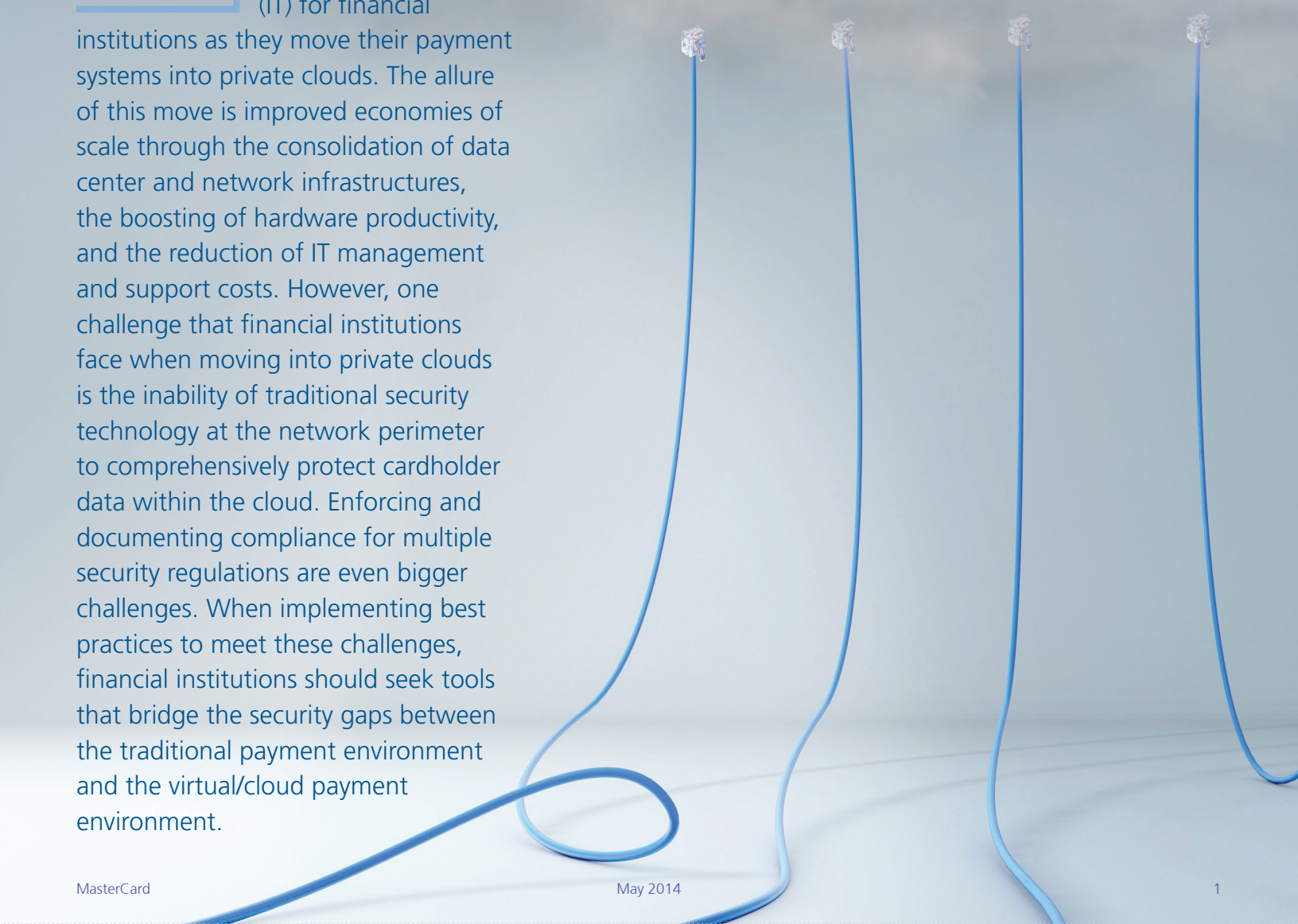
Enforcing Compliance in a Virtual Cloud Payment Environment

catbird

By Randal Asay, Chief Technology Officer

Virtualization is rapidly transforming information technology (IT) for financial institutions as they move their payment systems into private clouds. The allure of this move is improved economies of scale through the consolidation of data center and network infrastructures, the boosting of hardware productivity, and the reduction of IT management and support costs. However, one challenge that financial institutions face when moving into private clouds is the inability of traditional security technology at the network perimeter to comprehensively protect cardholder data within the cloud. Enforcing and documenting compliance for multiple security regulations are even bigger challenges. When implementing best practices to meet these challenges, financial institutions should seek tools that bridge the security gaps between the traditional payment environment and the virtual/cloud payment environment.



By virtualizing physical assets, a financial institution can save

40%

or more on overall IT costs, according to several industry studies.

WHY VIRTUALIZATION IS IMPORTANT TO FINANCIAL INSTITUTIONS

The basic premise behind virtualization is abstraction—using software to create fully functioning IT assets (such as servers, personal computers, network adapters, switches, and routers) that each in turn run on a single high-powered server. These virtual assets (called virtual machines or VMs) are independent software containers, each with its own unique operating system and application. Another software component, called a hypervisor, is the "traffic police" managing separate computing resources for each of the VMs operating on a single physical host server.

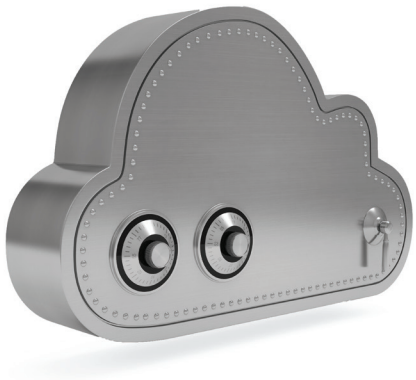
Virtual assets provide an organization with all of their respective functional benefits for IT operations without requiring the typical infrastructure of physical hardware. In a physical data center, common practice is to assign at least one or more servers to a single application. This "application isolation" strategy often leads to underutilization, where many servers operate at less than 20 percent of their capacity—yet these servers still demand a full overhead for operations, maintenance, and management. By virtualizing these physical assets, a financial institution can save 40 percent or more on overall IT costs, according to several industry studies.[1]

In a similar manner, using a private cloud to virtualize systems that process payment card transactions can lower operational costs. A private cloud is a virtualized data center operating under the direct control of an organization. The private cloud may exist on site inside an organization's firewall, or it may be run externally by a third party commercial service provider (such as Amazon.com®, Rackspace®, Salesforce.com, Verizon, Microsoft, or Google). Virtualization using private clouds is a well-established trend that will continue to grow in use by financial services organizations as they pursue efficiencies in payment processing.

CHALLENGES OF ENFORCING AND DOCUMENTING COMPLIANCE IN THE CLOUD

Virtualization offers the potential benefits of payment processing efficiencies, but it also comes with a "cloud" of challenges. Financial institutions are required to secure sensitive information, such as cardholder data, personally identifiable information (PII), and other financial account data. In addition to protecting such data, financial institutions must document compliance for applicable regulatory and industry requirements, including:

- The Sarbanes-Oxley (SOX) Act
- The Gramm-Leach-Bliley Act (GLBA)
- The Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH)
- The Federal Information Security Management Act (FISMA)



Without the use of controls specifically engineered for cloud environments, a financial institution will not have continuous visibility into sensitive data located in the cloud, nor the technical capability to protect it and prove to auditors that their organization is compliant with regulatory requirements.

The technical paths for meeting regulatory requirements are typically guided by:

- IT security frameworks (such as COBIT 5[2]); or
- Publications on security and privacy controls (such as the *National Institute of Standards and Technology [NIST] Special Publication [SP] 800-53*[3]), which also guide the operational surveillance work of auditors.

For virtualized payment systems, the Payment Card Industry Security Standards Council (PCI SSC) offers supplemental *PCI Data Security Standard (DSS) Virtualization Guidelines*[4] and *PCI DSS Cloud Computing Guidelines*[5] to help organizations parse through technical and process options.

Securing cardholder data, PII, and other sensitive information in the cloud can be challenging, because traditional security technology (deployed at the edge of a network) is unable to easily and comprehensively protect such data inside the cloud. Specifically, challenges can include the implementation of best practices for data segmentation, IT asset management, and policy enforcement. Although best practices are widely used to address these issues on physical networks, they do not easily extend to virtual environments.

MOVING TOWARD SOLUTIONS FOR VIRTUAL SECURITY AND COMPLIANCE

Financial institutions are in the early stages of enforcing security and verifying compliance for private clouds. Some institutions are attempting to adapt traditional physical security tools toward this end, but that process is complex, labor-intensive, and ill-suited to the dynamic nature of cloud environments that change as VMs are rapidly turned on or off in the flow of payment processing operations.

A more practical strategy is to use new technology that enables the virtual implementation of historically proven best practices from the physical world of security and compliance.

[1] The studies are summarized at http://www.energystar.gov/index.cfm?c=power_mgt.datacenter_efficiency_virtualization.

[2] http://www.isaca.org/COBIT/Pages/default.aspx

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[4] https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

[5] https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Consider segmentation (also referred to as isolation or zoning), which is using network control technology to separate IT assets into logical partitions or firewalled zones of operation. As the foundation of enterprise security, segmentation hides internal network activity from external attackers; if a breach occurs, it is limited to data and IT assets within the affected segment. A network segment logically groups data flows and restricts cardholder data to trust zones within the enterprise network. Segments also can improve manageability by automatically applying security and compliance policies to virtual assets and data in the cloud.

Achieving virtual security and compliance requires financial institutions to implement technical tools that provide full visibility into the virtual environment. These tools need to enable similar applications used in physical data centers, including:

- Firewalls
- Network access control
- Net flows
- Vulnerability scanning
- Intrusion detection and prevention systems
- Mapping
- Asset management

Virtual assets need this full range of security applications, because they are subject to exploitable software vulnerabilities—just like their physical counterparts.

Cloud security tools also should enable automatic protection by policy (such as for the PCI DSS, SOX, and other regulations), as well as ensure compliance of virtual data and assets—just as legacy tools can provide for the physical data center.

Automation simplifies the compliance process and reduces the audit scope, especially when frequent audits are the norm. For example, if a large financial institution is incurring numerous audits per year, then manually controlling the complexity of its dynamic private cloud security can be impractical, as can manually assembling documentation required to meet the auditors' recurring demands. The solution to these challenges would be to provide such institution with automated control of virtual security and compliance—including all necessary documentation produced on demand for auditors with a near real-time representation of compliance posture.

CONCLUSION

Virtualized IT is providing financial institutions with many economic and operational benefits as they move payment processing into private clouds. Now is the time for financial institutions to take the next step and seize granular control of security and compliance for sensitive data within the cloud. By adopting new, automated tools that are engineered specifically for virtual environments, financial institutions can ensure the protection of cloud-based data and provide auditors with evidence to verify regulatory compliance. In addition to complying with applicable laws and avoiding assessments, financial institutions will be able to ensure the protection of their cardholders' data, as well as boost their brand and reputation. ■

Virtualization and the New PCI DSS 3.0

The PCI DSS Version 3.0 has four additional significant requirements related to the virtualization of a cardholder data environment (CDE):

1 SCOPING

All virtualization technology in the CDE is in scope for a PCI DSS assessment. For the purposes of an audit, the following was added to PCI DSS 3.0 under Network Segmentation: "To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE."

2 NETWORK DIAGRAM

PCI DSS sub-requirement 1.1.2 and its test procedures were modified: "Current network diagram that identifies all connections between the cardholder data environment and other networks, including wireless networks." Given the dynamic nature of a virtualized CDE, use of an automated network diagramming solution will help provide 24-hours-per-day/7-days-per-week, complete visibility into security and compliance.

3 DATA-FLOW DIAGRAM

A new PCI DSS sub-requirement 1.1.3 was added relevant to virtualized CDEs: "Current diagram that shows all cardholder data flows across systems and networks." Tracking and diagramming all data flows in a dynamic virtual CDE will be nearly impossible without automation.

4 SYSTEM COMPONENTS INVENTORY

A new PCI DSS requirement 2.4 was added: "Maintain an inventory of system components that are in scope for PCI DSS." Given the dynamic nature of virtual components, using an automated inventory discovery and management system will help financial institutions to comply with this requirement.