Runtime Protection: The Secret Weapon for Stopping Breaches in the Cloud

April 4, 2022

David Puzas Endpoint & Cloud Security

Mistakes are easy to make, but in the world of cloud computing, they aren't always easy to find and remediate without help.

Cloud misconfigurations are frequently cited as the most common causes of breaches in the cloud. According to a 2021 survey from VMware and the Cloud Security Alliance, one in six surveyed companies experienced a public cloud security breach or incident due to a cloud misconfiguration in the previous 12 months.

Cloud security posture management (CSPM) tools have emerged as excellent solutions for catching manual errors and policy violations. But pre-runtime security is only one layer of comprehensive cloud security. For organizations to safely and confidently embrace the cloud, they need to protect workloads against the threats that appear once they are live.

What CSPM Tools Do —— and What They Don't

Cloud security posture management tools are designed to automate the identification and remediation of security risks in your private, public and hybrid cloud infrastructure. When it comes to the cloud, security risks come in two flavors: intentional and accidental. While the first category makes for dramatic headlines, it is the second that is the focus of CSPM solutions. These tools provide discovery and visibility into cloud assets as well as security configurations. Cloud resources and details including misconfigurations, metadata, change activity and compliance are discovered automatically as soon as the tool is deployed.

CSPM tools compare application configurations to various benchmarks to identify and fix deviations in real time. Open ports, unauthorized changes and other issues can be resolved quickly via guardrails and guided and automated remediation. All of these capabilities provide essential protection against cloud security threats. However, though effective, these defenses are only part of the cloud security puzzle.

CSPM solutions take a moment-in-time approach to security. A CSPM tool can tell administrators details such as whether they have failed to implement encryption for sensitive data or have not implemented multifactor authentication (MFA) for privileged accounts. But while these tools can continuously check for compliance violations and security risks, they do not provide the uninterrupted protection against runtime threats that you need to secure your environment. On their own, CSPM tools provide valuable insights into cloud infrastructure but are limited when it comes to protecting workloads when they are most vulnerable: during runtime.

Why You Need Runtime Protection

As cloud adoption has increased, it has done so in tandem with DevOps and a growing acknowledgment of the need to shift security left in the application development lifecycle. Weaving security deeper into the development process has enabled organizations to deliver applications faster and more securely. However, regardless of the security measures implemented in the build environment, there remains a risk of attackers circumventing those security measures due to errors or zero-day vulnerabilities. Even if an image is verified, it can be compromised, making image scanning alone insufficient.

Fixing vulnerabilities takes time, and the dynamic nature of the cloud and the sheer size of the attack surface make closing these holes challenging. The combination of tactics, such as password spraying and zero-day attacks such as the recent assault on the Log4j vulnerability, demonstrates the precariousness of not addressing runtime security. Without continuous threat detection, analysis and prevention, attacks launched at production environments will slip under the radar.

Say Hello to Cloud Workload Protection

Organizations need effective runtime protection that uses comprehensive visibility into workload events to protect containers and the hosts they run on. Enter cloud workload protection (CWP) tools. These solutions provide an additional layer of security for cloud environments against attackers by

blocking exploitable vulnerabilities based on indicators of attacks (IOAs). The IOAs enable proactive protection and, combined with the ability to continuously identify new vulnerabilities at runtime, provide comprehensive protection for cloud workloads when they are most vulnerable.

True runtime protection requires knowing when attacker-influenced code begins to run. To do so requires key runtime protection capabilities including:

- Ability to detect and prevent zero-day threats in K8 (e.g., cr8escape), as well as workloads in production
- Image and registry scanning prior to being pushed to production
- Visibility into running applications, active processes, system or network calls as well as listing and monitoring all active ports ingoing and outgoing
- Visibility into host incidents, including cryptominers, malware downloaded, suspicious executable and linkable format (ELF) headers, and more

These capabilities can be bolstered by threat intelligence that can be fed into both the CSPM and CWP tools to more effectively detect misconfigurations and attacks. The more the capabilities of your CSPM and CWP tools can be married to improve security, the better. Still, many solutions for protecting workloads will fall short if the solution slows down DevOps teams in any way. Failing to integrate into the continuous integration/continuous delivery (CI/CD) workflows undermines the ability of developers to move quickly, which could lead to increased pressure to meet deadlines and ultimately, increased mistakes as corners are cut.

Doing cloud security right requires limiting its impact on performance while delivering the level of visibility, analysis, blocking and remediation capabilities organizations need.

Building a Better Defense

There are several key building blocks for a robust cloud security defense.

- Runtime protection for cloud workloads: Preventing attacks takes more than pre-runtime security measures such as basic vulnerability scanning. It also takes continuous monitoring and the ability to block attacks based on indicators of compromise and most importantly indicators of attack that are unique to cloud workloads.
- Endpoint detection and response (EDR) for the cloud: EDR for cloud capabilities enable threat hunting and forensic investigation and allow organizations to distinguish activity within a container from activity on a host.
- Performance: A layered approach to cloud security adds protection with minimal to no impact on performance and brings no added complexity.
- Threat hunting: Armed with up-to-date threat intelligence, an effective cloud defense can respond to changes in the threat landscape and incorporate that information into defenses. That includes information about zero-day attacks and vulnerabilities.

Just as IT security generally is thought of in terms of defense-in-depth, so should the cloud. Protecting your cloud assets requires covering the entire cloud-native stack, from virtual machines to containers to the app development pipeline. Static defenses are not sufficient in a dynamic environment. To truly safeguard your workloads, comprehensive runtime security must be a prominent element of your defense.

CrowdStrike stops cloud breaches by providing a unified approach to cloud security delivered through a single, powerful platform. Falcon Cloud Workload Protection delivers deep visibility through the Falcon sensor and enhanced security across the entire cloud-native stack, including all workloads, containers and Kubernetes applications, while Falcon Horizon Cloud Security Posture Management extends the powerful, agentless cloud-native protection of Falcon Horizon to cover all three major cloud providers: Google, AWS and Azure.

Additional Resources

- Learn how you can stop cloud breaches with CrowdStrike unified cloud security posture management and breach prevention for multi-cloud and hybrid environments —— all in one lightweight platform.
- Learn more about how Falcon Cloud Workload Protection enables organizations to build, run and secure cloud-native applications with speed and confidence.
- See if a managed solution is right for you. Find out about Falcon Cloud Workload Protection Complete: Managed Detection and Response for Cloud Workloads.

- Tweet
- Share

Related Content