CrowdStrike White Paper

CROWDSTRIKE

Improve Cyber Insurability with Falcon Identity Protection

Key Security Controls for Insurability

Organizations seek to stop breaches, minimize revenue loss and lawsuits, and protect their brand reputation. And, insurers want a definitive handle on continuously assessing the risks for existing and prospective cyber insurance customers. This has resulted in a number of cybersecurity controls, with some of them being an absolute minimum, non-negotiable set of security controls to become insurable.

With all of these controls becoming an absolute minimum to be insurable, organizations should prioritize where they are most vulnerable, and where to invest to remediate known and evolving threats, reduce cyber risk and stay insurable.

Why Focus on Identities?

According to the **CrowdStrike 2023 Global Threat Report,** adversaries are getting faster. The **breakout time** declined to **just 84 minutes in 2022**, from the previous year's 98 minutes. They can move laterally faster than ever. From 2021 to 2022, there was a **112% increase in access brokers** that specialize in acquiring and selling credentials — making it easier for adversaries to get to valid credentials.

Work from anywhere and digital transformation have further increased the attack surface. In fact, about **25% of attacks observed by the CrowdStrike® Falcon OverWatch™ threat hunting team are from unmanaged hosts** — for example, vendor/contractor laptops and legacy systems. This means identity-based attacks can originate from unprotected endpoints using compromised credentials to access resources and applications.

There is also the risk of hybrid lateral movement when signing into cloud applications from the internal network using domain-joined, trusted endpoints, as Kerberos is used for authentication. If the adversary can generate a Kerberos ticket for the user, this will enable unchallenged access to all applications and data that the user does.

When **80% of all breaches use compromised identities**, strengthening the identity security posture is critical to protecting businesses and improving insurability.

Insurers and Underwriters Want a Robust Identity Protection Strategy

With ransomware being one of insurers' cybersecurity insurance policy factors, insurers have reiterated the need for organizations to deploy MFA for accessing applications, privileged accounts and backup folders/drives as a prerequisite for cyber insurability. In short, insurers may decline to do business with organizations that don't enforce MFA and deploy endpoint security like endpoint detection and response (EDR).

Organizations applying for cyber insurance should exercise identity store hardening (e.g., Active Directory, Azure Active Directory), along with the security controls to detect all/unauthorized RDP, remote access sessions and use/misuse of service accounts. Organizations should have risk-based conditional access enforcement to stop the aforementioned identity-based incidents and malicious activities in real time.

Insurers look at these key security controls:

1. Multifactor authentication (MFA)
2. Secured and tested backups
3. Patched systems and applications
4. Filtered emails and web content
5. Protected privileged accounts
6. Protected network
7. Secured endpoints (endpoint detection and response)
8. Logged and monitored network
9. Phishing-aware workforce
10. Vulnerability management
11. Hardened device configuration
12. Prepared incident response

25%
of attacks are from unmanaged hosts

CrowdStrike Falcon® Identity Protection

Falcon Identity Protection Overview

The CrowdStrike Falcon® Identity Protection modules — CrowdStrike Falcon® Identity Threat Detection and CrowdStrike Falcon® Identity Threat Protection — enable frictionless security with hyper-accurate threat detection and real-time prevention of identity-based attacks. With continuous behavioral analytics and a flexible policy engine to enforce risk-based conditional access, Falcon Identity Protection accelerates cyber insurability **by securing regular human and service accounts**, including **privileged accounts.** Falcon Identity Protection provides unified visibility and security control across Microsoft AD and Azure AD, integrates with multiple SSO and MFA vendors, and stops lateral movement and attack progression across the hybrid IT infrastructure.

How Falcon Identity Protection Improves Insurability

Falcon Identity Protection helps you comply with the important identity and access management questions seen on several cyber insurance applications.

Do you enforce MFA for all user accounts, including domain admin accounts?
Falcon Identity Protection enables real-time enforcement of MFA, not just for privileged and domain administrator accounts, but also for regular human and service accounts. Falcon Identity Protection integrates with a majority of MFA vendors that the organization may have, maximizing the return on investment.

Is MFA limited to remote access to corporate networks, or is it for externally hosted assets and applications too?
Falcon Identity Protection extends identity verification/MFA to any resource or application, including legacy and proprietary systems and tools that traditionally could not be integrated with MFA — for example, desktops that are not covered by cloud-based MFA solutions, and tools like **PowerShell and protocols like RDP over NTLM** — to reduce the attack surface. In addition to risk-based MFA, Falcon Identity Protection's conditional access actions include allow, block and audit.

How many service accounts are in your IT environment?
Falcon Identity Protection provides automatic classification of all accounts and enables **dedicated insights into service accounts**, their risk posture, group membership (e.g., Domain Admin), risk score and risk trend, services accessed (e.g., RDP), endpoints used and applications accessed.

Do you have specific monitoring rules for service accounts to alert/identify abnormal behavior, and detect and deny interactive logins?
Falcon Identity Protection baselines every account, including service accounts, to identify deviations and risky activity and provides a detailed account of every identity-based security incident tied to the service account(s), such as service account misuse, interactive logins and stale account activity (**see how it's done in this video**).

Do you use Remote Desktop Protocol (RDP) and MFA to control access?
Falcon Identity Protection detects suspicious protocol activity, not limited to only RDP, and enforces MFA based on the risk and least privileged access policy requirements. Adversaries gaining access to domain controllers (DCs) via RDP is a common technique in most ransomware (**see how Falcon Identity Protection stops ransomware**) and supply chain attacks. Falcon Identity Protection enforces risk-based conditional access (risk-based MFA) in real time to **stop adversary action and lateral movement**.

Are there controls in place for Server Message Block (SMB) — i.e., Windows file sharing — communications?
In addition to real-time analysis and detections covering Kerberos, NTLM and LDAP/S, Falcon Identity Protection extends the protocol coverage enabling detection of authentication attempts over SMB to DCs. Also, Falcon Identity Protection enables risk-based MFA to **stop SMB access to a file share**.

Do you use a Privileged Access Management (PAM) tool?
Falcon Identity Protection enables visibility and security control of all accounts tied to AD, Azure AD and SSOs like Okta, Ping and Active Directory Federation Services (AD FS). Falcon Identity Protection looks at live authentication traffic and analyzes behavior and risks for **ALL** users, including regular human, service and **privileged accounts**.

Falon Identity Protection provides deep insights into the behavior and risks associated with every privileged account, and stops lateral movement and attack progression in real time. In addition, Falcon Identity Protection detects privilege escalation of regular accounts in real time and enforces policies to stop breaches.

Most importantly, this holistic understanding of risks, not restricted to just privileged accounts, enables organizations to assess cyber insurance readiness, demonstrating the ability to reduce risks and stop breaches with risk-based conditional access (risk-based MFA) applied to privileged accounts.

Why CrowdStrike Falcon Identity Protection?

The growth in frequency and severity of cyberattacks has caused organizations to rethink their security strategies. Cyber insurers expect organizations buying cyber insurance policies to be equipped with the right tools to detect, mitigate and respond to evolving adversarial tactics. Whether you are in the middle of a ransomware breach or are electing for cyber insurance, Falcon Identity Protection takes only a few hours — not days — to give you holistic visibility of your identity threat landscape.

Deployment and operational simplicity: Falcon Identity Protection accelerates time-to-value with rapid deployment and scalability with a single lightweight-agent architecture and unified threat-centric data fabric for identities, endpoints and privileged access. It provides an instant overview of the identity store security posture, with automatic classification and privilege assessment of all identities, to fast-track cyber insurability.

Superior protection: Falcon Identity Protection reduces the attack surface with **identity segmentation** and granular visibility into behavioral (access) changes not only for privileged accounts but also for regular human and service accounts. It provides dynamic risk scoring for every account, spanning multi-directory environments, and supports Microsoft AD, Azure AD and seamless integrations with SSO/federation solutions like Okta, AD FS and PingFederate.

Attack path visibility for audits: Falcon Identity Protection captures deviations, failed logins, service account misuse and other identity-related incidents in real time to enable audits. These can also be fed into SIEM tools for compliance reasons or to enhance SOC operations and facilitate threat hunting.

Extended MFA coverage: With support for multi-vendor MFA solutions, including Okta, PingID, Azure MFA, DUO and more, Falcon Identity Protection provides risk-based MFA without degrading the user experience. Falcon Identity Protection extends MFA to even legacy and proprietary systems and tools that are not covered by cloud-based MFA solutions and tools like PowerShell and protocols like RDP over NTLM.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Request a free review

Get a no-cost, complimentary AD Risk Review with our identity experts.