WHITE PAPER

AS CLOUD ADOPTION ACCELERATES, SECURITY MUST KEEP PACE

Cloud security posture management tools ensure compliance and monitor real-time threats in evolving cloud environments.

EXECUTIVE SUMMARY

Cloud security requires the same level of governance, compliance and risk management that organizations apply to on-premises security, yet it often falls short of that objective.

Numerous factors make it difficult to mitigate cloud risk manually, but poor visibility and a lack of staff expertise are two of the most common. The nature of public clouds themselves can pose challenges: Each service provider has distinct default configurations, and providers are continually making changes to their environments.

As a result, many IT departments find it difficult to confidently and effectively assess the security of a given cloud environment, let alone take action to reduce that risk.

A risk-based approach to cloud procurement and operation is essential, however. It allows organizations to leverage the significant benefits of the cloud without jeopardizing their data assets, financial resources, compliance and reputation.

Multicloud environments are both powerful and complex, and they do pose unique security considerations, particularly with regard to configuration. The need for better control and visibility drives many organizations to deploy a cloud security posture management platform. CSPM tools examine cloud security configurations and compare them against best practices and compliance frameworks to identify (and, depending on the solution, automatically correct) any gaps.

The Changing Landscape of Cloud Security

One of the most telling statistics about cloud security comes from the Cloud Security Alliance's 2021 report, "State of Cloud Security Concerns, Challenges and Incidents." When asked whether their organizations had experienced a cloud security incident in the past year, 41 percent of respondents said they did not know. "Unsure" was the most common response, and that percentage had doubled since 2019.

Now, consider that the average organization has workloads placed with two or more public cloud providers, according to the SANS Institute's "Extending DevSecOps Security Controls into the Cloud: A SANS Survey."

Together, these trends represent a dangerous combination: increased reliance on multicloud environments, impaired by a lack of knowledge about security. This is, further, a problem that is difficult to solve manually.

This challenge is the primary reason organizations are turning to cloud security posture management platforms: CSPM solutions provide visibility and automation to identify and remediate cloud-based vulnerabilities. They allow organizations to leverage the cloud within risk management parameters that protect cloud-based resources just as diligently as those on-premises.

The Multicloud Expansion

The landscape for computing, and cloud's place in it, has changed immensely over the past decade. Virtualization was a significant shift, first in on-premises data centers and now in the cloud, with Infrastructure as a Service and Platform as a Service. Containers helped to build out IaaS and PaaS further, as did widespread adoption of high-speed internet.

Many organizations with significant IT needs moved their infrastructure into data centers, creating private clouds while retaining data center ownership.

The percentage of organizations that apply orchestration and configuration management tools to cloud security[1]

Virtualization allowed cloud providers to offer private clouds, which delivered improvements in scalability, flexibility, reliability and other areas. Now, public cloud providers deliver the same capabilities while removing the burden of hardware management. This enables environments such as serverless architectures, which make it possible for many organizations not to own their infrastructure.

An array of benefits spurred this evolution. Among them:

- Cloud computing provides economies of scale.
- The shift from capital expenditure to operational expenditure models changes the ROI conversation by making it possible for organizations to buy only what they need and pivot quickly and easily.
- Cloud providers take on infrastructure management, which significantly reduces the burden on IT departments.
- The cloud offers better uptime and business continuity, facilitating the resilience organizations need to adapt and thrive.
- Public clouds offer cost savings.

The Pandemic Effect

The pandemic unquestionably accelerated cloud adoption. The same agility and scalability that served organizations well before the pandemic became critical to support large-scale remote work. With organizations reaping the benefits of this approach across nearly every industry, cloud adoption will continue to rise. Gartner predicts a 23 percent increase in public cloud spending in 2021, with the largest categories being Software as a Service, IaaS and PaaS.

The SANS Institute's "The State of Cloud Security: Results of the SANS 2020 Cloud Security Survey" documents the widespread (and growing) reliance on the cloud. More than 65 percent of organizations surveyed were already

Source: [1]Cloud Security Alliance, "State of Cloud Security Concerns, Challenges and Incidents," March 2021

using cloud, multicloud or hybrid environments, and 84 percent expected to migrate to cloud-based models within one year.

Lasting consequences of the pandemic will cement this expansion further. One is a recognition that organizations will need to be technologically agile to survive and adapt to future disruptions, whether those arise from pandemics, natural disasters or other causes. Another driver, of course, is the widespread expectation that higher levels of remote and hybrid work will continue.

Eighty-three percent of employers report that remote work has been successful, and only 17 percent anticipate a complete return to fully in-person work, according to PwC's US Remote Work Survey. In education, particularly at the college level, many institutions are reformulating their offerings in ways that allow for the continuation of distance learning. Finally, government agencies have continued their strong adoption of the cloud.

All these factors indicate that organizations should be maturing their cloud environments not only technologically, but also strategically: developing security strategies and governance processes, and establishing best practices throughout.

Building Cloud-Specific Threat Intelligence

Rapid response to potential threats is imperative, but security teams must also plan for the long term. How will organizations continue to deepen expertise and refine their defenses as the cloud (and attacks against it) continue to evolve?

"The cloud shifts threat detection in a number of ways," the SANS Institute notes.

Addressing that shift requires IT departments to develop a comprehensive threat analysis; increase their use of cloud-native intelligence, such as IPS signatures, behavior patterns and other elements; and emphasize cloud-specific events and scenarios.

To build on this intelligence and establish a robust cloud security program, the SANS Institute recommends creating a comprehensive model, or ecosystem, to gather, analyze and manage cloud threat intelligence. Follow these best practices:

- Review data sources, both internal and external, to ensure data is appropriate and accurate.
- Verify that integration is functional; that is, ensure that data from cloud events is going to security analysis services as intended.
- Perform event reviews to ensure that any event data updates properly and furnishes enough detail to inform analysis and investigation.
- Validate information related to cloud security events, with an eye toward capturing all relevant data.
- Assess value periodically to ensure threat intelligence activities yield "useful, actionable and timely" insights.

The Costs of a Breach

Despite the many benefits of the cloud, organizations that increase their cloud use need to address a major hurdle: A broader presence in cloud creates a larger attack surface and increases vulnerability.

Well-publicized cloud breaches have borne this out. IBM's most recent annual study of data breaches, "Cost of a Data Breach Report 2021," states that organizations in a mature stage of cloud modernization took an average of 252 days to detect and contain a breach. Those in the early and middle stages of cloud modernization took even longer: 329 and 278 days, respectively. When breaches do happen, they're expensive: $4.8 million, on average, in the public cloud and $3.6 million in a hybrid cloud.

The financial impact, of course, is just one consequence. Others may include:

- Loss of intellectual property
- Fines and legal ramifications arising from regulatory noncompliance
- Downtime related to breach containment and systems rebuilding
- Reputational impact and reduced trust among the public, customers and partners

In analyzing the vulnerabilities that most often lead to cloud breaches, the National Security Agency identified four categories:

- Misconfiguration
- Poor access control
- Shared tenancy vulnerabilities
- Supply chain vulnerabilities

"Cloud vulnerabilities are similar to those in traditional architectures, but the cloud characteristics of shared tenancy and potentially ubiquitous access can increase the risk of exploitation," the NSA notes.

Although organizations can take steps to minimize risk arising from shared tenancy and supply chain vulnerabilities, the primary areas of risk mitigation within their control are configuration and access control.

Closing the Gap

Within the shared responsibility model, one of the most important tasks for organizations is the proper configuration of application-level security. Misconfigurations are one of the most common sources of data breaches, so it is imperative for organizations to get this task right.

The problem is that, for many organizations, lack of visibility and control, exacerbated by a deficiency in cloud security expertise, make it nearly impossible to configure cloud environments correctly and to consistently apply security controls and policies.

For example, one of the most common types of attack against IaaS virtual machines is a Remote Desktop Protocol brute-force attack that strikes exposed ports. In one study, 10 RDP honeypots on a major public cloud secured their first probe within two minutes. By the end of day one, all 10 honeypots had been attacked, ramping up to 4.3 million attempted logins within the month. Proper configuration would disable ports that should not

be exposed, restrict access to trusted IPs, impose multifactor authentication and monitor for these types of suspicious activity.

Secure Shell is another common vulnerability, with SSH servers open at approximately one-third of exposed public cloud hosts. SSH access lures attackers who are eager to install cryptocurrency mining software, exfiltrate data or leverage an opening to inflict other types of damage. Better security would eliminate unrestricted access, require stronger authentication and, again, monitor for red flags.

In the absence of a holistic, proactive cloud security strategy, vulnerabilities like these are almost certain to occur, especially when cloud environments are known to be susceptible to breaches. As of this year, in fact, Verizon's "2021 Data Breach Investigations Report" found that external cloud assets were involved in cybersecurity incidents and data breaches more commonly than on-premises assets.

What Is Cloud Security Posture Management?

CSPM solutions help organizations solve potential liabilities related to visibility, configuration, compliance and ongoing management of the cloud environment. Without question, these challenges are exacerbated by a lack of experienced cybersecurity professionals in general and by a dearth of cloud security experts in particular. Research from the Cloud Security Alliance shows that staffing-related issues (a lack of cloud expertise and insufficient staff to manage cloud environments) are among the top concerns about cloud adoption.

CSPM technology addresses these issues by supporting adherence to security best practices and regulatory requirements, facilitating inventory management, and providing log and alert capabilities. These and other functions explain why CSPM is among the top three recommended technologies in Gartner's "Hype Cycle for Cloud Security, 2020," together with secure access service edge and cloud access security brokers.

As an agentless solution based on SaaS, CSPM tools make calls via an application programming interface to examine how cloud services are configured in comparison with cloud security best practices. In doing so, they essentially provide governance, risk management and compliance (GRC) capabilities for cloud environments.

Establishment of a GRC foundation is important in any case, but particularly because cloud environments can be opaque. All too often, organizations lack critical knowledge about the cloud environments they are using and the assets stored therein. Research has shown, for instance, that organizations use an average of 1,935 unique cloud services — but most organizations estimate that they use approximately 30.

Organizations that have deployed CSPM tools have discovered:

- Data in the cloud that is not encrypted, but should be
- Data in the cloud that is publicly accessible, but should not be
- Activity in the cloud that is not being logged or monitored appropriately
- User/identity configurations that do not follow security best practices

In addition to visibility, CSPM tools deliver:

- **Configuration management:** Public cloud providers continuously adapt and evolve their environments, which means that default configurations and other critical settings also change. CSPM tools assess environments against target compliance or security rules and alert IT staff or automatically make the necessary fixes. Proactive identification and elimination of improper configuration is a must, because it reduces one of the largest sources of cloud risk.
- **Alerting, monitoring and notification:** Threat intelligence is a broad umbrella, encompassing data related to threats and vulnerabilities, as well as bad actors, exploits, malware and indicators of suspicious activity or compromised systems. The concept is certainly not new, but it has taken on renewed importance in relation to the cloud. As organizations establish a cloud-specific threat intelligence program, CSPM solutions can serve as a foundational component. Better intelligence makes it possible to resolve security events faster and more effectively, while providing insights to further enhance strategy.
- **Multicloud support:** There are many reasons why multicloud has become the norm, but its benefits come with an added layer of complexity. When multiple cloud services communicate with each other, the landscape becomes even

SaaS Security Posture Management

SaaS is the largest category of public cloud spending in 2021, according to Gartner, representing a $122.6. billion market that is projected to reach $145.4 billion in 2022.

As with other cloud services, SaaS is subject to shared responsibility. Providers may handle some aspects of infrastructure and security, but organizations take ownership of key security tasks, such as classifying data correctly and establishing identity and access management controls.

In doing so, organizations often confront a familiar litany of challenges: poor visibility, limited control over data and the insurmountable task of manually adjusting the hundreds of settings that may exist in a single platform. Some organizations rely on the native security support of the SaaS platform. However, this approach may not provide the necessary assurance that configurations and compliance are in order and that data is protected.

To overcome these hurdles, organizations may deploy SaaS security posture management (SSPM) tools, which serve a similar function as CSPM: assessing risk and managing security posture. SSPM uses automation to ensure that security configurations align — and stay aligned — with organizational policy, compliance requirements and best practices.

With so many critical workloads, SaaS warrants the same scrutiny and risk management that organizations apply to the rest of their sensitive data.

more difficult to parse. CSPM restores control and oversight to cloud ecosystems that can quickly feel unmanageable if they are not subject to proper controls.

- **Continuous compliance:** Many organizations must comply with regulatory requirements, such as HIPAA or the General Data Protection Regulation, that apply highly specific requirements to cloud security. CSPM tools assess compliance against specific sets of rules and best practices. Equally important, organizations can choose to have CSPM tools automatically make corrections to maintain compliance, even as circumstances shift either within the requirements or the cloud environment.

The CSPM market has grown relatively quickly, making it easier for organizations to find the capabilities and features that best complement their environments or advance specific objectives. Some tools assess multiple platforms and specific types of platforms, while others look at containers.

Test-Drive a CSPM with a Custom Assessment

CDW's complimentary Cloud Security Posture Assessment provides visibility into cloud environments, plus analysis and recommendations to enhance security — information that empowers organizations to immediately mitigate risky misconfigurations.

The assessment starts with a discussion of the organization's goals, followed by a kickoff call with an assessment lead. CDW then onboards the organization to an industry-leading CSPM solution and, as needed, provides ongoing support during the assessment. This read-only connection lets CDW see only information about how the cloud is configured, not any data inside the cloud.

The organization's IT staff can test-drive the tool to see how it works in their environment.

Organizations may have several reasons to request an assessment:

- Ensure configurations are secure across cloud platforms
- Evaluate compliance with regulatory requirements
- Gain hands-on experience with a variety of CSPM tools
- Get help analyzing findings and making recommendations
- Obtain quick, actionable information that addresses time constraints, knowledge gaps and lack of visibility

After this guided trial of the CSPM solution, CDW shares its findings and recommendations in a brief presentation, including guidance on which issues to prioritize. In addition, the organization can export a variety of compliance framework reports.

Organizations may choose to augment the value of this assessment by pairing it with an annual penetration test.

Distinguishing features of individual CSPM solutions may include:

- Enhanced visibility into cloud costs
- Cost optimization capabilities
- Emphasis on seamless compliance and governance
- Network visualizations that depict trust relationships and guide remediations
- Threat remediation capabilities, including integrated cross-team capabilities
- Compatibility with other cloud security tools
- Robust customization of rules and reports, allowing for more granular control and analysis

Strategies for Effective CSPM

In general, cloud security strategies should incorporate the same fundamentals as on-premises security: defense in depth; least-privilege access controls; and the exercise of continuous, adaptive monitoring and management. Two additional principles define the tactics and the value that CSPM delivers: automation and visibility. Organizations will gain the most from these tools by choosing a solution that best aligns these core capabilities with their unique IT and business needs.

Automation

Research shows that many IT professionals are concerned they are not adequately leveraging automation to effectively manage their cloud infrastructures. Faced with the persistent gap between consistent, reliable data protection and the shifting sands of the cloud, these professionals recognize that where manual processes are insufficient, automation is key.

CSPM tools address this concern by automating an organization's GRC for the cloud. Automation minimizes the burden on IT staff, which in itself is a significant advantage. But it also gives organizations a fighting chance against attackers, who are arming themselves with the same powerful tools.

"In the same way automation may be helping you scale up your defensive operations, it can also help attackers scale up their offense," as noted in Verizon's "2021 Data Breach Investigations Report."

Automated capabilities include:

- **Cloud asset inventory:** CSPM tools provide continuous visibility across all deployed assets from a single, unified console. They can automate both workload and application classification and full lifecycle asset change attribution.
- **Configuration assessment:** Many CSPM solutions can enforce configuration policies across multiple cloud services and fix common misconfigurations before they lead to security incidents. Some CSPM platforms allow users to build custom rule sets and reports. All CSPM tools can flag misconfigurations, and many can also enforce policies through auto-remediation. Some solutions allow users to build custom rule sets and reports.
- **Compliance management:** Continuous compliance posture monitoring for a variety of standards and frameworks helps to investigate and remediate compliance violations.
- **Automated remediation:** CSPM can automatically resolve policy violations, such as misconfigured security groups.

Visibility

A need for greater visibility, particularly in hybrid and multicloud environments, is consistently the top driver for adoption of cloud security posture management tools.

Visibility is broader, however, than simply understanding the cloud environment from a security perspective. The reporting features of CSPM tools deliver visibility that is actionable, both within the specific cloud environment itself and, more broadly, for the organization's overall cloud and security strategies.

From a practical perspective, reporting is a key CSPM capability that helps organizations prioritize issues. By identifying which concerns are most important and what steps need to be taken to address them, CSPM solutions provide IT teams with a launch point and a road map for remediation.

Getting Started

Organizations should start by determining whether CSPM is appropriate for their needs. The first questions to ask are "Do you have IaaS?" and "Are you using cloud services that require CSPM?" To get the most from these solutions, organizations need to be engaged with the cloud beyond SaaS. (Organizations that consume only SaaS services should consider SSPM tools to assess the configurations of SaaS applications.)

An assessment can help organizations determine which CSPM tool makes the most sense for a specific environment. Third-party partners can provide insight into the capabilities of various CSPM offerings, as well as how to use them to improve the cloud environment and remediate security issues.

Ultimately, CSPM is one component of an overarching cloud security strategy. It brings cloud security under the same stringent protections that govern on-premises security, making governance and risk management an integral, ongoing aspect of cloud operations. As CSPM solutions check the most critical boxes for cloud security (visibility, control, proper configuration and automation to augment staff limitations) they allow organizations to take full advantage of the power of the cloud.

CDW: We Get Cloud Security

CDW helps organizations manage their cloud security infrastructure and leverage technologies, in concert with strategy, to keep data secure. Our years of experience, industry-leading expertise and partnerships with leading technology providers help organizations create a custom cybersecurity solution that dynamically addresses vulnerabilities.

Our team has capabilities for support in:

- **Design:** Our security consultants offer comprehensive assessments of organizations' environments and build strategies that address their unique requirements.
- **Orchestration:** Our certified engineers can assist with everything from simple anti-virus installation to sophisticated network segmentation, ensuring operational continuity and reliable protection.
- **Management:** Our managed services team can help automate routine cybersecurity procedures and ease the burden on your IT staff.

CDW's complimentary Cloud Security Posture Assessment lets organizations try CSPM tools in their own environments and then receive an analysis of the results.

CDW AMPLIFIED™ Services

CDW Amplified™ Security services are composed of both information security and network security practices, offer an objective look at your current security posture and provide continuous defense against, detection of and response to growing threats.

DESIGN for the Future
All CDW Amplified Security services provide a comprehensive approach to prevent data breaches and proactively respond to cyberattacks.

ORCHESTRATE Progress
CDW Amplified Security engineers can assist with installation and deployment of advanced security techniques and ensure technologies are optimized for your needs.

MANAGE Operations
We can manage security solutions for you, helping you stay vigilant and maintain compliance while easing the burden on your IT staff.

Sponsors

Barracuda · Cisco Partner · Check Point Software Technologies Ltd. · Trend Micro

Learn how Cloud Security Posture Management can protect your data and workloads.

CDW PEOPLE WHO GET IT