



The Impact of Securing Your Cloud Environment with Falcon Cloud Security

Increase speed, reduce complexity,
drive greater efficiency and
strengthen protection

Today's modern cloud-powered organizations have their hands full trying to maintain a productive application-powered business. Vendor and tool consolidation have become critical for successful businesses to manage cost and increase efficiency and productivity. CrowdStrike prides itself on delivering the best security outcomes for customers to stop breaches and prevent unnecessary downtime. This white paper outlines some of the key cloud security challenges organizations are facing, shares data about what customers are experiencing in efficiency and security outcomes, and highlights the essential components required to deliver positive outcomes.

Securing Your Cloud in a Complex and Dynamic Threat Environment

The [CrowdStrike 2023 Global Threat Report](#) revealed a 95% increase in cloud exploitation and a 288% increase in cases of threat actors specifically targeting cloud environments. Today's adversaries are growing faster and more sophisticated, as evidenced by their tactics in pursuing initial access, lateral movement, privilege escalation, defense evasion and sensitive data.

For example, consider breakout time — the time it takes an adversary to move laterally from an initially compromised host to another host within the victim environment. The average breakout time has dropped to only 79 minutes, and the fastest observed breakout time was a mere 7 minutes, according to the [CrowdStrike 2023 Threat Hunting Report](#).

Cloud applications can be vulnerable to a wide range of threats that can exploit system misconfigurations, software vulnerabilities and poor identity management practices. Some of the most common issues that organizations must consider when developing and implementing their cloud application security strategy and technology include:

Complexity from multiple siloed tools: Many misconfigurations result from the complexity of using multiple security solutions. Complex tooling makes it difficult to consistently enforce a strong security posture and continuous compliance, and it can interfere with detecting and preventing fast and sophisticated attacks. In addition to driving complexity and expanding the attack surface, relying on multiple security tools can create silos and drive up costs.

Lack of visibility: Cloud breaches often occur due to a lack of unified, real-time visibility and protection across multi-cloud and hybrid cloud environments. Adversaries are becoming more sophisticated and exploring

The Impact of Securing Your Cloud Environment with Falcon Cloud Security

new ways to move laterally in target environments. Without unified visibility across the entire cloud infrastructure, this lateral movement can occur without alerting the enterprise security team to a breach.

Evolving sophistication of attacks: Adversaries understand the cloud. They understand containers, they understand the details and vulnerabilities of each cloud service provider, and they know how to move laterally between systems. This understanding is manifest in increasingly subtle and advanced cloud-focused attacks.

Poor threat detection and response: Some organizations may not have the security maturity needed to operate safely in a multi-cloud environment. They must implement the right tools and technologies to monitor cloud applications and workloads and remove any assets not needed by the business to reduce their attack surface.

Essential Elements for Effective Cloud Security

Organizations using the cloud must implement a comprehensive cloud security solution to protect against a growing range of fast and sophisticated threats targeting cloud environments — from development to runtime.

Organizations must take these critical steps to ensure speed, efficiency and accuracy in protecting their cloud-native applications.

Be faster than the adversary

Accelerate cloud threat detection and response: Organizations need accurate and complete detection and response in the cloud to efficiently stop breaches. Employing tested agent-based and agentless technology in a single platform empowers organizations to identify and remediate vulnerabilities and misconfigurations in real time.

Consolidate tools: Having a cloud-native application protection platform (CNAPP) solution containing both agent-based and agentless detection and response is essential to stop breaches. This combination ensures complete visibility across the entire cloud estate in a single console, along with security consistency, faster response time and reduced costs.

Stop sophisticated attacks

Gain complete visibility: Ensure full visibility — with no gaps — across the entire multi-cloud and hybrid cloud estate through a single console.

Understand your adversaries: With the massive increases in cloud exploitation and sophisticated cloud attacks, it's vital to understand adversaries and their motivations and techniques. Industry-leading threat intelligence enables faster and more accurate incident response.

Gain efficiency through experts: Leverage expert cloud services to stop sophisticated attackers and respond rapidly to potential threats with 24/7 managed detection and response (MDR) and incident response services.

CrowdStrike's Approach to Cloud Security

CrowdStrike Falcon® Cloud Security is the world's most advanced unified platform built on an agent-based and agentless approach for all cloud environments. These critical capabilities help organizations stay faster than the adversary and stop sophisticated attacks while preventing human error and enforcing compliance.

Speed is critical in defending against modern adversaries. Falcon Cloud Security delivers fast, accurate and proven threat detection and response in a unified CNAPP, using one agent and one console to improve efficiency for incident responders across the entire cloud ecosystem. It eliminates the silos between disparate cloud security solutions to provide consistency and visibility throughout the cloud environment, reducing complexity and cost while helping organizations more quickly detect and stop threats across their entire infrastructure.

To stop sophisticated attacks, Falcon Cloud Security correlates attack path analysis across on-premises, hybrid and multi-cloud environments through agentless detection with real-time, agent-based security. With one-click remediation testing and agent deployment, organizations can rapidly identify and secure unprotected assets without disrupting operations.

Adversary intelligence plays a huge role in cloud threat detection and response. CrowdStrike has proven, accurate, built-in indicators of attack (IOAs) to identify attacker behaviors and trends, indicators of compromise (IOCs) to recognize when an attack has started, and indicators of misconfiguration (IOMs) to prevent misconfigurations from leaving doors open for attackers. The CrowdStrike Falcon® platform regularly analyzes trillions of security transactions each day and combines data with human intelligence from one of the largest incident response teams in the industry to address vulnerabilities and stop breaches. Falcon Cloud Security detects cloud-specific IOAs sourced from adversary intelligence to prevent runtime attacks. CrowdStrike tracks 220+ adversaries and their tactics, techniques and procedures to create this collection of intelligence.

The Impact of Securing Your Cloud Environment with Falcon Cloud Security

Stopping cloud breaches demands a smarter and faster approach to cloud security

Get Smarter

We Know Cloud-Conscious Adversaries - Threat Intel
Knowledge of real-world attacks, TTPs, for 100s of cloud conscious adversaries for accurate info

They Can't Hide - No Gap Protection
Full multi-cloud and hybrid deployment coverage

Get Faster

Automation - Built for Scale
Automated policies with built-in IOCs, IOAs, IOMs and compliance assessments

Consolidation - One Agent, One Console
Proven agent-based and agentless tech for every cloud, in one console to see/stop everything, everywhere

Expert Services
Cloud-specialized teams to support companies at any stage of their cloud security journey

2021 CrowdStrike, Inc. All rights reserved. CROWDSTRIKE

Code-to-runtime security is available to Falcon Cloud Security customers. CrowdStrike has added Bionic's application security posture management (ASPM) capabilities to the Falcon platform. This new capability will help drive greater security outcomes for customers across the application life cycle. In short, the additional security provided by ASPM will help make applications more secure for companies operating in industries such as financial services, retail, travel and more. It helps security professionals contextualize and prioritize vulnerabilities, secure architecture, protect sensitive data flows and conduct dependency impact analysis.

Bionic Integration

Revolutionizing Cloud Security with Integrated Application Security Posture Management (ASPM)

Complete Code-to-Runtime Platform

- ✓ A Complete Picture of Risk
- ✓ Protect What's Running in the Cloud
- ✓ Simple, Frictionless Deployment

Manage vulnerabilities and misconfigured cloud resources and triage remediation based on a complete picture of risk

Monitor posture, detect and respond to threats and ensure compliance

Deep visibility into compromised infrastructure across the cloud estate and the foundation of application services

2021 CrowdStrike, Inc. All rights reserved. CROWDSTRIKE

Organizations using Falcon Cloud Security trust the solution to detect potential threats and find the detailed security data they need to quickly act on them.

CrowdStrike is widely regarded as a global cloud security and CNAPP leader among the top industry analysts and by global customers and partners, which include three of the top U.S. banks, one of the largest U.S. airlines and 30+ government entities across the globe. To fully secure your organization no matter where you are on your cloud journey, CrowdStrike offers a full range of cloud detection and response services, including threat hunting, incident response, assessment and 24/7 MDR services.

By delivering all of these security tools through one integrated platform, customers have access to a unique set of powerful capabilities unmatched in the market.

Results Falcon Cloud Security Customers Are Seeing¹

Falcon Cloud Security has a significantly positive net impact for our customers. (This data is just an average, with some customers seeing significantly higher impact and return on investment.)

Faster time to respond and detect

On average, Falcon Cloud Security customers saw a 74% faster response rate to cloud incidents, with an average of 784 hours saved per year and close to \$50,000 in real dollar value.

Why it matters

The faster you respond, the less time the adversary has to succeed. AI-native cloud security paired with automation and rich threat scoring tools helps customers remain one step ahead of the adversary at all times.

More efficient protection

Falcon Cloud Security customers saw a reduction in the number of cloud incidents, with an average of 1,761 hours saved and approximately \$105,689 saved annually.

Why it matters

Organizations have more time to focus on security improvements and running the business. CrowdStrike leverages crowdsourced knowledge about the latest threat environment from across its customer base and pairs it with the Common Vulnerability Scoring System (CVSS) to provide a dynamic, real-time threat score. When CrowdStrike threat intelligence identifies a high-risk vulnerability, it is flagged as a priority rather than relying only on what the common industry guidance recommends. This supercharges customers' ability to prioritize threats and decreases wasted time on less impactful security changes.

Reduced complexity

Falcon Cloud Security users achieved an average of 71% improvement in cross-functional processes to manage and maintain cloud policy. This reduced the total cost of full-time employees, with an average savings of \$72,000 annually.

Why it matters

Reducing complexity is the first essential step when organizations are trying to improve efficiency. Leveraging unified CNAPP technology combined with the power of the unified Falcon platform and product suite gives teams greater flexibility and efficiency to focus on what matters most and save money.

¹All data in this section was sourced from CrowdStrike Business Value Assessments with customers from 2022-2023.

Efficiency gains

On average, Falcon Cloud Security customers were 72% faster in discovering and monitoring their entire cloud estate, saving an average of 809 hours and \$48,000 annually.

Customers also saw a reduction in the number of hours spent triaging low-impact alerts, with an average of 800 hours and \$48,000 saved annually.

Why it matters

Efficiency gains mean the difference between actively stopping breaches in real time or simply reacting to them. Improved response time and a reduction in the hours spent trying to discover and monitor the cloud estate for threats give customers the edge in the fight against threat actors. In addition, time not spent triaging false positives and working on low-impact alerts means money saved and hours not wasted.

Reduced complexity

Falcon Cloud Security drives value by reducing the run rate customers experience through consolidation. The average improvement is an 83% reduction in run rate, with an average of 3,950 licenses displaced. The financial impact based just on this metric is an average of \$67,000 annually.

Why it matters

Money saved by not using multiple vendors and paying for multiple licenses ensures that security teams and organizations can focus on funding top-priority projects while getting the highest return on investment for their organization.

What CrowdStrike Customers Are Saying

Many customers highlight these impacts and experiences in reviews on [Gartner® Peer Insights™](#) and through customer testimonials. Check out some of these case studies.

Geisinger

Since 2017, Geisinger Health System has used CrowdStrike to protect its on-premises electronic health record (EHR) software. As one of America's most innovative health systems, Geisinger decided in 2021 to migrate its EHR to Amazon Web Services (AWS). But this is no small feat. Some 400 applications and numerous workflows needed to be migrated to AWS. Critically, these applications needed to be protected — as did the sensitive data contained within them. Geisinger relied once again on CrowdStrike.

CoreWeave

CoreWeave is a specialized cloud provider. When the time came to implement a modern cybersecurity platform, the company needed protection from endpoint to cloud workload and everything in between. But critically, it also needed a lightweight agent that wouldn't slow down its high-performance cloud. After a successful proof of concept with CrowdStrike, CoreWeave licensed the Falcon platform.

Mercury Financial

Mercury Financial is a Texas-based credit card and consumer lending company. Operating in a cloud-native environment that requires complete protection of its infrastructure and customer data, Mercury Financial needed more than just security tools — it needed a full suite of products, services and threat intelligence. Mercury Financial also wanted to consolidate its security stack with a single platform to protect endpoints, cloud and workloads. That's when the company turned to CrowdStrike.



“By giving us end-to-end protection, CrowdStrike has helped us build a culture of security.”

Alex Arango

Head of Cyber Threat Management
— Deputy CISO at Mercury Financial

Trusted by customers and recognized by analysts

**CrowdStrike
Falcon® Cloud
Security Protects**


Three of the **top US Banks**

One of the **largest US airlines**

30+ **government entities**
globally

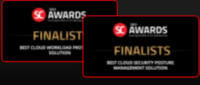
Gartner


Representative Vendor in
Gartner CNAPP Market Guide



SC AWARDS


SC Mag Awards 2023
Finalist for CWP and CSPM
Categories



 **4.9 Rating**

"CrowdStrike Cloud Security has enabled more profound insights and visibility into processes running within our cloud infrastructure." "With CrowdStrike Cloud Security implemented across our entire cloud environment, we now have a trusted sense of what is going on 24/7 with continuous monitoring + CrowdStrike Overwatch." **G2**

"With CrowdStrike Falcon® Cloud Security with Containers, they get real-time visibility into cloud workloads, containers and Kubernetes, enabling faster and more accurate detection, response, threat hunting and investigation." **Matt Bellinger, CISO**

© 2023 CrowdStrike, Inc. All rights reserved. 

Next Steps

Customers using Falcon Cloud Security experience greater speed and effectiveness, stopping sophisticated cloud adversaries and achieving greater economic benefits thanks to simplified licensing and scalability. To learn more about Falcon Cloud Security and why it's the best fit to stop cloud breaches, visit the [product webpage](#), where you can sign up for a complimentary [CrowdStrike Cloud Risk Review](#) and speak to CrowdStrike experts to learn more.

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.

