

Falcon Privileged Access

Powered by Falcon Identity Protection

Eliminate standing privileges and stop identity-based attacks — without the complexity of traditional privileged access management (PAM) solutions

Identity is under attack. The CrowdStrike 2025 Global Threat Report revealed a 442% surge in vishing attacks between the first and second half of 2024 and a 50% year-over-year increase in dark web ads selling stolen credentials — giving adversaries a direct path into your environment. Threat actors like CURLY SPIDER have used social engineering to trick employees into gaining access and creating backdoor users within minutes. FAMOUS CHOLLIMA has also been observed escalating privileges by assigning cloud administrator policies to backdoor users to aid in data exfiltration. SCATTERED SPIDER took it further, requesting and receiving elevated privileges through a PAM solution, effectively granting themselves full control.

When attackers move this fast, security teams need real-time defense that doesn't slow users down. **CrowdStrike Falcon® Privileged Access** eliminates standing privileges and enforces just-in-time access to stop identity-based attacks — without the complexity of traditional PAM tools. Built on the CrowdStrike Falcon® platform and powered by CrowdStrike Falcon® Identity Protection, it delivers real-time, risk-based privileged access control across hybrid environments without requiring manual onboarding of identities or resources.

With Falcon Privileged Access, dynamic environments are supported out of the box — no enrollment or reconfiguration needed as users, roles, and systems change. Granular, risk-aware policies adapt dynamically, enabling security teams to respond instantly to threats without disrupting business productivity.

By combining privileged access control with Falcon Identity Protection's industry-leading identity threat detection and response (ITDR), comprehensive visibility, and proactive prevention capabilities, CrowdStrike keeps the full identity attack lifecycle secured. From initial compromise to privilege escalation, everything is secured through a single, unified platform.

Key benefits

- **Reduce the identity attack surface** by eliminating standing privileges and enforcing just-in-time access across hybrid environments
- **Accelerate time-to-value** with a platform-native solution — no additional PAM infrastructure or credential vaults required
- **Stop lateral movement and privilege escalation** through continuous risk monitoring and automated access revocation
- **Unify identity, endpoint, and privileged access security** on the Falcon platform
- **Simplify operations** with frictionless automation, saving time for both security and identity teams

Key capabilities

Block Adversaries and Insider Risks

Remove always-on privileged access that attackers exploit. Enforce just-in-time access to grant privileges only when needed, and revoke them instantly when risk conditions change.

- **Real-time access control:** Evaluate and enforce access policies dynamically at the time of login or when user risk changes.
- **Context-aware enforcement:** Base privilege access decisions on dynamic user, device, and behavioral risk signals from the Falcon platform.
- **Continuous privilege evaluation:** Re-evaluate privileges throughout the session — not just at the point of access request — to allow real-time revocation via CrowdStrike Falcon® Fusion SOAR signals (e.g., high-severity endpoint incidents).

Simplify Privileged Access with Real-Time Enforcement

Automate privileged access without operational complexity or user friction.

- **Grant and elevate access automatically at login:** Accelerate adoption with just-in-time access based on dynamic risk, eliminating portals, manual approvals, infrastructure overhead, and maintenance complexity.
- **Deliver a seamless user experience:** Allow users to work in their native environments with no jump servers, ticketing systems, or credential vaults required.
- **Integrate with existing tools:** Connect to IAM, SOAR, and ticketing systems via API to streamline privileged access workflows.

Unify Identity Protection and Privileged Access

Protect privileged access across hybrid identity providers — without siloed tools or fragmented enforcement.

- **Unified enforcement:** Apply consistent just-in-time access policies across Active Directory (AD), Microsoft Entra ID, and other identity providers including Okta, AWS, and SaaS apps.
- **Cloud and legacy support:** Enforce privileged access control across cloud platforms and legacy protocols to support modern and transitional environments.
- **Privileged account risk reduction:** Eliminate excessive access for administrators, service accounts, and shared identities across identity stores.

Frictionless Privileged Access Security

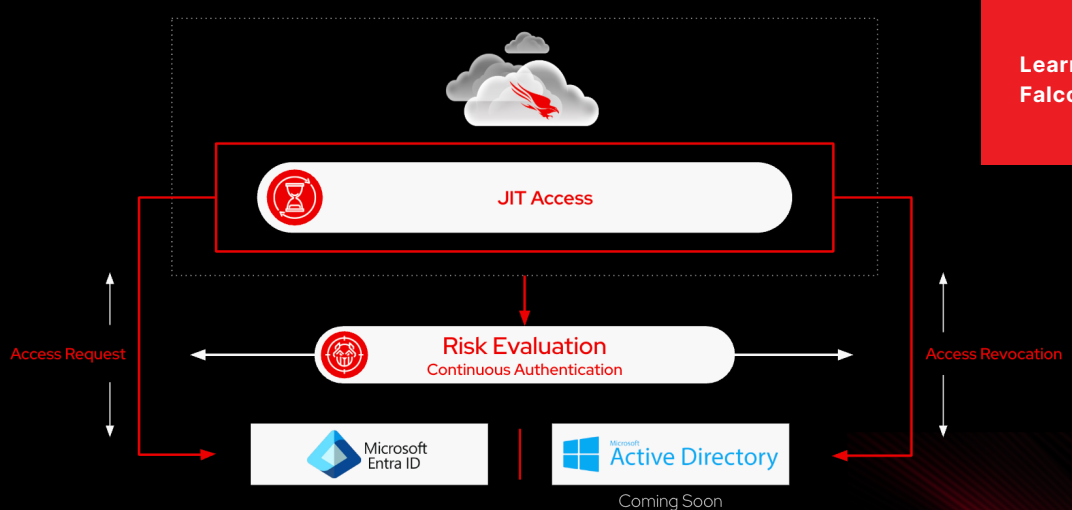
- **Platform-native deployment:** Falcon Privileged Access is built on the Falcon platform with shared policy, telemetry, and automation workflows.
- **Effortless adaptability:** There are no extra infrastructure, reconfigurations, or disruptions as environments evolve.
- **No separate PAM tools required:** CrowdStrike delivers privileged access control and identity protection in one unified solution.

How It Works

Users request privileged actions, which trigger real-time risk evaluation based on signals from the user, device, session, and other contextual factors.

CrowdStrike analyzes these risk signals and makes an instant access decision, granting or denying access based on policy and current risk posture.

Access is continuously enforced and revoked the moment risk changes, using built-in threat detection and response capabilities from Falcon Identity Protection.



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 at www.crowdstrike.com/

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

