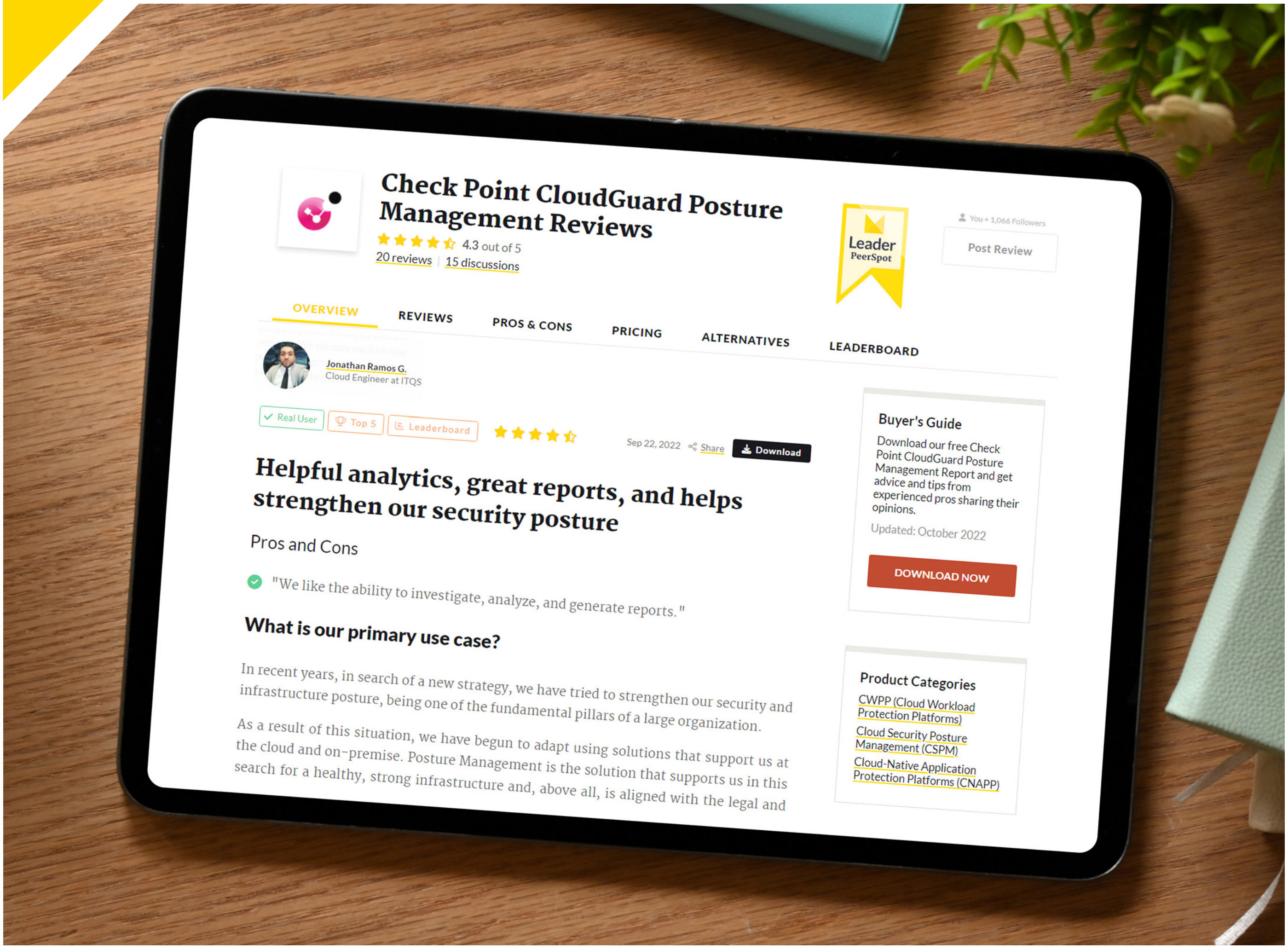
PeerPaper™ Report 2022

Based on real user reviews of Check Point CloudGuard

Eight Key Success Factors for Cloud-Native Application Protection (CNAPP)


Check Point CloudGuard Posture Management Reviews

★★★★☆ 4.3 out of 5

20 reviews | 15 discussions

Jonathan Ramos G.
Cloud Engineer at ITQS

Helpful analytics, great reports, and helps strengthen our security posture

Pros and Cons

"We like the ability to investigate, analyze, and generate reports."

What is our primary use case?

In recent years, in search of a new strategy, we have tried to strengthen our security and infrastructure posture, being one of the fundamental pillars of a large organization.

As a result of this situation, we have begun to adapt using solutions that support us at the cloud and on-premise. Posture Management is the solution that supports us in this search for a healthy, strong infrastructure and, above all, is aligned with the legal and

Buyer's Guide

Download our free Check Point CloudGuard Posture Management Report and get advice and tips from experienced pros sharing their opinions.

Updated: October 2022

Product Categories

CWPP (Cloud Workload Protection Platforms)

Cloud Security Posture Management (CSPM)

Cloud-Native Application Protection Platforms (CNAPP)

PeerSpot

Contents

Introduction

Cloud-native applications can be difficult to defend. First, the cloud infrastructure is subject to a two-tier or “shared responsibility” security model that requires the client, rather than the cloud provider, to secure the application. Second, cloud app development and deployment processes are happening off-premises, away from established security policy controls. They may be developed in a sandbox environment, for instance. If the development environment has cloud access, apps may be deployed right into the cloud without security review. If development occurs outside of security guardrails, vulnerabilities such as misconfigurations can arise, exposing organizations to security risks and actual incidents.

To mitigate the resulting risks and secure the application layer, many organizations have considered a Cloud-Native Application Platform (CNAPP). Gartner defines CNAPP platforms as “an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production.” CNAPPs consolidate previously siloed capabilities like container scanning and cloud security posture management.

CNAPP Definition

Advisory Information Security Analyst at a financial services firm with 501-1,000 employees

★★★★★

> “We don’t have to spend all day maintaining cloud environments. They take care of that for us.”

Read review »

This paper features insights into the key success factors for CNAPP, garnered from reviews by real users of Check Point CloudGuard on the PeerSpot peer review site. With CloudGuard, PeerSpot members can take advantage of the platform’s capabilities for cloud security posture management, workload protection, threat intelligence, AppSec, and developer-first security.

According to CloudGuard users, a key factor for success with CNAPP comes from having the ability to automatically manage security on multiple clouds across the development lifecycle. Automation is crucial, as are visualization and reporting. The ability to manage access control is also important. When these functions are present in a CNAPP solution, stakeholders gain efficiency along with capabilities for risk management and compliance.

IT Professionals Quoted in This Paper

This paper draws on experiences from 12 CloudGuard users:

- Senior Manager at a financial services firm with over 10,000 employees
- Advisory Information Security Analyst at a financial services firm with more than 500 employees
- Senior Security Engineer at an insurance company with over 10,000 employees
- Senior Manager at a financial services firm with over 10,000 employees
- Senior Network/Security Engineer at Skywind Group, a software company with more than 500 employees
- Network Engineer at L&T Technology Services, a tech company with over 10,000 employees
- Product Manager at a tech services company with more than 50 employees
- Senior Manager of IT Security at a financial services firm with over 10,000 employees
- Cloud Support Leader at a tech company with more than 50 employees
- IT Security Engineer at ProsourceIT, a financial services firm with over 1,000 employees
- Senior Consultant at a small tech services company
- Network Security Engineer/Architect at a tech services company with over 1,000 employees

An Overview of CNAPP Challenges

Security teams often struggle to protect cloud-native apps for two primary reasons. First, these apps are usually constructed using more diverse and distributed elements than their traditional, on-premises peers. A cloud-native app might consist of a collection of microservices and code components that call on Application Programming Interfaces (APIs) residing in third party entities. This kind of application architecture, with multiple dependencies on third-party components, is harder to protect than a monolithic code base that sits in a single, walled-off domain.

The other reason cloud-native apps are hard to protect has to do with access and control. By definition, a cloud-native app is not hosted on the app owner's infrastructure. It is subject to the public cloud's standard two-tier or "shared security" model. The cloud platform provider secures the network and underlying infrastructure. The app owner is responsible for securing everything else.

However, the app owner may not always have a good sense of who is accessing the app, either legitimately or maliciously. In addition, the app often operates outside of existing policy monitoring tools. Well-intentioned IT personnel or developers who are not always aware of potential threats might accidentally expose the app to risk without realizing it.

Shared Responsibility

Eight Key Success Factors for CNAPP

Keeping these challenges in mind, it is important that a solution for CNAPP should provide multi-cloud capabilities and security across the development lifecycle. Security must be built into the app. As apps deploy, success with CNAPP depends on the breadth of security across all microservices throughout the software development life cycle, automation and access control. CNAPP solutions should provide effective visualization and reporting, resulting in efficient security operations for the cloud and developers—ultimately enabling risk management, compliance, and the remediation of vulnerabilities.

#1 Multi-Cloud Capabilities

Organizations that deploy apps to the cloud are increasingly doing so on multiple cloud platforms. Few IT departments are dealing exclusively with Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP). Most are managing apps on at least two of these platforms. For this reason, multi-cloud security capabilities are a key success factor in CNAPP, especially when provided to the user from an efficient single-pane-of-glass interface.

Multi-Cloud Capabilities

Chris D.
Senior Consultant at a tech services company with 11-50 employees

★★★★½

> "A good tool for a large enterprise operating across multiple cloud environments, like AWS, Azure, or a hybrid infrastructure."
>
> Read review »

A Senior Manager at a financial services firm with over 10,000 employees spoke to this need when he praised Check Point for its ability to centralize visibility for their complete cloud environment, which consisted of workloads hosted on multiple cloud platforms (AWS, Azure, and GCP). He said CloudGuard "provides visibility of organization-complete cloud infrastructure hosted on different cloud platforms such as AWS and Azure. It also provides visibility of different accounts hosted on multiple tenants on a single dashboard."

"I love the work involved in maintaining and scaling security services and configurations across multiple public clouds using this solution, versus using native cloud security controls. It is so much better," said an Advisory Information Security Analyst at a financial services firm with more than 500 employees.

This user discussed how each cloud platform has its own way of handling services and configurations. "Even within their platform, they are in a lot of disparate places, e.g., in AWS, there are five different tools," he added. "You have to jump between them to get the same information that you can just pull in automatically on CloudGuard, which is just one platform."

A Senior Consultant at a small tech services company found that CloudGuard is "a good tool for a large enterprise operating across multiple cloud environments, like AWS, Azure, or a hybrid infrastructure." For him, CloudGuard's posture management offered visibility across the entire cloud infrastructure, to help with management, maintenance, and compliance. He commented, "With visibility across all these cloud platforms, you can protect against compromised credentials or identity theft."

#2 Breadth of Security Across the Development Lifecycle

The rapid growth of cloud computing and the complexity of providing multi-layer security has led to a myriad of niche "point" solutions, which often don't share context between themselves and require even more operational overhead.

Effectively securing cloud applications requires breadth of coverage for all microservices at a granular level, starting in development and continuing across the software lifecycle to app deployment and operation. CNAPP needs to be embedded in the Continuous Integration/Continuous Deployment process (CI/CD) pipeline because it is effectively impossible to stop the pipeline for ad-hoc security checks. With CNAPP in the CI/CD pipeline, vulnerabilities get discovered when they are easiest to be fixed and with lowest cost. In contrast, later disruptions to the releasing process may result in significant delays to the release, which no one wants. As more software projects adopt agile methodologies, this issue is more urgent than ever.

As a Senior Manager of IT Security at a financial services firm with over 10,000 employees mentioned, the value of a solution for securing cloud-native apps comes from the fact that "it helps us to analyze vulnerabilities way before they get installed in production and the web. It gives us more security in the production environment."

Provides Multi-Layer Security

A Network Security Engineer/Architect at a tech services company with over 1,000 employees concurred, noting, "CloudGuard integrates security best practices and compliance regulations into the CI/CD, across cloud providers." Figure 1 shows a simple depiction of this capability. For a Senior Security Engineer at an insurance company with over 10,000 employees, the value came from the solution's ability to integrate security best practices into CI/CD. He also said, "You can set up the automation so that if any group is created outside of CloudGuard, it is reverted. You can also run scheduling functionality to identify anything that is not compliant."

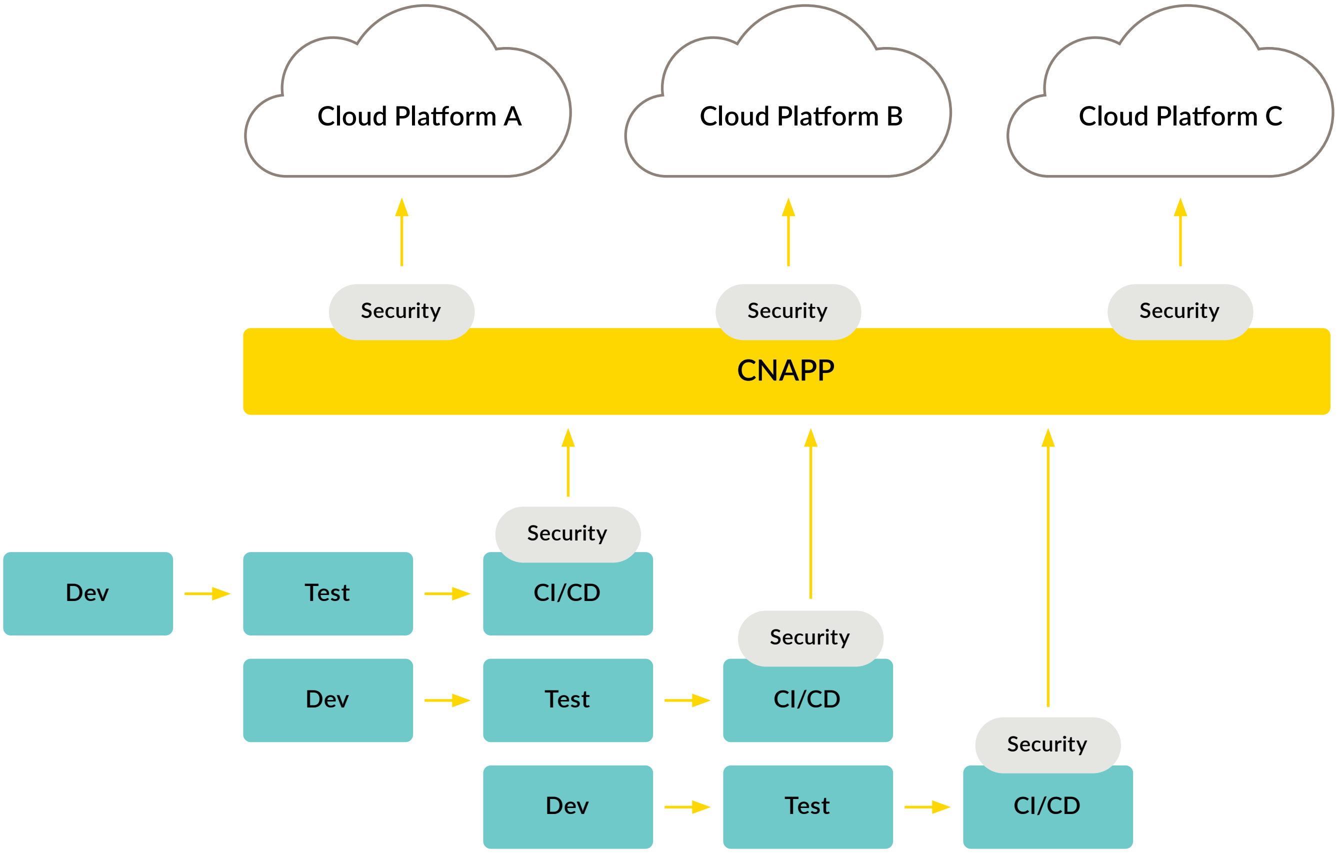


Figure 1 - Integrating security into CI/CD across multiple clouds.

Time Saving

“CloudGuard helps our developers save time by as much as 50 percent,” said the financial services Advisory Information Security Analyst. “It prevents us from having to make them go back and redo their work. They do not even have the option to be out of compliance. It stops them from building machines and non-compliant stuff only to have to go back and redo them later, especially if CloudGuard will shut that down before it even starts.”

The Cloud Support Leader who uses CloudGuard Spectral offered the following insight: “One of the best features is the use of technology to verify if the development has any security problems, generate reports, and shield our application.”

A Cloud Support Leader who uses CloudGuard Spectral at a tech company with over 50 employees was pleased that the developer-first cloud security solution could scan code in different program languages across public repositories. He acknowledged the value of working within the CI/CD code build to ensure the applications were secure when running live in the public cloud environment. He said Spectral “generates great confidence in the environment that can be checked, which has been very useful for the company.” He then added, “It intelligently validates known and unknown threats to provide an excellent layer of security.”

This developer-first approach allowed them to expand their original cloud security strategy to add countermeasures to the development process. Being developer-first means automating security at build time and throughout the overall CI/CD process. The team could also monitor security blind spots in the cloud and uncover vulnerabilities and supply chain gaps.

#3 Automation

Automation is essential for success because securing cloud-native apps is a complex task whose scale makes it unsuitable for a human team. The CI/CD process deploys new cloud assets with agility and high velocity; thousands of short-lived automated microservices are created and deleted daily; the cloud is ephemeral, cloud information is distributed across the environment and constantly moving. There is too much to be done for people to handle it all manually without risk and inefficiency. And, that's assuming a security organization can even find qualified cloud security engineers to perform CNAPP tasks. Automation is necessary because it can execute security tasks accurately while solving the staff shortage problem and reducing the organization's risk.

In this context, a Senior Manager at a financial services firm with over 10,000 employees shared that CloudGuard's task delegation, which enables automation of security process steps, is a valuable aspect of the solution. He also valued the tool's security configuration review along with automatic remediation, saying, "You can do automatic remediation, where you need to define the policy for which unit that you are doing remediation."

The auto-healing of configurations of the security groups and firewall rules are what stood out as valuable to a Senior Network/Security Engineer at Skywind Group, a software company with more than 500 employees. Further to this point, the financial services Advisory Information Security Analyst said, "If I have a user who will try to spin up a network in the cloud that isn't in line with our policies, it will automatically stop that from being able to be created, then delete it. Therefore, it will take action whether or not we are explicitly looking at the platform, keeping it in compliance with the rest of the company at all times."

Advisory Information Security Analyst at a financial services firm with 501-1,000 employees

★★★★★

"A unified security solution across all major public clouds affects our cloud security operations by saving us a ton of time and effort."

Read review »

Automation of Security Processes

Kirtikumar P.
Network Engineer at LTTS

★★★★★

“IAM is a very good and unique feature of CloudGuard. IAM gives us complete control of our cloud environment.”

Read review »

#4 Least Privilege Access Control and IAM

Effective CNAPP depends on being able to track who is accessing cloud assets. There are typically too many people with direct access to a cloud app environment during development. Broad access is convenient for developers, but it is not secure. To avoid risks of malicious activity, the best practice is to adopt a policy of “least privilege” to make sure users have appropriate access rights. This usually means using Identity and Access Management (IAM) controls within a CNAPP solution to provide flexible privilege administration and visibility.

In particular, a CNAPP solution must control administrative (privileged) users, as depicted in Figure 2. As the financial services Senior Manager stated, “IAM role is the feature which is widely used as it provides a granular level of control and visibility of any changes happening within our Cloud network. [An] admin is not allowed to create or add any user or change security policy directly with an admin account, unless the same has been approved via IAM role.”

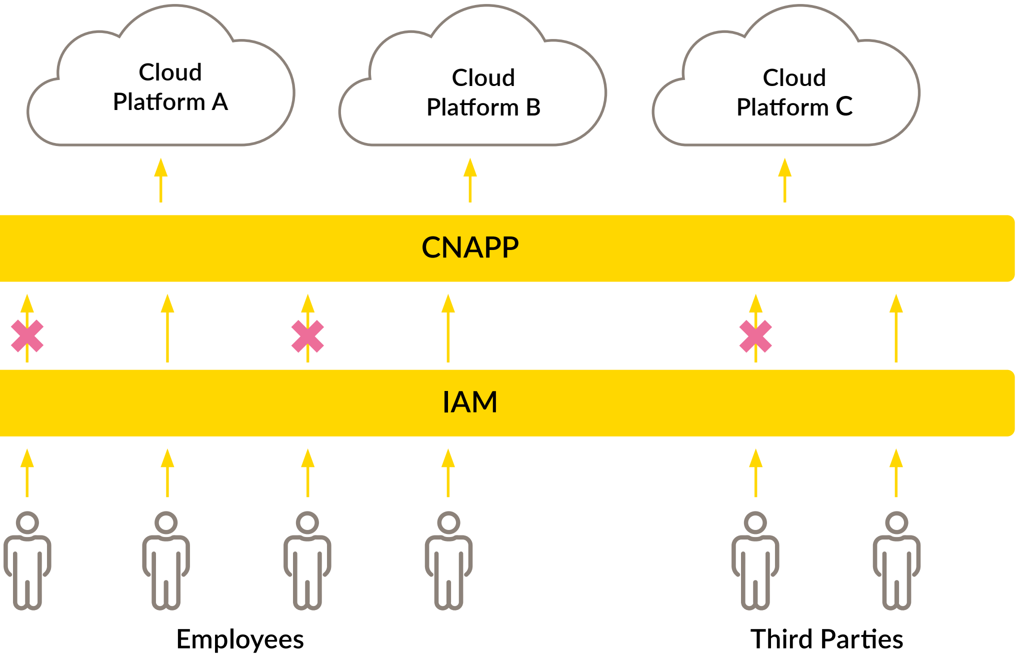


Figure 2 - IAM and the control over administrative access to cloud platforms.

Other notable comments about access control include:

- “In case someone tries to bypass and create a user or policy locally, which is not allowed or defined in CloudGuard, changes will be rolled back and a notification will be sent to the concerned team.” - Senior Manager at a financial services firm with over 10,000 employees
- “IAM is a very good and unique feature of CloudGuard. IAM gives us complete control of our cloud environment. For example, if someone tries to bypass the policy and attempts to configure or create some users, then it will not allow them to do so.” - Network Engineer at L&T Technology Services, a tech company with over 10,000 employees

#5 Visualization and Reporting

Cloud security and infrastructure managers have to be able to see what’s happening in their cloud environments if they want to secure cloud-native apps. Even more, they need the ability to quickly identify the risks that matter most and jeopardize security posture. Visibility and reporting are thus key success factors for CNAPP.

A Product Manager at a tech services company with more than 50 employees explained, “CloudGuard is very good if you need to get an inventory and reporting on the current state of your environment.” This is helpful in particular, because, as he said, “Very often, there can be a proliferation of cloud-based accounts and applications that the organization on a wider basis is not aware of.”

CloudGuard “provides and facilitates compliance,” according to the financial services Senior Manager. He added, “It gives you complete visibility, including the IP-to-IP flow, which is happening from the workloads to the Internet or the Internet to the workloads. Even in the case of getting a threat intelligence from Check Point, for which we have the integration, if some workflows are communicating any suspicious IPs, then the reports are available on the flow logs.”

Product Manager
at a tech services company
with 51-200 employees

> “CloudGuard is very good if you need to get an inventory and reporting on the current state of your environment.”

Read review »

A Cloud Support Leader at a tech company with more than 50 employees, who uses CloudGuard's Intelligence capability, appreciated that the solution provides his team "the visualization of the network analysis, which gives us a map of connectivity between services, to be able to visually identify any threat." Skywind's Senior Network/Security Engineer likewise observed that Check Point "provides good visualization of infrastructure."

#6 Efficiency and Time Management

Businesses are migrating to the cloud to achieve levels of effectiveness and agility that eluded them with on-premises infrastructure. It's all part of a never-ending push for greater efficiency. A CNAPP solution should therefore endeavor to make cloud security teams efficient.

The insurance company Senior Security Engineer put it this way: "It also helps developers save time and increase their productivity. If they save time, they have more time to do other things, whether within CloudGuard or elsewhere. The features that are offered by CloudGuard definitely make developers more productive." In his case, he felt the toolset saves developers 10 to 15 percent of their time, while increasing productivity for security teams by about 20 percent.

"A unified security solution across all major public clouds affects our cloud security operations by saving us a ton of time and effort," said the financial services Advisory Information Security Analyst. This user estimated that his team realized a 90 percent time savings for security by avoiding having to manually check their tasks, which would be, in his words, "a nightmare."

Senior Security Engineer
at a insurance company with
10,001+ employees

★★★★☆

"It also helps developers save time and increase their productivity. If they save time, they have more time to do other things, whether within CloudGuard or elsewhere. The features that are offered by CloudGuard definitely make developers more productive."

Read review »

Improves Security Team Productivity

He added, “We don’t have to redo things manually or check every individual environment all the time for compliance. This frees us up to build out and make a more sophisticated environment, really working on fine tuning things. We have a smaller team, so this has definitely helped us.” From this, he estimates they have seen a 100 percent return on investment (ROI) from money and time savings. He added, “We don’t have to spend all day maintaining cloud environments. They take care of that for us.”

#7 Effective Risk Management and Vulnerability Remediation

Risk management that can be contextualized across complex applications and cloud environments is foundational to CNAPP, as a user of CloudGuard revealed. The Cloud Support Leader at a tech company said, “Forensics and threat hunting is one of the features that we liked the most.” In their case, the solution takes native event and log data from Microsoft Azure and gives them contextualized views of all the public infrastructure in Azure, which helps improve security.

The insurance company Senior Security Engineer said, “It helps minimize attack surface. For example, you can lock the security groups to be managed only through CloudGuard, so any change made directly on AWS would be reverted by CloudGuard. That helps minimize the risk.”

Risk remediation is also important, as PeerSpot members mentioned in their reviews. The financial services Advisory Information Security Analyst remarked, “It works great at identifying, prioritizing, and auto-remediating events.” An IT Security Engineer at ProsourceIT, a financial services firm with over 1,000 employees, similarly noted, “Today CloudGuard is helping us analyze what we have out there and what our priorities should be from a remediation perspective. We do have multiple accounts today with the different cloud providers, so it’s imperative to use a tool like CloudGuard.”

Most CNAPP users only want their solution to serve as a guardrail for their cloud infrastructure or edge security for APIs/applications. That way, Dev, Ops and other teams can continue their daily work transparently. At the same time, security teams know the policies and controls are in place to help mitigate risks that arise from misconfigurations and bad day scenarios.

#8 Compliance

Companies that must comply with regulations need their CNAPP solution to support that objective. This is partly because meeting compliance requirements tends to be overly complex and time-consuming when done manually. A CNAPP solution must provide continuous compliance and remediation that enables stakeholders to meet the required industry standards easily and seamlessly. The tech services Product Manager made this point when he said, "The reporting against compliance is an important feature that helps you comply with policies and standards within your organization."

The tech services Network Security Engineer/Architect made a comparable comment, saying, "We have full visibility of our cloud infrastructure in terms of compliance and security. For example, if someone has a machine that doesn't comply with the company policy, then we get an alert." The financial services Sr Manager IT Security liked that Check Point provides a granular level of reports along with issues based on compliance standards, which are defined depending upon organizational requirements.

Basilio A.
IT Security Engineer at Bayview

★★★★☆

> "Today CloudGuard is helping us analyze what we have out there and what our priorities should be from a remediation perspective. We do have multiple accounts today with the different cloud providers, so it's imperative to use a tool like CloudGuard."

Read review »

Conclusion

Cloud-native applications are becoming the norm for competitive, forward-looking businesses. They offer many advantages, including flexibility and interoperability with third parties and legacy systems. At the same time, cloud-native apps can be hard to secure. The very qualities that make them great for business, such as their agility and heterogeneous design, make them vulnerable to attack.

A CNAPP solution can address these concerns. It has to be multi-cloud capable, offering security across the full software development lifecycle. In deployment, cloud-native apps need CNAPP with automation and access controls, especially at the admin level. CNAPP personnel need data visualization and reporting so they can stay on top of security monitoring and configurations. A successful CNAPP enables the IT department and security teams to gain efficiency in managing and securing cloud-native apps. They can manage risk and hit compliance targets as they automatically remediate vulnerabilities.

About PeerSpot

PeerSpot is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

PeerSpot does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, PeerSpot websites, and PeerSpot materials do not reflect the opinions of PeerSpot.

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel security architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.