribuem para o risco dentro da sua organização, categoriza-os em estágios de ataque do Risk360 e quantifica cada fator de acordo com seu peso de risco.
- O Data Fabric for Security da Zscaler detalha e correlaciona os dados de CVE da CrowdStrike com fluxos de dados simultâneos para fornecer insights contextualizados e em tempo real sobre vulnerabilidades e exposições em todo o seu patrimônio de TI.
- Desenvolvido nativamente pela CrowdStrike, o aplicativo Falcon Foundry Zscaler serve como base para a integração da Zscaler com a plataforma de gerenciamento de eventos e incidentes de segurança de última geração (NG-SIEM) da CrowdStrike. A oferta predefinida automatiza e orquestra o compartilhamento de informações sobre ameaças e permite ações políticas coordenadas para uma resposta rápida e eficaz às ameaças à segurança.

O desafio

O trabalho híbrido dissolveu o perímetro e continua a reinventar o cenário de negócios, deixando as organizações com a complexa tarefa de gerenciar com segurança equipes de trabalho distribuídas de qualquer local e em qualquer dispositivo, ao mesmo tempo em que protegem seus negócios de ataques cibernéticos.

A mudança de paradigma na forma como o trabalho é feito levou a um crescimento exponencial no número de dispositivos conectados a redes corporativas atualmente. Cada dispositivo conectado representa um possível ponto de entrada para ataques cibernéticos, complicando ainda mais os esforços de segurança.

Em meio aos desafios do setor, as equipes de TI e segurança lutam para manter o acesso seguro aos aplicativos em diversos ambientes multinuvem e cenários de ameaças flutuantes. Elas precisam de visibilidade e controle para dimensionar a segurança em todo o vasto ecossistema de terminais e aplicativos para proteger todas as superfícies de ataque em potencial.

As equipes de operações de segurança enfrentam seus próprios desafios específicos. Encarregadas de detectar ameaças avançadas e monitorar riscos de grandes volumes de dados desconexos, espera-se que elas respondam a incidentes de segurança no menor tempo possível. Tudo isso enquanto coordenamos de forma superlativa estratégias de resposta em diversas ferramentas e plataformas. Para agravar esses desafios, há uma lacuna entre a segurança de TI e as operações de segurança, que muitas vezes atrasa a resolução de incidentes, enfraquecendo a postura geral de segurança da organização.

Zscaler e CrowdStrike: uma abordagem incomparável de defesa em profundidade

A Zscaler e a CrowdStrike oferecem uma solução de segurança zero trust integrada que simplifica a segurança do terminal ao aplicativo em um mundo híbrido. Expandindo os principais recursos de zero trust, a solução oferece um conjunto de novas integrações poderosas que transformam o centro de operações de segurança (SOC).

A plataforma Zscaler Zero Trust Exchange™, disponibilizada na nuvem da Zscaler, serve como uma central inteligente que conecta com segurança milhões de usuários, dispositivos e aplicativos em qualquer rede e local. A Zscaler ampliou ainda mais o poder de sua plataforma com novos recursos para quantificação de riscos e contextualização de dados para ajudar a resolver as dificuldades cotidianas enfrentadas pelas operações de segurança na detecção e resposta a ameaças.

Ao integrar a segurança zero trust líder do setor da Zscaler e o gerenciamento de riscos com tecnologia de IA com a proteção avançada de terminais, inteligência sobre ameaças e recursos de SIEM de última geração da CrowdStrike, a solução integrada simplifica todo o ciclo de vida de gerenciamento, detecção e resposta de risco, alinhando de maneira eficaz a segurança de TI e as operações de segurança.

A integração da Zscaler e da CrowdStrike é multicamadas e compatível com vários casos de uso:

- **Acesso zero trust adaptável:** a Zscaler aproveita as pontuações do dispositivo CrowdStrike Falcon Zero Trust Assessment (ZTA) e os sinais de incidentes de segurança para habilitar controles de acesso adaptáveis, garantindo que apenas dispositivos seguros tenham acesso a aplicativos.
- **Compartilhamento de inteligência sobre ameaças:** os indicadores de comprometimento (Iocs) da CrowdStrike alimentam o mecanismo de inteligência sobre ameaças da Zscaler, aprimorando suas listas de bloqueio personalizadas para prevenção proativa de ameaças.
- **Detecção avançada de ameaças de dia zero e quarentena:** a Zscaler Cloud Sandbox integra-se à telemetria da CrowdStrike Falcon para detectar malware de dia zero e facilitar ações rápidas de quarentena em terminais afetados.
- **Iscas para inteligência sobre ameaças antecipadas:** o Zscaler Deception implementa iscas em terminais, redes, nuvens e sistemas de identidade para fornecer alertas de alta fidelidade sobre indicadores antecipados de ataque (IOAs) e compartilhar essa inteligência sobre ameaças de alta confiança com a CrowdStrike.
- **Visibilidade holística de riscos cibernéticos, avaliação de riscos e gerenciamento** o Zscaler Risk360 e o Data Fabric for Security assimilam fatores de risco exclusivos em toda a cadeia de ataque e dados de CVE, respectivamente, da CrowdStrike para quantificar riscos e priorizar vulnerabilidades críticas em fluxos de trabalho de correção automatizados.
- **Compartilhamento e correlação de telemetria entre plataformas:** a Zscaler integra-se à CrowdStrike para compartilhar logs relevantes da Zscaler para melhor visibilidade de ponta a ponta com telemetria de terminais, redes e aplicativos na nuvem para maximizar a eficácia entre plataformas para investigações aceleradas.
- **Detecção e resposta entre plataformas:** o SIEM de última geração CrowdStrike Falcon agora se integra à Zscaler por meio do aplicativo Falcon Foundry for Zscaler e fornece correção totalmente integrada entre a sandbox avançada do ZIA, o SIEM de última geração da CrowdStrike e o mecanismo de aplicação de políticas do ZIA.

As integrações mais recentes da Zscaler e CrowdStrike são compatíveis com os seguintes novos casos de uso:

Caso de uso 1

Aplicação de política de acesso adaptável com base no contexto

Expandindo o escopo dos recursos de acesso adaptável, a Zscaler agora aproveita o contexto em tempo real da CrowdStrike, oferecendo avaliação de risco superior e tomada de decisões de aplicação de políticas. A nova integração vai além da aplicação de políticas de controle de acesso com base nas pontuações de integridade do dispositivo Falcon ZTA e agora incorpora dados detalhados de incidentes de segurança da CrowdStrike para avaliar riscos em tempo real.

A Zscaler coleta e analisa sinais ativos de incidentes de segurança que ocorrem no terminal da CrowdStrike, adicionando uma camada detalhada de contexto ao seu mecanismo de política de controle de acesso adaptável e tornando o controle de acesso zero trust orientado pela postura do dispositivo ainda mais robusto.

O fluxo contínuo de dados de incidentes de segurança da CrowdStrike fornece uma postura de segurança dinâmica e responsiva do terminal ao aplicativo, ampliando significativamente os recursos de acesso adaptável da Zscaler e oferecendo controles de acesso mais granulares e sensíveis ao contexto.

Com esse novo recurso, os administradores da Zscaler agora podem definir limites de incidentes de segurança e conceder acesso de aplicativos a terminais que atendem à conformidade do Falcon ZTA e aos critérios de limite de incidentes de segurança especificados.

A integração da CrowdStrike com a Zscaler compartilha inteligência sobre ameaças e oferece fluxos de trabalho automáticos bidirecionais para ajudar as organizações a reduzir o número de incidentes de segurança e, se ocorrer um incidente, oferece tempo rápido de detecção e correção.

Caso de uso 2

Quantificação e visualização holística de riscos cibernéticos

O Zscaler Risk360 é uma poderosa estrutura de quantificação e visualização de riscos para remediar riscos de cibersegurança. Ele assimila dados reais de fontes externas, do ambiente do cliente da Zscaler e de pesquisas de segurança da ThreatLabz para gerar um perfil detalhado da postura de risco da organização. A estrutura abrange os quatro estágios de ataque (superfície de ataque externo, comprometimento, propagação lateral e perda de dados) e todas as entidades do seu ambiente, incluindo ativos, aplicativos, usuários e terceiros.

O serviço Risk360 integra-se à CrowdStrike para fornecer insights sobre fatores que contribuem para riscos dentro da sua organização. Uma vez configurado, a Zscaler extrai informações relacionadas a riscos da plataforma Falcon, categoriza-as em categorias de estágios de ataque do Risk360 e quantifica cada fator de acordo com seu peso de risco.

Essa integração permite que os clientes tomem medidas com base nas políticas para atualizá-las ou alterá-las. Ela também inclui fluxos de trabalho investigativos guiados que permitem análises mais profundas para investigar questões específicas.

Caso de uso 3

Contextualização de dados de segurança e gerenciamento unificado de vulnerabilidades

Atualmente, as equipes de segurança utilizam uma infinidade de tecnologias e soluções para proteger seus negócios de uma superfície de ataque em expansão. Cada uma dessas ferramentas produz grandes quantidades de dados valiosos. No entanto, esses dados geralmente ficam isolados e são duplicados entre as ferramentas. Como resultado, as equipes de segurança precisam lidar com sobrecarga de informações, fluxos de trabalho pouco transparentes e crescente dificuldade em defender sua postura de cibersegurança.

O Data Fabric for Security da Zscaler agrega dados de diferentes ferramentas, tornando-os mais práticos e úteis. Ele transforma a maneira como as operações de segurança gerenciam e respondem a ameaças de segurança, agregando perfeitamente dados de mais de 150 fontes, incluindo vulnerabilidades e exposições comuns (CVEs) detectadas nos terminais pela CrowdStrike. O Data Fabric enriquece e correlaciona os dados de CVE da CrowdStrike com fluxos de dados simultâneos para fornecer insights contextualizados e em tempo real sobre vulnerabilidades e exposições em todo o seu patrimônio de TI.

Munidos desse conhecimento, os analistas de segurança podem conectar dinamicamente os pontos entre vulnerabilidades, ameaças, descobertas, incidentes, ativos, componentes de software e usuários, e contar com inteligência prática e de referência cruzada para priorizar e abordar com eficiência as vulnerabilidades e os riscos mais críticos primeiro.

Caso de uso 4

Compartilhamento, detecção e resposta coordenados a ameaças

Desenvolvido nativamente pela CrowdStrike, o aplicativo Falcon Foundry Zscaler serve como base para a integração da Zscaler com o SIEM de última geração CrowdStrike Falcon. O aplicativo predefinido automatiza e orquestra o compartilhamento de inteligência sobre ameaças e oferece ações políticas coordenadas para uma resposta rápida e eficaz às ameaças à segurança.

Disponível no CrowdStrike Marketplace, o aplicativo predefinido permite que clientes mútuos licenciados melhorem a segurança de seu perímetro por meio de monitoramento avançado e detecção de ameaças, utilizando indicadores de comprometimento (IoCs) provenientes dos repositórios de informações sobre ameaças da CrowdStrike. Além disso, ele permite que os clientes desenvolvam e implantem fluxos de trabalho personalizados, adaptados para casos de uso específicos de detecção, investigação e resposta a ameaças.

Ao criar um ciclo de feedback contínuo e um mecanismo de resposta coordenado entre a sandbox avançada do ZIA, o SIEM Falcon de última geração e o mecanismo de aplicação de políticas do ZIA, o aplicativo pronto para uso simplifica a automação e a orquestração do fluxo de trabalho de segurança para acelerar as operações de segurança.

Benefícios do trabalho em conjunto

- **Políticas de acesso adaptáveis com contexto detalhado:** melhore sua postura de segurança do terminal ao aplicativo aplicando políticas zero trust que se adaptam dinamicamente às condições de mudança.
- **Visibilidade holística do cenário de risco cibernético:** obtenha uma visão precisa da exposição ao risco nos quatro estágios do ataque e aproveite a pontuação de risco consolidada em várias fontes para uma compreensão completa do risco cibernético.
- **Dados de segurança contextualizados para melhor avaliação de riscos:** agregue e contextualize dados de segurança para priorizar seus maiores riscos e automatizar o fluxo de trabalho para correção.
- **Integração de SOAR pronta para uso:** comece a usar o aplicativo Foundry para Zscaler para compartilhamento de inteligência sobre ameaças. Crie fluxos de trabalho de SOAR personalizados do Falcon Fusion rapidamente para automatizar a detecção, a investigação e a resposta de ponta a ponta.
- **Detecção rápida e resposta coordenada:** acelere o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR) com ações coordenadas de resposta e aplicação de políticas que eliminam as brechas entre a segurança de TI e as operações de segurança.

Fortaleça as operações de segurança com Zscaler e CrowdStrike

A Zscaler e a CrowdStrike têm a missão de aumentar a aplicação do zero trust e fortalecer as operações de segurança com poderosos recursos complementares. Nossas integrações mais recentes funcionam perfeitamente em conjunto para elevar suas operações de segurança ao próximo nível. Em conjunto, expandimos a aplicação do zero trust de ponta para inaugurar a era do SOC moderno.

CROWDSTRIKE

Sobre a CrowdStrike
A CrowdStrike redefiniu a segurança com a plataforma nativa da nuvem mais avançada do mundo, que protege e capacita as pessoas, os processos e as tecnologias que impulsionam as empresas modernas. A CrowdStrike protege as áreas de risco mais críticas (terminais e cargas de trabalho na nuvem, identidade e dados) para manter os clientes à frente dos adversários atuais e impedir violações. Com a tecnologia CrowdStrike Security Cloud, a plataforma CrowdStrike Falcon® utiliza indicadores de ataque em tempo real, inteligência sobre ameaças sobre a evolução da tecnologia dos adversários e telemetria aprimorada de toda a empresa para fornecer detecções hiperprecisas, proteção e remediação automatizadas, caça a ameaças de elite e observabilidade priorizada de vulnerabilidades; tudo por meio de um único agente leve. Com a CrowdStrike, os clientes se beneficiam de proteção superior, melhor desempenho, complexidade reduzida e retorno imediato do investimento. Saiba mais em crowdstrike.com.

SAIBA MAIS EM
zscaler.com/partners/crowdstrike

Baixe nosso guia de implantação Zscaler + CrowdStrike

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus 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 SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

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