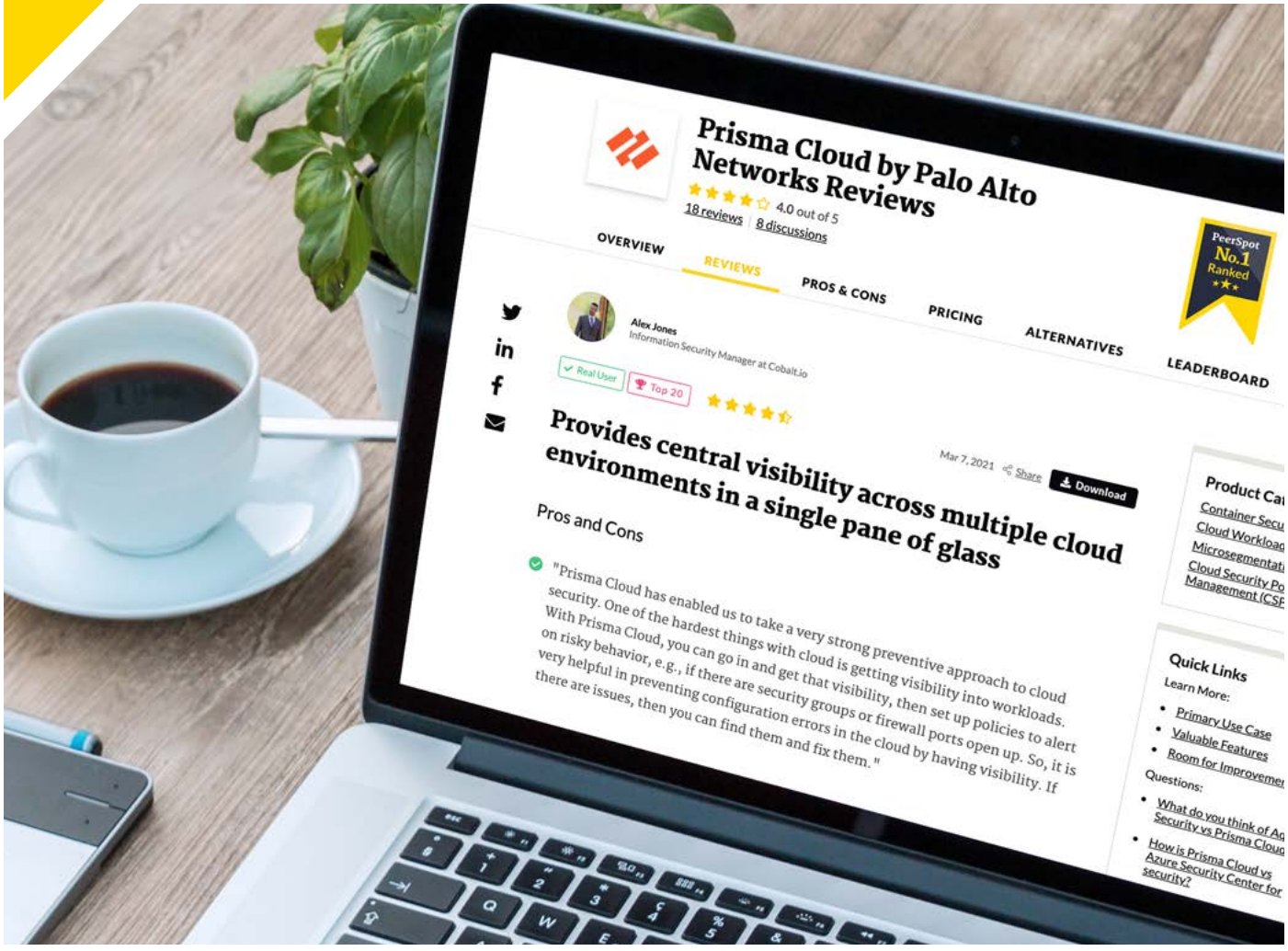
PeerPaper™ Report 2021

Based on real user reviews of Palo Alto Networks Prisma Cloud

Managing Security in the Cloud: The Top 5 Factors for Assessing Cloud Security Platforms



PeerSpot

CSO FROM IDG

Contents

Introduction

Its economic and technological advantages aside, cloud native application development has the potential to increase security risk exposure. As organizations adopt public, private and hybrid cloud infrastructures, they are confronting a host of security management challenges. Mitigating risk in the cloud is partly about people and processes, but choice of security tools is also critical.

This paper highlights the five top factors for assessing a prospective cloud security platform. It is based on real user experiences with the cloud native Palo Alto Networks Prisma Cloud security platform. As the users described in reviews on PeerSpot, the right platform will be one that offers Cloud Security Posture Management (CSPM), the ability to protect cloud workloads, Cloud Network Security, infrastructure entitlement management and secure DevOps. An effective platform will also enable the management of cloud security across cloud service providers, and throughout the cloud tech stack—integrating data and workflows while breaking down silos among SecOps, Development/DevOps and compliance teams.

Use Cases

According to Prisma Cloud users, the security tool supports a number use cases, including CSPM and cloud workload protection (CWP). The CSPM aspect utilizes data from public cloud service providers to deliver security policy compliance, continuous visibility, and threat detection across different users, data, cloud resources, and apps. CWP helps secure cloud native applications across the development lifecycle, protecting hosts, containers, and serverless functions from code through to runtime.

A Cloud Security Specialist at a financial services firm with more than 500 employees offered an example of the CSPM use case, saying, "Prisma cloud was originally destined for cloud security posture management, to determine how the configuration of cloud services aligns with given standards. Through the evolution of the product, they then integrated a capability they call Prisma Cloud Compute. That is derived from point solutions for container and image scanning. It has the capabilities on offer within a single pane of glass."

Prisma Cloud users also appreciate the platform's scalability. A Software Security Analyst at an energy/utilities company with over 10,000 employees enjoys the simplicity of the console and the API. He believes this simplicity helped him to scale easily. He went on to say, "There was no complexity; it was straightforward. The API documentation was also very good so it was pretty easy to scale." In his case, his team found they automate pretty much everything. He added, "You could automate the certificate information; you could

> **"It's easier for me to categorize and understand things exactly, on a single dashboard."**
>
> Read review »

automate the access for developers, and a lot of other stuff. It was a pretty modern solution. Using APIs and containers, it was pretty scalable."

Many users also effectively use Prisma Cloud to reduce security alert volume and lessen alert fatigue . A Governance Test and Compliance Offer at Thales, an Aerospace company with over 10,000 employees, primarily uses Prisma Cloud to filter alerts by levels of severity . This helps her team understand which notifications warrant immediate attention. Based on the priorities she receives she can determine which items need to be addressed first. As she put it, "That means it's easier for me to categorize and understand things exactly, on a single dashboard. Out of them, I can see, for example, the five major vulnerabilities that I have--and it shows my risk tolerance--so I know that these five are above my risk tolerance. I know these need immediate attention and I can assign them to the team to be worked on immediately."

Easy to scale

Similarly, a Sr. Security Operations Manager at a healthcare company with more than 5,000 employees uses Prisma Cloud "for monitoring our cloud environment and detecting misconfigurations in our hosted accounts in AWS or Azure."

Meanwhile, the financial services Cloud Security Specialist uses Prisma Cloud to gain a better understanding of the firm's cloud security and to measure "how well our existing estate in cloud marries up to the industry benchmarks, such as CIS or NIST, or even AWS's version of security controls and benchmarks." He then said, "When a stack is provisioned in a cloud environment, whether in AWS or Azure or Google Cloud, I can get an appreciation of how well the configuration is in alignment with those standards. And if it's out of alignment, I can effectively task those who are accountable for resources in clouds to actually remediate any identifiable vulnerability."

The Top 5 Factors for Assessing Cloud Security Platforms

PeerSpot members highlighted five key factors that should be considered when measuring a successful cloud security platform. Most notably, users identified the ability to manage security posture and Cloud Workload Protection across multiple cloud service providers and technology stacks as critical for success. Users also emphasized the need to break down silos among security teams and development/DevOps staff.

Cloud Security Posture Management (CSPM)

One of Prisma Cloud's main advantages is that the platform can effectively detect and prevent misconfigurations and other threats. In turn, risk of data breaches and compliance violations are greatly reduced. For example, a Cloud Security Manager at a manufacturing company with over 10,000 employees uses Prisma Cloud to prevent potential security issues. In fact, the company has remediated "thousands of high impact misconfigurations or vulnerabilities that have been detected by the tool." Specifically, they are using Prisma Cloud to lock down Amazon S3 buckets, RDS to EC2 instances, and/or other administrative access points that may otherwise be easily compromised.

> **"...thousands of high impact misconfigurations or vulnerabilities that have been detected by the tool."**
>
> Read review »

Along similar lines, a Senior Information Security Manager at a small healthcare company is quite pleased with Prisma

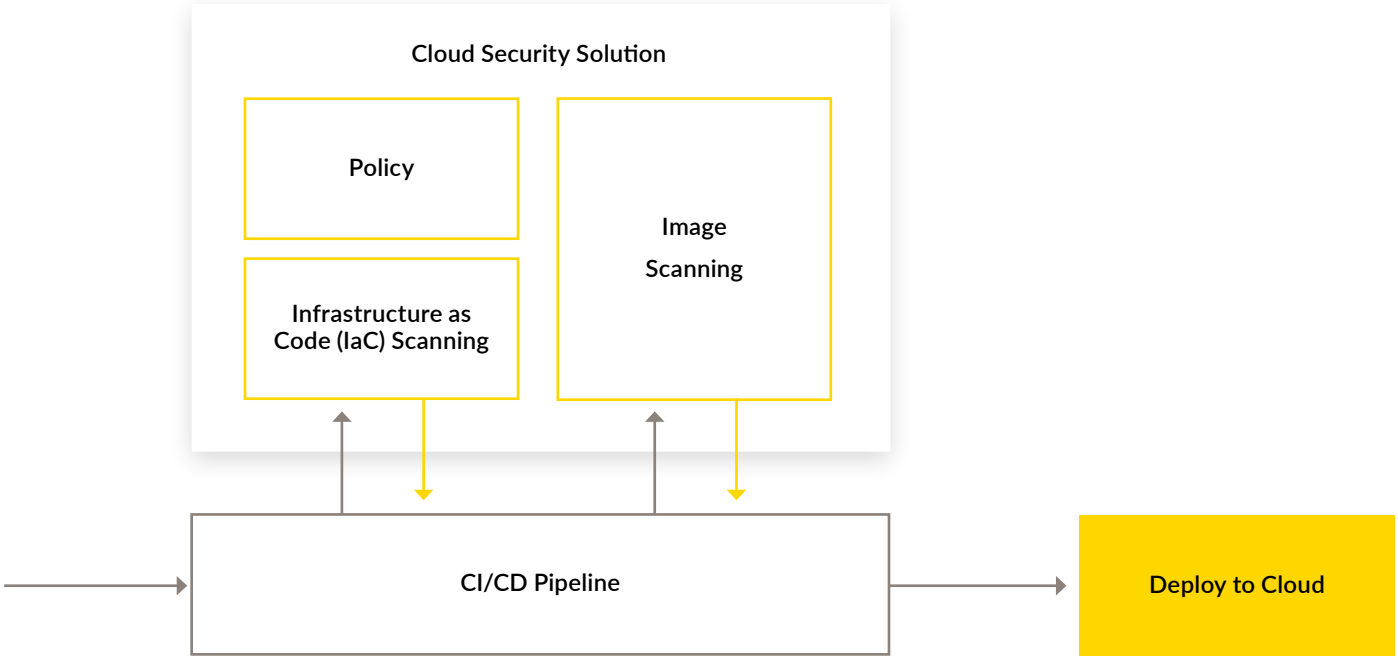


Figure 1 – The cloud security solution conducts scans of multiple cloud platforms, while also combining alerts into a unified view.

Cloud's alert feature. Because of the information provided with each alert, the company has significantly reduced the time it spends investigating alerts. The Manager goes on to say, "We're able to identify things because it uses a protocol called a NetFlow. It tracks the network traffic for us and says, 'This alert is generated because these attackers are generating alerts,' or, 'It's coming internally from these devices,' and it names them." Figure 1 offers a simple reference architecture to depict this process.

His company also runs weekly vulnerability scans to look for weaknesses. He added, "At times, alerts may be triggered during this process and Prisma will for example say that 'something is scanning your environment.' Using the information Prisma provides, the team is able to properly identify the resources that have been scanning their environment."

Meanwhile, the financial services Cloud Security Specialist likes Prisma Cloud as it provides a time saving out-of-the-box solution. Prior to using Prisma Cloud, he would have run

"With Prisma Cloud, I can just select 30 AWS accounts, generate one report, and I've got everything I need to know..."

Read review »

Trusted Advisor from AWS to look at a particular account, or run a number of reports from Trusted Advisor to look at multiple accounts. With Trusted Advisor, as he shared, "I could never get a collective view on what the overall posture was of workloads within AWS. With Prisma Cloud, I can just select 30 AWS accounts, generate one report, and I've got everything I need to know..." He likes that he instantly receives information regarding which services may be compliant or non-compliant. For each service, he gets a pass or fail with detail about whether they contain high, medium, or low vulnerabilities.

"It saves me having to go to market and also run a number of proofs of concepts for point solutions."

Read review »

Cloud Workload Protection

Prisma Cloud users appreciate the platform's ability to keep workloads secure across different cloud services. As an example, the financial services Cloud Security Specialist appreciates the fact that "Prisma not only looks at the workloads for an existing cloud service provider, but it also looks at multiple cloud service providers outside of the native stack."

He also likes that Prisma Cloud integrates capabilities across both cloud security posture management and Cloud Workload Protection. He went on to say, "The cloud security posture management is what it was initially intended for, looking at configuration of cloud service workloads for AWS, Azure, Google, and Alibaba. And you can look at how the configuration of certain workloads aligns to standards of CIS, NIST, PII, etc."

The Cloud Security Specialist is fond of the ability to view private, public, or hybrid offerings at will. As he put it, "It saves me having to go to market and also run a number of proofs of concepts for point solutions. It's an indication of how the market has matured and how Palo Alto, with Prisma

Detected thousands of high impact misconfigurations or vulnerabilities

Cloud in particular, understands what their consumers and clients want."

An Information Security Manager at Cobalt.io, a small security firm likes how comprehensive Prisma's workload protection features are. He went to say that he looked at other vendors with similar cloud workload protection features. However, he concluded, "Based on the relationships that we have with Palo Alto, we knew that Palo Alto was kind of the leader in this space." He explained that the other vendors that he looked at were either focused more on the container side or on the cloud API layer. Consequently, because Prisma Cloud unified these different pieces into one platform, he said, "We ultimately decided that Prisma Cloud was going to be the best solution for us."

Cloud Network Security

According to the reviews, users are very pleased with the level of cloud network protection they receive from Prisma Cloud. For example, the manufacturing Cloud Security Manager appreciates Prisma Cloud's ability to provide strong security in multi-cloud and hybrid-cloud environments. In fact, he believes that this ability was of critical importance to them as they have workloads both on premise and with multiple cloud providers.

Cobalt.io's Information Security Manager was equally impressed with Prisma Cloud's abilities. He especially liked the ability to manage Cloud Security Posture Management, Cloud Workload Protection, Cloud Network Security, and Cloud Infrastructure Entitlement Management within one dashboard.

He stated, “It is particularly challenging, especially in a multi-cloud environment, where you would have to log into your Google Cloud, then look for your infrastructure and alerting within Google. In addition, you have to switch over to Amazon and log into an AWS Console to do some work with Amazon. Having that central visibility across multiple cloud environments is definitely important when you have different sources and different dashboards for the cloud...”

Enhanced cooperation between DevOps and SecOps

Cloud Infrastructure Entitlement Management

Prisma Cloud offers dynamic and secure Cloud Infrastructure Entitlement Management services. This is part of the broader realm of Identity and Access Management (IAM). As an example, the financial services Cloud Security Specialist uses Prisma Cloud with Amazon Managed Services. He likes that he can generate a snapshot in time, whether that’s over a 24-hour period, seven days, or a month, to determine what the estate might look like at a certain point in time and to generate reports from that.

He further praised Prisma Cloud because he “can get a snapshot of what I deemed were the priority vulnerabilities, whether it was identity access management, key rotation, or secrets management. Whatever you deem to be a priority for mitigating threats for your environment, you can get that as a snapshot.”

Meanwhile, the healthcare Senior Information Security Manager primarily uses the Prisma Cloud platform to monitor the security configurations of their Azure and AWS

clouds. More specifically, the manager uses Prisma Cloud to monitor "storage, networking, IAM, and monitoring of malicious traffic."

That said, a Consultant at a Tech Services Company with more than 500 employees loves that Prisma Cloud is extremely easy-to-use. As he said, "It's very user-friendly. You can easily make customized dashboards as well." He elaborated by saying that he further appreciates that he can easily restrict users if needed. He can also "even restrict them from accessing certain applications or services."

Secure DevOps

Prisma Cloud users at different organizations noted that the platform offers a superior way to secure DevOps. DevOps is a fusing of software development (Dev) and IT operations (Ops) that streamlines the process of writing and releasing software code. One user, the healthcare Senior Information Security Manager, is integrating Prisma Cloud into the organization's Continuous Integration/Continuous Deployment (CI/CD) pipeline. For example, they are integrating container scanning into their CI/CD. As a result, when a container is built into the pipeline, it's automatically deployed and the results come back to the console where the security team manages it. Figure 2 shows a cloud security solution fits in the CI/CD pipeline.

He explained, "The beauty of it is that we give our developers access to this information. That way, as they build, they actually get near real-time alerting that says, 'This configuration is good. This configuration is bad.' We have found

> **"The beauty of it is that we give our developers access to this information... We have found that very helpful because it provides instant feedback to the development team."**
>
> Read review »

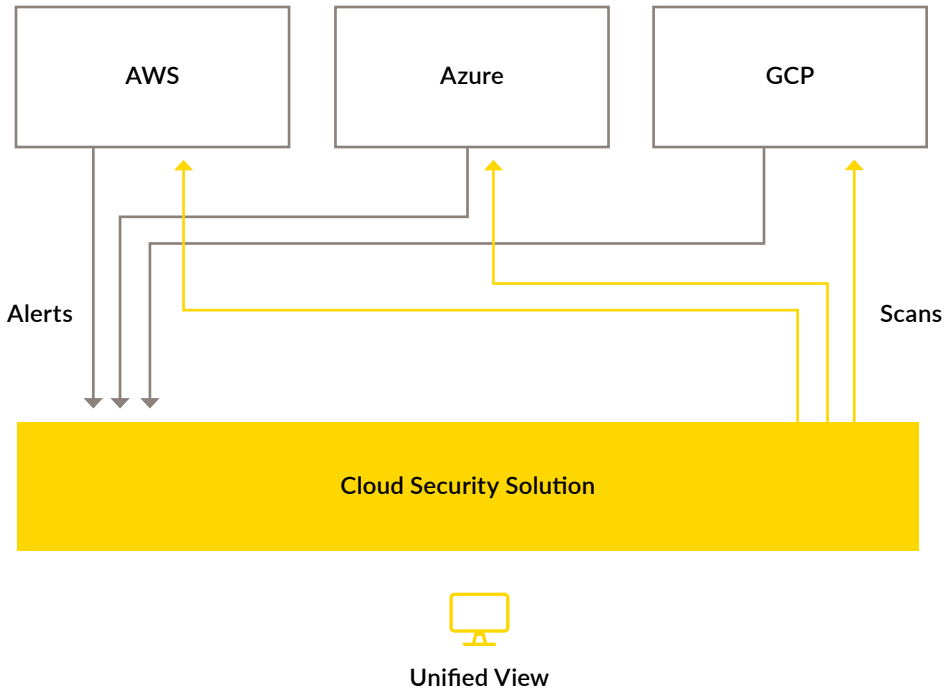


Figure 2 – How a cloud security solution like Prisma Cloud fits into the DevOps CI/CD workflow.

that very helpful because it provides instant feedback to the development team."

The Senior Information Security Manager believes that this transparency has enhanced cooperation between his DevOps and Security Operations (SecOps) teams. He then noted, "We're also integrating it into our CI/CD pipeline. That's our strategy. Whatever we in security know, we want them to know, because it's a collaborative effort. We all need each other to get things fixed. If they're configuring something and it comes to us, we want them to see it. And our expectation is that, hopefully, they've fixed it by the time we contact them. Once they have fixed it, the alert goes away. Hopefully, it means that everyone has less to do."

The manufacturing Cloud Security Manager also likes Prisma Cloud's ability to integrate and participate in its DevOps lifecycle. Prisma Cloud allows the company to integrate secu-

> **"The integration of security into our CI/CD pipeline has affected collaboration and trust between our DevOps and SecOps teams has improved."**
>
> **Read review »**

rity into their CI/CD pipeline and touch points into already existing DevOps processes. He revealed, "The integration of security into our CI/CD pipeline has affected collaboration and trust between our DevOps and SecOps teams has improved."

A Director of Cloud Engineering at a pharma/biotech company with over 10,000 employees similarly stated that Prisma Cloud allows the business to integrate security into the CI/CD pipeline and add touch points into existing DevOps processes for a container. In the container, he said, "touch points are seamless. We've been able to implement security control gates and automate notifications back to teams of vulnerabilities in the container orchestrator."

Conclusion

This paper highlights the factors to look for when assessing cloud security platforms, based on real user reviews of Palo Alto Networks Prisma Cloud. It also explores a few emerging security trends that are critical to managing security in the cloud successfully going forward. Security teams need to develop a practical strategy for managing security in the cloud—one that works within their organization's unique constraints and requirements. Getting started with cloud security can be daunting, but by focusing on the top functional areas for success noted here, organizations are better positioned to build comprehensive long-term approaches to cloud security.

About PeerSpot

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. PeerSpot provides technology professionals with a community platform to share information about enterprise solutions.

PeerSpot is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.peerspot.com

About Prisma Cloud

Prisma Cloud is the industry's most comprehensive Cloud Native Security Platform (CNSP) with the broadest security and compliance coverage – for applications, data, and the entire cloud native technology stack – throughout the development lifecycle and across multi- and hybrid-cloud environments. Our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively and accelerate securecloud native application development.