CrowdStrike Products

CROWDSTRIKE

FALCON COMPLETE

Managed detection and response (MDR) delivered by CrowdStrike's team of experts to protect endpoints, cloud workloads and identities

CHALLENGES

Operating an effective security program is extremely challenging. Adversaries are increasingly fast and stealthy, don't respect time zones or holidays, and often execute damaging intrusions in hours. The necessary tools to defend against these threats can be difficult to use and can require a lot of resources to appropriately implement, operate and maintain.

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

SOLUTION

CrowdStrike Falcon Complete™ delivers 24/7 expert management, monitoring and response for the CrowdStrike Falcon® platform and is backed by CrowdStrike's industry-leading Breach Prevention Warranty.*

Falcon Complete is CrowdStrike's most comprehensive endpoint protection solution. It delivers unparalleled security by augmenting Falcon Prevent™ next-gen antivirus (NGAV), Falcon Insight™ endpoint detection and response (EDR), Falcon Identity Threat Protection and Falcon OverWatch™ managed threat hunting together with the expertise and 24/7 engagement of the Falcon Complete team. The team manages and actively monitors the Falcon platform for customers, remotely remediating incidents in minutes. The Falcon Complete team solves the challenge of implementing and running an effective and mature security program without the difficulty, burden and costs associated with building one internally.

A leader in...

- Forrester MDR[1]
- IDC MDR[2]

1. IDC MarketScape U.S. Managed Detection and Response
2. Services Vendor Assessment, IDC #US48129921, August 2021

KEY BENEFITS

Immediate value with a seamless extension of your team:

- Delivers focused expertise 24/7 to stop breaches
- Provides the equivalent of 5 expert SOC analysts and 5 elite human threat hunters**
- Supplies continuous management, optimization and monitoring
- Completes onboarding and provides full protection in an average of 10 days

Rapid response and surgical remediation in minutes:

- Provides rapid response at the endpoint, cloud workload and identity layers
- Conducts hunting at unprecedented speed and cloud-scale
- Reduces business disruption to processes or users
- Instills confidence that threats are handled completely and correctly

Reduced cybersecurity risk and enormous cost savings:

- Shrinks the attack surface across endpoints, cloud workloads and identities
- Saves over 2,500 hours per year from a reduction in security incidents**
- Delivers an ROI of more than 400%**
- Is backed by the industry's strongest Breach Prevention Warranty*

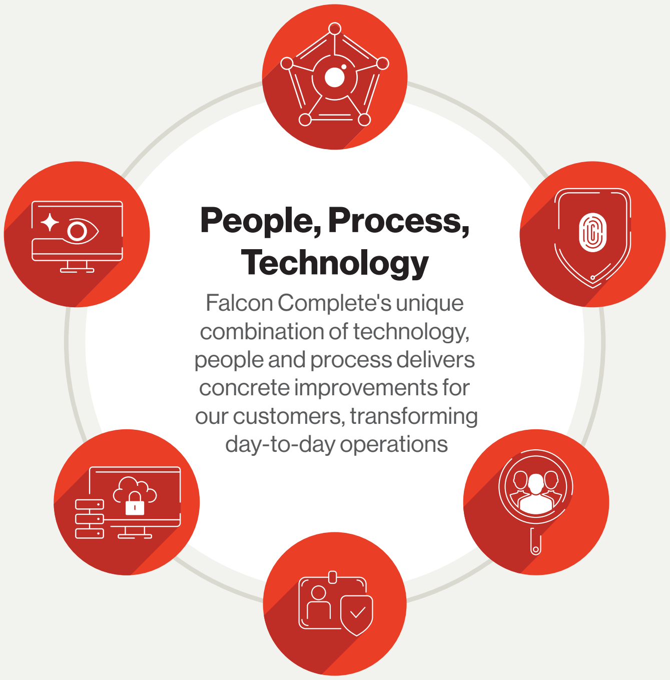
* Breach Prevention Warranty not available in all areas. See **FAQ** for details.

** Total Economic Impact of Falcon Complete, February 2021 Forrester Wave for Managed Detection and Response, Q1 2021

FALCON COMPLETE:
A SYMBIOSIS OF PEOPLE, PROCESS AND TECHNOLOGY

Falcon Complete Expertise

Provides expert security analysts to manage, monitor, respond to and remediate threats



People, Process, Technology

Falcon Complete's unique combination of technology, people and process delivers concrete improvements for our customers, transforming day-to-day operations

Falcon Discover: IT Hygiene

Provides visibility into assets, systems and applications for a comprehensive topography of your IT environment

Falcon Prevent: Next-gen AV

Provides the ideal AV replacement solution by combining the most effective prevention technologies with full stack visibility and simplicity

Falcon Insight: Endpoint Detection and Response

Delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches are stopped

Falcon OverWatch: Managed Threat Hunting

Adds a human threat detection engine that operates as an extension of your team, hunting relentlessly to see and stop the most sophisticated hidden threats

Falcon Identity Threat Protection

Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

KEY CAPABILITIES

LAYERS OF EXPERTISE

The Falcon Complete team is composed of seasoned security professionals with experience in incident handling, incident response, forensics, SOC analysis, identity protection and IT administration. The team has a global footprint, allowing true 24/7 coverage.

- **Experts in the CrowdStrike Falcon platform:** The Falcon Complete team holds CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) certifications.
- **Experts in incident response:** The Falcon Complete team has years of experience in digital forensics and incident response (DFIR).
- **Experts in threat hunting:** The Falcon OverWatch team sees and stops undetected, sophisticated threats 24/7.
- **Experts in threat intelligence:** Falcon Complete is powered by the CrowdStrike global threat intelligence team, bringing critical context to the response process.

POWERED BY THE FALCON PLATFORM

CrowdStrike pioneered a new approach to endpoint protection, designed and built to overcome the limitations of legacy security solutions. The Falcon platform delivers the foundation for true next-generation endpoint protection.

- **100% cloud-native:** The Falcon platform delivers immediate time-to-value — no hardware, additional software or configuration is required, which drives down cost and complexity.
- **CrowdStrike Security Cloud:** The CrowdStrike Security Cloud is the brains behind the CrowdStrike Falcon platform, providing complete real-time visibility and insight into everything happening on your endpoints throughout your environment.
- **Single lightweight agent:** An intelligent, lightweight agent, unlike any other, blocks attacks while capturing and recording endpoint activity as it happens to detect threats fast.
- **Detection across endpoints, cloud workloads and identities:** Falcon Complete enables frictionless endpoint, cloud workload and identity security, delivering real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics.

WHAT FALCON COMPLETE CUSTOMERS SAY

"By analysing the millions of data points generated by a vast and diverse customer base, often in real time, CrowdStrike is able to provide our team with a comprehensive and clear picture of exactly what is happening across the globe, 24/7. That's an essential ingredient in protecting us from issues long before they become a problem."

Michael Taylor,

IT Director, Mercedes-AMG Petronas Formula One Team

"We remediate no malware whatsoever, and not only am I saving money, which makes me look like a hero to the finance department, but our malware instances have just plummeted. The CrowdStrike platform lets us forget about malware and move onto the stuff we need to do."

Dawn Armstrong,

VP of IT, Virgin Hyperloop

PROACTIVE MANAGEMENT AND OPTIMIZATION

CrowdStrike experts ensure your environment is continuously optimized to combat the latest threats, achieving the best levels of performance and protection from your Falcon investment and instilling confidence that your endpoint protection and identity protection are always under complete control.

- **Comprehensive control of unmanaged systems:** Falcon Complete helps customers ensure all assets are properly grouped, sorted and protected.
- **Tight control over the Falcon agent:** Falcon Complete ensures that the most current Falcon agent is installed, delivering the best level of protection available.
- **Rigorous configuration management:** Falcon Complete systematically applies proven, best-practice policies to endpoints, cloud workloads and identities.

24/7 EXPERTISE TO DEFEND THE CLOUD

- **Experts in Falcon Cloud Workload Protection:** The Falcon Complete team ensures your environment is continuously optimized to combat the latest threats, enable DevOps and achieve the best levels of performance and protection.
- **Multi-cloud:** Falcon provides a single platform to protect AWS, Azure and Google Cloud.
- **Broad visibility:** Uncover AWS EC2 instances, GCP Compute instances and Azure VMs without installing an additional agent.
- **Secure hosts and containers:** Falcon runtime protection defends containers against active attacks.

CONTINUOUS HUMAN THREAT HUNTING

- **The SEARCH Methodology:** Falcon OverWatch analysts leverage their proprietary SEARCH methodology — Sense, Enrich, Analyze, Reconstruct, Communicate and Hone —to shine a light into the darkest corners, leaving adversaries with nowhere to hide.
- **Cloud-scale data:** Scalable and effective threat hunting requires access to vast amounts of data and the ability to mine that data in real time for signs of intrusions. CrowdStrike's rich telemetry creates the foundation for Falcon OverWatch threat hunting.
- **Years of combined diverse expertise:** Falcon OverWatch employs elite experts from a wide range of backgrounds, including government, law enforcement, commercial enterprise, the intelligence community and defense and defense.

24/7 MONITORING AND RESPONSE

- **Around-the-clock active monitoring:** Falcon Complete is always watching, ensuring that emerging threats are addressed in real time, as they happen.
- **Human eyes on detections:** Falcon Complete investigates detections in a timely manner, identifying intrusions at the earliest possible stage.
- **Average time to begin response <10 minutes:** Falcon Complete builds and continuously tunes a repeatable playbook to ensure all threats are investigated quickly and efficiently.

SURGICAL REMEDIATION

When an intrusion is identified, the Falcon Complete team acts quickly and decisively, remotely accessing the affected system using native Falcon capabilities to surgically remove persistence mechanisms, stop active processes, disrupt identity-based threats and clear other latent artifacts. Falcon Complete restores systems to their pre-intrusion state without the burden and disruption of reimaging systems.

- **Surgical remediation performed in under 60 minutes:** Falcon Complete executes surgical remediation remotely, eliminating the cost and burden of reimaging.
- **Greatly reduced impact for the end user:** Falcon Complete can often perform remediation without the user being aware that it has happened.

TRANSPARENT AND SECURE COLLABORATION

- **Message Center:** This secure bi-directional communication channel allows for information exchange about emerging incidents as well as asking ad hoc questions, all from directly within the Falcon console. Keeping communications close to the Falcon data provides maximum efficiency, ensuring that the full context associated with emerging threats is never more than a click away.
- **Executive Dashboards:** Gain at-a-glance visibility into the day-to-day activity that Falcon Complete performs, including trends and actionable insights.
- **Message Analyst:** Fast access to CrowdStrike experts is embedded throughout the Falcon console. This helps analysts to more quickly understand threats and get fast answers to their cybersecurity questions.

CROWDSTRIKE'S BREACH PREVENTION WARRANTY*

REST ASSURED WITH THE MOST COMPREHENSIVE BREACH PREVENTION WARRANTY

CROWDSTRIKE
BREACH PREVENTION
WARRANTY

CrowdStrike stands strongly behind its breach protection capabilities. Falcon Complete comes with a Breach Prevention Warranty to cover costs in the event a breach occurs within the protected environment.

	Other Warranties	CrowdStrike
Time to report requirements	24-48 hours	72 hours
Categories covered	Limited	✓
Backed by the largest insurance providers	Varies	✓
Primary coverage	Varies	✓
Policy requirements	Extensive	Minimal

*The Breach Prevention Warranty is not available in all regions. Learn more in the Breach Prevention Warranty FAQ.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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, 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 enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**