

Falcon Next-Gen SIEM: Identity Hygiene Now Included

See identity risk in real time to strengthen your security posture

Identity-related risks and user details are now visible directly within CrowdStrike Falcon® Next-Gen SIEM — powered by CrowdStrike Falcon® Next-Gen Identity Security. Get unified visibility across endpoint, identity, and SaaS to stop adversaries in their tracks.

Why it matters

Identity is the new front line — and attackers know it. From SCATTERED SPIDER's credential theft to FAMOUS CHOLLIMA's exploitation of overprivileged accounts, adversaries are evolving faster than traditional defenses can respond. Every identity — human, non-human, and AI — is now a potential entry point.

- **81%** of detections are malware-free¹
- **442%** increase in vishing attacks²
- **50%** increase in access broker activity²

Identity Hygiene in Falcon Next-Gen SIEM

Identity Hygiene delivers real-time visibility into 26 critical identity risks from Active Directory and Microsoft Entra ID including.

- Compromised credentials
- Stealthy privileges
- Aged passwords
- Kerberos pre-auth disabled
- GPO-exposed passwords
- Suspicious SPNs
- Vulnerable OS

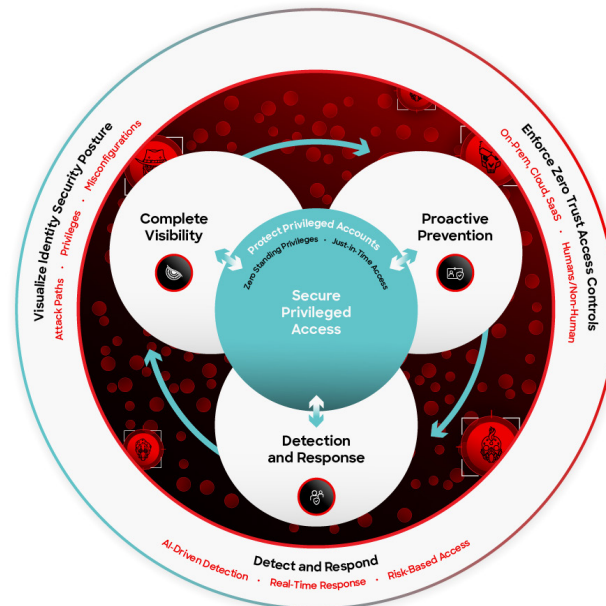
¹CrowdStrike 2025 Threat Hunting Report

²CrowdStrike 2025 Global Threat Report

Key benefits

- **Protect against credential theft and abuse by tracking suspicious users and privileged accounts.**
- **Accelerate response with unified visibility of identity, endpoint, and cloud telemetry that are automatically correlated into Falcon Next-Gen SIEM cases.**
- **Strengthen your SIEM posture with early detection of compromised identities.**

Falcon Next-Gen SIEM: Identity Hygiene Now Included



Unlock full protection with Falcon Next-Gen Identity Security

Upgrade from visibility to real-time protection with Falcon Next-Gen Identity Security, delivering AI-powered security across the entire identity attack chain.

Extend your defense to:

- Protect every identity, everywhere — human, non-human, AI, and SaaS
- Eliminate standing privileges with just-in-time privileged access
- Secure the full identity lifecycle: access → privilege → lateral movement → impact
- One platform, total security — unify identity threat detection and response (ITDR), privileged access, and SaaS security in one platform

Transform identity insights into full protection

Ready to take the next step? Contact your CrowdStrike representative to activate Falcon Next-Gen Identity Security and stop identity-based attacks before they start.

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.



Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>