HORANGI
CYBER SECURITY

Whitepaper

The Ultimate Guide: What Is CSPM? And How To Select One

Contents

Foreword

by Raphael Peyret, Horangi Director of Product

Cloud Security Posture Management (CSPM) solutions have the potential to be a major security asset for organizations leveraging cloud computing. The ability for a single tool to aggregate security and compliance risks from a myriad of evolving cloud instances and services — and in many cases, automatically reduce these risks — severely handicaps attackers who target this exploding attack vector in the cloud.

Gartner, 2018

> “Through 2024, organizations implementing a CSPM offering and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%.”

To help businesses better select a CSPM solution that suits their needs, this whitepaper documents the common factors for CSPM purchases based on responses from Horangi’s prospects and customers using the public cloud.

Key Takeaways

- The widespread adoption of the cloud, coupled with the fact that teams managing infrastructure lack cloud security experience, increases the attack surface for data breaches
- CSPMs are focused on helping organizations stop the leading cause of IaaS-based data breaches
- Organizations who are considering CSPM solutions should prioritize features including resource inventory, risk prioritization, and compliance management

1. A Growing Security Concern: Misconfigured Cloud Infrastructure

Over the last few years, cloud adoption has become mainstream with a growing number of organizations moving from small-scale proof of concepts to large deployments and embracing a cloud-first strategy.

This reality is reflected in the forecasted revenue growth of public cloud services in the coming years, with Gartner forecasting a 22.1% CAGR for Infrastructure-as-a-Service (IaaS) revenue between 2019 and 2022[1].

Unfortunately the skills and expertise required for cloud technologies, in particular around security, has not been able to match this rapid rate of adoption and left many organizations ill-equipped to manage the transition. This shortage of cloud skills compounds with a global shortage of cybersecurity skills, with unfilled cybersecurity positions expected to rise to 3.5 million by 2021, according to Cybersecurity Ventures[2].

> “Through 2024, 99% of cloud data breaches will be the customer’s fault.”
>
> **Gartner, 2019**

The most viable approach for tackling this skills shortage is leveraging automation and tooling to supplement security teams, with expertise baked into processes and software that enables organizations to scale security faster than their security teams. Cloud security and management is a constant work-in-progress and the combined effort of multiple teams. If the investment makes sense, anything that can be automated should be automated to increase work efficiency in the organization.

Classifying Cloud Security Controls for IaaS

The move to the cloud has radically changed the paradigm for how infrastructure is managed and secured, largely due to the introduction of new technologies and that the central management plane of IaaS allows infrastructure to be provisioned, modified, and deleted instantly at the click of a button or with a single line of code.

The shift also introduces the concept of a shared security responsibility model into the relationship between the Cloud Service Providers (CSP) like Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure and their customers. This model changes who handles the security requirements, who the assumed security risk resides with, and has implications on how organizations should handle compliance requirements.

Thus, traditional security controls that have historically worked well for on-premise environments need to be adapted and tuned towards cloud-based environments.

Some of the most important security controls are still applicable within an IaaS cloud context and can be broadly divided into the following categories:

- Identity and Access Management
- Network Protection
- Data Protection
- Audit Logging and Monitoring

[1] Forecast: Public Cloud Services, Worldwide, 2017-2023, 4Q19 Update
[2] Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, Cybercrime Magazine, 2019

NETWORK PROTECTION

Proper configuration of Identity and Access Management (IAM) is essential to establishing a strong security posture in the public cloud given that it governs access to the management of IaaS as a whole. It is mainly concerned with proper account monitoring and control, controlled access to administrative accounts, and the need-to-know principle.

Key controls in this category would include:

- Proper network segmentation
- Denying communication over unauthorized ports or to unauthorized addresses
- Recording network activity

DATA PROTECTION

Securing data in the cloud properly is essential to a strong security posture as more and more organizations shift critical or sensitive data into the cloud. It is mainly concerned with controlling access to the data based on the need-to-know principle, and preventing or mitigating the effects of data exfiltration and tampering to ensure the privacy and integrity of sensitive information.

Key controls in this category would include:

- Ensuring native configuration logging is enabled and well-configured
- Enabling native services for threat detection or tracking inventory configuration changes
- Setting up alerts for critical security events such as unsuccessful management console authentication attempts or changes to network configuration

AUDIT LOGGING AND MONITORING

Proper collection, management, and analysis of audit events is essential to a strong security posture as it is foundational for effective Incident Response and Management by helping to detect, understand, and recover from an attack.

Key controls in this category would include:

- Ensuring native configuration logging is enabled and well-configured
- Enabling native services for threat detection or tracking inventory configuration changes
- Setting up alerts for critical security events such as unsuccessful management console authentication attempts or changes to network configuration

The Grave Consequences of Mismanaged Controls

DATA LOSS AND BREACH

The CSPM tool Horangi Warden has found that 99% of cloud infrastructure scans we have conducted thus far have exposed security vulnerabilities that could have led to data breaches. Breach of an organization's systems leading to theft or loss of data is probably the most common public impact of unaddressed security risks in the cloud.

Theft of personal or publicly identifiable information is increasingly common and has the potential for serious reputational and financial implications for organizations depending on the amount and sensitivity of the data that was stolen.

This risk has been exacerbated recently by the recent regulatory developments around privacy like GDPR, which has strict disclosure requirements and hefty fines.

Theft of an organization's intellectual property or trade secrets in order to gain a competitive advantage is another regularly seen but less publicized impact of data breaches, particularly in the case of state-sponsored actors.

Ransomware is another cause of data loss that is often top of mind for IT and security leaders but protection efforts often forget to consider cloud infrastructure. Insufficient security controls can allow malicious actors to encrypt data and systems stored in the cloud and hold it for ransom. If a robust backup and recovery plan was not previously put in place, recovery from such an event can be costly even without paying the ransom.

COMPLIANCE VIOLATIONS

Violations of compliance requirements due to inadequate security controls can have a significant financial and operational impact on an organization.

For organizations in regulated industries such as finance, healthcare, services, or government, breach of compliance can, in very severe cases, lead to losing their license to operate. Compliance standards like the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) or the Monetary Authority of Singapore's (MAS) Cyber Hygiene Notices are applicable examples of this.

Some organizations may also have compliance requirements stemming from voluntary certifications such as ISO 27001 or SOC2, which may be a prerequisite for doing business with large enterprises that have strict vendor management processes in place.

In addition to the compliance standards listed above, all organizations, regardless of industry or choice, need to comply with a growing number of local privacy regulations. The painful financial impact of compliance violations are not just felt by organizations hit by data breaches.

Organizations that fail to meet compliance requirements are also liable to be fined. Under the European Union's General Data Protection Regulation (GDPR) law, violators may be fined up to 4% of annual worldwide turnover or €20 million, whichever is greater.

ABUSE OF CLOUD RESOURCES

A weak cloud security posture can also lead to various types of abuse of cloud services and the unsanctioned use of an organization's cloud resources.

Malicious actors that gain access to cloud infrastructure will in some cases use the organization's infrastructure for greater anonymity when carrying out criminal activities such as:

- Hosting of malware in cloud storage
- Running command and control servers
- Storing stolen data after an attack on another organization
- Launching Distributed Denial-of-Service (DDoS) attacks

These types of misuse may make an organization unknowingly complicit in these activities and potentially liable to prosecution or fines.

Another type of abuse that is frequently seen is the use of an organization's cloud infrastructure to benefit from computing resources without paying. Most commonly, high-performance cloud instances will be launched to mine cryptocurrencies for an attacker and racking up large bills with the cloud provider that the organization is left to pay.

On a much smaller scale, employees may sometimes provision cloud resources for personal projects in the organization's cloud infrastructure, leading to increased costs to the business.

> 99% of cloud infrastructure scans have exposed security vulnerabilities that could have led to data breaches.

2. Making The Case For A CSPM

A frequent question Security, Risk and IT leaders ask regarding CSPM is:
Why do I need a new tool for this? Surely my existing resources and tools can cover this.

Simple answer: *It depends*.

THE MANUAL APPROACH

A manual approach of addressing these problems would typically be in the form of quarterly or annual reviews of the configuration of infrastructure. The value of this approach is severely limited due to the scale and dynamism of cloud infrastructure.

What are the limits of a manual approach?

Scale: A manual inspection of a single resource's configuration is easily done by a DevOps or Security team via the web console or Command Line Interface (CLI) of Cloud Service Providers (CSPs), but becomes impractical when considering the large number of different services, resource types and resources deployed in most organizations. Frequency of assessment is another.

Dynamism: Manual reviews of configurations are very time-consuming and therefore can only be performed infrequently. This leaves a large window of opportunity for misconfigurations to go unnoticed and cause damage, as changes to the infrastructure can be introduced at any time both during the standard development process or by an administrator.

Cost: Large security teams with highly customized needs and the necessary expertise can certainly consider building CSPM functionalities in-house, but this is generally much costlier than buying an out-of-the-box solution.

ALTERNATIVE TOOLS WITH CSPM FUNCTIONALITIES

Tools like Cloud Access Security Brokers (CASBs), Cloud Management Platforms (CPMs) and Cloud Workload Protection Platforms (CWPPs) may help to address the risk of misconfigured cloud controls. These may already be deployed in existing cloud environments.

CWPPs are software platforms that monitor and protect cloud workloads, designed to address the requirements of server workload protection. CWPP tools may support container-based application architectures and hybrid data center architectures. With the right configurations, CWPPs can provide security and compliance teams the reports they require for internal audits and logging.

Likewise, CASB tools provide organizations with visibility and control across IaaS, PaaS, and SaaS, typically integrated with firewalls, detection capabilities, and traffic encryption. Organizations that already have CASBs may be able to pay an additional license fee to extend infrastructure monitoring services.

The difference in dedicated CSPM tools tend to be the wider range of cloud services assessed, providing more details about security posture in an organization's cloud infrastructure setup. That's why dedicated CSPMs are most suited for teams that process sensitive data in IaaS.

What Are The IaaS Security Risks?

The security risks to take into account for a cloud deployment are not fundamentally different from those of an on-premise infrastructure, however the relative importance of those risks will be very different due to the programmable nature of the cloud.

1. LACK OF VISIBILITY AND TRANSPARENCY

As cloud infrastructure typically follows a self-service model with application or project teams managing their infrastructure directly, centralised visibility into what is deployed can be a challenge. Security teams can't protect what they can't see, leaving *invisible* resources vulnerable as they may not be managed or monitored for risks.

2. WEAK AUTHENTICATION

Weak authentication is a key security risk in all enterprises across all IT services, and cloud infrastructure is no exception. Weak password policies or lack of multi-factor authentication are the primary risks to look out for here.

3. EXCESSIVE ACCOUNT PERMISSIONS

Excessive account permissions go against the principle of least privilege access and may significantly increase the impact of a breach by allowing attackers to move laterally inside an organization.

4. EXCESSIVE NETWORK CONNECTIVITY

Overly permissive access rules and resources directly accessible from the internet are the security risks behind some of the most publicized data breaches in recent times like cloud storage storage containers (AWS S3 storage buckets, Azure Blob Storage Container, GCP Cloud storage bucket) or databases publicly accessible.

Attackers are continuously scanning IP ranges of CSPs for accessible resources that may be unprotected, and the cloud's move away from perimeter security has made these risks much more critical to monitor in the cloud than they were on-premise.

5. INSUFFICIENT OR IMPROPER ENCRYPTION

Lack of encryption can be a significant compliance risk when sensitive application traffic is not protected, opening the door to man-in-the-middle attacks.

Equally important, for encryption to be effective in protecting data, organizations must use secure cryptographic schemes and appropriately managed encryption keys that are regularly rotated. This reduces the risk that older encryption standards with known weaknesses can be successfully exploited, giving an attacker only a very small window to take advantage of a compromised encryption key.

6. INSUFFICIENT LOGGING AND MONITORING

If monitoring and logging is not properly set up, organizations will have a high risk of not being able to:

1. Detect an intrusion or abuse early
2. Understand the extent or impact of a breach ie. which data was exfiltrated, how long an attacker remained in the network
3. Respond to a breach appropriately to stop an attacker
4. Know whether the attacker has retained access to the system

Logging is also essential to provide law enforcement forensic information to help with a criminal investigation following a breach.

Defining CSPMs

Cloud Security Posture Management (CSPM) tools are security solutions dedicated to the continuous assessment and monitoring of the security and compliance of an organization's public cloud infrastructure.

At its core, CSPM functionality is the detection of cloud misconfigurations that put an enterprise at risk of security breaches or compliance violations. This is generally done via use of native cloud provider APIs to monitor the configuration of cloud resources against a desired security posture.

CSPM solutions are relatively new in the security market and have quickly gained traction by filling in security needs unaddressed by both traditional on-premise security solutions like firewalls as well as native cloud security solutions like CASB or CWPP.

CASBs primarily focus on the data plane and SaaS, used as a visibility and monitoring tool rather than for prevention and compliance. CWPPs focus on the protection of workloads themselves — OS, VM or containers — rather than how the infrastructure running these workloads is managed and configured.

CSPMs — Built For IaaS Security

PURPOSE-BUILT FOR THE CLOUD

CSPMs are built to address the unique nature these risks pose in a modern cloud deployment. As such, their areas of coverage are aligned with and match the most important risks organizations face in the cloud.

With the understanding that cloud deployments are the business of different functional teams, CSPMs come built-in with a variety of requirements, workflows, specializations and expertise. This facilitates easier implementation of cloud risk management, with CSPMs handling most of the integration and translating of requirements between Compliance, Security, and Development teams.

INTEGRATED INTO THE CSP FABRIC

Secondly, the technical approach taken by CSPMs to assess these risks — that of integrating directly with a CSP's APIs, rather than using agents or a proxy — gives them unparalleled visibility into the configuration of the cloud environment. Assessments are based on accurate, trustworthy, up-to-date, and comprehensive data coming directly from the CSP itself.

What To Look For In A CSPM?

RESOURCE VISIBILITY

How do you protect what you can't see? The importance of visibility into your cloud workloads is without equal. A CSPM should continuously scan cloud environments for services, sensitive data, and instances that would otherwise be invisible and vulnerable to exploits.

RISK COVERAGE PRIORITIZATION

If everything is high-priority, nothing is. A CSPM needs to recognize and provide comprehensive coverage of the cloud services most used by your organization. It is important for the CSPM provider to flag the areas of excessive risk through ontinuous scanning. This not only gives a snapshot of security posture, but also provides direction to the respective teams to address the risks.

AUTHORIZATION & AUTHENTICATION CHECKS

Nobody in your organization needs more power than their role requires. Anything excess is unnecessary security risk. Look for a CSPM that is able to assess your accounts and services for excessive entitlements, and suggest authorization policies based on the principle of least privilege.

BUILT-IN COMPLIANCE REPORTING

Every organization has different compliance requirements and may face specific regulations in their place of business. CSPMs can extend the compliance support for recognized frameworks and standards including PCI DSS, ISO 27001, NIST, and GDPR. Some CSPMs even provide region or country-specific compliance support, allowing their customers to service their compliance needs in an all-in-one tool.

Some CSPMs go a step further and offer built-in compliance reporting for auditors, providing the auditor with complete mapping to the common compliance requirements.

RISK MANAGEMENT

CSPMs are built on the best practices and well-architected frameworks belonging to CSPs. On top of the risk flagging, CSPMs ought to provide the ability to modify risk ratings and prioritize remediation of these risks according to the organization's specific needs.

SECURITY POSTURE OVER TIME

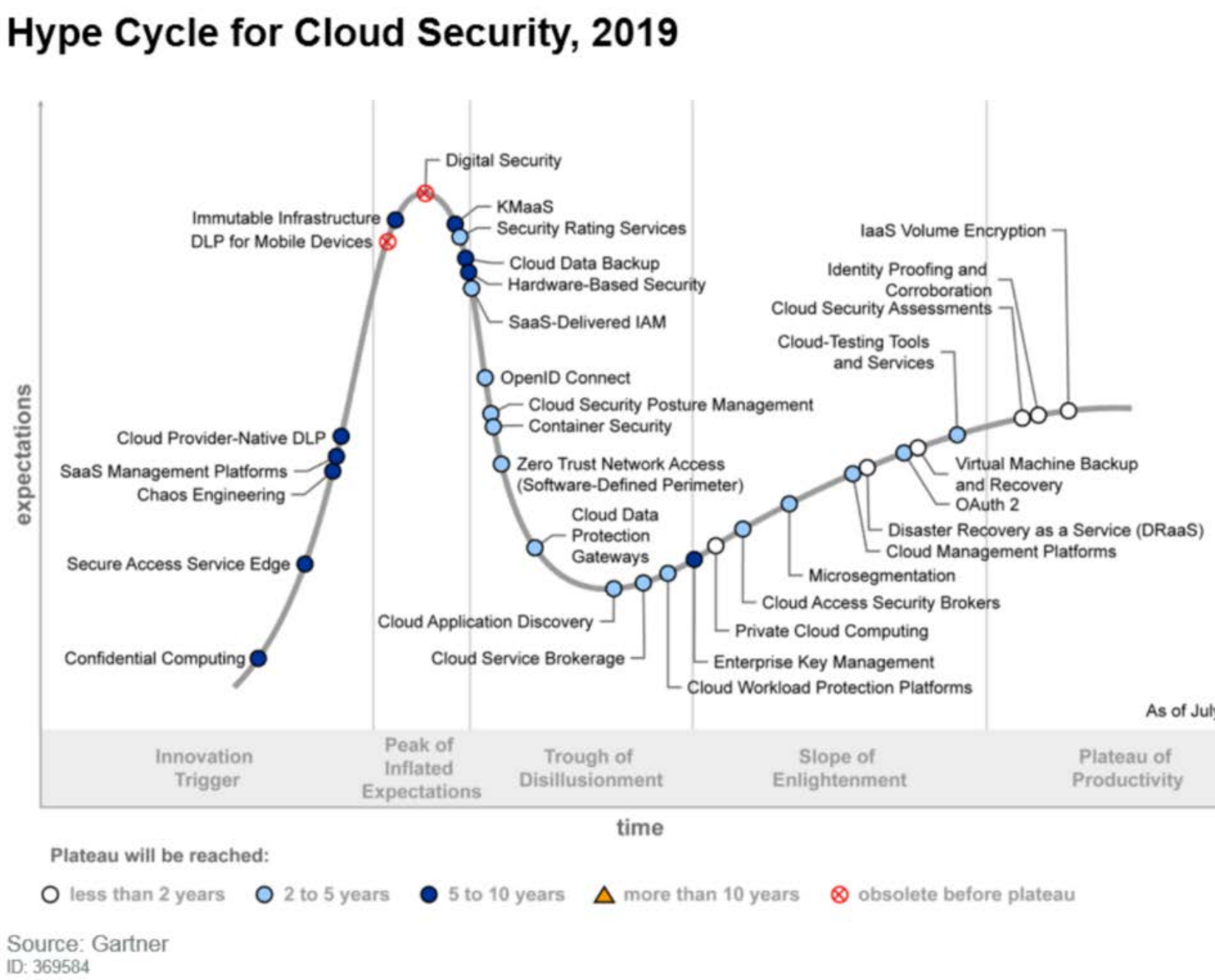
The ability to track historical information and past configurations facilitate digital forensics and incident response initiatives. CSPMs should be able to provide that evolution of security posture over time. Advanced CSPMs are able to identify trends in configuration logs, helping to translate that information into automated risk prioritization.

3. CSPM Vendors Today

CSPM ADOPTION CHART

According to the Cloud Security Hype Cycle by Gartner 2019, CSPM as a solution is just starting its third phase — the Trough of Disillusionment — and is expected to reach its plateau of mainstream usage within 2-5 years.

Before CSPM becomes mainstream, early adopters can get ahead of the curve by integrating the automated cloud security checks and remediations into your DevSecOps and compliance workflows. Especially as organizations look to adopt multi-cloud environments, it becomes crucial to find a CSPM solution that can accommodate both your CSP as well as your compliance needs.



Source: Gartner
ID: 369584

Warden, Horangi's CSPM solution

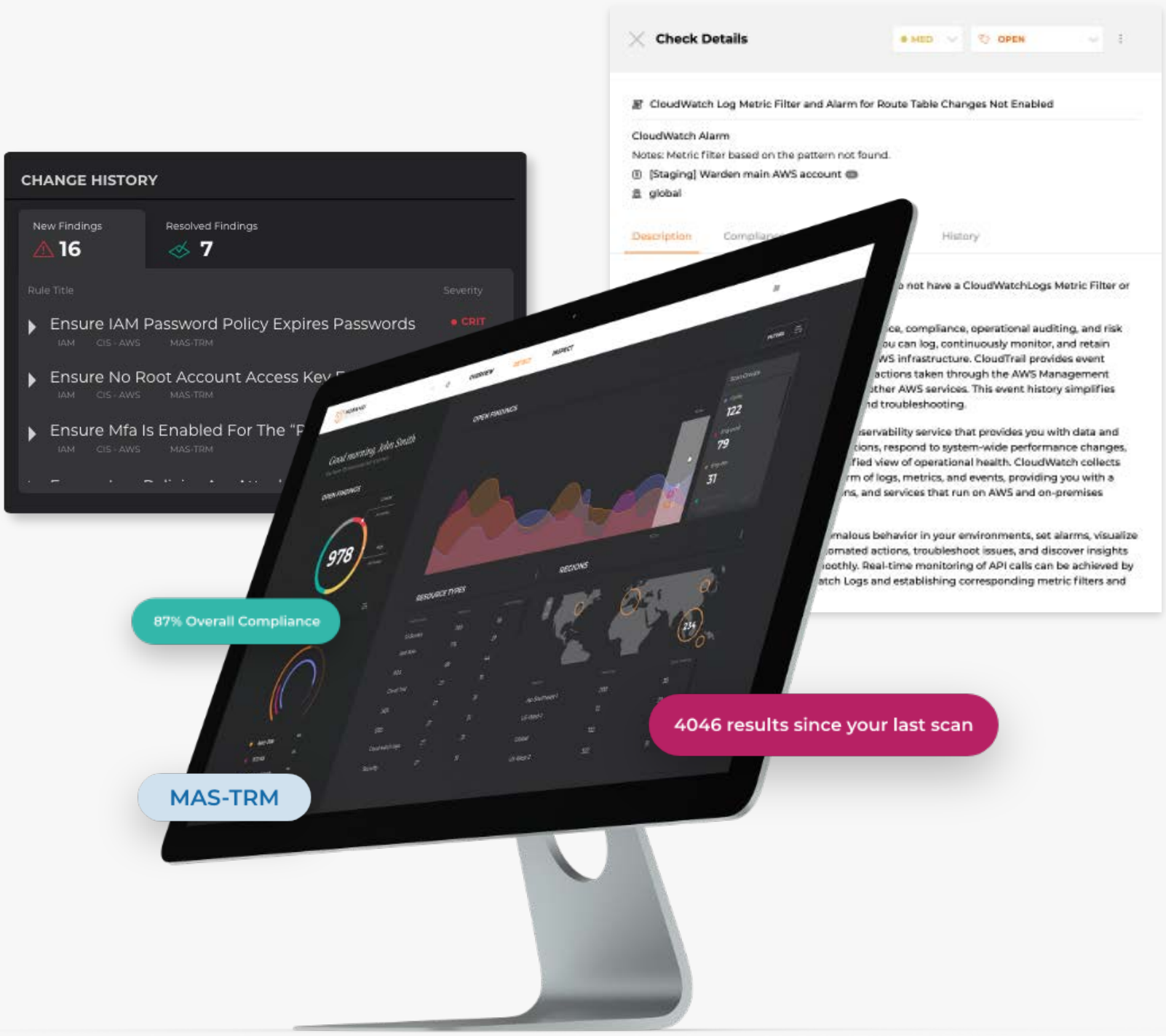
Horangi Warden helps organizations on AWS and GCP manage their security and compliance risks without requiring any cloud security expertise. For ease of procurement and billing, Horangi Warden can be purchased directly from AWS Marketplace. While usable from anywhere in the world, Warden is especially relevant for organizations based in Asia because of the unique compliance standards supported, namely MAS TRM, MAS Cyber Hygiene, and BNM-RMiT aside from international standards such as PCI-DSS and ISO 27001.

Warden provides visibility of cloud posture across the major AWS and GCP resources including IAM, Amazon S3, ElasticSearch, ELBv2, CloudFront, Cloud Storage, Compute Engine, Firewall Rules, and more. Risky configurations are automatically detected and alerts are sent to the team in charge, complete with risk prioritization and actionable remediation steps for DevOps to triage issues. This is supported by Warden's integration with Slack, Jira, GitHub, GitLab, and Bitbucket.

For its depth in cloud compliance automation, Warden is named in the Gartner 2020 Market Guide for Compliance Automation Tools in DevOps.

FREE TRIAL

REQUEST A DEMO



CSPM Vendor Comparison Chart

Unlike Warden's unique place in Asia, the majority of CSPM vendors are based in the U.S. and Australia. Several of these vendors, including Dome9 and DivvyCloud, offer a large array of features that is reflected in the cost. To help you do a comparison, we have picked Palo Alto Network's Prisma Cloud and Qualys so you get an accurate feature-for-feature breakdown.

	Palo Alto Networks Prisma Cloud (Redlock)	**Horangi Warden**	**Qualys Cloud Security Assessment**
CSPs supported	AWS, GCP, Azure, AliCloud, IBM Cloud	AWS, GCP	AWS, GCP, Azure
Integrations	APIs, JIRA, Email, Slack, Splunk, PagerDuty, Microsoft Teams, AWS GuardDuty, AWS Inspector, GCP Security Command Center, CSV Exports	JIRA, GitHub, GitLab, BitBucket, Email, Slack, CSV Exports	APIs, CSV Exports
Visibility	Asset Inventory, Historical View, Resource Map Visualization, Tagging	Asset Inventory, Change History	Asset Inventory, Historical View
Security rules and scan frequency	Hundreds of policies Scans every 45 minutes	160 rules on AWS 70 rules on GCP Scanned daily	159 rules on AWS 84 rules on Azure 15 rules on GCP Scanned daily
AWS Security coverage	Information not found	IAM, S3, ElasticSearch, ELBv2, ELB, CloudFront, EC2, VPC, KMS, CloudWatch, EFZS, EBS, SNS, SageMaker, SQS, Lambda, Kinesis, DynamoDB, AWS Config, AWS GuardDuty, RDS, CloudTrail, ElastiCache	S3, RDS, IAM, CloudTrail, VPC, AWS Config, Lambda
GCP Security coverage	Information not found	IAM, Audit Logging, KMS, Logs Router, Logs-based metrics, Storage Network, Firewall rules. Subnetwork. Cloud SQL. VM Instances, Persistent Disk, BigQuery, Cloud DNS, GKE	IAM, Audit Logging, KMS, Logs Router. Logs-based metrics, Storage, Network, Firewall rules. Subnetwork, Cloud SQL, Cloud Functions, VM Instances, BigQuery. Cloud DNS, GKE
Compliance Standards Supported	CIS, CSA CCM, HIPAA, NIST 800.53, PCI DSS, SOC 2, GDPR, NIST CSF, HITRUST	CIS-AWS, CIS-GCP, PCI-DSS, GDPR, MAS-TRM, MAS Cyber Hygiene, NIST, AWS Well-Architected Framework, BNM-RMiT, ISO 27001, APRA, CIS-GKE (Q4 2020)	CIS-AWS, AWS Best Practices, AWS Lambda Best Practices, CIS-Azure, Azure Best Practices, CIS-GCP
Compliance Report Availability	Report downloadable as a PDF and interactive on the Web	Report downloadable as an Excel file and interactive on the Web	Report not downloadable. Static report visible on the Web ("Mandate Based Reports")
Risk Management	Information not found	Risk profiles editable with ability to log notes	No
Audit Log	Yes	Yes	Information not found
Remediation	Auto remediation	Playbook remediations, One-Click Remediations (Q4 2020)	No
Risk Profile Description	Low	High	Low
Pricing model (AWS)	Per 100 workloads[3] 9000 USD yearly (AWS Marketplace) per 100 workloads	Per cloud account subscription 300 USD monthly per cloud account	Per cloud account subscription by 5 account increments (AWS Marketplace - US only) 113 USD monthly based on 10 cloud accounts 1130 USD yearly based on 10 cloud accounts

[3] A cloud workload is a discrete capability or amount of work run on a cloud instance eg. a container, web server, hadoop node.

Cloud Automation On The Rise

The more organizations move their services to the public cloud, the more pertinent it is to leverage scalable solutions for secure configurations. When infrastructure and data is spread out across hundreds of different services, the need for automation of cloud configuration checks is stronger than ever.

CSPM tools from both CSPs and third party vendors will continue to rapidly develop, and the acquisitions by Trend Micro and Palo Alto Networks are a testament to this critical market. Organizations who already own CASB or CWPP solutions need to assess if the basic features there are sufficient for their growing infrastructure needs.

We hope this whitepaper has shed light on the important role of CSPM tools and the features organizations need to look out for in their purchase consideration. Continuously take stock of your security risks and your IaaS needs down the line in order to pick a vendor that you can establish a long-lasting relationship with.