White Paper da CrowdStrike

CROWDSTRIKE

Principais motivos para adicionar o Falcon Identity Threat Protection ao seu portfólio de ciberdefesa agora mesmo

Os ataques baseados em identidade são a principal ameaça à cibersegurança que as organizações enfrentam atualmente. Na verdade, mais de 80% dos incidentes cibernéticos envolvem o uso indevido de credenciais válidas para obter acesso à rede de uma organização.

O CrowdStrike Falcon® Identity Threat Protection, um módulo da plataforma CrowdStrike Falcon®, detecta e interrompe ataques direcionados a identidades em tempo real, em um cenário complexo de identidade híbrida, com um único sensor e uma interface unificada de ameaças com correlação de ataques entre endpoints, workloads, identidade e dados. Aqui estão cinco benefícios esperados que você pode ter ao adicionar proteção de identidade ao seu portfólio de ameaças à cibersegurança hoje.*

1. Possibilita respostas às ameaças até 85% mais rápidas

As soluções tradicionais somente para endpoint ignoram ameaças à identidade, e a abordagem atual de correlacionar manualmente ameaças entre endpoint e identidade com várias ferramentas autônomas — ferramentas de higiene do AD, logs de eventos do Windows, PAM, UEBA, SIEM e muito mais — retarda as respostas da equipe do SOC. Com a plataforma unificada CrowdStrike Falcon, os clientes do Falcon Identity Threat Protection podem ver caminhos de ataque completos e correlacionar ameaças em um único console. Isso pode resultar em **respostas até 85% mais rápidas** e proteção em tempo real, compensando milhares de horas de investigação pós-ataque todos os anos.

2. Aumenta a eficiência operacional em até 84%

O CrowdStrike Falcon é **uma solução nativa da nuvem com um único sensor** que pode ser implementado em qualquer lugar do ambiente do cliente, simplificando a coleta de telemetria (do endpoint ou da identidade). Um grande distribuidor de varejo **consolidou mais de 5 ferramentas** (típicas de muitas empresas) em uma para gerenciar ameaças de identidade com o Falcon Identity Threat Protection. A consolidação do SOC com uma plataforma e um sensor elimina ferramentas e agentes autônomos, resultando em economia direta de ferramentas e custos operacionais. E, ao eliminar a necessidade de empregar uma ingestão diferente de log, a detecção em tempo real pode reduzir o total de horas de manutenção e **aumentar a eficiência operacional em até 84%**, reduzindo o número de funcionários a aproximadamente quatro FTEs.

3. Reduz os custos de conformidade e suporte em até 75%

A visibilidade profunda de senhas comprometidas, contas com privilégios excessivos e uso indevido de contas de serviço permite que os clientes resolvam proativamente os problemas de higiene do Active Directory e estabeleçam controles proativos, reduzindo assim os custos de conformidade. Em um caso, um CISO relatou uma **redução de 75% no suporte às redefinições de senha e custos associados,** uma redução de 8% na suscetibilidade ao phishing e uma redução de 32% nos direitos de acesso desnecessários do usuário. Um grande provedor de telecomunicações relatou ter melhorado a postura de conformidade com a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) ao usar o Falcon Identity Threat Protection para estender a autenticação multifatorial (MFA) em todos os lugares, incluindo aplicativos legados.

4. Reduz o risco de roubo de credenciais que levem a um ataque em até 57%

Com oito em cada dez ataques envolvendo credenciais roubadas ou comprometidas, a redução do risco de credenciais roubadas tem um impacto direto na melhoria da postura de risco. A capacidade do Falcon Identity Threat Protection de detectar ameaças específicas de identidade permite que os clientes identifiquem contas de alto risco e possíveis caminhos de ataque em todo o ambiente, reduzindo a superfície de ataque. Recentemente, o CISO de uma cadeia de hospitalidade compartilhou como o Falcon Identity Threat Protection revelou imediatamente 250.000 possíveis caminhos de ataque no ambiente da empresa e como 93% deles poderiam ser corrigidos com três mudanças de configuração específicas. As avaliações de valor de negócio da CrowdStrike mostraram uma **redução de até 57% no risco de credenciais roubadas** levarem a um ataque. Isso também foi demonstrado por testes de intrusão bem-sucedidos feitos por clientes que falharam nos mesmos testes antes da implementação do Falcon Identity Threat Protection.

5. Melhora a segurabilidade cibernética e reduz os prêmios

À medida que os adversários continuam explorando controles fracos de segurança de identidade para lançar ataques, **as empresas de seguro cibernético enfatizam** a necessidade de reforçar os controles para reduzir o risco cibernético. Como o ransomware é um dos principais fatores do seguro de cibersegurança, as seguradoras reiteraram a necessidade de as organizações fortalecerem o AD, aplicarem a MFA em aplicativos, incluindo os legados, protegerem contas privilegiadas e de serviço e implementarem a detecção e resposta de endpoint (EDR) como pré-requisitos para a segurabilidade cibernética. Os clientes que implementaram o Falcon Identity Threat Protection afirmam que isso impactou positivamente seu programa de seguro de cibersegurança e reduziu os prêmios.

O que os clientes da CrowdStrike dizem

"Depois de implementar o Falcon Identity Threat Protection, fizemos outro teste de intrusão e imediatamente vimos os benefícios da visibilidade aprimorada."

Ryan Melle
SVP, CISO, Berkshire Bank
(**Leia o estudo de caso**)

"Desde a implementação do Falcon Identity Threat Protection, tivemos uma grande melhoria no que podemos ver com relação a credenciais, identidades privilegiadas, diferentes caminhos de ataque e como podemos mitigá-los."

Steven Townsley
Chefe de Segurança da Informação, Mercedes-AMG Petronas F1 Team.
(**Assista ao vídeo**)

"Duas horas após a implementação do Falcon Identity Threat Protection, identificamos 10 contas privilegiadas com senhas comprometidas e começamos a redefini-las imediatamente."

CISO de uma região na área de Washington, D.C.
(**Leia a postagem do blog**)

"Aproveitamos o valor do Falcon Identity Threat Protection logo no primeiro minuto, quando vimos 250.000 possíveis caminhos de ataque e 93% deles puderam ser corrigidos com apenas três mudanças de configuração."

CISO de uma cadeia de hospitalidade multinacional

"É mais fácil manter tudo em uma tela para a maior parte do seu SOC do que examinar 13 consoles e páginas diferentes para analisar e rastrear algo."

CISO de uma empresa de agronegócio e alimentos

A proteção de identidade é essencial, não opcional

O Relatório Global de Ameaças 2023 da CrowdStrike mostra que os ataques a identidade estão aumentando, com um crescimento de **112% nos anúncios de broker de acesso** na dark web em 2022. O Microsoft Active Directory continua sendo o ponto fraco a ser perseguido pelos adversários, com mais de 90% das organizações confiando nele.[1] Uma recente análise de metadados de milhões de contas (humanas, de serviços, privilegiadas) feita pela CrowdStrike revelou que **50% das organizações têm contas privilegiadas com uma senha comprometida**.

Para agravar esse problema, os ataques à identidade são notoriamente difíceis de detectar, exigindo uma média de **cerca de 250 dias para identificar**[2] sem as ferramentas certas. Durante esse período, os adversários podem se mover lateralmente sem serem detectados em seu ambiente e realizar ataques catastróficos. Com o tempo médio para comprometimento **de 84 minutos em 2022**, de acordo com o Relatório Global de Ameaças de 2023 do CrowdStrike, as organizações não têm o luxo de esperar que ocorra um grave ataque à identidade. Na verdade, o adversário pode já estar em seu ambiente e você pode não estar ciente disso.

Pode haver sérias consequências por ignorar ameaças baseadas em identidade, incluindo comprometimento total do domínio de sua infraestrutura de AD, ataques paralisantes de ransomware e interrupções catastróficas nos negócios. De acordo com a IBM e o Ponemon Institute, o **custo total médio global de um ataque de dados é de US$ 4,35 milhões (custo médio de ataque de US$ 9,44 milhões nos Estados Unidos)**.[3] Com **8 em cada 10 ataques** envolvendo credenciais roubadas ou comprometidas, a implementação da proteção de identidade terá impacto imediato, potencialmente economizando milhões de dólares e protegendo sua marca e reputação de danos irreversíveis.

Lembre-se de que os adversários não estão esperando que você bote suas luvas antes de lhe darem porrada. Interrompa o ataque hoje mesmo com o Falcon Identity Threat Protection.

Entre em contato com seu representante de conta CrowdStrike ou solicite sua análise de risco gratuita do Active Directory.

[1]Frost & Sullivan, "Active Directory Holds the Keys to your Kingdom, but is it Secure?"

[2]IBM e Ponemon Institute, "Cost of a Data Breach Report 2022"

[3]IBM e Ponemon Institute, "Cost of a Data Breach Report 2022"

*Os resultados esperados e reais não são garantidos e podem variar para cada cliente. Os benefícios esperados 1, 2 e 4 são baseados em médias agregadas de mais de 100 casos de Avaliação de Valor de Negócio (BVA) e Valor de Negócio Realizado (BVR) conduzidos com clientes da CrowdStrike Enterprise e concluídos pela equipe de Valor de Negócio da CrowdStrike de 2018 a dezembro de 2022. Os BVAs são uma análise de ROI projetada com base no valor da CrowdStrike em comparação com a solução atual do cliente. Os BVRs são uma análise de ROI realizada para clientes, implementada por mais de 6 meses usando entradas do cliente e telemetria gravada. O benefício esperado 3 é baseado em dados compartilhados por um cliente diretamente com a CrowdStrike.

Sobre a CrowdStrike

CrowdStrike (Nasdaq: CRWD) é a líder global em cibersegurança que redefiniu a segurança moderna com a plataforma nativa em nuvem mais avançada do mundo para proteger áreas de risco corporativo crítico — endpoints e workloads, identidade e dados na nuvem.

Impulsionada pela CrowdStrike Security Cloud e por IA de alto nível, a plataforma CrowdStrike Falcon® utiliza indicadores de ataque em tempo real, inteligência de ameaças, estratégias adversárias em evolução e telemetria enriquecida de toda a empresa para fornecer detecções hiperprecisas, proteção e correção automatizadas, investigação de ameaças de elite e observabilidade priorizada de vulnerabilidades.

Construída especificamente em nuvem com arquitetura de um único agente leve, a Plataforma Falcon fornece uma implementação rápida e escalável, proteção e desempenho superiores, complexidade reduzida e retorno imediato.

CrowdStrike: **Nós interrompemos ataques.**

Siga-nos: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Inicie uma avaliação gratuita

Saiba mais em **www.crowdstrike.com.br**