August 5, 2021

BULLETIN: THE IMPORTANCE OF PROPERLY SCOPING CLOUD ENVIRONMENTS

The PCI Security Standards Council (PCI SSC) and the Cloud Security Alliance (CSA) are issuing a joint bulletin to educate stakeholders on the importance of properly scoping cloud environments and good cloud security measures for payment security protection.

Why Cloud Matters

The use of cloud computing services has accelerated in recent years and is projected to continue expanding in the future. According to an Accenture survey, more than 90 percent of today's enterprises have adopted cloud services in some form.[1] Along with this increased use has come increased worry about security. A 2020 AWS study found that 95 percent of organizations are concerned about cloud security with the two biggest concerns being loss of data and data privacy.[2]

This dramatic increase in use of cloud services makes sense given the many benefits cloud computing can provide to businesses large and small. Cloud computing can be used to provide customers with access to the latest technologies without a costly investment in computing resources. Due to the economies of scale associated with the delivery of cloud services, cloud service providers (CSP) can often deliver access to a greater range of technologies and security resources than that to which the customer might otherwise have access. Organizations without a depth of technically skilled personnel may also wish to leverage the skills and knowledge provided by cloud service providers to securely manage their cloud operations. Cloud computing therefore holds significant potential to help organizations reduce IT complexity and costs, while increasing agility.

Cloud computing is also seen as a means to accommodate business requirements for high availability and redundancy, including business continuity and disaster recovery. Another significant benefit to cloud environments is scalability: organizations can optimize the available computing capacity (for example, data storage, processing power and network bandwidth) as demand increases or decreases.

Because of these many benefits, investment in cloud computing is projected to be an ever-increasing priority for businesses around the world.

[1] Why & How to Move to the Cloud | Accenture
[2] 2020-AWS-Cloud_Security-Survey-Report.pdf (cloudpassage.com)

Understanding the Definition of Cloud as a Precursor to Cloud Scoping

A common understanding of what cloud computing actually is helps facilitate conversations about how to best manage risks and assure optimized security. Definitions range from the notional "running your programs on someone else's computer" to the more formal "on demand network access to a shared pool of rapidly provisioned computing resources" that emanates from NIST's original definition of cloud[3] authored in 2009 and revised in 2011.

Central to the original NIST definition of cloud are the three service delivery models, SaaS (Software-as-a-Service, which are complete business applications such as payment systems), PaaS (Platform-as-a-Service, application development systems) and IaaS (Infrastructure as a Service, compute, and storage datacenter facilities). This definition implies that CSPs can have very different business models, ranging from a virtual software developer to a global operator of cloud datacenters. Cloud Security Alliance has depicted NIST's service delivery definition in its popular Cloud Reference Model, which represents SaaS, PaaS, and IaaS as a layered model.

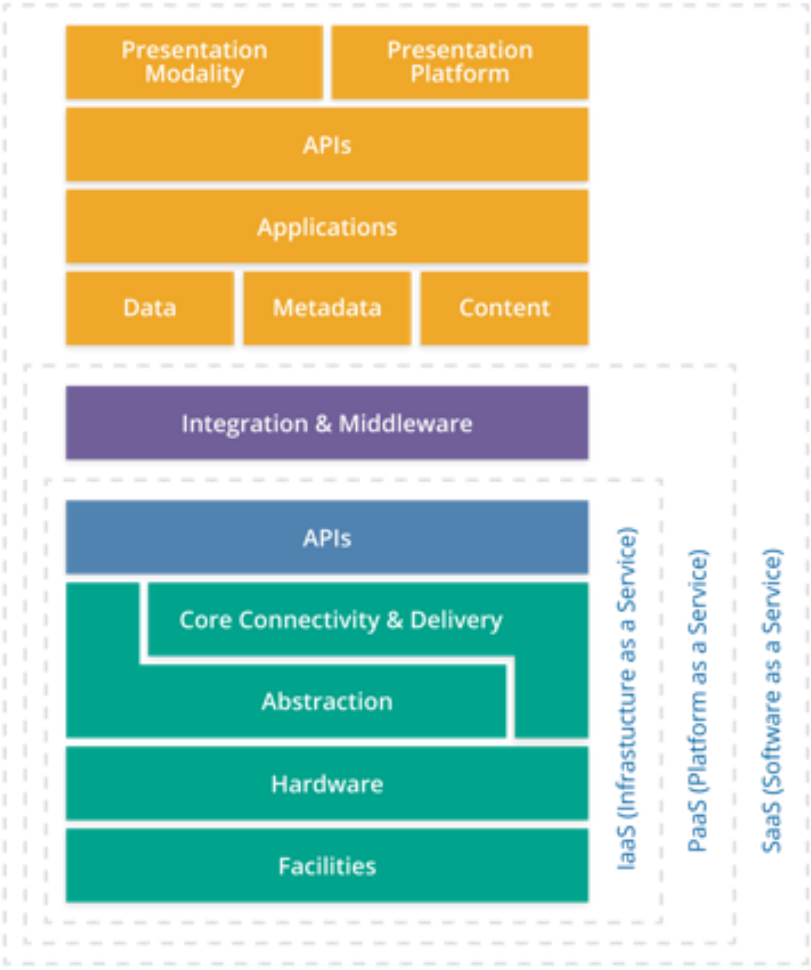

Figure 1 - CSA Cloud Reference Model

The CSA Cloud Reference Model matches real world cloud very well. Cloud payment systems are SaaS applications that are typically hosted within the cloud data centers across the globe. The implication is that cloud is multi-vendor, and in the context of this bulletin, the central actors are the merchant (cloud customer) and at least two CSPs: the cloud-based payment system (SaaS) and the cloud datacenter (IaaS).

The Importance of Cloud Scoping to Payment Environment Security

At a high level, scoping involves the identification of people, processes, and technologies that interact with or could otherwise impact the security of payment data or systems. When utilizing cloud security for payments, this responsibility is typically ***shared*** between the cloud customer and the cloud service provider.

[3] NIST SP 800-145, The NIST Definition of Cloud Computing

Data breach investigation reports continue to find that organizations suffering compromises involving payment data were unaware that cardholder data was present on the compromised systems. Proper scoping should be a critical and ongoing activity for organizations to ensure they are aware of where their payment data is located and that the necessary security controls are in place to protect that data. Improper scoping can result in vulnerabilities being unidentified and unaddressed, which criminals can exploit. Knowing exactly where payment data is located within your systems will empower organizations to develop a game plan to protect that data.

Segmentation of the payment card environment from all non-payment environments is an important strategy in any cloud scoping exercise and is intended to minimize the number of systems that have access to cardholder data. This not only helps to improve efficiencies and streamline efforts, associated with implementing, maintaining, and assessing security controls required by the PCI Data Security Standard (DSS), but also provides greater focus to evaluate and monitor those critical systems that remain relevant to protect payment card data.

Understanding Roles and Responsibilities

Organizations that outsource payment services to CSPs, often rely on the CSP to securely store, process, or transmit cardholder data on their behalf, or to manage components of the entity's payment data environment. CSPs can become an integral part of the organization's payment data environment and directly impact the security of that environment.

For too many organizations, bringing in a third party CSP for payment security services is seen as the only step necessary to securing payment data. The use of a CSP for payment security related services does not relieve an organization of ultimate responsibility for its own security obligations, or for ensuring that its payment data and payment environment are secure. Clear policies and procedures should be established between the organization and its CSP for all applicable security requirements, and measures developed to manage and report on security requirements. Implementation of a robust third-party assurance program can assist an organization in ensuring that the payment data and systems it entrusts to CSPs are maintained in a secure manner. Proper due diligence and risk analysis are critical components in the selection of any CSP.

Some guidance for selecting and working with a CSP include:

Third-Party Service Provider Due Diligence: When selecting a CSP, organizations should vet CSP candidates through careful due diligence prior to establishing a relationship. This will assist organizations in reviewing and selecting CSPs with the skills and experience appropriate for the engagement.

Service Correlation to PCI DSS Requirements: Organizations should understand how the services provided by CSPs correspond to the applicable PCI DSS requirements. This will assist an organization in determining the potential security impact of utilizing CSPs on the organization's payment data environment. This information can also be used to determine and understand which of the payment security requirements will apply to and be satisfied by the CSP, and which will apply to and be met by the organization.

Note: Regardless of how specific responsibilities may be allocated between an organization and a CSP, ultimate responsibility for payment data security rests with the

organization. Engaging a CSP does NOT relieve an organization of their security obligations. This responsibility cannot be outsourced.

Written Agreements and Policies and Procedures: Organizations should consider detailed written agreements such as contracts, services agreements, and responsibility matrices to promote consistency and mutual understanding between the organization and its CSP(s) concerning their respective responsibilities and obligations with respect to PCI DSS requirements.

Monitor Third-Party Service Provider Compliance Status: Organizations should be aware of the CSP's PCI DSS compliance status. This helps to provide the organization engaging a CSP with assurance and awareness about whether the CSP complies with the applicable requirements for the services provided. If the CSP offers a variety of services, this knowledge will assist the entity in determining which CSP services will be in scope for the entity's PCI DSS assessment.

Reducing Risks – Best Practices

Limiting exposure to payment data reduces the chance of being a target for criminals. In addition, consider the following best practices:

- ✓ **Data protection:** Assure that information is protected by maximizing use of strong cryptography and key management practices, tokenization, and masking where feasible and employing robust data loss prevention solutions. Best practices call for protection of data in three states: Data in Transit (network encryption), Data at Rest (storage encryption) and Data in Use (masking, tokenization, and emerging encryption technologies). Data loss prevention solutions detect, log, and potentially block unauthorized access to sensitive data.

- ✓ **Authentication:** Assure that strong multi-factor authentication is pervasive to protect against common attacks against the credentials of consumers, merchants, and service providers. Strong authentication should be based upon industry standards, such as FIDO (Fast IDentity Online), SAML, OpenID and OAuth. Payment CSPs may vary in what they consider their scope of responsibilities for strong authentication. Is it optional or mandatory for users? Is it compatible with the pervasive authentication features available to consumers, such as mobile device biometrics? Does the strong authentication solution provide a frictionless consumer experience, or does it require significant user configuration?

- ✓ **Systems management:** Recent high-profile breaches have pointed to weaknesses in how responsible parties perform routine systems management functions, such as patch management, verification of code updates and configuration management. Most of these responsibilities should be undertaken by the payment CSP, however some components may be the responsibility of the infrastructure CSP.

- ✓ **DevOps & DevSecOps:** These terms describe emerging best practices for frameworks used for developing software in the cloud that is designed, coded, and tested to be as secure and defect-free as possible. DevOps processes will define both original code developed by the CSP as well as APIs and third-party modules that are incorporated into the finished software product. Merchants should determine if the CSP has a documented DevOps software development lifecycle and can provide evidence of what code it developed and what third party technology is included in the payment solution.

Software supply chains are important areas of exposure for malicious attackers and merchants should understand the original source of all components of the payment solution.

- ✓ **Data governance:** With global nature of cloud, assure that information stays within the appropriate jurisdiction boundaries and is accessed by stakeholders with legitimate needs. This relates back to understanding the payment CSP's selection of cloud infrastructure and how it is configured to use different datacenters in selected geographical regions.

- ✓ **Resiliency:** Assure that service providers take advantage of cloud's nearly unlimited capabilities to provide redundancy for application availability and data backups. From a scoping perspective, the merchant should examine the payment CSP's selection of cloud infrastructure. Is the system using multiple, redundant data centers? Is the data replicated between multiple data centers? Is the appropriate level of data tiering in place, including offline backups and archiving, to protect against data destruction attacks such as ransomware? Does the application automatically failover if a single datacenter has network or system availability issues?

The PCI DSS provides a solid baseline of security practices. For assistance understanding PCI DSS scoping and how PCI DSS applies to your cloud environments, we recommend consulting a Qualified Security Assessor (QSA). The list of QSAs can be found here.

In support of the PCI DSS security requirements, the CSA Cloud Controls Matrix can be used in an assessment to determine which CSP is responsible for which security controls. The related CSA STAR program provides over 1,000 CSP security assessments online, which can accelerate due diligence for determining scope of applicability. These tools are regularly mapped to the latest PCI DSS requirements.

Conclusions & Resources

By better understanding the importance of cloud scoping, the need for segmentation and recognizing the various security roles and responsibilities, organizations can fully utilize the benefits of the cloud while protecting payment data and mitigating disaster recovery. For more information about cloud security and the importance of protecting payment environments, please consider the following resources:

PCI SSC Resource Links:

PCI SSC Cloud Computing Guidelines
Guidance for PCI DSS Scoping and Network Segmentation
Information Supplement: Third-Party Security Assurance
PCI Perspectives | Cloud Security (pcisecuritystandards.org)
Qualified Security Assessors (pcisecuritystandards.org)

CSA Resource Links:

Cloud Controls Matrix
Certificate of Cloud Auditing Knowledge
CSA (STAR) Security, Trust, Assurance and Risk Program
Top Threats to Cloud Computing

###

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) leads a global, cross-industry effort to increase payment security by providing industry-driven, flexible and effective data security standards and programs that help businesses detect, mitigate and prevent cyberattacks and breaches. Connect with the PCI SSC on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

About Cloud Security Alliance

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, training, certification, events, and products. CSA's activities, knowledge, and extensive network benefit the entire community impacted by cloud — from providers and customers to governments, entrepreneurs, and the assurance industry — and provide a forum through which different parties can work together to create and maintain a trusted cloud ecosystem. For further information, visit us at www.cloudsecurityalliance.org, and follow us on Twitter @cloudsa.