Continuously Monitor and Assess Your Security Posture in the AWS Cloud

Dave Shackleford
As organizations start using more cloud services and resources, they become responsible for a staggering variety of cloud administrative consoles and interfaces, known collectively as the cloud control plane. The cloud control plane can encompass a wide variety of elements. The simplest is the cloud administrative console itself. This console needs to be locked down as carefully as possible, with limited privileges and user access, for example, and multifactor authentication (MFA).

Because the cloud is a software-defined infrastructure platform, many other aspects of the cloud environment might fall into this category. The first is the wide variety of APIs open and available in the cloud. This could be the command line interfaces for IaaS (AWS Command Line Interface [CLI],\(^1\) for example) or others associated with Kubernetes or other technologies. Another aspect of cloud control plane security is the network zoning and segmentation put in place: What is exposed to various network environments? Cloud computing is a large, often interconnected ecosystem of software-defined infrastructure and applications, and the cloud control plane offers a wide variety of configuration options for consumers to leverage. In this paper, we describe several best practices that organizations can put in place to strengthen and maintain their cloud security posture in the cloud.

---

\(^1\) This paper mentions solution names to provide real-life examples of how cloud security tools can be used. The use of these examples is not an endorsement of any solution.
Several factors tend to consistently drive the need for enhanced cloud security management and oversight, including the following:

- **The cloud is programmable.** Because the cloud is a software platform built for application development and deployment, configuration errors are common. However, proper oversight can improve this situation.

- **“Cloud” easily leads to significant sprawl in new technology implementations.** With the availability of so many new technologies that are only a click away, cloud environments may grow organically over time, which naturally leads to technology sprawl. As most security professionals know, this can take effort to contain.

- **The cloud is different from on-premises tools, technologies and services.** While the concepts might be similar in some cases, the cloud is its own software platform. (And every cloud is unique.)

- **Cloud inventory can be challenging as a result of more sprawl and a lack of monitoring.** While the cloud is a platform that enables greater flexibility in building and querying an inventory of assets, achieving a continuous asset inventory without deep and highly embedded monitoring can be a challenge.

Many cloud security needs arise from a lack of oversight into what controls are in place, the configuration of those controls, and what changes are made in cloud environments. Some of these controls are central to the entire cloud account environment, while others are specific to one or more types of cloud services or assets. Based on the Center for Internet Security (CIS) Amazon Web Services Benchmarks,² categories of controls to focus on include identity and access management (IAM), logging, monitoring, and networking. Table 1 provides a few examples of control recommendations. While these are simply examples, it is easy to see why large, rapidly growing cloud environments require constant monitoring and oversight to ensure that controls are in place and compliance status is maintained.

In addition, privacy and regional requirements for security controls can make sound cloud security management even more challenging. In 2015, Gartner, along with industry analysts, proposed a category of cloud monitoring services labeled Cloud Infrastructure Security Posture Assessment (CISPA). Although this set of solutions centralized cloud visibility by scanning IaaS cloud interfaces, the products and tools needed improvement and created a variety of false positives.

### Table 1. Examples of Control Recommendations

<table>
<thead>
<tr>
<th>Control</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>Enable MFA for all users with cloud console access. Ensure MFA for the root account and ensure that this account does not have programmatic access keys assigned to it.</td>
</tr>
<tr>
<td>Logging</td>
<td>Enable AWS CloudTrail in all regions and ensure log file validation is enabled. Ensure that VPC flow logging is enabled in all virtual private clouds (VPCs).</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Enable metric filters and alarms for any use of the root account. Enable metric filters and alarms for any S3 bucket policy changes. Ensure that no security groups allow access from anywhere to ports 22 (SSH) or 3389 (RDP).</td>
</tr>
</tbody>
</table>

² Center for Internet Security, CIS Benchmarks, [www.cisecurity.org/benchmark/amazon_web_services/](http://www.cisecurity.org/benchmark/amazon_web_services/)
with overly complex user interfaces and weak reporting. Several years later, Gartner defined Cloud Security Posture Management (CSPM) as a group of security products and services that focus on compliance monitoring, dynamic cloud and DevOps integration, more thorough investigation and incident response capabilities, and risk assessment and reporting (that is much more accurate) for the cloud control plane.

### Continuous Monitoring Strategies for Cloud Services

Public cloud environments are constantly changing due to the more rapid and dynamic deployment models that modern development and DevOps teams are using. As enterprises deploy more frequently, security teams will need greater, always-on visibility into the configuration of the cloud environments they operate. To successfully achieve this continuous monitoring model for all public cloud accounts and assets, a successful CSPM model should have the capabilities shown in Figure 1.

#### API Integration with Cloud Providers

The first aspect of any mature CSPM service or solution is deep integration with the cloud service providers that you plan to monitor. With many CSPM solutions, cloud account access is provisioned through a dedicated IAM service account and privileged role that grants access to internal cloud service and asset configurations for monitoring. CSPM suites also integrate directly with a number of cloud provider APIs to natively query for specific information programmatically. For example, a strong CSPM solution that monitors Amazon Web Services (AWS) accounts should include API support. See Table 2 for examples.

![Figure 1. Key Components of a CSPM Model](image)

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>API Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS CloudTrail</td>
<td><code>aws-cloudtrail-describe-trails</code></td>
<td>Lists information about defined AWS CloudTrail logging trails</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td><code>aws-cloudfwatch-describe-alarms</code></td>
<td>Lists information about defined Amazon CloudWatch alarms in place</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td><code>aws-ec2-describe-instances</code> and <code>aws-ec2-describe-images</code></td>
<td>Lists information about EC2 running workloads and image templates</td>
</tr>
<tr>
<td>Amazon S3</td>
<td><code>aws-s3control-public-access-block</code></td>
<td>Describes protective controls in place within Amazon S3 to prevent buckets from being made public</td>
</tr>
<tr>
<td>Amazon VPC</td>
<td><code>aws-ec2-describe-security-groups</code></td>
<td>Lists information about network traffic access controls applied to instance workloads within Amazon EC2 for a specific VPC</td>
</tr>
</tbody>
</table>

The better integrated a CSPM solution is with the individual provider’s APIs, the more accurate and efficient monitoring will be.
Scanning and Validating Configuration of Cloud Assets

A CSPM solution should offer a breadth of security policy coverage in terms of the variety of supported cloud services within a provider environment. For example, common services used within AWS to deploy assets may include Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Relational Database Service (RDS), Amazon Virtual Private Cloud (VPC), and more. After assets are created, there are numerous configuration options that can be applied and managed. For example, Amazon EC2 workloads are often configured with Amazon Elastic Block Store (EBS) volumes attached for storage. These Amazon EBS volumes can be configured automatically to support drive encryption using a variety of different encryption keys within the environment. CSPM solutions should be able to assess running workload configurations and determine whether encryption is enabled by default and applied currently during runtime. Flexible CSPM policies would also enable a security team to specify which keys should be in use for the encryption operations.

Examples of common asset configuration policies/alerting might include:

- Instance workloads started from unapproved images
- Container workloads using unapproved or stale images within an image repository
- Lack of encryption enabled for cloud storage or databases
- Lack of encryption for traffic in sensitive data in motion
- Exposed data storage, such as accessible Amazon S3 buckets

Because everything running in the cloud is comprised of software-defined objects connected to the cloud provider fabric, native API queries should provide the most accurate and up-to-date information about all assets.

Scanning and Validating Configuration of Cloud Control Plane Settings

In addition to asset information, the cloud provider environment and core enablement services include a plethora of configuration options and security controls to monitor. This often includes the definition of IAM users, groups and permissions, for example, as well as completely cloud-native services that don’t necessarily consist of workloads or storage. CSPM solutions should be able to continuously monitor these services and configurations through the same types of APIs used to assess distinct objects and assets. Examples of cloud control plane settings and controls to monitor may include:

- Lack of sound key management (e.g., old keys or stale keys)
- Overly permissive IAM policies that don’t adhere to least privilege principles
- Privileged accounts without MFA enabled
- Minimal or no logging enabled within the cloud environment
In addition, it is important to detect the lack of certain controls and configuration within the control plane, particularly for security-related services that CIS and other best practice guidelines recommend. Examples of these within the AWS cloud could include a lack of:

- Amazon CloudWatch monitoring rules and alarms
- AWS Config rules that monitor the environment
- AWS CloudTrail logging, which is disabled in specific regions

**Monitoring Cloud Network Controls and Network Traffic**

The final category of CSPM monitoring focal areas relates to networking. Cloud providers offer a range of cloud-native network access controls and tools for network monitoring, and organizations should configure them in accordance with security best practices, just as with other assets and control plane elements. For an AWS environment, examples of networking controls that CSPM policies should monitor include:

- Open or permissive network access control lists (NACLs)
- Open or permissive security groups
- Lack of VPC flow logging for all VPCs

Now that we have a better understanding of the capabilities necessary for a successful CSPM model, we turn our attention to using CSPM to improve visibility.

**How CSPM Fits into Detection and Response**

When applying CSPM to security operations, organizations should consider the following:

- Doing asset inventory and classification (the faster and more accurate, the better)
- Identifying access to the cloud control plane
- Monitoring policies for configuration and compliance
- Monitoring operational policies and configuration (e.g., performance)
- Collecting artifacts and insight into incidents for incident response (IR)
- Visualizing and reporting control plane risks

Security operations teams should plan to use CSPM platforms and services to improve visibility into the types of cloud environment events that occur over time, which can indicate a pattern or trend of behavior. Particularly in cases of insider abuse, account hijacking and unlawful use of cloud resources, security operations teams need insight into larger datasets over longer periods of time to really see whether anomalous or illegal activities are afoot. While a CSPM solution is not going to replace dedicated security monitoring tools that focus on specific log events or network traffic, they are useful for identifying patterns of changes, configuration gaps or IAM privilege assignments that may indicate security events or insider threats.
The second key CSPM area of focus for security operations is monitoring and alerting. To that end, CSPM tools can provide a more complete inventory of assets and service configuration within a cloud environment over time, which can then be reviewed against specific policies to send alerts to email, open tickets, and more.

Finally, organizations can use CSPM solutions in conjunction with other tools and services to improve security event correlation and develop more insightful prioritization on where to focus. This enables an augmented and more cloud-aware set of response practices that organizations can put into practice based on detected risks. Exposure time matters more than ever, and rapid detection and alerting of potential weaknesses or incidents can potentially make the difference between a relatively minor remediation effort and an event response. There are many possible playbooks that security operations and response teams can build using coordinated CSPM monitoring and alerting, including:

- Detection of a new account that has a wide range of privileges to cloud services and does not have MFA enabled
- Creation of a new set of containers using an old or unapproved image

When correlated with cloud environment logs and other contextual detail, this information could reveal an account hijack that led to new resource creation or attempted insider threat activity, for example. Security operations teams that are enabling and monitoring CSPM platforms should:

- **Define priorities.** Security analysts focused on cloud must first of all decide what conditions and behaviors are most critical to monitor. Look for high-risk exposed assets as a starting point, along with IAM policy or best practices violations.

- **Tune alerts.** While tuning is, in general, a common-sense practice, it is incredibly important for cloud monitoring scenarios such as those involving CSPM. To build appropriate behavioral baselines of events in the environment, analysts will likely need to allow several weeks or even months of data to accumulate. Make tuning a regular part of overall monitoring processes.

- **Build detection and response workflows.** In conjunction with tools such as SIEM, CSPM alerts and insights can be extremely helpful in developing more thorough and insightful response use cases. Mature CSPM tools usually include robust query engines and tools that provide security operations teams with even more granularity and flexibility in performing targeted searches for specific conditions within cloud environments. This can enable targeted vulnerability hunting use cases, as well, which then result in remediation and additional monitoring outcomes.

In the next section, we look at how to integrate CSPM services into the DevOps pipeline through infrastructure-as-code (IaC) evaluation.
Integrating CSPM into a DevSecOps Pipeline

As CSPM evolves and matures, several new trends that are emerging make these solutions even more capable and vital to cloud security programs. The first is the ability to perform IaC assessments on deployment templates built for tools and services such as AWS CloudFormation and Terraform. By evaluating the IaC templates in the DevOps pipelines, CSPM tools can ensure configuration best practices before they manifest in production (or even test) environments. For example, consider the AWS CloudFormation syntax for defining a new security group in AWS, as shown in Figure 2.

In this example, the code highlighted in red points out that SSH inbound access is allowed for any source (represented as 0.0.0.0/0). This is not in accordance with security industry guidelines and best practices, which suggest limiting remote workload access to only trusted IP addresses and ranges where possible.

The second major emerging enhancement to CSPM services is integration with workload protection tools. Cloud workload protection platforms (CWPPs) are workload-centric security offerings that target the protection requirements of server workloads in modern cloud data center architectures. CWPPs should provide visibility and control for virtual machines, containers and serverless workloads, regardless of location. CWPP offerings protect the workload from security events, typically using a combination of network segmentation, system integrity protection, application control, behavioral monitoring, host-based intrusion prevention and optional anti-malware protection. Leading providers include functionality such as strong endpoint malware sandboxing and detection/response, threat intelligence integration, encryption for data at endpoints, and application control/whitelisting. More advanced detection and prevention capabilities may also include exploit prevention/memory protection and behavioral monitoring. When paired with highly capable monitoring of the environment and assets, detected issues can potentially be remediated automatically. This can serve to make even highly dynamic DevOps pipeline scenarios much more secure through a combination of continuous monitoring, flexible policy evaluation and protective controls that automatically keep workloads in their desired security posture.

```
"InstanceSecurityGroup" : {
    "Type" : "AWS::EC2::SecurityGroup",
    "Properties" : {
        "GroupDescription" : "Allow SSH to workloads",
        "VpcId" : {"Ref" : "myVPC"},
        "SecurityGroupIngress" : [{
            "IpProtocol" : "tcp",
            "FromPort" : 22,
            "ToPort" : 22,
            "CidrIp" : "0.0.0.0/0"
        }],
        "SecurityGroupEgress" : [{
            "IpProtocol" : "tcp",
            "FromPort" : 22,
            "ToPort" : 22,
```

Figure 2. Defining a New Security Group
CSPM Reporting and Compliance

Regulated industries must adhere to specific industry and government requirements, such as PCI DSS for retail, HIPAA for healthcare and FFIEC for financial services. In addition, many enterprise organizations must meet internal audit standards. CSPM solutions can provide deep visibility into the state of controls within cloud deployments, facilitating improved reporting on these controls and how control posture may affect internal and regulatory/industry requirements. Leading CSPM solutions can automatically map many detected and monitored controls to compliance requirements, alleviating manual efforts for compliance, audit and risk management teams in seeking to assess the state of controls at any given time. In addition, prebuilt reports are often built into CSPM solutions. These reports can be produced automatically or on demand to facilitate audits as needed.

In addition to compliance monitoring and reporting, CSPM platforms are excellent tools for developing baselines of controls and attributes in cloud deployments, as well as building metrics that can track security and operations improvements in controls posture over time. A few of the many possible metrics that can be derived from CSPM evaluation include:

- Number of total configuration items that did not meet industry best practices or internal standards (Organizations should seek a reduction in this number over time.)
- Number of unapproved or incorrect images used for workload deployments
- Number of IAM accounts that did not meet internal controls standards for privileges and MFA enablement, for example
- Increases or decreases in misconfiguration over time based on changes to deployment strategies and cloud growth

While a CSPM platform can generate many possible metrics, it’s critical for organizations to focus on those indicators that are most meaningful and impactful to their specific organization.
Conclusion

When evaluating any CSPM solution, security teams should look for key features that a mature service offering should provide:

- **Configurable and automatable remediation capabilities**—Ideally, any discovered issues can be remediated automatically or with minimal manual intervention.

- **Custom policy and rules engine enforceable across provider environments**—The granularity and flexibility of a policy engine is one of the most important features for any CSPM solution. Policies need to properly and accurately assess cloud service provider settings and asset configuration.

- **Integration with DevOps pipeline stages and tools**—For any code or image repositories and build tools, for example, a CSPM platform should ideally be able to integrate and monitor activity here as well. It should also be capable of evaluating IaC templates for configuration issues. Workload protection capabilities through integrated agents and service integrations can significantly enhance the entire security posture of deployments, too.

- **Detailed and configurable reporting**—Because CSPM is really a monitoring tool at heart, reporting is critical.

Finally, security teams should consider the integration of CSPM solutions with their various cloud service providers. Many CSPM platforms are integrated through cloud service provider APIs and IAM service accounts, but security teams should closely evaluate the privileges needed and ensure that any new IAM accounts are carefully set up and monitored.
**About the Author**

Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

---

**Sponsor**

SANS would like to thank this paper’s sponsor:

![aws marketplace](amazonaws.com)
## Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

<table>
<thead>
<tr>
<th>Training Name</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Sydney 2020</td>
<td>Sydney, AU</td>
<td>Nov 02, 2020 - Nov 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Thailand</td>
<td>Bangkok, TH</td>
<td>Nov 09, 2020 - Nov 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>APAC ICS Summit &amp; Training 2020</td>
<td>Singapore, SG</td>
<td>Nov 13, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Community CTF</td>
<td></td>
<td>Nov 19, 2020 - Nov 20, 2020</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS Wellington 2020</td>
<td>Wellington, NZ</td>
<td>Nov 30, 2020 - Dec 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>