

FALCON COMPLETE IDENTITY THREAT PROTECTION

Managed identity threat protection (ITP), powered by CrowdStrike's global team of MDR experts

CHALLENGES

The modern threat landscape continues to evolve with an increase in attacks leveraging compromised credentials. An attacker with compromised credentials too frequently has free rein to move about an organization and carefully plan their attack before they strike.

Identity threat protection technology can segment identities and autonomously enforce risk-based conditional access, reducing risk significantly. It also provides a perfect platform for responders to revoke access quickly when threats are uncovered in the environment. But technology alone is not a silver bullet to stopping breaches. Sophisticated attacks of this nature require a mix of technology and human expertise to mount an effective defense, ensuring defenses are optimized and response to threats can come in minutes.

SOLUTION

CrowdStrike Falcon® Complete Identity Threat Protection augments the core CrowdStrike Falcon® Complete managed detection and response (MDR) service, delivering unparalleled security for identities and identity stores. The solution combines CrowdStrike Falcon® Identity Threat Protection with the expertise of the Falcon Complete team, which manages and actively monitors Falcon solutions for customers, investigating and surgically remediating incidents in minutes. Managed identity threat protection helps organizations to run an effective and mature identity security program without the burden, costs and time associated with building one internally.

KEY BENEFITS

Stops identity-driven attacks:

- Delivers automated protection and real-time detection for identity-based attacks
- Provides focused expertise to stop identity-based breaches
- Offers expert management, optimization and monitoring

Shrinks attack surface:

- Enforces proper hygiene and strong authentication for privileged accounts
- Prevents abuse of compromised credentials
- Provides comprehensive visibility across all systems, eliminating blind spots

Provides immediate value:

- Includes a proven onboarding process in which CrowdStrike experts learn your needs and structure
- Immediately deploys policies aligned with best practices for your unique compliance, business and technical requirements
- Offers the industry's strongest Breach Prevention Warranty

FALCON COMPLETE IDENTITY THREAT PROTECTION

KEY CAPABILITIES

EXPERTISE TO DEFEND AGAINST IDENTITY-DRIVEN ATTACKS

The Falcon Complete team is composed of seasoned security professionals who have experience in security operations center (SOC) analysis, incident response and forensics, as well as Active Directory and other IT administration.

- **Experts in the CrowdStrike Falcon® platform:** The Falcon Complete team ensures your identity environment is continuously optimized to combat the latest threats and achieve the best levels of performance and protection.
- **Experts in incident response:** The team comes to you with multiple years of experience in digital forensics and incident response (DFIR).
- **Experts in threat hunting:** CrowdStrike's 24/7 human threat hunting uncovers the faintest trace of malicious activity in near real time.
- **Experts in threat intelligence:** CrowdStrike's global threat intelligence team brings critical context to the response process.

POWERED BY FALCON IDENTITY THREAT PREVENTION

Falcon Identity Threat Protection enables frictionless identity security, delivering real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics.

- **Segmented workforce identities:** Gain granular and continuous insights into every account and activity to highlight identity security gaps across identity stores, and empower security teams to better evaluate identities and the risks associated with them.
- **Automated identity threat detection and response:** Enable real-time identity threat detection and protection without time-consuming log processing. Eliminate risky guesswork and prioritize authentication tasks based on over 100 behavior analytics and risk factors for every account.
- **Verified identities with zero friction:** Secure employee or contractor access to applications, tools and resources with a zero-friction user experience. Ensure consistent login experience for genuine users, but automatically step up authentication when risk scores increase.

PROACTIVE MANAGEMENT AND OPTIMIZATION

The Falcon Complete team ensures that your Falcon Identity Threat Protection deployment starts on the right track with carefully crafted policies that meet your specific needs, and continuously tunes them to ensure your environment is always protected against emerging identity threats.

- **Deployment and managing of best practices policies:** Leverage the expertise of skilled CrowdStrike analysts to immediately stop anomalous authentication attempts, restrict use of privileged accounts and block lateral movement with compromised identities.
- **Continuous tuning and optimization:** As the Falcon Complete team learns more about your environment and unique requirements, it fine-tunes packaged and custom rules to reduce false positives and optimize protection.
- **Monthly metrics:** Regular reports provide relevant, up-to-date insights you can use to understand and improve your identity security program.

FALCON COMPLETE IDENTITY THREAT PROTECTION ENABLES:

- Containment of lateral movement across on-premises, hybrid and SaaS environments
- Rapid response to all threats at the code execution and identity layers
- Protection for Active Directory, which is often the weakest link in cyber defenses

SURGICAL RESPONSE TO IDENTITY-BASED THREATS IN MINUTES

Minutes matter when an attack occurs, and your defenders who need to act may be hours away from their keyboards. Falcon Complete executes surgical remediation to stop identity-driven attack techniques in their tracks, any time of day or night.

- **Enforcement of multifactor authentication (MFA):** When suspicious activity is identified, Falcon Complete analysts can trigger reauthentication with MFA, shutting the door on intruders.
- **Reset of compromised passwords:** An adversary with valid credentials is free to return again and again and move at will across the network. Falcon Complete takes decisive action to revoke unauthorized access at the source.
- **Surgical remediation in minutes:** The Falcon Complete team executes surgical remediation remotely in near real time, eliminating the cost and burden of reimaging.

BREACH PREVENTION WARRANTY

CrowdStrike stands strongly behind its breach protection capabilities. Falcon Complete comes with the industry's strongest Breach Prevention Warranty* to cover costs should a breach occur within the protected environment.



*Breach Prevention Warranty not available in all regions. See [FAQ](#) for details and restrictions.

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/>

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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

© 2023 CrowdStrike, Inc. All rights reserved.

