CrowdStrike Products

CROWDSTRIKE

A PROVEN APPROACH TO CLOUD WORKLOAD SECURITY

Lessons learned from securing one of the world's largest cloud platforms

EXECUTIVE SUMMARY

As a cybersecurity company that has built one of the biggest cloud architectures in the world, CrowdStrike has gained an exceptional vantage point and garnered unique experience on what it takes to secure cloud workloads.

Various security challenges come with the cloud. For example, the cloud is vulnerable to human errors and more prone to shadow IT than on-premises environments. And like any other compute environment, it is exposed to runtime threats. In addition, the teams that are implementing cloud workloads might not have the security knowledge necessary to adequately protect them.

CrowdStrike secures its cloud infrastructure by focusing on staying ahead of adversaries, relentlessly reducing its attack surface and obtaining total visibility of events taking place in the environment. CrowdStrike uses its own technology and expertise — the CrowdStrike Falcon® platform, the Falcon OverWatch™ and CrowdStrike® Intelligence teams, and CrowdStrike Services Cloud Security Assessment — to achieve those goals. These same CrowdStrike solutions are also available to customers who want to protect their cloud workloads.

As more enterprises adopt containers and public cloud IaaS (infrastructure as a service), the need for comprehensive security across cloud workloads increases exponentially. This need has become more urgent as attacks continue to move to the cloud.

As a cloud-native platform, CrowdStrike Falcon processes over 470 billion events per day — and that number represents only the streaming data. In addition, CrowdStrike stores 14 petabytes of data in the cloud, constituting the data at rest. As a cybersecurity company, CrowdStrike has gained a unique perspective on how to protect that data and the infrastructure that holds it.

The goal of this white paper is to share some of the knowledge and experience the CrowdStrike team has gained from securing its own cloud. It begins by describing the major factors that make the cloud vulnerable to threats and sharing some security-related observations made by the CrowdStrike cloud team. It then explains CrowdStrike's approach to protecting a cloud infrastructure that is processing trillions of events per week and continues to grow as the company adds new capabilities to the Falcon platform and gains new customers. The paper concludes by describing the role the Falcon platform can play in protecting cloud workloads.

As more enterprises adopt containers and public cloud IaaS (infrastructure as a service), the need for comprehensive security across cloud workloads increases exponentially.

SECURITY ISSUES WITH CLOUD INFRASTRUCTURE

The reasons behind breaches in the cloud can be broadly classified into four categories: human errors, runtime threats, shadow IT and lack of clear cloud security strategy.

HUMAN ERRORS

Due to the nature of cloud environments, the majority of breaches in the cloud are caused by human error. In the cloud, the absence of perimeter security can make those mistakes very costly. These errors can include misconfigured S3[1] buckets, leaving ports open to the public, or the use of insecure accounts or APIs. Sometimes, organizations are not even aware of what APIs are being used, let alone understanding whether or not they are secure.

Those errors transform cloud workloads into obvious targets that can be easily discovered with a simple web crawler. Multiple publicly reported breaches started with misconfigured S3 buckets that were used as the entry point. Other examples of misconfiguration leading to a breach involve servers in the DMZ that have ports wide open to the world. These configuration issues continue to happen, especially because some default settings can leave workloads exposed.

RUNTIME THREATS

In public clouds, much of the underlying infrastructure is already secured by the cloud service provider (CSP). However, everything from the operating system to applications and data are the responsibility of the user. This is what is referred to as the "shared responsibility model." Unfortunately, this model can be misunderstood, leading to the assumption that cloud workloads are fully protected by the CSP. This results in users unknowingly running workloads that are not fully protected, meaning adversaries can target the operating system and the applications to obtain access. Attackers use zero-day exploits to gain a foothold, then establish persistence by planting advanced persistent threats (APT) and moving laterally within the data center.

Any available attack surface will be leveraged by adversaries. Even securely configured workloads can become a target at runtime, as they are vulnerable to zero-day exploits and unpatched vulnerabilities. In addition, the cloud provides more than just compute power. It has also become a storage facility for intellectual property and confidential documents, making cloud workloads an increasingly attractive target for attackers.This is a trend observed by the CrowdStrike Services team across numerous breaches it investigated this year that originated in cloud workloads, which many adversaries seem to be targeting specifically.

SHADOW IT

Shadow IT, which describes applications and infrastructure that are managed and utilized without the knowledge of the enterprise's IT department, is another major issue in cloud environments, and DevOps often contributes to this challenge. The barrier to entering and using an asset in the cloud — whether it is a workload or a container — is extremely low. Developers can easily spawn workloads using their personal accounts. These unauthorized assets are a threat to the environment, as they often are not properly secured and are accessible via default

[1] S3 stands for Amazon Simple Storage Service, which provides object storage through a web service interface.

passwords and configurations, which can be easily compromised. In one major reported breach, the initial access was gained through a personal Kubernetes server used by a developer leveraging default credentials.

This situation is exacerbated by the requirement that cloud teams and DevOps run fast without friction, while at the same time the security team needs visibility to provide adequate protection. Security teams require basic information such as what accounts are present, who is deploying, who is creating new instances and who is using cloud resources. However, that information can be difficult to obtain without hampering DevOps activities. As cloud shadow IT and DevOps become more mainstream, both the security and core IT teams need to adapt. DevOps cannot be expected to insert suites of security software into their continuous integration/continuous delivery (CI/CD) pipeline or to modify the way they work, because this approach would not be scalable. Neither can security teams request that cloud teams provide the information they need because that would slow down the work DevOps is trying to conduct. IT and security need to find solutions that will work at the speed of the cloud — at DevOps' velocity.

LACK OF CLOUD SECURITY STRATEGY

As workloads move to the cloud, administrators continue to try and secure these workloads the same way they secure servers in a private or on-premises data center. Unfortunately, traditional data center security models are not suitable for the cloud.

For example, IT administrators continue to use static passwords for authentication and authorization, instead of MFA (multifactor authentication) and IAM (identity and access management). They also persist in using long-lived instances instead of ephemeral workloads and relying on DevOps to take responsibility for security, when the DevOps team may not have the knowledge or skills necessary to properly secure its workloads. For example, a developer may not know that instead of patching an instance or a container, he or she should create a new AMI (Amazon Machine Image) template or a new container image that is not vulnerable.

Even if customers own cloud security products, they often fail to secure their cloud workloads. In fact, all large companies that experienced a breach last year had some cloud security solution in place.

These issues reveal that a good cloud strategy must include education. Educating teams on secure practices such as how to store secrets, how to rotate keys and how to practice good IT hygiene during software development is key, but it is often lacking. DevOps may be happening, but DevSecOps may not — which is hampering the industry's ability to make the cloud secure.

Even if customers own cloud security products, they often fail to secure their cloud workloads. In fact, all large companies that experienced a breach last year had some cloud security solution in place.

LESSONS LEARNED

Although the cloud may still be new for many organizations, CrowdStrike has been building and securing its own cloud since 2011. During that time, CrowdStrike has observed the following trends.

THE CLOUD IS DYNAMIC

Providers and consumers of cloud services are moving fast with dozens of new cloud-native services being introduced each year. These services are often aimed at busy developers who are focused on keeping their friction low and their velocity high. While most security teams understand their roles in the shared responsibility model, it can be difficult for them to keep up with the changing landscape. Even companies with a strong security program and demonstrated expertise can be at risk of not having sufficient security. For example, a large financial services company with sophisticated cloud security capabilities suffered a breach involving its cloud infrastructure, even though it had previously contributed to an open-source cloud security toolkit.

DIFFERENT CLOUDS AND VARIED WORKLOADS

Attacks can traverse multiple planes and involve different types of workloads. The attack against the financial services company involved tactics that spanned traditional web applications, endpoints and cloud-native resources. Reports about the breach mentioned that an application flaw was exploited to pull a temporary station-to-station (STS) key from the underlying host's EC2 (Amazon Elastic Compute Cloud) metadata service. The key was then used externally to access sensitive cloud resources including S3.

CrowdStrike investigated an incident that started with an insider threat, with the perpetrator running an exploit on Amazon Web Services (AWS) resources. Leveraging a vulnerability in AWS, the attacker was able to obtain data that was stored in S3 buckets. CrowdStrike expects attacks involving multiple types of workloads and the cloud to become more common going forward.

The visibility needed to see the type of attack that traverses from an endpoint to different cloud services is not possible with siloed security products that only focus on a specific niche. Only a combination of endpoint and cloud-native security tools working together can see attacks of that nature.

Organizations often have more than one cloud to support. Companies running workloads in the public cloud look to improve reliability and availability by adopting a multi-cloud strategy. While definitely a step in the right direction, these companies are finding that not all cloud providers offer the same security features.

SECURITY CONTROL DIFFERENCES CAN LEAD TO MISCONFIGURATIONS

Security controls differ from cloud to cloud. Even when cloud service providers offer similar security controls, their behaviors and implementations can vary. Even elements as simple as the log trails needed to support threat hunting, and the design patterns for retrieving them vary from cloud to cloud. These variations make for a steep learning curve, with each public cloud provider offering different sets of security controls. Default configuration settings also vary by provider. Even where there is some overlap, there are different implementations and nuances to deployment. Until organizations become proficient at securing all of their different clouds, adversaries will continue to take advantage of misconfigurations.

This is why good multi-cloud security requires broad expertise, continuous learning and a clear strategy. CrowdStrike has long embraced the value of defining and enforcing a strong and clear cloud security strategy.

HOW CROWDSTRIKE SECURES ITS CLOUD

CrowdStrike uses a three-pronged security strategy to guide its cloud security initiatives.

FOCUS ON THE ADVERSARY

At its core, CrowdStrike's strategy for ensuring security puts the adversary first. In all areas of security, including the cloud, it is critical to understand your adversaries and their modus operandi: who they are, what they want, what they must accomplish to get it and how that maps to an attack surface.

CrowdStrike has observed that many of the same adversaries are active in the cloud and in other parts of the IT landscape. The difference is that the cloud offers adversaries the opportunity to use a new set of tactics, techniques and procedures (TTPs). CrowdStrike continues to research these cloud-native threats and has found that TTPs are maturing for AWS users and emerging across Google Cloud Platform (GCP) and Microsoft Azure. Most current techniques involve adapting traditional attack modes for the cloud, although cloud-only techniques are likely to emerge in the hands of sophisticated adversaries.

Current state-of-the-art techniques include:

- **Attack tools and post-exploitation frameworks.** These are now available for AWS with software such as PACU and Barq that can use IAM for privilege escalation or use Lambda functions for persistence and evasion.
- **S3 ransomware.** There is published research around S3 ransomware, which could be theoretically expanded to any cloud service that offers bring-your-own-key and easy rotation, as those could be potentially vulnerable too.
- **Traffic sniffing.** AWS recently introduced new capabilities in network mirroring, which in addition to improving network monitoring can also allow new paths for packet sniffing and bulk data exfiltration.

Staying informed about these threats can be challenging. That is why having strong partners for threat and situational intelligence helps. Third-party testing, internal red-teaming and bug bounty programs are also valuable when implementing an adversary-focused approach. CrowdStrike uses the CrowdStrike Intelligence and CrowdStrike Services teams to provide ongoing, comprehensive cloud security assessments.

REDUCE THE RISK OF EXPOSURE

CrowdStrike strives to drive down the risk of exposure, so that it is limited to what is needed to run the business. This includes continually searching for and removing unnecessary attack surfaces. As an organization, CrowdStrike cultivates a "security-first" culture that is embraced at all levels of the company — from the C-suite to the newest engineer.

Examples of tactics CrowdStrike uses to reduce the attack surface include:

- **Segmenting where possible to reduce a potential attack blast radius.** This entails using different cloud accounts, virtual private clouds (VPCs), subnets and roles for different types of workloads. Strive to avoid overlapping production, development and integration workloads.
- **Using cloud-native encryption where available** for data in flight and at rest in the cloud, and being proactive when it comes to ciphers, protocols, keys and certificates — including having a suite of internal tools to help.
- **Securing earlier in the process** — a practice also known as "shift left" — by implementing tools, automation and standards to enable engineers

to easily follow the desired security behavior. These tools reduce developer friction as well as diminish the likelihood that unsafe or default configurations in the wild will be used.

- **Using MFA where available and hard tokens for high-impact environments** such as GovCloud deployments.
- **Proactively maintaining good IT hygiene** by automatically discovering the cloud workload footprint.

MONITOR THE ATTACK SURFACE

Always look for ways to improve visibility into the necessary attack surface. This makes it more challenging for adversaries to hide and also drives up their attack costs.

The CrowdStrike Falcon platform provides comprehensive visibility across CrowdStrike's cloud infrastructure. In fact, the cornerstone of CrowdStrike's internal cloud visibility strategy can be summed up as "Falcon everywhere." This approach consists of deploying the Falcon agent on all cloud workloads and employing the Falcon OverWatch team to proactively hunt for threats 24/7. In addition, CrowdStrike uses specific cloud-native IOAs (indicators of attack), analyzes machine learning (ML) patterns and performs free-form threat hunting, looking for hands-on-keyboard activity by adversaries within CrowdStrike's cloud workloads and control plane.

This level of visibility coupled with proactive threat hunting has allowed CrowdStrike to detect subtle, nearly imperceptible behaviors with uncanny accuracy, such as an incident in which an adversary was probing for the existence of certain S3 buckets. Those buckets were not publicly accessible, and they were named in a way that made using brute force impossible, which prompted CrowdStrike analysts to investigate how the adversary could have obtained a list of the S3 buckets. After considerable research, CrowdStrike intelligence sources surmised that the adversary was probably pulling S3 bucket names from sampled DNS request data they had gathered from multiple public feeds. That type of data is easily obtained by accessing resources from public WiFi. The lesson here is that the adversary sometimes has more knowledge of and visibility into an organization's cloud footprint than you might think.

The expertise the CrowdStrike team has gained firsthand by defending its cloud helps the product team continue to expand the Falcon platform, fueling enhancements and creating new cloud workload security features.

The cornerstone of CrowdStrike's internal cloud visibility strategy can be summed up as "Falcon everywhere."

A CLOUD-NATIVE PLATFORM DESIGNED TO PROTECT ALL WORKLOADS

THE CROWDSTRIKE FALCON PLATFORM

The CrowdStrike Falcon platform has been designed to support workloads, regardless of their location. With the Falcon platform, organizations can secure instances running in all types of public clouds including AWS, GCP and Azure. Falcon protects physical servers and virtual machines in your private data center and instances in the public cloud. The platform is built on two common components: a single lightweight agent and a distributed cloud. The single-agent architecture supports all types of workloads but is tuned to collect data specific to the cloud infrastructure and the workload it is running on. For example, Falcon for AWS is designed to collect additional metadata from AWS. This has allowed CrowdStrike to provide its customers with multiple applications without requiring multiple agents, multiple consoles or any additional management component. Another big advantage of this cloud-native architecture is that it allows protection to be deployed seamlessly, regardless of the number of VPCs in use. Whether an organization is using 10 or 100 VPCs, no additional managers are required.

Visibility is the critical first capability provided by the platform because it is the foundation of breach prevention. Without visibility, defenders are blind. They cannot detect what is malicious and therefore cannot protect against it. Visibility is the first requirement to ensure nothing is missed and potential breaches are stopped.

As hybrid and multi-cloud environments are becoming the norm, attacks spanning multiple control panes are emerging, such as the financial services breach previously cited. Those attacks involve multiple types of workloads and move across different types of environments. To detect those threats, visibility needs to be centralized and happen in real time. The Falcon platform is uniquely designed to provide this type of end-to-end visibility in a single unified console — from endpoints and servers to workloads and containers. This allows security teams to see and hunt for threats across all of their workloads, regardless of their nature or location.

The second important set of capabilities includes prevention and automated detections. Both are powered by artificial intelligence (AI), ML and behavioral analysis, which are performed on the telemetry data being collected.

These visibility, detection and prevention capabilities are considered the core of the Falcon platform and can be augmented with other capabilities such as IT hygiene and vulnerability management.

As mentioned earlier, threat intelligence is also crucial for protecting cloud workloads. The threat intelligence produced by the CrowdStrike Intelligence team, from threat indicators to adversary profiles, is pervasively integrated throughout the platform. This allows Falcon to automatically leverage that intelligence for detections, prevention, and incident triage and prioritization.

Real-time visibility, threat prevention, IT hygiene, vulnerability management and threat intelligence integration are capabilities provided by the Falcon platform. In addition, Falcon includes many cloud-specific features.

FALCON PLATFORM CLOUD-SPECIFIC CAPABILITIES

Migration and Multi-cloud Support
Falcon ensures continuous protection through the same platform, agent and console as organizations migrate their workloads from on-premises to the cloud. The ability to use the same solution for all workloads is extremely well-suited for the

modern data center, which often follows a hybrid-cloud model that includes a mix of on-premises, private and public clouds. Using the same solution provides continuity and predictability in the level of protection, as well as centralized visibility across different data center environments.

Falcon is also designed to scale along with your ephemeral workloads, ensuring that security doesn't become a bottleneck for DevOps.

A flexible pricing model offers annual and consumption-based options to match the licensing needs of both regular or reserved instances and ephemeral workloads.

Containers

Another other major cloud trend is the growing use of containers. DevOps teams are increasingly migrating to containers, adding more of this type of workload to the environment. Protecting and obtaining visibility into containers has become imperative. However, most of today's solutions for protecting containers require procuring another product. In contrast, CrowdStrike uses the same platform and the same agent, making the platform container-aware and container-compatible. This ensures protection not only for the host but also for all of the containers running on it. As Falcon secures both hosts and containers using a single agent, there is no need to deploy an additional container for security or to deploy code within the container. In addition, cloud teams don't have to change their workflows or CI/CD pipelines. This approach provides a unique way to gain more comprehensive visibility without adding friction.

Being namespace aware allows the Falcon Linux sensor to see the activities happening on both the host and within the container. This provides security teams with the unique ability to see entire chains of events, from the host kernel level all the way to processes launched inside a container.

The platform also provides visibility into which container instances are being used on which hosts, and what images they are connected to, and also correlates the detections occurring in containers. This provides crucial visibility into container environments across the stack, whether they are running on-premises or in the cloud.

Cloud Workload Visibility and Discovery

The Falcon platform also provides visibility across public clouds. For example, organizations can quickly visualize existing Amazon EC2 deployments across all regions (including instances without a Falcon agent installed) and subsequently monitor cloud trail logs for any modifications to the environment. This is a huge benefit as it enables customers to have a more complete and centralized picture of their environments, from the workloads running in their own data centers to workloads in public clouds, all the way down to the containers running on those hosts.

Cloud Integrations

CrowdStrike believes that a collaborative and coordinated approach is key to stopping today's breaches. This is why the Falcon platform was built from inception to be open and extensible. This flexibility also allows customers and partners to easily leverage the platform to expand their security solutions. Some of the areas that are benefiting from CrowdStrike's integration strategy are product deployment, threat intelligence and telemetry sharing, and the streamlined availability of partner technologies in the Falcon platform.

- **Deployment:** Ease of deployment is key to the success of security initiatives. In the cloud, and even more importantly for containers, deployment needs to be frictionless, and integration with deployment tools is crucial. To ensure that DevOps can deploy at scale, Falcon can easily be added as part of the deployment process using DevOps tools such as Chef, Puppet or AWS Terraform. Falcon also integrates with Google Cloud Operating System (OS) configuration management so the Falcon agent can be deployed out of the box, directly from GCP, without the need for custom scripts such as Chef recipes.

- **Threat intelligence:** This has been a core part of the Falcon platform because it is a necessary component of a successful breach prevention

strategy. Over the years, CrowdStrike has emerged as a leader in threat intelligence and has made this information available to customers within the Falcon platform as a standalone subscription and also through OEM integration. For example, CrowdStrike is one of only two threat intelligence providers for AWS GuardDuty, enabling its users to benefit from CrowdStrike threat intelligence in many of their products.

- **APIs:** CrowdStrike is committed to making the Falcon platform both open and extensible — allowing customers and partners to easily integrate with CrowdStrike and extend their current solutions' functionalities. Using the APIs provided by CrowdStrike, customers can extract their data — from detections only to their full data set — whether in the cloud or on-premises. This allows customers to leverage their data for offline or custom analytics, for retrospective detections or for archiving.

- **The CrowdStrike Store:** The power and ease of integration with the Falcon platform can be seen in the CrowdStrike Store, where CrowdStrike partners can launch applications based on the data collected by Falcon. That integration manifests as an enterprise marketplace where customers can discover, try, buy and deploy trusted partner applications that extend and complete their investments in the CrowdStrike Falcon platform.

As a cybersecurity company that is also responsible for securing its own Falcon platform — one of the world's largest cloud architectures — CrowdStrike is in a unique position to help organizations secure their cloud workloads. The first step toward successfully securing cloud workloads is to define a clear strategy and establish a unified plan that covers all workloads.

CrowdStrike's own security strategy is centered around three pillars: focus on the adversary, reduce the surface of attack and gain complete visibility on the remaining necessary attack surfaces.

The company uses its own solutions to implement this strategy. It starts with the Falcon agent, which is deployed on every workload to provide visibility and protection and also across all of the clouds and data centers used by CrowdStrike. The Falcon platform also helps in identifying rogue and potentially insecure workloads. The Falcon OverWatch team proactively hunts for threats 24/7 across the entire environment. The CrowdStrike cloud team also collaborates with the CrowdStrike Intelligence team to stay ahead of the adversaries. And finally, the CrowdStrike Services team helps with conducting regular cloud security assessments. These tools and services are also available to other organizations.

CrowdStrike remains laser-focused on helping customers protect their organizations against today's sophisticated adversaries by providing the comprehensive visibility needed to effectively secure even the most widely distributed and diverse environments.

This means providing the ability to deliver a complete picture across all workloads — endpoints, mobile devices, servers, cloud workloads, containers — and across all types of environments: data centers, on-premises, cloud and hybrid. This comprehensive coverage means that customers are ensured complete centralized visibility and protection — the keys to a strong security posture.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Start Free Trial
of Next-Gen AV

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