Why Falcon Complete?

Healthcare security teams face increasing challenges from lack of visibility, complex solutions, and sophisticated attacks, especially related to COVID-19. CrowdStrike in collaboration with AWS services can help provide:

Enhanced Visibility — Continuous and comprehensive AWS workload monitoring, including container and VDI support, ensuring nothing is missed and stealthy attacks can be stopped.

24x7 Breach Protection — Protect against breach with unparalleled coverage. Defend AWS workloads against threats from malware to the most sophisticated attacks.

Reduced Overhead — Reduces the overhead, friction and complexity associated with protecting AWS cloud workloads.

Automated Security — Enable cloud security to keep up with the dynamic and flexible nature of AWS workloads.

Product overview

CrowdStrike Falcon Complete is endpoint protection delivered as-a-service that combines next-generation antivirus (AV), endpoint detection and response (EDR), and threat intelligence automation capabilities for expedited threat detection and response, threat remediation, and risk management managed and operationalized by Falcon Complete team of incident responders, all within a single lightweight agent. Falcon Complete combines the following Falcon modules and is delivered as a service to you:

Falcon Prevent™
Next-generation antivirus, machine learning (ML), exploit blocking, indicator of attack (IOA) behavioral analysis and more

Falcon Insight™
Endpoint detection and response (EDR) solution that delivers comprehensive and continuous real-time and historical visibility across detection, response and forensics

Falcon Discover™
IT hygiene and asset inventory

Falcon OverWatch™
24/7 managed threat hunting with managed detection and response (MDR) to help you proactively hunt, investigate, and advise on threat activity in your environment

Falcon Complete Team provides:

- On-boarding
- Proactive configuration management
- Prevention health checks
- Maintenance and operations
- Access to CrowdStrike security analysts
- Incident handling playbook
- Incident triage and handling
- Hands-on remote remediation
Key capabilities

Falcon Complete provides healthcare organizations with the technology and services you need to instantly implement and continuously run a mature endpoint security program.

Unmatched next-gen benefits

- **Guarantees protection**: Comes with a breach protection warranty that covers the costs of legal services, client notification, identity theft and credit monitoring, forensics investigation and public relations.

- **Protects against all types of attacks**: Protects against commodity and zero-day malware, ransomware, exploits and advanced malware-free, fileless attacks — keeping you ahead of the rapidly changing tactics, techniques, and procedures (TTPs) used by today’s adversaries.

- **Combines the best prevention technologies**: Combines technologies such as ML for malware protection, IOA behavioral blocking, and exploit blocking, for ultimate protection.

- **Single, lightweight agent**: Uniquely integrates powerful best-in-class prevention, detection, and response with IT hygiene capabilities to provide continuous breach prevention in a single agent.

A force multiplier: All the hands-on help and expertise you need, when you need it

- **Gets you up and running and fully operational**: The CrowdStrike Falcon Complete Team works with your organization to get you started and assists your team throughout the deployment process. During this interactive phase, CrowdStrike helps you understand the prevention capabilities of the Falcon platform and tailors these security postures to best fit your business and security needs.

- **Frees your IT and security teams from daily, time-consuming endpoint security tasks**: After initial implementation, the Falcon Complete Team administers the updates and maintenance of your solution, updating, monitoring and tuning Falcon to continually enhance your security posture. They also review, triage, prioritize, and resolve alerts generated by the Falcon platform and Falcon OverWatch. The Team identifies whether an alert is a false positive or a true incident and responds accordingly.

- **Reduces risk with immediate remote remediation of incidents**: When the Falcon Complete Team detects an incident, it can remotely remediate it. By ensuring that all incidents are handled immediately, Falcon Complete dramatically reduces the risks of a serious breach. In addition, the Team assists with guidance and expertise to help your teams with any security concerns they might have.

Immediate time to value (TTV)

- **Easy deployment**: As part of the CrowdStrike Falcon® platform, Falcon Complete requires the installation of a single lightweight 25 MB agent, without requiring management infrastructure or management consoles, making deployment easy and efficient.

- **Immediately operational**: Falcon Complete can be deployed instantly for unrivaled time-to-value. As soon as it’s installed, it hits the ground running, enabling the Falcon Complete Team to monitor and protect your organization without requiring additional components, reboots, query writing, staging or complex configuration.

- **Zero impact on performance**: Thanks to its cloud-native architecture, Falcon Complete causes no additional impact on endpoints or the network.
Where CrowdStrike and AWS work together

CrowdStrike and AWS compute services
- Amazon EC2 instances – including Graviton
- Amazon hosted EMR (such as Epic on Citrix/HP) and VDI
- Amazon WorkSpaces
- Amazon ECS, Amazon EKS, and Containers

CrowdStrike and AWS Cloud services integrations
- AWS Control Tower
- AWS Security Hub
- AWS Network Firewall
- AWS PrivateLink
- Amazon GuardDuty

Healthcare and Life Sciences
- HIPAA compliance
- Shared responsibility
- CrowdStrike Falcon for Healthcare
- AWS and data privacy

CrowdStrike security products
- Falcon Endpoint Protection
- Falcon Cloud Workload Protection
- Falcon Complete – Security as a Service
- Falcon Discover – discover Healthcare application across AWS environments

Strengthen Healthcare security and compliance with CrowdStrike and AWS

CrowdStrike and AWS help provide complete security for the cloud through a commitment to the Shared Responsibility Model.

```
| Commercial & Government Customers | AWS
|----------------------------------|---
| RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD | RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE
- EC2
- S3
- Aurora, RDS, Redshift

NETWORKING
- REGIONS
- AVAILABILITY ZONES
- EDGE LOCATIONS
```
CrowdStrike and AWS for Healthcare

CrowdStrike for Healthcare solutions

• Achieve a new standard in healthcare cybersecurity with scalable cloud-native products and turnkey services
• Achieve VDI security for the most tightly constrained and critical resources (such as Epic Systems on Citrix/HP)
• Gain granular visibility and continuous monitoring of healthcare infrastructure
• Discover connected devices and workloads with underlying security posture, risks, and vulnerabilities
• Achieve compliance with HITRUST and HIPAA with independently validated Falcon platform
• Gather full context of threats, including tactics, techniques, and procedures used by attackers to target healthcare organizations

AWS for Healthcare solutions

• Accelerate insights to improve outcomes through machine learning
• Optimize efficiency and make better informed decisions with data transparency, analytics, and machine learning
• Support regulatory compliance and enhance security
• Run sensitive workloads regulated under the U.S. Health Insurance Portability and Accountability Act (HIPAA)
• AWS GovCloud (US) is FedRAMP high certified

How Falcon Complete works

Solution available in AWS Marketplace