

Identity Security Assessment

Achieve a deeper understanding of your identity ecosystem across on-premises and hybrid identity environments

Challenge: Persistent threats to identity ecosystems

As organizations continue their transition to hybrid identity environments, combining on-premises Active Directory with cloud-based identity solutions, threat actors are increasingly exploiting these ecosystems. Misconfigured settings, overly permissive access controls, and legacy features provide ample opportunities for privilege escalation and lateral movement. These vulnerabilities, often overlooked in both traditional AD and hybrid (Entra ID) setups, serve as a gateway for attackers to gain unauthorized access, deploy ransomware, or exfiltrate sensitive data. Proactive measures to harden these environments, identify misconfigurations, and monitor for suspicious activity are essential to mitigate these risks and secure critical identity infrastructures.

Solution: Proactive risk and attack path discovery

The CrowdStrike Identity Security Assessment delivers an in-depth analysis of your identity ecosystem, including Active Directory and Entra ID domain configurations, account settings, privilege delegation, and hybrid attack paths across on-premises and cloud environments. By identifying misconfigurations and areas of exposure, this assessment empowers you to proactively secure your network and reduce the risk of breaches before they occur. It uncovers hygiene issues, misconfigurations, excessive administrative privileges, and anomalous authentication activity, and identifies hybrid attack paths that threat actors could exploit in on-premises and hybrid identity environments.

Key benefits

- Proactively fortify your identity ecosystem
- Maximize the power of CrowdStrike Falcon® Identity Threat Detection, CrowdStrike Falcon® Cloud Security, and CrowdStrike Falcon® Shield
- Gain unmatched visibility into your identity environment
- Identify hidden and stealthy administrators
- Pinpoint critical misconfigurations and exploitable vulnerabilities
- Gain clarity on exploitable identity-based attack vectors

Key service features

Strengthen Your Security Posture

Understanding which features are in use and how permissions are delegated is critical to defending your identity environment against attacks. Proactively identifying and addressing unauthorized systems and applications helps mitigate risks before they escalate.

- **Prevent Active Directory and Entra ID abuse:** Monitor and mitigate the exploitation of Active Directory permissions and misconfigurations to ensure proper and secure usage.
- **Detect password issues:** CrowdStrike Falcon Identity Threat Detection provides instant visibility into accounts with duplicated, weak, or compromised passwords.

Identify Attack Paths

The complexity of identity ecosystems — including on-premises Microsoft Active Directory and federated cloud identity providers like Entra ID — makes it challenging to visualize and understand potential attack paths. The CrowdStrike Identity Security Assessment team delivers actionable insights into how threat actors may exploit these environments.

- **Get detailed visual representations:** The team provides a comprehensive view of hybrid attack paths, illustrating how adversaries can target vulnerabilities to move laterally or escalate privileges.
- **Align to real-world adversary actions:** Attack paths are mapped using tactics and techniques observed in the wild, providing a realistic view of how attackers operate in similar hybrid environments.

Realize Immediate Time-to-Value

The CrowdStrike Falcon® platform delivers immediate deployment and value, allowing the CrowdStrike Identity Security Assessment team to analyze your Active Directory and Entra ID environment without the need for additional reboots, complex configurations, or staging.

- **Save time, effort, and costs:** Delivered via the cloud, the CrowdStrike Identity Security Assessment eliminates the need for on-premises devices or complex deployments.
- **Instant visibility:** Gain immediate context and actionable insights into your Active Directory domain and Entra ID tenants — data aggregation begins upon deployment.
- **Zero disruption:** The assessment operates seamlessly, without requiring reboots or impacting endpoints and networks.

Assessment output

With this assessment, organizations receive:

- A detailed report highlighting identity ecosystem issues, misconfigurations, and gaps
- Actionable, supplemental technical data designed for easy implementation by IT teams
- Weekly status reports to review and discuss findings, ensuring clarity and alignment on next steps

Why choose CrowdStrike?

- Highly skilled employees with a wide range of expertise across all areas of cybersecurity
- Superior platform spanning across network, endpoint, identity, and data
- Top-tier adversary and threat intelligence embedded into the platform
- Leading provider of proactive and reactive cybersecurity services

About CrowdStrike

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: www.crowdstrike.com/services/

Email: services@crowdstrike.com

