CROWDSTRIKE

The Buyer's Guide to Complete Cloud Security

Make the right decisions to protect your cloud assets from modern threats

Table of Contents

Introduction

Security threats originating in the cloud continue to rise, and adversaries show no signs of letting up. As revealed in the CrowdStrike 2023 Global Threat Report, cloud exploitation increased 95% in 2022, with a 288% uptick in cases involving threat actors targeting cloud environments.

At the same time, adversaries continue to grow smarter and faster as they innovate to exploit gaps in cloud security. It takes an average of just 79 minutes for adversaries to break out and begin moving laterally through an enterprise environment, according to the CrowdStrike 2023 Threat Hunting Report — with the fastest observed breakout time a mere 7 minutes.

Defenders Need to Stay Ahead of Adversaries

The effectiveness of cloud security hinges on defenders' ability to collect, correlate and analyze data across on-premises, hybrid and multi-cloud environments. Simply put, modern defenders need to find exploitable weaknesses before adversaries do. But, conventional approaches to security can't deliver the granular visibility and control needed to manage cloud risk, particularly risk associated with containers.

Hybrid deployments with components distributed between multiple cloud environments and on-premises systems also create complexity that leads to delayed response and excess operational overhead. Stitching together many siloed monitoring and remediation solutions paves the way for coverage gaps and visibility blind spots that make it hard to detect, prioritize and remediate risk.

To combat the sheer volume and evolving sophistication of modern cloud attacks, organizations need to take a smarter, faster approach to cloud security. This new approach must equip defenders with continuous visibility coverage and accurate intelligence to understand adversary tactics for initial access, lateral movement, privilege escalation, defense evasion and data collection. And, it must allow defenders to outpace and outsmart attackers.

Cloud-based risk continues to rise

288%
increase in cloud-conscious threat actors

95%
increase in cloud exploitation from 2021 to 2022

79 minutes
average eCrime breakout time

Sources: CrowdStrike 2023 Global Threat Report and CrowdStrike 2023 Threat Hunting Report

CNAPP Delivers a Smarter, Faster Approach to Stopping Modern Cloud Threats

Cloud deployments face a wide range of threats that exploit system misconfigurations, software vulnerabilities, and flawed or incomplete identity management practices. A cloud-native application protection platform (CNAPP) brings together multiple security and protection capabilities in a single platform focused on identifying and prioritizing risk across your entire cloud environment.

A CNAPP approach puts time back on defenders' side with a consolidated, intelligent, highly automated approach to cloud security. According to Gartner®[1]:

> "CNAPPs are a unified and tightly integrated set of security and compliance capabilities designed to secure and protect cloud-native applications across development and production." Also, "CNAPP offerings bring together multiple disparate security and protection capabilities into a single platform focused on identifying and prioritizing excessive risk of the entire cloud-native application and its associated infrastructure."

While security teams may adopt the CNAPP approach, development and product teams that deliver applications also play a role. A modern "shift-left" approach includes continuous integration/continuous delivery (CI/CD) and highlights infrastructure-as-code (IaC) scanning and other pre-image scanning capabilities early in the application lifecycle. Such scanning helps detect and eliminate vulnerabilities caused by human error.

CNAPP lets organizations accomplish the primary objective of rapidly building and deploying applications while helping defenders act smarter and faster than adversaries.

Finding the Right Cloud Security Solution

This buyer's guide captures the definitive criteria for choosing the right CNAPP platform and partner. It covers:

- The five pillars of a successful CNAPP
- How the right CNAPP makes cloud security smarter and faster
- Criteria for choosing the right platform and provider to accelerate your company's cloud journey
- How CrowdStrike Falcon® Cloud Security stops breaches faster with a unified CNAPP featuring agent-based and agentless protection from the endpoint to the cloud

[1] Gartner Market Guide for Cloud-Native Application Protection Platforms

The Five Pillars of a Successful Cloud Security Approach

Companies that deploy essential business services in the cloud continue to scale their infrastructures to support unprecedented volumes of buckets, containers, applications and services — all potentially at risk of attack. Traditional security platforms do not deliver the visibility and automation at the scale needed to stop innovative and relentless cloud-focused adversaries.

A modern cloud security platform simplifies and unifies security from the on-premises environment to the cloud to shrink your attack surface. Consolidation of siloed security capabilities within a framework such as CNAPP helps to eliminate pathways attackers might follow to exploit the cloud, access your network and execute sophisticated modern attacks.

CNAPP leverages consolidation, automation and intelligence to deliver CI/CD security, posture management and compliance, and runtime protection to reduce risks due to human error and stop misconfigurations and threats in real time. The resulting tools give application developers and security teams the insight needed for protection throughout the application lifecycle.

CNAPP promises to make your security infrastructure smarter and faster. A smarter approach requires **100% visibility** and **seamlessly integrated threat intelligence**. Mounting a faster response requires **consolidated tools** and **cloud-scale automation**. To fully leverage these capabilities, you also need proven **cloud and security expertise**.

These five core tenets of CNAPP position cloud security teams to outsmart modern adversaries and move faster than sophisticated attacks.

80%

of enterprises will have consolidated security tooling for the lifecycle protection of cloud-native applications to three or fewer vendors by 2026

Source: Gartner, Market Guide for Cloud-Native Application Protection Platforms

The Five Pillars of Smarter, Faster Cloud Security

1. 100% visibility
2. Integrated world-class threat intelligence
3. Consolidated tools
4. Cloud-scale automation
5. Broad cloud security expertise

Pillars 1 and 2: Outsmarting Modern Adversaries

Attackers are constantly innovating to devise new ways to automate and scale attacks. To stay a step ahead, those tasked with securing the cloud must understand adversary motivations and anticipate their tactics, techniques and procedures (TTPs).

Outsmarting adversaries encompasses two of the five core pillars of a unified CNAPP solution:

- **100% end-to-end visibility coverage** across multi-cloud and hybrid deployments ensures adversaries can't hide in preventable gaps.
- **Reliable real-time threat and adversary intelligence** helps understand attacks and recognize indicators of compromise (IOCs) for known and zero-day attacks. CNAPP should include correlating TTPs used by cloud-conscious threat actors against global threat intelligence based on trillions of events.

Pillars 3 and 4: Moving Faster than Sophisticated Attacks

To accelerate detection and response, proactively hunt for threats and prevent incidents before they occur, modern cloud security strategies include two additional core pillars:

- **Consolidation of security tools** streamlines operations and compliance. A unified CNAPP platform should combine agentless and agent-based detection and response to achieve complete visibility across your entire cloud estate.
- **Automation that promotes scale** eliminates manual efforts to operationalize telemetry, contextualize incidents and take the right action. Automation built to scale helps speed detection and response, policy management and delivery of secure applications throughout the cloud lifecycle.

Pillar 5: Expertise

To maximize the value of investments, security teams must possess the **expertise** to leverage them fully. Enterprises may acquire these skills by engaging trusted CNAPP providers that bring deep cloud and security knowledge to achieve 24/7 efficiency gains without having to hire and train their own in-house experts.

Criteria for Choosing the Right Approach

At a minimum, a robust approach:

Combines agent-based and agentless detection and response from endpoints to hybrid and multi-cloud environments. Pairing agent-based and agentless technology and coverage in a single unified platform empowers organizations to see everything happening in their environment and quickly identify and remediate vulnerabilities and misconfigurations.

Features cloud-native agents that provide runtime protection to defend cloud workloads and containers against malware. Solutions should distinguish container activity from activity on a host — even for the most short-lived containers in the environment — to aid a forensic investigation. CNAPP platforms designed from the ground up specifically for the cloud deliver significantly enhanced performance, agility and scalability. Cloud-based solutions can be successfully deployed in environments with tens of thousands of hosts, workloads and containers in a matter of hours.

Drives operational efficiencies by enabling secure practices across the development pipeline and runtime. A cloud-native platform scales on demand to provide pervasive protection throughout the enterprise — faster, at a lower cost and with reduced management complexity. Updates take place within the cloud infrastructure to keep pace with today's fast-changing threat landscape. The cloud makes it possible to store petabytes of data used to analyze threats in seconds without impacting workloads and endpoints.

Taken together, achieving these objectives improves your organization's overall security posture and helps to streamline security workflows, knowledge-sharing, and ongoing compliance efforts.

The 5 Essential Elements of Modern Cloud Security

100% visibility

Integrated threat intelligence

Consolidated tools

Cloud-scale automation

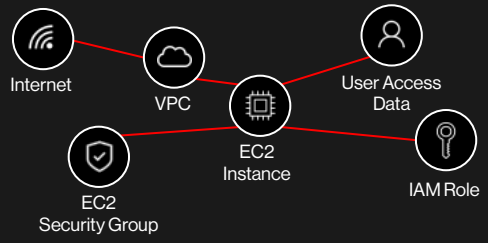
Cloud security expertise

Pillars 1 and 2: Making Cloud Security Smarter

Modern adversaries understand the cloud and how to automate attacks and take advantage of every weakness. Deep understanding of containers, vulnerabilities and cloud service provider (CSP) infrastructures equips them to not only find ways into your environment but also avoid detection while moving laterally through systems toward your business's most valuable assets.

In turn, effective cyber defense strategies incorporate deep knowledge of how adversaries think and act into prevention, detection and security posture management practices.

Cloud Attack Path Visualization
Correlated attack path analysis across endpoint and cloud — including behavioral cloud IOAs



Pillar 1: 100% Visibility to Avoid Dangerous Blind Spots

Cloud breaches often occur due to a lack of unified, real-time visibility and protection across hybrid and multi-cloud environments. Gaps in visibility allow threats to sneak in through blind spots between disparate monitoring solutions, increasing an organization's attack surface and the likelihood of attacks succeeding. Incomplete visibility also makes it possible for lateral movement to take place without alerting security teams.

Unified CNAPP eliminates the visibility gaps between security tools and across CI/CD pipelines. Complete coverage viewable within a single console and UI drives a faster, more intelligent response.

Falcon Cloud Security Provides Complete Coverage from Endpoint to Multi-cloud Environments
CrowdStrike Falcon® Cloud Security delivers unified agent-based and agentless protection from endpoints to all clouds to stop breaches. While other venders' solutions stop at detecting vulnerabilities and misconfigurations, CrowdStrike achieves the end goal of complete visibility, incorporating threat intelligence and automation to shut down attacks.

Combined agent-based and agentless monitoring to eliminate gaps
Where agentless-only approaches typically take snapshots of cloud risk once or twice per day, CrowdStrike delivers 24/7 continuous visibility coverage. This real-time insight proves essential to stopping breaches. The CrowdStrike Falcon® platform gives defenders complete visibility, all through a lightweight endpoint agent, integrated console and unified UI.

One-click XDR
CrowdStrike's CNAPP platform automatically detects and visualizes unprotected assets in easy to-read dashboards. One-click extended detection and response (XDR) capabilities equip analysts to deploy correctly configured agents to protect additional hosts instantaneously.

Industry-leading integration
CrowdStrike works with all major CSPs in and across hybrid and multi-cloud environments.

Pillar 2: Threat Intelligence to Understand Modern Cloud Adversaries

The epic rise in cloud exploitation and attack sophistication means security experts must understand adversary behavior more quickly than ever. A CNAPP should integrate reliable real-time threat intelligence to drive smarter, more confident decision-making that improves your response to incidents and events.

Combining up-to-the-minute threat intelligence with knowledge of what takes place in your environment equips security tools and teams to understand adversary motivations and predict attacks. Integrating world-class threat and adversary intelligence in the platform allows analysts to:

- Spot modern TTPs
- Correlate and contextualize risk
- Prioritize efforts to patch vulnerabilities and fix misconfigurations used to execute cloud attacks

Threat intelligence must be seamlessly integrated across all environments and controls so its consumption and application take place automatically. Solutions should leverage the agility of the cloud to store very large data sets for future use by analysts in incident response, threat hunting and forensics.

Falcon Cloud Security Leverages World-Renowned Adversary Intelligence

Falcon Cloud Security integrates CrowdStrike's award-winning threat and adversary intelligence collected from protecting thousands of customer organizations worldwide. The Falcon platform operationalizes insights from CrowdStrike's global Intelligence team to add rich, actionable context around incidents and alerts. Built-in, proven-accurate indicators of risk sourced from world-class adversary intelligence help analysts detect and prevent runtime attacks.

As a threat intelligence leader and pioneer, CrowdStrike maintains the industry's most extensive and robust adversary insight. The Falcon platform features:

- Indicators of attack (IOAs) to identify attacker behaviors and trends
- Indicators of compromise (IOCs) to recognize when an attack has started
- Indicators of misconfigurations (IOMs) to prevent human error and improperly configured controls from leaving doors open for attackers

CrowdStrike constantly detects and automatically updates cloud-specific IOAs and IOCs within the Falcon platform. As new threats and TTPs appear, analysts create detailed IOCs — many unique to CrowdStrike — to improve the security of the entire customer base against emerging risk.

CrowdStrike's World-Class Threat Intelligence
Continuous monitoring of adversaries through data analysis and Falcon OverWatch services

215+
Adversaries tracked

Captures
Trillions
of events per week

150 Million
IOA decisions per minute

The Falcon platform regularly analyzes trillions of security events per week and combines data with human intelligence from one of the largest incident response teams in the industry. CrowdStrike tracks 215+ adversaries and their TTPs to keep adversaries from exploiting vulnerabilities, ultimately stopping breaches.

Pillars 3 and 4: Making Cloud Security Faster

Enterprises move applications to the cloud to gain agility and speed, but a shortage of skilled resources keeps defenders from evaluating cloud threats 24/7. In-house teams may be ill-equipped to recognize sophisticated attacks, which can lead to longer dwell times for adversaries to lay low and orchestrate campaigns. Adding to the pressure to act quickly, DevOps teams resist letting security slow down application delivery.

The right CNAPP platform consolidates security components and automates detection and remediation to block attacks — without impeding DevOps teams from pushing applications quickly. A CNAPP uses extensive tool consolidation and automation to accelerate detection and response.

Pillar 3. Tool Consolidation to Streamline Operations

The traditional approach to cloud security relies on disparate tools from multiple vendors. This forces administrators to toggle between cloud workload protection (CWP), cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM) and other CNAPP toolsets and screens to create a holistic view of risk.

The complexity created by a patchwork approach increases the likelihood of visibility gaps and delays decision-making and response. Siloed tools provide a fragmented view that lacks sufficient context to prioritize threats.

Operations also suffer, as multiple tools:

- Generate excessive volumes of alerts to be investigated
- Increase the potential for vulnerabilities and misconfigurations to go unnoticed
- Consume more cycles to configure and maintain

These inefficiencies add risk and drive up costs while making it harder to maintain compliance and strengthen security posture.

60%
of enterprises will have consolidated cloud workload protection platform (CWPP) and CSPM capabilities to a single vendor by 2025, up from 25% in 2022.

Source: Gartner, Market Guide for Cloud-Native Application Protection Platforms

The Benefits of Tool Consolidation

As per Gartner, *"An organization could implement 10 or more tools to deliver fully against the capabilities. However, there are reasons that organizations are moving toward consolidation to a CNAPP offering:*

- *Better identification, prioritization and remediation of cloud-native application risk.*
- *Reduces operational complexity through consolidation of vendors, consoles, policies and contracts, thereby reducing chances of misconfiguration or mistakes. This enables:*
  - *A single place to define consistent security policies across development and operations.*
  - *Consistent enforcement of security policy across all application artifacts — code, containers, VMs and serverless functions.*
  - *Elimination of overlapping policies of disparate products and standardization of application policies and policy objects across all development artifacts.*
- *A single vendor should implement a single data lake, data model and unified graph database for all event logging, reporting, alerting and relationship mappings. This enables the vendor to deliver against the vision of RiskOps — finding the root cause of the risk, identifying the person/team responsible for fixing it and risk-prioritizing the remediation efforts. This reduces the attack surface and shortens remediation times.*
- *By having consistently enforced policies and by risk-prioritizing remediation efforts, a single-vendor CNAPP offering should reduce developer friction and improve developer experience.*
  - *By integrating security testing throughout the life cycle and directly into the developer's toolset versus one large test prior to production, CNAPP offerings enable fixing problems earlier and speeding application deployment.*
- *Eliminates redundant capabilities (for example, most cloud providers offer container vulnerability scanning).*
- *More easily enables visibility from runtime so that it can be used to feed back into development. Likewise, a single platform more easily enables visibility from development used to strengthen runtime protection."*[2]

Falcon Cloud Security Replaces Point Products

Falcon Cloud Security consolidates and unifies multiple CNAPP capabilities in one solution to streamline security operations. The platform consolidates a wide range of point products used to protect and monitor endpoints, cloud workloads, identity and data to provide end-to-end coverage and eliminate complexity.

A consolidated view lets defenders understand and track adversary behaviors and the progression of attacks without switching between multiple consoles to generate a reliable visualization of risk. CrowdStrike's unified approach combines monitoring capabilities from cloud-native agents and agentless coverage in places where deploying software proves challenging. Falcon Cloud Security delivers complete visibility across the entire cloud estate using a single agent, console and UI.

Replacing disparate tools with Falcon CNAPP capabilities also reduces operational overhead associated with licenses and enables security groups to quickly push policies across accounts, regions, projects and virtual networks.

[2] Gartner Market Guide for Cloud-Native Application Protection Platforms

Pillar 4: Automation Built to Scale

A CNAPP supports CI/CD best practices that call for security to be integrated and automated throughout the cloud application lifecycle. Manual efforts slow down security operations and application delivery while increasing the potential for human error.

Some standalone elements of a CNAPP solution detect threats but do not automate remediation capabilities to stop problems from becoming bigger issues. Without automated response, high volumes of alerts to investigate can delay decision-making among resource-constrained security staff.

A modern cloud security platform should do more than tell administrators a problem exists — it should allow them to take steps to address weaknesses.

Falcon Cloud Security Automates Response and Prevention
Falcon Cloud Security automatically correlates attack path analysis across on-premises, hybrid and multi-cloud environments. By allowing defenders to set rules that automate resolution of "low-hanging fruit" issues, Falcon helps organizations avoid threats at cloud scale.

For example, when Falcon Cloud Security detects a misconfiguration in containers that adversaries might exploit to launch attacks, it can be set to automatically shut down deployment of new containers at risk from that same flaw. Administrators can also program the platform to push policies based on CrowdStrike AI and machine learning — including unique IOCs, IOAs and IOMs — to improve response, threat hunting and compliance.

Falcon automatically discovers and visualizes protected and unprotected hosts and flags those that require protection. With a single click, administrators can instantly deploy correctly configured agent-based or agentless coverage. One-click remediation testing and agent deployment let organizations rapidly secure assets without disrupting operations.

Automation and tool consolidation provide a marked speed advantage that works hand-in-hand with complete visibility and intelligence.

> **CrowdStrike gave us the flexibility to quickly move from protecting our PCs to AWS pods at the click of a button, and with the same platform we know and trust."**
>
> — Zack Gable, Geisinger CISO
>
> Source: Geisinger Case Study

> **CrowdStrike extending the Falcon platform to support CNAPP provides comprehensive cloud security with threat hunting capabilities that no other vendor can match."**
>
> — Jason Waits, Inductive Automation
>
> Source: Inductive Automation Case Study

Falcon Automation

- **Deploys on unmanaged systems** with one-click deployment
- **Instant onboarding** with built-in agentless technology
- **Bulit-in policies** for IOCs, IOMs, IOAs, Kubernetes and compliance frameworks
- **Smooth workflows** with Falcon Real Time Response (RTR), custom policies and automated workflows

Pillar 5: Deep Cloud and Security Expertise

Attackers can afford to focus all of their energies on the cloud, but overworked security staffs rarely enjoy the same luxury. To extend the capabilities of enterprise defenders stretched too thin to keep pace with cloud risk, organizations may engage a proven leader to provide expert security services.

The right partner acts as a powerful force multiplier that brings deep cloud and security expertise to a modern CNAPP initiative.

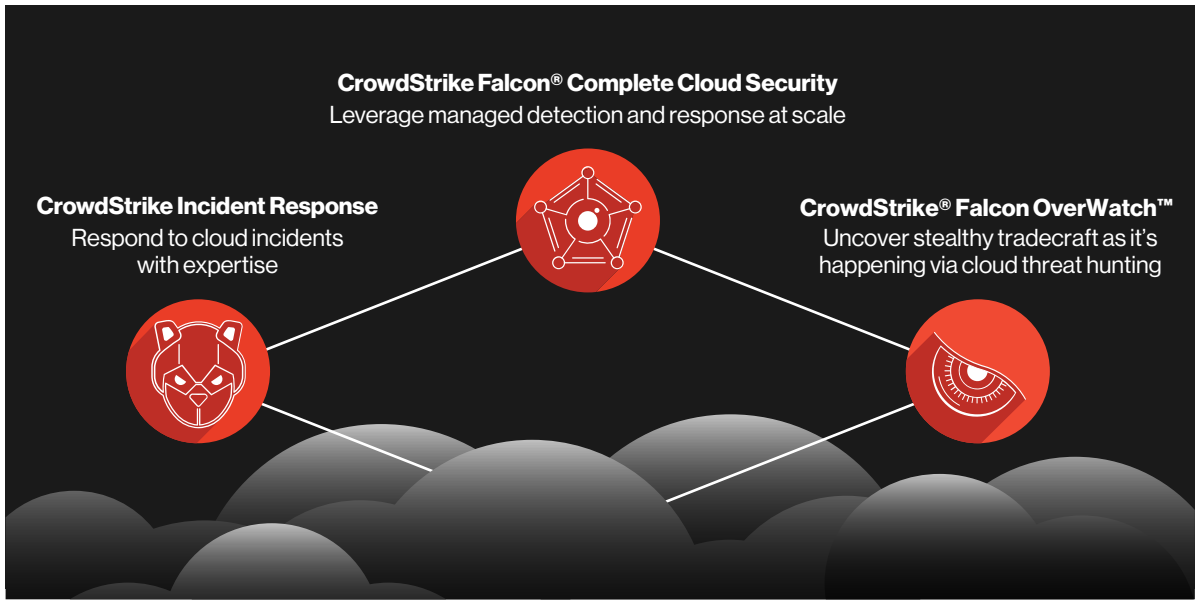
World-class Cloud Security Services

A provider should function as an extension of your team — like adding a highly skilled analyst that brings a wealth of global knowledge and decades of experience. Choose a CNAPP leader with a proven history of security and cloud innovation and outsmarting clever cloud adversaries. Make sure the platform is backed by expert services to detect, respond to and prevent potential threats.

CrowdStrike Delivers Unrivaled Technology and Analyst Capabilities

Industry analysts, partners and global customers widely regard CrowdStrike as a global cloud security and CNAPP leader — including top U.S. banks, airlines and government agencies. CrowdStrike functions as an extension of customer teams across all environments for seamless coverage, investigation, incident response and policy management.

The Falcon platform brings an unrivaled mix of technology and human intervention for fast, accurate, proven threat detection and response in a seamless unified solution. Automated detection includes prioritizing malicious activity, while manual analysis adds context needed for rapid response and proactive threat hunting.



CrowdStrike possesses the breadth of knowledge and depth of skilled resources to meet enterprises wherever they are in their cloud maturity journey and instantly up-level security. No other CNAPP provider brings comparable insights collected by sensors deployed across the globe.

Where some security solutions do not offer cloud-specific capabilities, CrowdStrike provides a full range of cloud-specific services to help customers improve their security posture. Expert professional services include:

- 24/7 managed detection and response (MDR)
- across all environments Cloud incident response
- Threat hunting to find potential cloud threats

Choosing the Right Solution

The decision to employ a comprehensive CNAPP strategy ultimately depends on an organization's business case for investing in cloud security. A consolidated solution that bundles multiple capabilities delivers the greatest investment value and operational efficiencies.

On average, CrowdStrike Falcon Cloud Security customers expect:[3]

- 74% faster cloud detection and response
- 780 hours saved per year by preventing and automating response to cloud-based incidents
- +$380K annual operational and efficiency savings

The innovative Falcon platform is a leader in endpoint detection and response (EDR), implementing a cloud-native agent on the endpoint to deliver efficient and effective cloud security in a single unified platform for optimal user experience. CrowdStrike covers all five pillars of a modern CNAPP approach:

- Full detection and response capabilities for 100% visibility
- World-class global intelligence
- Security point-tool consolidation
- Industry-leading automation capabilities
- World-class managed and professional services

CrowdStrike Delivers the 5 Pillars of Modern Cloud Security

	SMARTER		FASTER		MORE EFFICIENT
Capabilities	**1. Visibility**	**2. Threat Intelligence**	**3. Tool Consolidation**	**4. Automation**	**5. Expertise**
Impact	Stop attackers from hiding in blind spots	Understand modern adversaries	Work in a single unified console	Scale protection on demand	Gain efficiency through experts
Criteria	• Full coverage for hybrid and multi-cloud deployments • Run-time visibility • Continuous coverage (vs. 24-hour snapshots) • Discovery and visibility of all cloud resources • Ability to find and fix misconfigurations • CI/CD pipe scanning • Monitoring of cloud and privileged user accounts	• Knowledge of real-world attacks and TTPs of cloud-conscious adversaries worldwide • Threat intelligence integrated into cloud security	• Combination of proven agent-based and agentless technology for every cloud in one integrated console to see/stop everything everywhere	• Automated detection • and response • Automated policies with built-in IOCs, IOAs, IOMs and compliance • Ability to find misconfigurations through pre-built image scanning • Automated runtime protection and malware analysis (e.g., sandboxing)	• 24/7 MDR for cloud • Managed, analyst-led cloud threat hunting • Managed cloud incident response (IR)
Operational efficiency gains		• Eliminate silos between disparate cloud security solutions • Easily deploy coverage to unprotected hosts			

[3] These numbers are projected estimates of average cost benefit based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

Bonus: 10-Point Checklist for Evaluating CNAPP Solutions

- [ ] **1.** Does the solution consolidate multiple point tools to provide value out-of-the-box?
- [ ] **2.** Does the platform offer unified 100% visibility and security coverage from endpoints to the cloud? Can analysts avoid the need to switch within or between multiple consoles, toolsets and UIs?
- [ ] **3.** Does the platform pair the capabilities of cloud-native agents and agentless security?
- [ ] **4.** Can the solution automatically detect and visualize unprotected resources and easily allow defenders to deploy agents?
- [ ] **5.** Does the platform provide automated detection, response and remediation?
- [ ] **6.** Does the platform integrate proven global threat and adversary intelligence? Does it automatically correlate risk with TTPs to promote faster response?
- [ ] **7.** Is the provider a trusted global cloud and security innovator and leader? Is CNAPP part of a holistic enterprise security program?
- [ ] **8.** Does the solution simplify your licensing structure?
- [ ] **9.** Does the platform streamline complexity to promote smarter, faster detection, response and compliance?
- [ ] **10.** Is the solution backed by world-class managed and professional services?

Outsmart Today's Cloud Adversaries — Get Your Free Cloud Security Risk Review Today

Cloud attacks are becoming faster and more sophisticated. Learn how Falcon Cloud Security can improve your cloud incident response capabilities. Get a free Cloud Security Risk Review to identify your cloud vulnerabilities, provided through agentless scanning deployed in minutes with zero impact to your business.

Falcon Cloud Security provides 100% coverage to detect lateral movement from endpoints to modern hybrid and multi-cloud environments.

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

Follow us:

- **Blog ›**
- **Twitter ›**
- **LinkedIn ›**
- **Facebook ›**
- **Instagram ›**

Start a free trial today

Gartner, Market Guide for Cloud-Native Application Protection Platforms, Neil MacDonald, Charlie Winckless, and 1 more, 14 March 2023

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CROWDSTRIKE