GlobalDots

Comparison Guide


Guide
How To Select
Your Cloud Workload
Protection Solution

Background

By now, we have all seen this meme about what was 2020's main driver for digital transformation in enterprise companies - not the CIO, not the CTO, but rather COVID-19.

Multi-year long processes were accelerated to months and sometimes weeks long. Industries that didn't have public cloud migration on their horizon were urged to adopt it as soon as possible in order to support remote work, digitalize customer workflows and improve user experience through online channels.

Even during peacetime, cloud migration is not an easy process. It introduces many changes to the company's infrastructure, workflows and security. The public cloud isn't "more" or "less" secure - it is different and requires a different approach to security. It exposes companies to new attack vectors and security threats that should be handled in a different approach.

The challenge is how to make your public cloud environment secure while serving the purpose of adopting it in the first place - becoming a more agile organization that can move fast and react to changing circumstances. This is where cloud workload protection platforms come into the picture, to help companies continuously maintain their public cloud security posture and enable speed and agility.

New Security Threats in the Public Cloud

Recent reports show that overall enterprise use of cloud services spiked by 50% due to work from home mandates caused by the pandemic. From interactions with our customers - some were “born in the cloud” and some are just taking their first steps towards migration from on-prem environment to the cloud, we can share the typical security challenges companies face in the public cloud.

Publicly Accessible Resources

It's super easy to spin up new AWS instances of machines, databases and storage services, and this frictionless experience sometimes obscures the fact that not all resources should be accessible through the public internet by everyone. A well designed application has specific entry points end-users should use to access it from the public internet, but other components should be restricted from direct access.

It's a common mistake to accidentally leave exposed databases, S3 buckets or other compute resources open to the public internet, which hackers can gain access to and move laterally across the network, searching for valuable information they can exploit and exfiltrate outside of the organization.

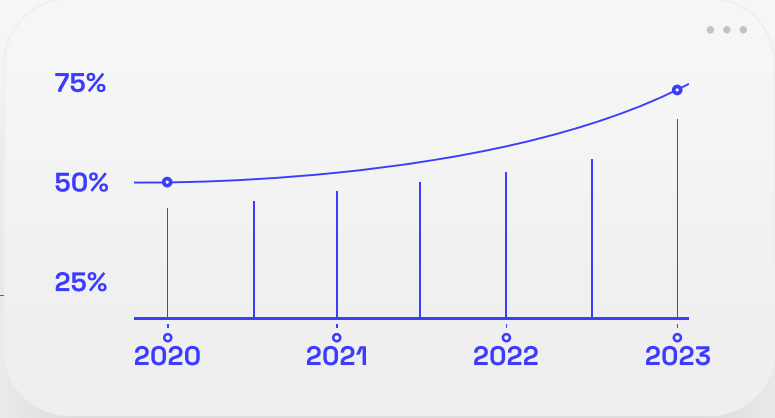
Publicly Accessible Resources

One of the major benefits of moving to the cloud is that it enables fast business operations. However, in the name of expediency, access credentials are frequently handed out in hasty and unnecessary manner, so that many users end up with excessive permissions for which they have no business need. The problem is that should any of those credentials fall into the wrong hands, attackers will have far-reaching access to sensitive data.

All too frequently, there is a gap between granted permissions and used permissions. In other words, many users have too many permissions, which they never use. Such permissions are frequently exploited by hackers, who take advantage of unnecessary permissions for malicious purposes.

According to Gartner, by **2023, 75%** of security failures will result from inadequate management of login credentials, identities and privileges, up from **50%** in **2020.**

Security failures from inadequate management of login credentials.

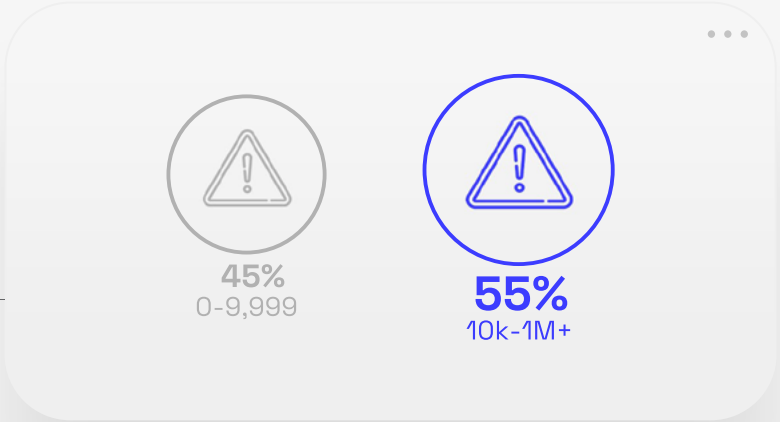


Alerts Overload

The common layered security approach or “defence in-depth” contribute to the abundance of security solutions. Each security component generates many alerts when detecting suspicious behavior. It is up to the customer’s SOC or security team to sift through the massive amounts of alerts and decide which are false positives compared to real malicious activity that can jeopardize the company’s sensitive assets.

According to study by IT security firm Bricata, the average SOC receives over 10,000 alerts each day. This is a massive figure, which no human (or team of humans) can realistically deal with. It means security managers must sift through a sea of excessive alerts and false positives to find the really important alerts which are indicative of actually malicious activity.

Number of daily security alerts your SOC receives.



Lack of Context

Everybody talks about ‘context’ but what does it actually mean? One of the key challenges in security is that looking at any single alert doesn’t actually tell you very much. Is that login in the middle of the night a hacker, or an admin working late? Is that first time API invocation an act of reconnaissance, or a DevOps engineer going about their business? Is that access to a sensitive storage bucket a new feature being released, or the last step in a data breach? Practically every user activity can be either legitimate or not, and looking at just that activity tells you almost nothing.

Cloud Workload Protection Criteria

In recent years new companies offering cloud workload security solutions emerged, with ways to handle excessive cloud permissions, misconfigurations and compliance requirements. Some do it better than others with components that allow for better automation, less false-positive noise and AI-based detection and correlation of sophisticated attacks that typically can go under the radar of traditional security solutions.

Here at GlobalDots, we've been evaluating new technologies for cloud workload protection and came up with the criteria and parameters you should look for when evaluating cloud workload protection solutions. At a high level, there are 3 aspects you should consider when evaluating a cloud workload protection solution: **Hardening, Threat Detection and Compliance.**

Hardening

The best way of stopping a data breach is preventing it before it ever occurs. Therefore, hardening your cloud security posture by eliminating excessive permissions and misconfigurations guarantees that even if a user's credentials become compromised, then attackers will not be able to do much with those permissions.

Cloud security posture hardening can be divided into 3 main areas: permissions hardening, resources hardening and configuration hardening.

Permissions Hardening

Flexibility is one of the biggest advantages of the public cloud - it provides all the nobes and whistles for developers to design and create the most innovative apps. On the flip side, too many options for developers that are not security minded, often leads to granting and using roles with excessive permissions than they should have to perform their job.

Simply put, permissions hardening is the process of detecting the gap between granted permissions of users, groups and roles compared to their actual usage, and tightening it up by removing unnecessary permissions in order to reduce the attack surface of a potential intruder. Unused permissions or even inactive users should be removed and reevaluated on an ongoing basis.

Resources Hardening

Public cloud resources are machines, databases or storage instances that are being used by the development team. As previously mentioned, mistakes of leaving cloud resources exposed to the public internet happen all the time - the goal is to detect, alert and remediate such occurrences by closing up inadvertent publicly exposed resources. Doing so on a continuous basis will reduce entry points attackers may use to infiltrate the company's infrastructure.

Another potential vulnerability of exposed resources is the abuse of public cloud resources by an attacker for crypto-mining or launching attacks from legitimate company's public cloud account. This can impact the public cloud costs if found too late, as the resources were exhausted by the attacker for his crypto mining or distributed attack activities on the company's dime.

Configuration Hardening

When business is growing and the company expands rapidly, misconfigurations in your cloud environment can happen all too often. Common examples might be: unenforced password policy for public cloud users, MFA not enabled for root users, encryption of assets improperly configured, disabled logging for critical services and open ports and protocols of cloud resources. Each one of these is an invitation for an attacker to sneak into the company's infrastructure and gain access to sensitive data and resources.

Threat Detection

Modern security systems detect a lot. In fact, they probably even detect too much: according to study by IT security firm Bricata, the average SOC (Security Operations Center) receives **over 10,000 alerts** each day from an ever-growing array of monitoring and detection products. This has inevitably led to what is known as **"alert fatigue"**. So clearly, not enough detection is hardly the issue.

Correlation is the process of taking independent, seemingly-unrelated events, and correlating them across threat surfaces, resources, and time frames. This is why correlation is so important: it allows you to identify a data breach in its entirety, not just the individual events that are part of it. It also helps prioritize a real attack from all the noise traditional security systems typically generate.

Once the solution is integrated and false positives are proved to be minimal, automatic remediation is the next step. Some organizations with small security teams prefer to mitigate the attack attempt with automatic response, given that the cloud workload protection solution can be trusted to catch only real high risk attacks.

An ideal cloud workload protection system should have an automatic, AI-based correlation engine which is a crucial component of cybersecurity, and one that can make the difference between stopping a breach in time, or reading about it in the news.

Compliance

There is no other way to say it - security compliance standards (PCI-DSS, SOC2, ISO-27001, GDPR etc.) are a hassle. Whether you work in a B2B startup and your target customers are large enterprises, or your employer is a publicly traded company that needs to comply with them, you'll face this challenge sooner or later. Based on the shared responsibility model, the cloud provider share the burden of keeping the hardware and software of their platform secure (security "of" the cloud), but the customer has to own the security "in" the cloud: managing their data (including encryption options), classifying their assets, and using IAM (Identity & Access Management) tools to apply the appropriate permissions.

Wouldn't it be wonderful if in a click of a mouse you could generate a report showing how does your cloud environment compare with popular security compliance standards? That's exactly what you should be looking for in the evaluation of cloud workload protection solutions. Detailed reports showing what checks your cloud environment passed based on the compliance standard, and which check failed and need to be fixed. Modern security solutions should provide the tools to help customers meet security compliance standards.

Compliance reports can also be used to track deviation from a company's security policy. Let's say only developers from a certain team should have specific permissions to access the AWS Redshift database service, you want to be able to track any drift from the company's security policy or violations of such policy, in order to fix them.

Payment Card Standards

Security, Availability, and Confidentiality Report

Security Management Controls

Comparison Parameters

Here are the 9 parameters we used to compare the various solutions based on our engagements with our customers and the developments in the public cloud platforms. These parameters include the main components discussed above (hardening, compliance and threat detection) as well as other important features and capabilities a cloud workload protection should have.

Cross-Platform / Multi-Cloud does the solution support multiple public cloud platforms: AWS, Azure, GCP or other CSPs.

Detection Speed how fast the solution can detect misconfigurations, publicly accessible resources or excessive permissions (minutes / hours / days).

Permissions Hardening can the solution alert on excessive permissions of groups, users, roles (including federated identities and machine roles), as well as inactive users (yes / partially / no).

Compliance Standards can the solution generate reports based on common security compliance standards: SOC2, ISO 27001, PCI-DSS, GDPR, HIPPA, others.

Custom Compliance Reports does the solution allow adding custom rules to compliance reports (yes / no).

Deployment Efforts the level of effort and resources required to deploy the system, does it require an agent or is it agentless (easy / moderate / intensive).

Automated Remediation can the solution enable automated remediation in case of real attacks on the public cloud environment (yes / partially / no).

Attack Detection, Correlations and Anomalies can the solution correlate multiple sporadic events into an attack timeline across time (basic / advanced / not supported).

Alert Prioritization can the system focus the DevOps / Security teams on the most important events (basic / advanced / not supported).

Solutions Comparison Matrix

Here are the 9 parameters we used to compare the various solutions based on our engagements with our customers and the developments in the public cloud platforms. These parameters include the main components discussed above (hardening, compliance and threat detection) as well as other important features and capabilities a cloud workload protection should have.

Solution / Criteria	Prisma Cloud by Palo Alto	Cloud Native Protector by Radware	Dome9 Cloud Guard by Checkpoint	GuardDuty by AWS
Detection Speed	Minutes	Minutes	Minutes	Minutes
Permissions Hardening	Yes	Yes	Partially	Partially
Compliance	PCI-DSS SOC2 ISO 27001 HIPAA NIST GDPR AWS CIS Azure CIS	PCI-DSS SOC2 ISO 27001 HIPAA NIST GDPR AWS CIS Azure CIS	HIPAA PCI-DSS NIST GDPR	PCI-DSS
Custom Compliance Rules	Yes	Yes	No	No
Deployments Efforts	Intensive	Easy	Moderate	Easy
Automated Remediation	Yes	Yes	Yes	No
Cross-Platform / Multi-Cloud	AWS Azure GCP Alibaba	AWS Azure	AWS Azure GCP	No, only AWS
Attack Detection, Correlations and Anomalies	Advanced	Advanced	Basic	No
Alert Prioritization	Advanced	Advanced	Basic	Basic

Prisma Cloud by Palo Alto

This solution gives a holistic view of cloud security posture across multiple cloud environments or multi-cloud deployments. DevOps and SecOps teams can integrate automatic scans of compliance reports into the CI/CD pipeline or send alerts into Slack when there is deviation from the company's security policy, whether it was identity access management, key rotation, or secrets management issues. It helps reduce time to mitigate security issues by providing specific instructions on how to resolve misconfigurations or excessive permissions issues inside the cloud provider's environment. Prisma also provides an intuitive root cause analysis for security breaches like publicly exposed assets that shouldn't be accessible to the public internet. This solution is not cheap, but provides a lot of value and capabilities for its premium pricing.

Cloud Native Protector by Radware

This one is one of our favorite solutions - it's graphical interface is clean, very intuitive as well its built in AI capabilities. The solution learns your public cloud environments in minutes, including user, group and role permissions, exposed machines and misconfigurations and provides a focused, prioritized list of recommendations on how to mitigate high risk vulnerabilities and which ones are important but not urgent. The attack storylines are very useful to understand how seemingly unrelated events connect together to an attack with malicious intent. Automatic remediation is also an option when integrating with AWS SNS and Lambda. It's a very DevOps friendly solution as it's quiet by nature with minimal false positives and only alerts on the important security events.

Dome9 Cloud Guard by Checkpoint

The Dome9 cloud guard solution seems to have all the bells and whistles - it integrates with Checkpoint's other cloud, end-point and infrastructure solutions through a single portal, as well with the ThreatCloud threat intelligence service for additional fees. However, the deployment efforts are more involved as the solution's built in capabilities doesn't have too much baked AI or ML capabilities that can build a baseline of typical user behavior and alert on abnormalities and deviations from the norm which may indicate on malicious activity, so it's up to the customer to define all the rulesets and alerts based on their environment. The solution is geared towards providing visibility across multi-cloud environments and delivering compliance reports for various security standards.

GuardDuty by AWS

This solution is good enough for companies looking for basic coverage only for AWS workloads. Not surprisingly it integrates well within the AWS platform, supports PCI compliance and is easy to deploy and cost effective. However, once your public cloud environment gets more complicated, you should be looking for more advanced solutions that can provide better correlation of suspicious activities, smart hardening recommendations that are backed by AI-based platforms.

Summary

The public cloud security niche is an emerging space that attracts hackers and malicious actors rapidly. There are multiple security providers that offer cloud workload protection or cloud security posture management solutions with various capabilities. Some parameters such as **hardening**, **compliance** and **threat detection** are must haves across the board, while others such as cross-platform or custom compliance reports can be nice to haves depending on your specific use-case.

While we've seen public cloud adoption accelerate in the past 12 months, we've also seen more and more security breaches and incidents in the media. The purpose of CSPM (Cloud Security Posture Management) and CWPP (Cloud Workload Protection Platforms) solutions is to allow businesses to be more flexible, provide robust cloud-based apps and services while keeping end-users sensitive data secure. DevOps and DevSecOps teams quickly adopt these kinds of solutions as they help them work more efficiently with less headcount.

As IT and security leaders, your job is to be a few steps ahead of the hackers. To do that, you spend a lot of time researching, learning and evaluating new technologies and security solutions. It's an oxymoron - you need to spend time looking for the most optimal solutions in the race to beat the bad actors before they breach your infrastructure and cause harm.

Being cloud explorers at GlobalDots means that we are always on the hunt for the next emerging, cutting edge cloud technology - we constantly test new solutions, experience with them and recommend what brings the most value to our customers and their business. We hope that this guide helped provide a comparison and evaluation framework when it comes to choosing your preferred security solution. If you'd like to have a chat with no commitment whatsoever - we're always available to listen to your challenges and find solutions that help you succeed.

About GlobalDots

GlobalDots is a 17-year world leader in cloud innovation, connecting businesses with the latest cloud & web technologies.

Fusing an insatiable hunger for innovation with a diligent team of hands-on experts, we help our customers maintain an up-to-date technology position in a quickly-changing world.

We consult, resell, implement, and customize full-stack solutions, including cost & performance optimization, security, connectivity, and managed services, to streamline business processes and provide the foundation for sustainable business growth.

Click here to talk to our cloud workload security experts

GlobalDots.com