

Falcon Next-Gen Identity Security

Stop identity-driven breaches in real time with continuous, AI-native control

The New Security Imperative

Identity is now the primary attack path — and attackers aren't breaking in, they're logging in. Modern adversaries use valid credentials to move laterally, escalate privileges, and operate undetected across hybrid environments.

Legacy identity and access management (IAM), privileged access management (PAM), and fragmented identity tools rely on static, point-in-time decisions that grant standing access and assume trust. They lack the ability to continuously validate risk, incorporate real-time context, and enforce access dynamically.

The result: Organizations can detect identity risk — but cannot act on it fast enough. The gap between detection and enforcement is where breaches happen.

The CrowdStrike Difference

CrowdStrike Falcon® Next-Gen Identity Security transforms identity from a static control into a real-time, always-on security system to outpace today's identity-driven attacks. Built on the AI-native CrowdStrike Falcon® platform, it unifies identity visibility and intelligence, identity threat detection and response (ITDR), modern privileged access, and SaaS and AI security into a single control plane, delivering Continuous Identity and real-time enforcement across every identity and environment.

Unlike many legacy solutions, CrowdStrike continuously evaluates identity, device, threat, and active business context signals to dynamically grant, adjust, or revoke access in real time.

- Identity risk is not just detected — it is stopped instantly
- Fragmented tools are replaced with one unified platform
- Implicit trust is eliminated in favor of dynamic, risk-based enforcement

This is Continuous Identity — purpose-built to stop modern adversaries before they escalate.

Key benefits

- Secure every identity — human, non-human, and AI agent — across hybrid environments with continuous, always-on protection built for today's adversaries.
- Eliminate standing privileges with context-aware access control that dynamically grants, adjusts, and revokes access the moment conditions change.
- Stop identity-driven attacks in real time by unifying identity, endpoint, cloud, browser, and SaaS signals into a single, AI-native platform that enables immediate, automated enforcement.

Key capabilities

Discover, Correlate, and Enrich Every Identity

- Continuously discover human, non-human, and AI identities across on-premises, cloud, and SaaS environments to eliminate blind spots
- Correlate identities with applications, workloads, and data to expose overprivileged accounts, misconfigurations, and attack paths
- Enrich identity data with device posture, threat intelligence, and identity risk signals for precise access decisions
- Incorporate business context (roles, workflows, ticketing systems) to ensure access aligns with real operational justification
- Create a unified, real-time identity fabric that enables confident, context-aware enforcement

Enforce Modern Privileged Access

- Dynamically grant just-in-time (JIT) privileges and application access based on real-time risk and business context
- Continuously validate access throughout the session — not just at login
- Automatically adjust or revoke privileges when risk, behavior, or device posture changes
- Enforce least privilege across all identities, eliminating persistent access and reducing the attack surface
- Extend Zero Trust access control across hybrid environments, including SaaS and cloud platforms

Stop Identity Attacks in Real Time

- Detect and respond to identity threats including credential abuse, lateral movement, and privilege escalation
- Revoke access mid-session to immediately cut off adversary activity
- Deliver phishing-resistant multifactor authentication (MFA) to block credential-based attacks in real time
- Dynamically trigger step-up authentication across environments and resources
- Detect and block session hijacking, token theft, and post-authentication attacks

SaaS and AI Agent Security

- Gain visibility into SaaS applications, users, and AI agents, including shadow IT and unauthorized AI usage
- Analyze permissions, access patterns, and integrations to identify excessive privileges and reduce risk from misconfigured or over-permissioned apps
- Monitor AI agent activity to detect anomalies, enforce governance, and mitigate risks
- Correlate identity, endpoint, and SaaS activity to uncover risky behavior and improve threat detection across the SaaS stack

One Platform. Identity-First Security. Complete Protection.

- Unify identity, endpoint, cloud, and SaaS protection in a single platform with one sensor and one console
- Deliver full visibility into identity-driven attacks across all domains
- Correlate identity activity with endpoint, SaaS, cloud, and business telemetry for faster investigation and response
- Enable immediate, cross-domain enforcement to stop attacks as they move between environments
- Eliminate gaps created by siloed tools and reduce operational complexity

[Get a free risk review](#)

Falcon Next-Gen Identity Security Maturity Model

Capabilities	Falcon Next-Gen Identity Security	Falcon Next-Gen Identity Security Privileged
Identity provider risk assessment (AD, Entra, Okta, Ping, etc.)	✓	✓
Identity attack path analysis	✓	✓
Privileged account visibility	✓	✓
Non-human identity (NHI) discovery, visibility, and classification	✓	✓
SaaS security posture management (SSPM)	✓	✓
Automated SaaS compliance reporting and assessment	✓	✓
Shadow SaaS and AI discovery	✓	✓
AI usage monitoring and governance	✓	✓
Interconnected application visibility	✓	✓
Identity threat detection and response (ITDR)	✓	✓
Authentication traffic inspection	✓	✓
Identity behavioral profiling (baseline and anomaly detection)	✓	✓
Password and credential-based risk detection	✓	✓
Malicious OAuth detections	✓	✓
SaaS threat detection	✓	✓
Conditional access policy enforcement	✓	✓
Phishing-resistant MFA	✓	✓
JIT privileged access for identities		✓
JIT privileged access for applications		✓
JIT privileged access for cloud resources		✓
Continuous access evaluation protocol (CAEP)		✓

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.

Learn more: <https://www.crowdstrike.com/>

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

