WHITE PAPER

MANAGE YOUR CLOUD SECURITY POSTURE EFFECTIVELY

Finding the right solutions for your environment is essential to protecting cloud data and workloads.

EXECUTIVE SUMMARY

Organizations across industries are deploying new cloud services almost daily. Whether they're choosing a cloud infrastructure provider for the deployment of large-scale cloud data centers or selecting a Software as a Service provider for payroll processing, each of these decisions alters the organization's cloud security posture. The adoption of a new service creates new risks to the confidentiality, integrity and availability of sensitive data, and cybersecurity professionals must adapt quickly to manage these risks.

Cloud security posture management (CSPM) tools are designed to help cybersecurity professionals identify and manage these risks. They reach directly into cloud solutions to analyze configurations and detect potential security issues before an incident occurs, allowing cybersecurity teams to track their risk mitigation efforts and rapidly identify new vulnerabilities when they arise.

Top-tier CSPM solutions share several key features. First and foremost, they must integrate directly with the cloud services that are most important to an organization. They then provide the ability to build an inventory of cloud configurations and map the current status of those configurations to security control frameworks and regulatory standards adopted by the organization. CSPM solutions support the DevOps model by providing automation capabilities that facilitate the prompt remediation of detected issues.

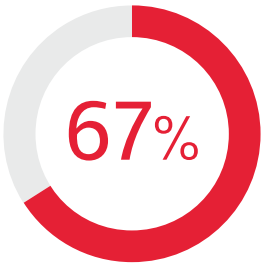
As organizations adopt an increasing number of cloud services, identifying the CSPM tool that best meets their needs is essential.

The Importance of Cloud Security

Cloud computing has played a significant role in the technology stacks of many businesses for more than a decade. Many organizations began their cloud deployments with the rollout of cloud-based email services 10 or 15 years ago and have continued to adopt a variety of cloud solutions that meet their business needs. In recent years, these adoption patterns have evolved from opportunistic shifts to Software as a Service solutions that meet a specific need to larger-scale deployments of custom-built Infrastructure as a Service and Platform as a Service solutions that serve the majority of an organization's computing needs.

These shifting adoption patterns have broad implications for cybersecurity. Organizations operating in multiple cloud and on-premises environments now manage significantly more complex computing environments than they did a decade ago. That complexity is amplified when enterprises adopt multicloud or hybrid solutions that attempt to seamlessly shift workloads among providers on demand. Cybersecurity professionals, charged with protecting the confidentiality, integrity and availability of sensitive information and resources, find themselves attempting to meet similar goals as they did a decade ago but in a far more technically complex environment that requires coordination with both cloud service providers and security vendors. This complexity extends beyond direct cybersecurity objectives and increases the burden of maintaining and documenting regulatory compliance.

While many organizations were already moving rapidly down the path of cloud adoption at the beginning of 2020, the coronavirus pandemic played a major role in accelerating those implementations. As organizations struggled with their inability to maintain on-premises data centers and their need to support hastily designed remote work and digital collaboration solutions, they turned to the cloud for the agility and flexibility it provides. However, this push caused some organizations to adopt cloud solutions more rapidly than they had planned, and without the rigorous preparation they might conduct under normal circumstances. This rapid shift to the cloud places organizations in a precarious security position. Worse yet, these organizations may not even be aware of how the shift to the cloud has affected their security posture.



The percentage of security professionals who cited compliance and a lack of visibility into cloud infrastructure security as among their leading operational cloud security headaches[1]

Cloud Security Technologies

Fortunately, cybersecurity teams don't need to navigate these waters on their own. Cloud security vendors offer an array of solutions designed to improve the way that organizations manage their cloud implementations and to help identify cloud security issues. Typically, these products directly integrate with other elements of an organization's cybersecurity infrastructure, providing streamlined alerting, tracking and remediation capabilities. In an era when organizations are increasingly turning to automation to improve the agility and efficiency of their IT teams, this integrated approach is crucial to security in general, and cloud security in particular.

Cloud access security broker solutions often top the list for security

Source: [1]Check Point, "2019 Cloud Security Report," July 2019

professionals seeking to bring their cloud security posture under control. CASBs are policy enforcement tools that integrate with a wide variety of cloud service providers, allowing cybersecurity teams to specify security policies in a centralized location using a single interface and then automatically enforce those policies across the range of cloud services that the organization uses. CASBs play an increasingly important role in the modern Software as a Service–based organization, where teams might overlook the nuances of product-specific security solutions. Through direct integrations with service providers, the CASB intercepts and blocks user requests that would violate security policies.

Multifactor authentication is already an important component of the cybersecurity programs at most organizations. MFA has come into widespread use over the past five years, as phishing, password spraying and credential stuffing attacks rendered simple password-based security mechanisms ineffective. By supplementing passwords with a "something you have" or "something you are" factor, MFA solutions strengthen authentication and provide strong protection against all types of credential theft. Organizations should work with their cloud service providers to ensure that their solutions incorporate MFA and, preferably, allow a direct integration with the organization's own identity and access management infrastructure to provide additional security and control over user accounts.

Understanding Cloud Service Models

Cloud service providers operate under a variety of deployment models that offer customers differing levels of service and customizability. The three major cloud service models are:

- **Infrastructure as a Service.** IaaS provides customers access to the basic building blocks of cloud computing. These include server capacity, storage, network bandwidth and related service offerings. Customers use these foundational offerings to build their own technology solutions in the cloud. IaaS providers include Amazon Web Services, Microsoft Azure and Google Cloud Platform.
- **Software as a Service.** SaaS offers customers access to a managed application in the cloud. The provider manages all of the infrastructure details and installs, configures and maintains the application. The customer typically bears responsibility only for configuration decisions within the application itself, such as customizing settings and managing user accounts. Examples of SaaS offerings include Google Apps, Workday and Salesforce.
- **Platform as a Service.** PaaS offerings fit somewhere in between IaaS and SaaS. They provide the customer with access to a managed computing platform where the customer may execute its own code with little concern for the underlying infrastructure. PaaS solutions vary widely, and the line between PaaS and SaaS/IaaS is easily blurred.

Information is the lifeblood of a cybersecurity program. Security information and event management solutions depend on a steady flow of timely, relevant security information to detect and react to unusual activity. Cybersecurity teams are generally familiar with the process of configuring on-premises solutions to report security events to the SIEM for correlation and analysis, but they often run into stumbling blocks when attempting to achieve the same level of visibility into cloud solutions. As organizations evaluate prospective cloud service providers, they should consider the level of visibility they will have into security information to be a key purchase criterion.

Every cybersecurity professional understands the importance of promptly applying new security patches and maintaining secure system and application configurations. Unpatched and misconfigured systems are the root cause of many security incidents, and seemingly minor oversights can have disastrous results. Patch and configuration management is just as important in the cloud as it is in on-premises environments. Organizations can meet many of their cloud patching and configuration management requirements using the same technology they use on-premises. For example, they might use their standard server management tools to maintain servers both onsite and in an Infrastructure as a Service environment. However, some cloud configuration tasks are beyond the reach of these tools and require the use of specialized CSPM solutions.

The cloud brings tremendous advantages to enterprise IT teams, including significant flexibility and agility, along with economies of scale. However, as organizations move to the cloud, it's important that they understand the impact of that move on their cybersecurity posture and continue to develop a cybersecurity program with the tools, technologies and processes required to support secure cloud implementations.

What Is CDW Cloud Check?

As organizations look for solutions to improve their cloud security posture, the importance of a trusted partner becomes clear. For example, CDW Cloud Check provides a valuable service for IT teams considering CSPM solutions.

CDW Cloud Check is a complimentary service available to help IT leaders understand the potential role that CSPM solutions might play in their normal operating environments. Instead of simply providing information and canned demonstrations of the products, CDW Cloud Check allows customers to get hands-on experience with a CSPM tool — not just in a real-world environment, but in *their own* real-world environment.

CDW Cloud Check engagements begin when an organization expresses interest in deploying cloud security tools in its environment. CDW account representatives then work with the organization to select an appropriate CSPM solution for its needs, sharing information about the products available from various vendors and helping the organization's IT leaders choose the CSPM platform that best meets their security and business objectives. During this early stage of the Cloud Check, CDW provides information from the vendor to IT leaders to help them through the decision-making process. When helping an organization select a tool, CDW takes its specific

cloud approach into account, helping IT leaders choose a tool that will work best with the infrastructure of its current cloud provider and the other tools in its cybersecurity ecosystem.

Once the organization selects a CSPM tool to explore, the Cloud Check begins in earnest. CDW helps the organization sign up for a complimentary trial license from the CSPM vendor and assigns an engineer to the project. That engineer gathers the necessary technical information and works hand in hand with the organization's technology team to connect to its cloud environment and install and configure the CSPM tool. CDW cloud security specialists then run the CSPM scan using the organization's selected product.

The CSPM scan provides a detailed look at the organization's current cloud security posture by reaching deeply into its cloud service provider's systems and analyzing the configuration of the cloud services. This includes everything from the network security groups assigned to cloud server instances to the access controls applied to cloud accounts.

Customers almost always find unexpected results from the detailed scan, discovering long-hidden misconfigurations and other security vulnerabilities that might pose a risk to the organization's cloud operations.

The percentage of cybersecurity and IT professionals who cited misconfiguration of cloud platforms among the leading public cloud security threats they faced[2]

Cloud Check analyses are based on industry-standard best practices. CDW begins with guidance from the National Institute of Standards and Technology, the Center for Internet Security, the Cloud Security Alliance and other independent industry standard-bearers. CDW also includes vendor-specific cloud security guidance, such as the implementation guidance from Amazon Web Services, Microsoft Azure and Google Cloud Platform. The selected CSPM solution is then used to compare the customer's existing cloud configuration to that standard, producing a gap analysis that flags any deviation from best practices.

The detailed reports produced by CDW Cloud Check engagements provide organizations with an in-depth look at their current cloud security posture and a prioritized list of possible improvements. The Cloud Check itself isn't designed to help remediate those gaps, but CDW experts are available to provide both consulting and implementation services to address any issues. The goal of the Cloud Check is to give organizations a hands-on look at a CSPM solution in their environment and determine whether it makes sense as a potential new component in their cloud security program.

At the conclusion of the assessment, a CDW solution architect works with the organization's IT team to analyze the outcome of the engagement and identify next steps. If the organization chooses to move forward with a CSPM solution, CDW will seamlessly transition from the Cloud Check engagement into a CSPM implementation project that will acquire permanent licensing for the product and develop both technical and operational plans for integrating the tool into its cybersecurity program. The results of the Cloud Check provide a head start on that work, as the customer is already familiar with the tool and CDW engineers already understand the organization's cloud environment.

Stealth Cloud

As CDW works with organizations to evaluate their cloud security posture, one of the most surprising discoveries they commonly make is that cloud computing has already penetrated more deeply into their operations than they knew or expected. Individual employees and business units often find and adopt cloud computing resources either to meet specific business needs or to bypass what they perceive as the cumbersome bureaucracy of formal IT projects. The adoption of "stealth cloud" approaches to technology is a natural extension of the "shadow IT" phenomenon that has affected centralized IT organizations for years.

Organizations adopting CSPM tools should use their deployment projects to get a handle on the stealth cloud solutions deployed in their environments. This work often requires going beyond purely technical solutions to develop trusting relationships with the business leaders and others who influence cloud adoption across the organization and to educate them about the importance of gaining centralized visibility into the security of their cloud operations. To gain this trust, it's important to reassure them that the CSPM effort is not intended to disrupt their existing use of the cloud, but rather to help them find ways to securely integrate cloud computing into their work.

Essential Capabilities of CSPM Tools

Several vendors offer comprehensive solutions in the CSPM space. As organizations work to select an appropriate tool to incorporate into either a CDW Cloud Check engagement or a permanent CSPM deployment, they should be aware of the essential capabilities of these tools and any available features that can help make their cloud security efforts more effective. Knowing these capabilities and features allows organizations to better select the CSPM tool that will best meet their needs and understand the top benefits of CSPM tools in general.

The most important consideration when selecting a CSPM platform is verifying that the tool supports the cloud environments used by the organization. Most major CSPM platforms now support cloud Infrastructure as a Service providers such as Amazon Web Services, Microsoft Azure and Google Cloud Platform. Enterprises using other cloud providers should verify that the tool supports those providers and that it has a rich-enough integration with them to perform detailed

Source: [2]Check Point, "2020 Cloud Security Report," August 2020

security assessments. As organizations adopt multicloud and hybrid cloud approaches to IT, they should verify that their CSPM tool will work effectively across those environments. Multicloud CSPM solutions should be able to not only validate configurations across all of an organization's providers but also integrate the findings from those environments into a consolidated dashboard.

Another core capability of CSPM tools is their ability to perform assessments against a variety of industry and regulatory standards. The major tools are all capable of performing assessments against the same core set of standards: the Amazon Web Services security framework, National Institute of Standards and Technology cloud security standards and the Payment Card Industry Data Security Standard regulatory requirements for organizations involved in processing credit card transactions. Organizations with specific regulatory needs should determine how well the prospective CSPM solutions support those regulatory standards and the ease of reporting against those standards during internal and third-party audits. Well-designed tools can dramatically simplify the process of preparing for an audit by producing artifacts that validate security controls while directly mapping those controls to the standards used by the auditors. This approach makes the auditors' job easier, reduces the burden on IT teams to produce audit artifacts and improves the overall audit experience for all concerned.

It's common for organizations to have assets deployed in the cloud that fall outside the scope of their existing configuration management tools. Whether they are services that were expected to be set up temporarily but became permanent or they were built by people outside of the central IT unit, these untracked services can pose significant security risks because they are often unmonitored and unmaintained. CSPM solutions include asset inventory and management capabilities that allow organizations to discover what services are deployed in their cloud environments and track those services from initial deployment through deprovisioning.

Another way that CSPM platforms distinguish themselves is in the degree of customization that they allow organizations to perform to tune the tool for use in their technical and regulatory environments. This may be as simple as allowing the creation of customized analysis and reporting templates, or it may be as complex as providing application programming interface (API) integration capabilities that allow direct, real-time interaction between the CSPM and other security tools. This integration allows other tools to trigger CSPM scans and to provide configuration and other information that helps inform the results of a CSPM analysis.

Exposing the capabilities of a CSPM tool through an API also allows a deep integration of CSPM capabilities into a DevOps automation approach to systems and application development. Organizations operating modern software development shops seek to rapidly deploy software and reduce the overhead associated with security analysis and testing. CSPM tools that expose an API may be directly integrated into a DevOps deployment model, automatically triggering an assessment at the time that a new system or code modification is deployed to production and automatically adding new systems to recurring CSPM configuration checks. This approach increases the agility of software development and security teams, and it improves the visibility of the tool into an organization's cloud environment.

CSPM tools also provide the ability to directly integrate with an organization's identity and access management infrastructure. These IAM integrations provide users with a familiar single sign-on experience when they interact with the tool and improve the ability of CSPM administrators to monitor and control user access to the tool. IAM integrations prove especially useful in the provisioning and deprovisioning processes. New administrators may be quickly added to the

Cloud Controls Matrix

Organizations often struggle to identify the appropriate security controls to use in cloud computing environments and, in the case of regulated industries, to map these controls to the specific regulatory requirements that they face. The Cloud Security Alliance is an industry organization dedicated to improving the state of cloud security efforts across verticals. The alliance produces the Cloud Controls Matrix to help both cloud service providers and cloud customers identify the appropriate security controls to use in different situations.

The goal of the matrix is to provide details on the possible options that organizations can use, and it covers numerous domains of cloud security:

- Application and interface security
- Audit assurance and compliance
- Business continuity management and operational resilience
- Change control and configuration management
- Data security and information lifecycle management
- Data center security
- Encryption and key management
- Governance and risk management
- Human resources
- Identity and access management
- Infrastructure and virtualization security
- Interoperability and portability
- Mobile security
- Security incident management, e-discovery and cloud forensics
- Supply chain management, transparency and accountability
- Threat and vulnerability management

The matrix covers in detail the possible control strategies for each of these domains and provides a convenient mapping to common security frameworks and regulatory standards, making it an ideal companion to a CSPM effort.

system when they assume a related role in the organization, and departing employees may be automatically removed from the system as part of the offboarding workflow.

The goal of deploying a CSPM tool is to provide an organization with deep visibility into the current state of its cloud security posture. Effective CSPM solutions integrate findings from across the variety of cloud services used by an organization and provide administrators with the ability to quickly recognize and correct security vulnerabilities and potential regulatory issues. In some cases, this situation may be automatically remediated to prevent even a temporary exposure of cloud assets that might result in a compromise. CSPM solutions offer security administrators a holistic view of their cloud security environment that allows them to focus their efforts on the most pressing security issues.

CDW: We Get Cloud Security

CDW's team of account executives and solution architects can assist your organization with all of its cloud security needs. Our team routinely works with organizations of all sizes and across industries in different stages of the cloud adoption lifecycle.

Our large and experienced staff of security and industry experts can help you find the right solutions and services to build a robust and secure cloud environment and optimize your cloud security strategy. In addition to the CDW Cloud Check approach to cloud security posture management, CDW's team assists customers with a variety of other cloud security efforts, from developing new cloud security programs to assessing and fine-tuning existing efforts. CDW's comprehensive set of cloud security services includes:

- CDW Cloud Check (complimentary)
- Penetration testing
- Compliance assessment
- Framework assessment
- Professional services
- Consultation services

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. Your journey, secured.

TREND MICRO

Check Point SOFTWARE TECHNOLOGIES LTD.

Learn more about how CDW solutions and services can help you protect your data in the cloud.

CDW®, CDW·G® and PEOPLE WHO GET IT® are registered trademarks of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. Together we strive for perfection. ISO 9001:2000 certified
MKT42779 — ©2020 CDW LLC

CDW PEOPLE WHO GET IT®