Top Use Cases for PCI Compliance in the Cloud

Introduction

You're probably reading a lot about "use cases" now. So we'll be brief and to the point.

The digital transformation of the retail industry is driving a range of technology advances. To stay competitive, your organization is probably looking to more agile, cloud-based solutions, from customer-facing systems for point of sale to CRM and back office applications for accounting and inventory management. As you use more cloud services, however, it's important to understand and manage the risks that can come with the cloud. You are still responsible for maintaining PCI compliance, governing usage and protecting customer data — as well as your own proprietary information — when you transition to cloud services.

Cloud access security brokers (CASBs) enable organizations to extend their information protection policies and programs from on-premises infrastructure and applications to cloud services. A good CASB can detect PCI data and other sensitive content at rest in sanctioned cloud services or en route to or from any cloud service with advanced, enterprise cloud DLP. Further, you can define granular policies — based on identity, service, activity and data — to automatically protect your data by blocking activities, restricting access, encrypting data, and more.

Here are the top three use cases for retail organizations that want to take advantage of the productivity gains and cost savings associated with moving to the cloud, while managing risk:

- Enforce PCI compliance across all cloud services
- Intelligent encryption
- Cloud ransomware protection to an unsanctioned service

1 Enforce PCI compliance across all cloud services

According the the Ponemon Institute, the current average cost of PCI data breaches is $4 Million, up 29 percent since 2013.[i]

And according to Verizon, the majority of consumers would be hesitant to do business with an organization that has suffered a data breach[ii]. That's not good news for major brand names that suffered loss of control of millions of customer records, just in the month of September 2017: Whole Foods, Sonic Corporation, and Equifax.

To maintain compliance in the cloud, retail companies need advanced CASB controls that are context-aware, able to differentiate between sanctioned and unsanctioned services — and even between corporate and personal instances of the same services — and provide granular and customizable DLP policies.

[i] Ponemon Institute, "2017 Cost of Data Breach Study", June 2017
[ii] Verizon "PCI Compliance Report", 2015

Functional Requirements

- Be aware of context, e.g., activities such as "upload," "download," and "share"
- Correlate users' identities (e.g., bob@netskope. com = bob123@yahoo.com = bobaran@gmail.com)
- See and control usage in both sanctioned and unsanctioned cloud services, including unsanctioned instances of sanctioned cloud services (e.g., personal vs. corporate instances of Office 365)
- Integrate with enterprise directory to enforce policies at a group or organizational unit level, e.g., visiting medical staff, hospital administrators, finance staff
- Decrypt SSL and decode the unpublished API to understand the transaction

2 Intelligent encryption

Encryption of card data is critical for PCI DSS compliance, and that includes any information that may be in cloud services.

The industry-leading Netskope Active Platform has enabled the world's largest retail brands to accurately enforce data loss prevention (DLP) policies on content already uploaded to cloud services — or en route to or from cloud services.

Functional Requirements

- Be aware of context, e.g., activities such as "upload"
- See and control usage in both sanctioned and unsanctioned cloud services, including unsanctioned instances of sanctioned cloud services (e.g., personal vs. corporate instances of Box)
- Detect sensitive content in a variety of methods, including via a custom keyword dictionary
- Apply strong encryption to sensitive content with enterprise key management
- Integrate with KMIP-compliant key manager
- Decrypt SSL and decode the unpublished API to understand the transaction

3 Cloud ransomware protection

Falling victim to a ransomware attack can do irreparable damage to a retail institution's brand (not to mention damage to one's career), so it's unsettling to know that the retail industry is now one of the top ransomware targets: attacks against the retail industry account for 15 percent of all recent incidents[iii].

Even if organizations aren't specifically targeted, the synchronization and sharing functionality of popular cloud services makes for a perfect medium for distribution of malware, making it more likely that any organization will fall victim to ransomware as worldwide cloud usage increases.

Netskope protects retail organizations from ransomware in the cloud with advanced visibility and control. For example, providing the ability to detect, quarantine, and remediate ransomware being downloaded from unsanctioned cloud services in real time.

Functional Requirements

- Inspect, detect, block, and remediate malware in sanctioned cloud services
- Inspect, detect, block, and remediate malware en route to/from unsanctioned cloud services
- Have visibility over cloud traffic even if it's coming from a sync client, native app, or mobile device

[iii] NTT Security, Global Threat Intelligence Report 2017

Conclusion

When evaluating CASBs for data governance and regulatory compliance in the cloud, be sure to verify the vendor's ability to support these top use cases, including the ability to define and enforce policy across all cloud services, including those known to IT and the unknown "shadow IT" services; the ability to find and encrypt PCI data in cloud services or en route to or from the cloud; and the ability to detect, block and remediate ransomware. Look for vendors who can do all this for data en route to or from cloud services as well as data already resident in the cloud.

About Netskope

Netskope is the leader in cloud security for retail. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope — security evolved. To learn more, visit https://www.netskope.com/solutions/retail-and-hospitality.

Netskope Active Platform | Security Evolved

Want to see cloud security for financial services in action?

www.netskope.com