Optimal security of cloud-native applications requires an integrated approach that starts in development and extends to runtime protection. SRM leaders should evaluate emerging cloud-native application protection platforms that provide a complete life cycle approach for security.
Overview

Key Findings

- Cloud-native applications arise from the combination of microservices applications (typically using Linux containers), built using rapid DevOps-style development and automatically deployed onto programmatic cloud infrastructure.

- The unique characteristics of cloud-native applications makes them impossible to secure without a complex set of overlapping tools spanning development and production including:
  - Infrastructure as code (IaC) scanning
  - Container scanning
  - Cloud workload protection platforms (CWPPs)
  - Cloud infrastructure entitlement management (CIEM)
  - Cloud security posture management (CSPM)

- Cloud-native applications are typically built from containers and serverless platform as a service (PaaS), but most communicate with virtual machine (VM)-based workloads and on-premises data centers, complicating protection strategies.

- Understanding and addressing the real risk of cloud-native applications requires advanced analytics combining siloed views of application risk, open-source component risk, cloud infrastructure risk and runtime workload risk.

- There is a shift in focus in leading-edge security organizations from protecting infrastructure to protecting workloads and the applications that run on these workloads.

Recommendations

As a security and risk management (SRM) leader responsible for infrastructure security, you should:

- Implement an integrated security approach that covers the entire life cycle of cloud-native applications, starting in development and extending into production.
Introduction

Every business is a digital business and boards of directors indicate their digital business initiatives have accelerated as a result of COVID-19.¹ To support these initiatives, developers have embraced cloud-native application development, typically combining microservices-based architectures built using containers, assembled in DevOps-style development pipelines, deployed into programmatic cloud infrastructure and orchestrated at runtime using Kubernetes and maintained with an immutable infrastructure mindset.² This shift creates significant challenges in securing these applications.

Security testing needs to be integrated as seamlessly as possible into the DevOps-style development and deployment of cloud-native applications. We refer to this as DevSecOps (see 12 Things to Get Right for Successful DevSecOps and Integrating Security Into the DevSecOps Toolchain). In a recent Gartner survey, 44% of the participating organizations indicated they have already implemented a DevSecOps pipeline to secure cloud-native apps, with most of these in limited deployment.³ These organizations have manually stitched together DevSecOps with 10 or more disparate security tools – some old and some new – each with siloed responsibility and view of application risk.³

- In development, static application security testing (SAST), API security testing, dynamic application security testing (DAST), IaC scanning and threat modeling were identified as the five most commonly used tools to secure cloud-native applications.
- In production, web application firewalls (WAF)/web application and API protection (WAAP), application security monitoring, DAST, CWPP and CSPM were identified as the five most commonly used tools to secure cloud-native applications.
In the same Gartner survey, the most commonly cited method of integrating different security tools to streamline DevSecOps was manual integration. There is a more convenient and effective way to approach cloud-native application security.

Securing cloud-native applications offers enterprises the opportunity to redesign security approaches. Rather than treat development and runtime as separate problems — secured and scanned with a collection of separate tools — enterprises should treat security and compliance as a continuum across development and operations, and seek to consolidate tools where possible (see Figure 1).

**Figure 1. Cloud-Native Application Protection Platform Scope**

To successfully implement cloud-native application security, enterprises should use an integrated platform approach — in Gartner research referred to as cloud-native application protection platforms (CNAPPs) (alternatively, some vendors offering capabilities in this emerging market refer to this as a “cloud-native security platform”).

**Description**

CNAPPs are an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production. CNAPPs consolidate a large number of previously siloed capabilities, including:

- Development artifact scanning, including containers
- Cloud security posture management
Benefits and Uses

The most significant benefit of a CNAPP approach is better visibility and control of cloud-native application risk. Attempts to identify and remediate application risk have been fragmented across multiple toolsets spanning development and runtime. For example, for known vulnerabilities, a vulnerability score — such as the common vulnerability scoring system (CVSS) — is a measurement of risk, but it represents only one aspect of overall application risk (see Note 1). Yet, a vulnerability score is the most commonly cited metric used by enterprises to measure the risk of a vulnerability in application code or software components. Enterprise security teams and DevSecOps architects need an integrated way of understanding and addressing application risk that spans: Open-source software (OSS), custom code, container contents, cloud infrastructure configuration and runtime protection (see Figure 2).

Figure 2. Detailed CNAPP Capabilities

**Detailed CNAPP Capabilities**

<table>
<thead>
<tr>
<th>Artifact Scanning</th>
<th>Security</th>
<th>Runtime Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SAST/DAST</td>
<td></td>
<td>• Web Application and API Protection</td>
</tr>
<tr>
<td>• API Scanning</td>
<td></td>
<td>• Application Monitoring</td>
</tr>
<tr>
<td>• Software Composition Analysis</td>
<td></td>
<td>• Cloud Workload Protection Platform</td>
</tr>
<tr>
<td>• Exposure Scanning</td>
<td></td>
<td>• Network Segmentation</td>
</tr>
<tr>
<td>– CVEs</td>
<td></td>
<td>• Exposure Scanning</td>
</tr>
<tr>
<td>– Secrets</td>
<td></td>
<td>– CVEs</td>
</tr>
<tr>
<td>– Sensitive Data</td>
<td></td>
<td>– Secrets</td>
</tr>
<tr>
<td>– Malware</td>
<td></td>
<td>– Sensitive Data</td>
</tr>
<tr>
<td>– Attack Path Analysis</td>
<td></td>
<td>– Malware</td>
</tr>
</tbody>
</table>

Cloud Configuration

• Infrastructure as Code Scanning
• Network Configuration and Security Policy
• Cloud Infrastructure Entitlements Management
• Kubernetes Security Posture Management
• Cloud Security Posture Management

Source: Gartner
342808_01
By integrating vulnerabilities, context and relationships across the development life cycle, excessive risk can be surfaced, enabling development teams and product owners to focus on remediating the areas of the application that represent the most risk.

Other benefits of CNAPP adoption includes its ability to:

- Reduce the chance of misconfiguration, mistakes or mismanagement as cloud-native applications are rapidly developed, released into production and iterated.
- Reduce the number of tools and vendors involved in the CI/CD pipeline.
- Reduce the complexity and costs associated with creating secure and compliant cloud-native applications.
- Allow developers to accept security-scanning capabilities that seamlessly integrate into their development pipelines and tooling.
- Allow security departments to place an emphasis on scanning cloud-native applications for risk proactively in development and rely less on runtime protection. This strategy is well-suited for container-as-a-service and serverless function environments and enterprises that have adopted an immutable infrastructure mindset.
- Allow security departments to understand attack path analysis based on relationships — identities, permissions, networking and infrastructure configuration that would enable an attacker to target an application.
- Bidirectionally link development and operations visibility and insight into risk analysis to improve the overall enterprise security posture (see Figure 3)
SRM leaders interested in securing cloud-native applications face many risks, including:

- Enterprise security and development teams lack the right skills. In a recent Gartner survey, the highest rated challenge when securing cloud-native applications in a DevSecOps pipeline was a lack of internal knowledge about security. 3

- Organizational immaturity, in terms of cloud-native application development, may inhibit adoption.

- Incumbent security protection vendors used by an enterprise (e.g., CWPP, WAF and WAAP vendors) aren't necessarily good at integrating into development and often don't understand the needs of modern DevOps style development pipelines or developers, hampering adoption.
Developers won't accept cumbersome intrusion into the development/deployment process, nor will they accept security tooling that wastes their time with false positives or low-risk findings.

Developers may have adopted OSS tools that achieve some of the desired outcomes of CNAPP but not all, creating visibility and control gaps the security team is unaware of.

Cloud-native application security strategies may fail to address all types of development artifacts (see Note 2) within the project scope, creating visibility and control gaps.

Organizations may have siloed purchases of application security testing tooling, often caused when chosen by a different team than the team that manages the runtime protection of workloads. Unclear boundaries between application and infrastructure was the third highest challenge to successfully secure cloud-native applications cited in a recent Gartner survey. The increasing overlap is driven by cloud-native application developers (see Figure 4).

**Figure 4. Blurring Boundaries of Responsibilities**

<table>
<thead>
<tr>
<th>Traditional Developer Responsibility</th>
<th>Cloud Native Developer Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Workloads</td>
</tr>
<tr>
<td>• Custom code</td>
<td>• Containers</td>
</tr>
<tr>
<td>• APIs</td>
<td>• Serverless functions</td>
</tr>
<tr>
<td>• OSS components</td>
<td>• Virtual Machines</td>
</tr>
<tr>
<td>• Infrastructure as code scripts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Infrastructures</td>
</tr>
<tr>
<td>• Platform as a Service</td>
<td>• Networking</td>
</tr>
<tr>
<td>• Networking</td>
<td>• Storage</td>
</tr>
<tr>
<td>• Storage</td>
<td>• Compute</td>
</tr>
<tr>
<td>• Compute</td>
<td>• Identities and Permissions</td>
</tr>
</tbody>
</table>

Source: Gartner

3 The increasing overlap is driven by cloud-native application developers (see Figure 4).
CSPM vendors have been slow to add IaC scanning capabilities that enterprises need. Without this, full integration into development can't be accomplished.

Information security isn't always involved in the buying decision. New buying centers are emerging outside of traditional information security including DevOps architects, DevSecOps architects and cloud security architects, application development and cloud engineering. In a recent survey, budget owners for cloud-native application security tools were fragmented and, although information security was the most commonly cited budget owner, it was only selected by 32% of respondents.

There is increasing overlap with development tools and artifact repository platforms providing integrated security capabilities (e.g., Gitlab, Github). So there is a risk in duplication of efforts or licensing, and developers may simply prefer to use what their favorite platform has built-in.

Kubernetes is a cloud platform of its own, and its correct and compliant configuration is often overlooked or considered outside of the scope of CNAPP.

Alternatives

As an alternative to an integrated CNAPP offering adoption, enterprises could:

- Use separate CWPP, CSPM, and container scanning solutions and integrate these into the development pipeline using APIs. Integrating results and identifying risks would require the organization to build their own solution or introduce yet another vendor to consolidate risk visibility.
- Use the integrated security capabilities of modern cloud platforms. All major cloud platform providers offer some degree of integrated security capabilities. However, cloud-provider specific solutions don’t address the needs of hybrid multicloud deployments.
- Adopt emerging service mesh alternatives to address at least some of the runtime security protection requirements of cloud-native applications. However, the market for service mesh is highly fragmented (see Emerging Technologies: Service Mesh is Being Pushed by Containers and Key Open-Source Projects), and service mesh offerings only address a portion of application security requirements (namely service discovery, service identity, network encryption and certificate rotation).
Recommendations

SRM leaders responsible for the security of cloud workloads and applications should:

- Pursue strategies that use minimal runtime in-workload protection. Containers and serverless functions are the primary building blocks of cloud-native applications and are becoming increasingly granular with shorter life cycles, requiring less in terms of workload runtime protection. At the application layer, enterprises will use application-layer in-line runtime protection in the form of web application firewalling, API protection and anti-bot protection. Gartner survey results show that web application firewalling and web application API protection suites are the mostly commonly used tools in production to secure cloud-native applications.  

- Develop an overall strategy for cloud-native app protection that spans development and runtime.

- Evaluate emerging CNAPP offerings as contracts for CSPM and CWPP expire, and use this opportunity to reduce complexity and consolidate vendors.

- Sign one to two year contracts only, because the market for CNAPP is still evolving.

- Require CNAPP vendors to charge for licenses-based modules you use, as it may take several years to adopt the entire integrated set of capabilities.

- Scan all cloud-native development artifacts for vulnerabilities and compliance: source code, containers, VM images, IaC scripts, API declarations and cloud configuration files.

- Require CWPP vendors to scan containers in development and add CSPM capabilities, including IaC scanning.

- Require CSPM vendors to add scanning of Kubernetes security posture (KSPM) and IaC scanning in development, as well as runtime assessment using APIs.

- Evaluate the opportunity to consolidate OSS vulnerability scanning, license scanning and software composition analysis from a unified CNAPP offering.

- Scan development artifacts proactively in development for all types of vulnerabilities, not just vulnerable components — but also including hard-coded secrets and malware.
Representative Providers

Example vendors listed offer a combination of development scanning, cloud infrastructure scanning, and runtime visibility/control specifically designed to address the security requirements of cloud-native applications. Since this is an emerging market, not all vendors have fully featured capabilities across all areas:

- Accurics
- Aqua Security
- Data Theorem
- DoSec XIAOYOU TECH (China)
- JFrog
- Lacework
- McAfee
- Orca
- Palo Alto Networks
- Qualys
- SafeDog (China)
- Snyk
- Sonatype (integration of NeuVector)
- Sonrai Security
- Sysdig
- Trend Micro
- Wiz

In addition, these cloud-native application platform vendors provide CNAPP capabilities integrated within their platform typically at extra cost:

- Google Anthos
Evidence

1 The 2021 Gartner View From the Board of Directors Survey found that boards of directors are prioritizing digital technology initiatives as a response to the COVID-19 pandemic. When asked to indicate what kind of impact COVID-19 had on their digital business initiatives, the most frequently selected impact was an acceleration of digital business initiatives, with 69% of survey respondents selecting this (n = 260; see Survey Analysis: Board Directors Say Pandemic Drives Increased Investments in IT).

2 Building Sustainable Ecosystems for Cloud-Native Software, The Cloud Native Computing Foundation (CNCF)

3 Gartner's Enabling Cloud-Native DevSecOps survey was conducted online from May 12th to May 21st, 2021, to identify the emerging governing structures, security owners, technologies used and the current challenges in the DevSecOps pipeline to secure cloud-native applications.

In total, 85 IT and business leaders with involvement in DevSecOps initiatives participated in the survey. Eighty-two were from Gartner's IT and Business Leaders Research Circle — a Gartner-managed panel — and three were from an external sample. Participants from North America (44%), EMEA (35%), Asia/Pacific (8%) and Latin America (13%) responded to the survey.

The survey was developed collaboratively by a team of Gartner analysts and was reviewed, tested, and administered by Gartner's Research Data and Analytics team.

Note: The results of this study are representative of the respondent base and not necessarily of the market as a whole.
Note 1. Vulnerabilities Alone Don’t Capture Overall Application Risk

The true overall risk of an application requires assessment and correlation of a broad set of information. For example, even if a component is vulnerable, the component may not be used in production and therefore represents no risk. Or, the application may not be externally accessible, reducing the risk. For cloud-native applications, an overall view of application risk is more complicated than this. An otherwise secure application may be left vulnerable through infrastructure misconfiguration. For example, a cloud networking path left open or its storage left exposed to the public internet.

Note 2. Development Artifacts That Should Be Scanned for Vulnerabilities, Misconfiguration, Malware and Secrets

The following artifacts should be scanned to ensure they are secure, configured correctly and free from malware or sensitive information:

- OSS modules and frameworks
- Containers
- Serverless functions
- APIs and declarative API schemas
- Custom application code
- Infrastructure as code
- YAML Ain’t Markup Language (YAML) and other cloud configuration files
- VM images

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

- Market Guide for Cloud Workload Protection Platforms
- How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB
- Market Guide for Software Composition Analysis
- 12 Things to Get Right for Successful DevSecOps
Integrating Security Into the DevSecOps Toolchain

How to Make Cloud More Secure Than Your Own Data Center

Innovation Insight for Cloud Security Posture Management

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. It consists of the opinions of Gartner’s research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see “Guiding Principles on Independence and Objectivity.”