Cloud Security Is a Shared Responsibility

There is a shared responsibility between AWS and the organization in the public cloud. AWS’ commitment is to secure and manage the cloud foundation. This includes the physical assets, data center operations, and cloud infrastructure. An organization using this infrastructure is responsible for their information and data, applications and code, identity and access control, and containers and workloads. Areas of shared management of risk between an organization and AWS would be to secure the software or applications running on the hardware, networking, or data centers. But securing the data that exists is the organizations’ responsibility.

Therefore, with this model, it becomes imperative for the customers to have complete visibility into the security posture of their assets in the cloud at all times.

Accountability Remains

Regardless of where the data resides, the IT organization has the task of maintaining security and compliance. When it’s stored on someone else’s server outside of the organization, the challenges range from figuring out where the data is to what’s stored there. When data is safely stored within the perimeter defenses, that’s a more straightforward job. IT security teams are held responsible if there is an attack on an organization or a data breach, no matter where it originated from.

Top Cloud Challenges

The Flexera 2021 State of the Cloud Report identified that 81% of respondents chose security as the top cloud challenge.

Enterprises choose a presence in AWS for many reasons, including:

- Agility through innovation to maintain a competitive edge
- Benefits gained by leveraging the different service capabilities that AWS offers natively rather than the effort of hosting them on-premises
- Avoiding the cost of capital expenditure and instead pay by usage as an operational expense

As AWS adoption continues to accelerate, this creates a newly expanded attack surface that organizations need to be aware of to put the proper controls in place to protect against evolving threats.
Cloud Security Posture Assessment (CSPA)

CSPA monitors enterprise public cloud environments to identify and report on deviations of an enterprise's security posture against best practices.

This assessment includes deviations based on:

- Compute instances for compromises
- Network traffic for suspicious traffic flows
- Storage buckets for vulnerabilities and misconfigurations
- Sensitive data exposure
- Malware
- Compliance deviations

The assessments of the cloud assets and their behavior occur continually, leveraging global threat intelligence to detect risks and exposures at the earliest possible opportunity.

A report on the findings, including deviations from compliance standards, is generated for organizations to take remedial action following the assessment.

Risks

Risk can be defined as the likelihood of an enterprise being impacted by a threat.

Gartner predicts that through 2025, 99% of cloud security failures will be the customer’s fault. Some of the risks that customers face include:

- **Misconfigurations** that allow sensitive data to be publicly accessible and expose it to data leak of confidential information or personally identifiable information.
- **Malware** in storage that moves laterally when executed and impacts many services.
- **Known vulnerabilities that are exploited** and result in compromised hosts. The compromised hosts could communicate externally with botnets, resulting in data exfiltration or reduced security capabilities, making them more susceptible to ransomware attacks.
- **Vulnerabilities that cause performance issues** or launch additional instances, thus causing unnecessary operational expenses.
- **Multiple login attempts** to break into accounts, with the attempts going undetected.

### Risk Assessment

To assess the risks outlined above, Fortinet's CSPA service offering uses the following methodology:

1. **Establish connectivity** to the customer's cloud environment
2. **Assess compute instances, network traffic, and data stores** for anomalies
3. **Generate best-practice report and recommendations**

Once the prerequisite steps are established to gain visibility into the cloud resources across Amazon Web Services (AWS), the service utilizes global threat intelligence on zero-day threats, botnets, viruses, and indicators of compromise to report on the risks and exposures.

### The Assessment

Your assessment will provide results in these areas:

- Identification of misconfiguration of the cloud resources for exposure to threats
- Reporting on data stores containing sensitive information
- Reporting on data stores for content infected with malware
- Highlighting open alerts by severity to help prioritize actions
- Highlighting suspicious data flows and user behavior

- Reporting on compliance with industry standards

- Recommendations to remediate issues found in the environment

**Scope**

CSPA operates within the following guidelines:

- Assessment based on **7 days of data collection/monitoring**
- **Details of top 10 exposures** found in severity levels of Critical, Alert, and Warning
- **Details of a maximum of 10 workloads** compromised by botnets and risky connections
- Details of a maximum of **10 storage resources by exposure level**
- Details of a maximum of **10 storage resources** infected with malware and known sensitive data
- Details of a maximum of **10 activities indicating suspicious traffic flows and user activity**
- **Compliance** to any one of HIPAA, PCI DSS, SOX-COBIT, GDPR, NIST, or ISO standards

**A Typical Assessment Outcome Includes:**

![Cloud Security Posture Assessment Report]

Figure 2: Files with sensitive content were found configured to be publicly accessible. The scope of exposure of these files needs to be ascertained and the right level of security controls applied.
Several alerts with different levels of severity were found during the assessment.

Of particular note is the number of critical severity alerts deserving the highest level of attention.

Over 9,000 of these were reported during the assessment.

AWS VPCs and Security Groups instances had critical alerts reported against them.

We found compromised resources making risky connections and connecting to botnets.
We also detected malware in the files.

We detected suspicious user activity such as a user logging in from a location that is not expected or allowed by policy.

It also detected policy violations pertaining to personally identifiable information.

A list of recommended actions will be included with your assessment report to improve your security posture.
Estimated Level of Effort:

- Fortinet’s estimated staffing requirements for this engagement are as follows:
  
  **Three days**
  
  - One or more Fortinet staff will be assigned for effort in each of the consulting days, which may not be contiguous.
  - Currently, all work will be done remotely due to COVID-19 limitations.

Why Fortinet?

- Every minute gone by with an undetected exposure in the cloud presence is a minute of an incident waiting to occur.
- Fortinet leads the industry with our products across networks, endpoints, and applications and our personnel with expert consulting on best practices across all major cloud providers.
- Our services will help identify gaps and deviations from best practices and offer recommendations on addressing them.
- If you are interested in this service or would like to know more, please contact consulting@fortinet.com.

---