ESG SHOWCASE

Unifying Cloud-native Security with Check Point CloudGuard

Date: August 2020 **Author:** Doug Cahill, Senior Analyst

ABSTRACT: The use of public cloud services and cloud-native technologies is not only expanding, but is becoming more strategic with cloud-native applications, especially when serving business-critical functions. The sheer velocity at which cloud services are being adopted, often outside of the purview of IT and cybersecurity teams, is challenging all aspects of traditional cybersecurity programs. In response, many organizations have defaulted to a siloed approach, one in which different teams use different controls to secure different environments. As businesses mature their cloud security program, they will need to converge their teams and employ purposeful security controls that enable an automated and unified approach to securing their cloud footprint. Check Point CloudGuard provides coverage across the heterogenous elements of today's hybrid, multi-cloud environments, providing visibility into cloud assets, as well as a unified platform to automate cloud security best practices and investigative controls to bring cloud security into the SOC.

Cloud Heterogeneity Drives Complexity

It is no surprise that nearly two-thirds of participants in a recent ESG study stated that IT is more complicated than it was two years ago, with nearly a third (31%) citing the changing cybersecurity landscape as a cause of increased complexity, and more than a quarter (26%) identifying the need to use both on-premises data centers and public cloud providers as a cause.[1] Hybrid, multi-clouds are just one dimension of the heterogenous nature of such environments, including disparate infrastructures and disparate technologies.

With the exception of cloud-native companies who have already digitally transformed or are born in the cloud, most enterprises' journey to the cloud includes retaining some infrastructure on-premises while consuming infrastructure-as-a-service (IaaS) from multiple providers. There is a clear trend to public cloud as more production server workloads are shifting to public cloud IaaS platforms. In fact, the percentage of organizations that have 50% or more of their production workloads running in a public cloud today will triple from 10% to 30% over the next 24 months.[2] Because server workloads are deployed in multiple public clouds, the most often cited challenge securing cloud-native applications is maintaining consistency across the environments in which cloud-native applications are deployed.

Because server workloads are deployed in multiple public clouds, the biggest challenge securing cloud-native applications is maintaining consistency across the environments in which cloud-native applications are deployed.

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019. All ESG research references and charts in this white paper have been taken from the master survey results set, unless otherwise noted.

Spotlight: Serverless Functions Join the Mix of Server Workload Types

If we think of the environments in which cloud-native applications are deployed as a horizontal dimension driving complexity, there is also a vertical dimension: the heterogenous mix of server workload types that comprise cloud-native applications. While many project teams are now employing applications containers as part of their cloud-native stack, software developers are increasingly leveraging functions-as-a-service (FaaS) to expedite software development. In fact, over a third (35%) of the respondents in a recent study conducted by ESG shared they are using serverless functions extensively. The abstracted nature of serverless functions means project teams need to revisit the associated threat model and employ purposeful controls to secure the full continuous integration and continuous delivery (CI/CD) lifecycle—from development, through to a cloud-native production environment.

Workload Configurations Is the Top Visibility Gap

This level of abstraction is compounding security concerns around a common refrain in cloud security: a visibility gap rooted in a lack of physical access to the infrastructure hosting cloud-native applications. Identifying workload configurations that are out of compliance with industry best practices and frameworks is the top area in which organizations need to improve visibility into their public cloud-hosted assets. Our research respondents also shared they need an audit trail of system activity and the use of privileged user accounts including, importantly, those used to execute serverless functions.

The abstracted nature of serverless functions means project teams need to revisit the associated threat model and employ purposeful controls to secure the full cloud-native environment.

Multiple Controls Contribute to Complexity

The perennial cybersecurity issues of a shortage of skills and proliferation of tools has been exacerbated by the adoption of IaaS services, application containers, and, now, serverless functions. Because of the differences in the composition of cloud-native applications and the infrastructure environments that host them, many organizations initially employ different policies and controls. Such a siloed modality in which multiple cybersecurity controls are used has increased cost and complexity, a sentiment shared by 35% of organizations that identify this as a top challenge in securing cloud-native applications.

The Requirements for a Unified, Automated Approach to Cloud Security

Location Agnostic

The deployment plans for applications containers highlights the need for cloud-native security solutions to be location agnostic by supporting hybrid, multi-cloud environments. ESG research highlights this requirement per the projected doubling of organizations that deploy their container-based applications across a combination of public cloud platforms and private data centers from 23% today to 46% in the future. Portability is, after all, a core value proposition of modern applications built on containers and serverless functions-as-a-service (FaaS).

Secure the Build-time to Runtime Lifecyle

A central feature of cloud-native applications and the associated use of cloud services is change—change via elasticity to dynamically allocate resources, and change via the continuous integration and continuous delivery (CI/CD) processes that automate builds and deployments. Security controls designed to protect the use of cloud services will do so across the lifecycle of the application from pre-deployment stages starting with a “shift-left” approach that hardens cloud services

and server workloads by identifying and remediating both software and configuration vulnerabilities through to production environments. In production, they must be secured via anti-threat detection and prevention measures while also capturing system activity for incident response investigations and proactive threat hunting use cases.

DevSecOps Automation via CI/CD Integration

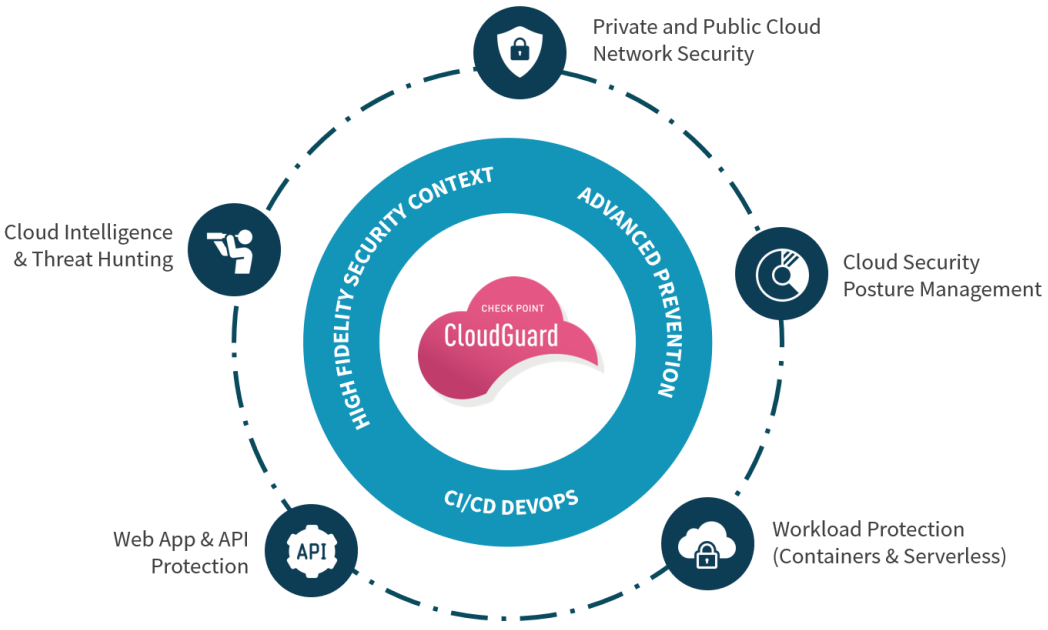
Securing the application lifecycle from build-time to runtime requires integration with the processes and tools already employed to automate the CI/CD of new code to production. Such secure DevOps practices (DevSecOps) are being adopted, with 36% of organizations doing so extensively while others are expanding or planning a secure DevOps program. DevSecOps use cases span the application lifecycle:

- Pre-deployment: Automated software and configuration vulnerability scans via integration with source code repositories that store source code and infrastructure-as-code (IaC) templates and build tools so such checks happen upon commit or as part of a build.
- Runtime: Integration with orchestration tools that push new code to production automates that application of controls with policies based on metadata such as tags that denote the role of server workloads.
- Workflow: Integration with the DevOps equivalent of IT service management (ITSM) streamlines workflows by automatically opening and assigning a ticket when, for example, a build fails or a runtime anomaly is detected.

Securing with Cloud-native Lifecycle with Check Point CloudGuard

The functional capabilities of Check Point's CloudGuard platform meet the aforementioned requirements to secure dynamic cloud-native applications deployed across multi-cloud environments. The solution converges cloud security posture management (CSPM) and cloud workload protection (CWP) capabilities with integrated controls including network security, web and API security, and threat hunting (see Figure 1).

Figure 1. Check Point CloudGuard Cloud Security Platform



Source: Enterprise Strategy Group

Discovery for Visibility

To address the cloud security visibility gap, CloudGuard discovers an organization's collection of cloud assets to provide a consolidated view of the footprint. The product's dashboard visualizes a centralized view of an organization's cloud footprint inclusive of providers, accounts, virtual private clouds (VPCs), security groups, and service assets with alerts organized accordingly and prioritized based on severity.

Posture Management for Hardened Configurations

CloudGuard cloud security posture management automates governance across assets and services including the visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks. CloudGuard's integrated asset management module shows a relationship mapping of workloads and services via a topological rendering that allows for quickly identifying misconfigured cloud services such as externally facing server workloads. This allows projects teams to gain an understanding of what other cloud assets are at risk due to such misconfigurations, the first step toward remediation.

To apply best practices for the secure configuration of cloud services, including those prescribed by CSPs, the Center for Internet Security (CIS), and others based on industry regulations; CloudGuard includes out-of-the-box rule sets. These rules can be applied to test the current configurations for an assessment of severity or to automatically remediate misconfigured services. The product also allows for the creation of custom rule sets via the Governance Specification Language (GSL).

Rule sets can also be employed pre-deployment via integration with CI/CD controls such as repositories and build tools so that configuration issues can be discovered and corrected before deployment to production. The pre-deployment capabilities of CloudGuard also leverage these rules to scan registry-resident container images for vulnerabilities, assuring only hardened containers are then built and pushed to production.

Anomaly-based Runtime Threat Prevention to Secure Serverless Functions

The theme of least privilege extends into the ability to discover over-privileged serverless functions, often the biproduct of the use of the wildcard operator that grants a given function excessive privileges when, for example, it may only need the ability to perform database inserts.

CloudGuard helps organizations understand and secure their use of serverless functions from development through runtime. CloudGuard provides a contextual inventory of function calls by region. A visual mapping of the relationship of a function call to the upstream triggering event(s) and the downstream affected service(s) enables a least privilege approach of scoping to just those events that should invoke a call and those services that function then instruments. The theme of least privilege extends into the ability to discover over-privileged serverless functions, often the biproduct of the use of the wildcard operator that grants a given function excessive privileges when, for example, it may only need the ability to perform database inserts.

With function call now properly scoped, CloudGuard employs an anomaly-based approach to detect activity that could be indicative of a compromise. By monitoring steady state activity, the product establishes a normalized baseline of activity from which non-standard behavior is flagged as potentially malicious. The product can be configured to block such runtime behavior and to generate an alert.

Integrated Web Application and API Protection (WAAP)

CloudGuard's runtime threat prevention capabilities include protecting an organization's web applications and use of APIs against a range of known and zero-day threats. The WAAP component automizes the protection of web applications by leveraging a combination of behavioral analysis and machine learning. By continuously learning an application's normal behavior, CloudGuard creates an in-depth understanding of what constitutes steady state as the basis to detect and prevent threats. Runtime behavior then automatically adapts, providing an alternative approach to rule-based traditional web application firewalls (WAF).

By continuously learning an application's normal behavior, CloudGuard creates an in-depth understanding of what constitutes steady state as the basis to detect and prevent threats.

The use of client-side JavaScript monitors biometric activity such as keystrokes and mouse movements for a broadened picture of normal behavior. CloudGuard employs multiple machine learning engines to both establish a baseline of normal behavior and to generate accurate alerts of anomalous and thus potentially malicious activity. These alerts are contextual and risk-based, allowing security analysts to prioritize triage activity, expediting incident investigations.

Contextualized Events to Expedite Incident Response

CloudGuard also readies security operations center (SOC) teams to respond to cloud incidents via a set of investigatory capabilities. The product's cloud intelligence and threat hunting module puts alerts on anomalous activity into context by visualizing the affected assets so analysts can expedite remediation by quarantining potentially infected systems while continuing their investigation. CloudGuard provides additional context by correlating events from AWS VPC Flow Logs and AWS CloudTrail to identify, for example, outbound traffic to a known bad IP address that could be a command and control server or outbound traffic to a Tor exit node that could be indicative of data being exfiltrated. Organizations can also query CloudGuard for both incident response and threat hunting purposes.

The Bigger Truth

The now critical nature of how businesses rely on cloud services has made cloud security a strategic imperative. Not only to catch up to the degree to which lines of business are leveraging the cloud, but also to keep pace with expanded use, organizations are now retooling their cloud security programs by unifying their teams to assure consistency of policy and process across the disparate infrastructures of today's hybrid, multi-cloud environments. To do so, purposeful controls are required to unify cloud security measures by converging the functional capabilities of cloud security posture management (CSPM), cloud workload protection (CWP), and web application and API Protection (WAAP) into a single solution. Check Point's CloudGuard cloud security platform allows organizations to meet these objectives with an offering that integrates configuration management, runtime threat prevention, threat-hunting and intelligence capabilities, and more from build-time to production.