

IDENTITY PROTECTION SERVICES

Gain deeper visibility to protect against identity-based attacks

THE MISUSE OF VALID CREDENTIALS IS TODAY'S BIGGEST CYBER THREAT

Identity-based attacks are the No. 1 cybersecurity threat facing organizations of all sizes today. Over 80% of cyber incidents involve the misuse of valid credentials to gain access to an organization's network.

Once initial access is gained, threat actors escalate their privileges and begin laterally moving across your systems looking to exfiltrate your data and detonate a major cyberattack.

IMPLEMENT A ZERO TRUST APPROACH TO IDENTITY PROTECTION

Information security leaders need visibility into the risks associated with their user passwords and permissions and their Active Directory configuration so they can reduce their organizational attack surface, detect suspicious lateral movements and prevent unauthorized access to their systems.

CrowdStrike Identity Protection Services deploys the Falcon Identity Protection modules to ensure real-time prevention of identity-based attacks even if adversaries manage to bypass endpoint security and are using valid, stolen credentials.

KEY BENEFITS

Reduce attack surface: Harden your Microsoft Active Directory configuration to reduce your attack surface

Stop lateral movement: Identify and prevent unauthorized users from accessing and moving laterally across your systems

Extend MFA to legacy systems: Extend multifactor authentication to legacy protocols (e.g., NTLM) that are most prone to identity-based attacks

KEY SERVICE FEATURES

OPERATIONALIZE AND CUSTOMIZE IDENTITY SOLUTIONS

- Assists in deploying and operationalizing CrowdStrike Identity Protection solutions.
- Integrates the Falcon Identity Protection platform with on-premises and cloud-based identity and access management solutions.
- Gives guidance and recommendations on effective implementation and configuration of multifactor authentication across your environment.
- Implements conditional access policies and reporting.

IDENTITY SECURITY ASSESSMENT

- Conducts an in-depth assessment of your endpoints, identities and Active Directory environment highlighting major risks and issues.
- Provides guidance on identity and Active Directory hygiene best practices and policies.
- Highlights areas of major risk including privileged accounts, compromised passwords, password aging and stale or inactive accounts.
- Proactively identifies misconfigurations known to be exploited by knowledgeable threat actors.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services delivers Incident Response, Technical Assessments, Training, and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more at www.crowdstrike.com/services/

Email: services@crowdstrike.com

WHY CHOOSE CROWDSTRIKE?

Enhance security with continuous Zero Trust Assessment: CrowdStrike's superior technology platform delivers continuous real-time security posture assessments across your endpoints

Implement frictionless risk-based authentication: Enable the enforcement of conditional access based on device health and compliance checks to mitigate risks

Stop identity-based attacks: Stop attacks in real time even if adversaries manage to bypass endpoint security and are using valid, stolen credentials

