Automating Cloud Security Control and Compliance Enforcement for PCI DSS 3.0

How Catbird Enables Security and Compliance with the PCI Data Security Standard in a Private Cloud

EXECUTIVE SUMMARY

All merchants, financial institutions and other entities that store, process, or transmit payment cardholder data are required by card brands to comply with the Payment Card Industry Data Security Standard (PCI DSS). The use of virtualization technology in private clouds is not exempt from requirements of PCI DSS 3.0, which raises the bar for security in a virtualized Cardholder Data Environment (CDE). Traditional physical security components that are usually deployed at the network edge make it difficult if not impossible to effectively monitor and control virtual components, so it is vital for organizations using virtual technology in the CDE to adopt tools that protect cardholder data. Catbird is a unique solution engineered to automate seamless, comprehensive network security and PCI DSS compliance for organizations with a virtual CDE. This paper describes how Catbird addresses security and compliance in a virtualized CDE prescribed by the PCI Security Standards Council. The paper also describes how Catbird addresses specific compliance issues for virtualization in PCI DSS 3.0.

CHALLENGES OF PCI COMPLIANCE WITH A VIRTUAL CDE

The processes of securing the Cardholder Data Environment (CDE) and validating PCI DSS compliance can be complex for large organizations. The complexity may become overwhelming when an organization attempts to achieve these goals for a virtualized CDE. Traditional security technology, which is deployed at the edge of a network, is unable to easily and comprehensively protect cardholder data (CHD) inside a virtualized CDE. Without the use of controls that are specifically engineered for a virtualized environment, an organization will be unable to have continuous visibility on CHD in the cloud, nor the technical capability to protect virtualized CHD and prove to auditors that the organization is compliant with PCI DSS requirements. Some organizations are attempting to adapt traditional security tools for this task, but that process is complex, highly manual and ill-suited to the nature of dynamic cloud environments.

The table below summarizes primary virtual components, the effect these have on physical security controls, and associated risks.

Change	Effect	Risk
Virtual networks	Flattens infrastructure and networks; blinds non-virtualized tools	Unauthorized access, anonymous access, denial of service
Machines are files	Increases transience, enables VM mobility, and increased frequency of change within the data center	Denial of Service, data or intellectual property theft, unauthorized access fraud
Virtual administrator	Collapses roles and increases privilege of administrators	Escalation of privilege, abuse of privilege fraud
Hypervisor	Adds new operating system and infrastructure layers	Denial of Service, anonymous access, data theft, fraud

HOW CATBIRD ADDRESSES RECOMMENDATIONS BY PCI COUNCIL

The PCI Security Standards Council's Virtualization Special Interest Group has published an Information Supplement called PCI DSS Virtualization Guidelines. This document provides guidance on the use of virtualization in accordance with PCI DSS. It states that if virtualization technologies are used in a CDE, PCI DSS requirements apply to those technologies. The supplement notes that virtualization technology introduces new risks that may not be relevant to other technologies. The supplement notes that virtualization can bring significant operational benefits to organizations that choose to leverage them. Catbird's multi-functional, virtualized security solution is a manifestation of those benefits for security and continuous compliance monitoring. Entities that adopt virtualization technologies must assess the risks, including unique characteristics of their particular virtualized implementation and all interactions with payment transaction processes and CHD. The document provides several recommendations for PCI DSS compliance.

Catbird fulfills many of the Council's general recommendations as follows:

Section 4.1.4 – Implement Defense in Depth

- Catbird provides the industry's broadest set of logical security controls within the virtual host and on the data plane required for defense in depth: NAC, Firewall, Vulnerability Management, Incident Response (IDS/IPS), Zone Configuration, Change Management, and Auditing.
- Catbird automates monitoring for continuous positive assurance of controls to ensure effectiveness and reduce compliance cost and complexity.

Section 4.1.5 – Isolate security functions

- Catbird's management console (Catbird Control Center), responsible for all security management and auditing, resides on an isolated and independent host.
- Catbird achieves security isolation with hardened virtual machine appliances (VMAs) responsible for enforcement within the host.

Section 4.1.6 – Enforce least privilege and separation of duties

- Catbird monitors and enforces access controls to the hypervisor and the management network.
- Catbird audits the use of hypervisor administration privileges.

Section 4.1.8 – Harden Hypervisor

- Catbird monitors and enforces best-practices for hypervisor hardening.
- Catbird secures access to the hypervisor management network.

Section 4.1.9 – Harden Virtual Machines and other components

- Catbird secures and protects virtual machines.
- Catbird vulnerability scanning identifies all network accessible services and supports identification of unnecessary or insecure services.
- Catbird configuration management automates application of a secure configuration baseline with Security Content Automation Protocol (SCAP) validating secure configurations for operating systems and applications

Section 4.1.11 – Recognize the dynamic nature of VMs

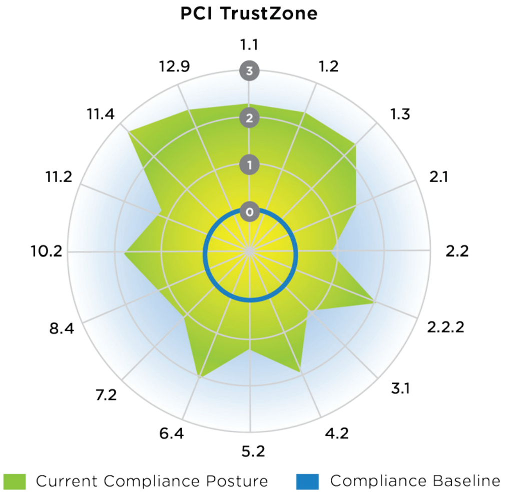
- Catbird is architected to address the increased complexity in enforcing boundary controls including monitoring and enforcement of port-group membership and number/configuration of vNICs.
- Catbird monitors and enforces secure configurations.

Section 4.1.12 – Evaluate virtualized networks security features

- Catbird audits and controls access to virtualized networks.
- Catbird policies support alerting and enforcement actions for virtual network access and configuration for all VMs.
- Catbird network flow auditing and firewall segmentation features audit and enforce virtual network isolation.
- Catbird audits and controls virtual network configuration changes assuring isolated configurations are maintained.

Catbird's virtualized and virtualization-aware solution delivers crucial capabilities not available from physical security software and devices. With Catbird, virtualization improves security by making it more fluid and context-aware. It lowers costs. It works because security policies are automated and can move along with VMs. Catbird makes network based security controls more accurately applied, more pervasively applied, easier to manage and less expensive than traditional physical security solutions have ever been. Catbird delivers more security that is more deterministically applied, and more stringently audited than any other available solution.

Catbird operates inside the virtual infrastructure, securing from within, leveraging precise contextual information available only through hypervisor APIs. This methodology produces enhanced monitoring and enforcement previously impossible with physical security. Catbird injects PCI DSS security policies into the infrastructure when and where it's needed, based on pre-defined policies built upon best practices and compliance standards. These capabilities enable instant, real-time compliance monitoring and enforcement of PCI DSS requirements..



This radar graph illustrates near real-time PCI DSS compliance posture as seen within the Catbird web interface. The blue line indicates the PCI DSS compliance controls baseline and the shaded area represents the actual PCI DSS compliance level within this virtual infrastructure.

ABOUT THE SOLUTION

COMPONENTS

Catbird provides a 100 percent software solution that is deployed on virtual and cloud infrastructure. It includes:

- Catbird Control Center, a web management console and central processing hub for all security and compliance operations, providing visualization, workflow, and reporting for Catbird TrustZones (logical zoning) policy and virtual compliance.
- Virtual Machine Appliances (VMAs), deployed on the virtual network itself – one per virtual switch or hypervisor.

FEATURES

Technical security controls within VMAs consist of:

- Firewall orchestration
- Network Access Control (NAC)
- Intrusion Detection and Protection (IDS/IPS)
- Net Flow
- Vulnerability monitoring and SCAP configuration checks
- Virtual Infrastructure Monitoring, integrated with hypervisor APIs for network configuration, access control, auditing, monitoring and policy enforcement

COMPLIANCE

Catbird provides assurance and evidence of control for industry standards including::

- PCI DSS 2.0 and 3.0
- HIPAA
- FISMA / FedRAMP (NIST 800-53)
- DIACAP
- COBIT (SOX / GLBA)
- ISO27001

HOW CATBIRD ADDRESSES REQUIREMENTS IN PCI DSS 3.0

Matrices below for requirements of PCI DSS 3.0 describe primary issues related to compliance for a virtual CDE, and how Catbird addresses those issues.

Scoping and Network Segmentation

PCI DSS	Catbird
PCI DSS security requirements apply to all system components included in or connected to the CDE, including: virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. Segmentation is not an official requirement of PCI DSS, but the standard strongly recommends it as a method that may reduce the scope and cost of an assessment, the cost and difficulty of implementing and maintaining PCI DSS controls, and the risk to an organization. Visibility of all assets, CHD, and net flow in a virtual CDE is mandatory in order for an auditor to validate the segmentation. In a virtual CDE, segmentation requires a special tool to establish zoning, enable visibility, ensure enforcement of policy, and verify compliance. (See PCI DSS 3.0, p.10-11.)	Catbird is the industry's only comprehensive solution for automating security controls in a virtual environment and enabling compliance with PCI DSS. Catbird reduces scope and enables virtual network segmentation for PCI compliance by providing: ■ **Enterprise-wide logical zoning.** Catbird creates logical zoning for consistent segmentation in a virtual CDE, enabling constituent firewall rules across multiple data center instances within a single Catbird instance, thereby reducing the risk and cost of copying and duplicating rules. ■ **Firewall event capture for continuous enforcement.** Catbird continually monitors virtual CDEs, capturing firewall events and automatically mapping those events to the corresponding PCI control. This provides a continuous compliance state and audit record to verify effective segmentation.

Requirement 1 – Install and maintain a firewall configuration to protect cardholder data.

PCI DSS	Catbird
Requirements to establish and implement firewall and router configuration standards (1.1), build firewall and router configurations that restrict connections between untrusted networks and any system components in the CDE (1.2), and prohibit direct public access between the Internet and any system component in the CDE (1.3) carry special challenges for a virtualized CDE. ■ PCI DSS 3.0 has new requirements for a network diagram is required identifying all connections between the CDE and other networks, and all cardholder data flows across systems and networks. Tools for physical networks may have limited visibility on components and data flows within a virtualized CDE. ■ Documenting use of all services, protocols, and ports allowed – with corresponding security features – may be problematic with a virtual CDE, particularly when virtual components are unpredictably dormant or off-line. ■ Firewalls and routers for physical networks may not extend granular security controls to virtual firewalls and virtual routers.	Catbird includes PCI DSS policy automation with security templates. This allows operators to define one or more CDEs and then apply PCI DSS security policy automatically or via "drag and drop" to 10's or 100's (or more) of similar CDE virtual assets. Catbird supports the configuration of multi-compartment DMZ, internal, and CDE zones. Catbird enables policy-based automated enforcement of: ■ **Catbird TrustZones segmentation isolates** the CDE from non-CDE resources, preventing direct access from the Internet; ■ **Zone access controls** for the CDE boundary and for limiting traffic to only that which is explicitly authorized; ■ **Zone network flow auditing,** FW-pass/FW-block/IDS/IPS displayed on a current traffic map and zone flow history table with ad hoc filter capabilities; ■ **Automated TrustZone policy application** supports default deny firewall policy for new assets, default scanning policies for incorrect asset configuration, and firewall compliance analysis; ■ **Virtual infrastructure audit and control** for virtual machine and virtual network changes; ■ **Federation of virtual CDE firewall rules,** auditing and control for virtual firewall management access.

Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters.

PCI DSS	Catbird
PCI DSS 3.0 has enhanced requirements for password controls (2.1, 2.2). These include always changing all vendor-supplied default passwords and defaults, and removing or disabling unnecessary default accounts before installing a system on the network. Configuration standards must be developed for all system components, addressing all known security vulnerabilities and consistent with industry-accepted system hardening standards. Another new requirement is to maintain an inventory of system components that are in scope (2.4). These rules apply to components in a virtualized CDE. ■ Specialized tools may be required as password and configuration tools for physical environments may not extend all functionality to virtualized components in the CDE. ■ Password and configuration controls must address virtualized components in the CDE that are dormant or off-line. ■ Vulnerabilities for virtualized components may be different from vulnerabilities tracked by security tools for a physical environment. ■ Vulnerabilities must be addressed for virtualized components in the CDE that are dormant or off-line.	Catbird includes control capabilities for identification and blocking of insecure services, zone-based control of access to network services, and net flow 9-tuple data augmented with virtualization tuples for zone, port group, and virtual hosts. The solution also produces a real-time map or inventory of all assets in the virtual CDE with data flows producing a real-time data flow diagram. These controls enable capabilities including but not limited to: ■ **Identification of application services** and/or multiple primary functions via network scanning; ■ **Limitation of services** to explicitly enabled ports and protocols; ■ **Identification of any enabled** insecure services or protocols; ■ **SCAP configuration security baselines** reduce use of vendor default configurations and passwords; ■ **Trusted and network based vulnerability scanner** supports vulnerability management programs.

Requirement 3 – Protect stored cardholder data.

PCI DSS	Catbird
PCI DSS 3.0 requires keeping CHD storage to a minimum. When storage of PAN is required, it must be rendered unreadable anywhere it is stored. 3.4 permits four approaches including strong cryptography. ■ Key-management processes and procedures for a physical environment may not extend to a virtualized CDE, which would require specialized tools. ■ 3.4.1 requires that logical access to disk encryption be managed independently of native OS authentication and access control mechanisms. In many cases, access to the hypervisor will also provide access to traditional encryption controls used on virtualized data and assets, so specialized tools may be required. ■ 3.5.1 requires restriction of access to cryptographic keys. In many cases, access to the hypervisor will also provide access to cryptographic keys stored on virtualized assets, so specialized tools may be required.	Catbird provides logical zoning to ensure continuous protection of stored data in the virtual CDE – including data stores connected to VMs that are powered off and on by system operators.

Requirement 4 – Encrypt transmission of cardholder data across open, public networks.

PCI DSS	Catbird
4.2 requires never sending unprotected PANs by end-user messaging technologies. A virtual CDE requires a special tool to secure cardholder data transmitted over virtual networks.	Catbird includes TrustZone access, vulnerability scanning and IDS controls that may be used to limit services to encrypted ports and to detect unencrypted traffic on any port.

Requirement 5 – Protect all systems against malware and regularly update anti-virus software or programs.

PCI DSS	Catbird
5.2 and 5.3 require controls to be fully operative in the virtual CDE. Multiple anti-virus products may be need to protect guest OSes and underlying host OSes. ■ Traditional anti-virus mechanisms may interfere with certain virtualization functions. ■ Traditional anti-virus mechanisms may not provide adequate protection for all virtualization layers.	Catbird provides vulnerability and configuration scanning of virtual system configuration for verification of anti-virus status in the virtual CDE.

Requirement 6 – Develop and maintain secure systems and applications.

PCI DSS	Catbird
6.1 requires using a process to identify and rank security vulnerabilities in the CDE. 6.2 requires protecting all system virtual system components and software from known vulnerabilities by installing the latest security patches. 6.4 requires following change control processes and procedures for all changes to virtual system components. Specialized tools may be required to deploy and verify patches for virtual assets. ■ Vulnerability management and patching tools for physical environments may not work in a virtual CDE. ■ Patching must account for scheduling system layers and virtualization technologies – including dormant or off-line VMs. ■ Requires separation of duties and access controls across multiple levels. ■ Requires isolation of development and test environments from production environments. ■ Testing of changes to virtualized assets may have multiple layers of potential impact.	Catbird provides vulnerability and configuration management for scanning applications in the virtual CDE. It includes zone access and IDS controls that may be used to segment and prevent unauthorized communications between test, development and production environments. Its reporting capability allows an independent board to oversee changes in the hypervisor environment or virtual infrastructure configuration.

Requirement 7 – Restrict access to cardholder data by business need to know.

PCI DSS	Catbird
7.2 requires an access control system, and the virtual CDE requires implementation across multiple layers to be effective. ■ Not all virtualization technologies can separate administrative access to the host or hypervisor from individual hosted virtual components. Granular virtual access control requires a specialized tool.	Catbird includes virtual access policy automation, security templates, and expert system compliance visualization to: ■ **Automate controls** for virtual firewall and network access on a business need to know basis; ■ **Detect unprotected** virtual machines; ■ **Report** when default deny-all settings are not in place.

Requirement 8 – Identify and authenticate access to system components.

PCI DSS	Catbird
PCI DSS 3.0 has augmented requirements for identity and access authentication, such as minimum requirements for passwords / phrases, for regular changes (8.2), and use of two-factor authentication for remote access (8.3). In a virtualized CDE, these controls may be needed across multiple virtual layers and intermediate technologies used to access virtual components. ■ Access restrictions may be required such as remote access to the hypervisor to defined source systems, management interfaces, and consoles. ■ Dormant or off-line virtual components containing CHD require strong access controls. ■ Virtual images and snapshots could capture passwords in active memory, causing unintentional and unprotected storage of CHD.	Catbird TrustZones and security controls enable controlling access to hypervisor management services from specific and limited authenticated sources.

Requirement 10 – Track and monitor all access to network resources and cardholder data.

PCI DSS	Catbird
The audit trail and logging requirements of Requirement 10 also apply to the virtual CDE. Challenges include: ■ Specific system functions and objects to be logged may differ according to specific virtualization technology in use. ■ Audit trails in VMs are usually accessible to anyone with access to the VM image. ■ Specialized tools may be required to correlate and review audit log data from within virtualized components and networks. ■ It may be difficult to capture, correlate, or review logs from a virtual shared hosting or cloud-based environment.	Catbird enables virtual zone access, net flow, and common event format auditing to: ■ **Protect and audit network access** to audit and log aggregation servers. ■ **Provide an event stream for all controls** indicating: policy application, policy changes, control operation, control, configuration, compliance state, and network events via syslog, enabling the most comprehensive event audit trail from a single source.

Requirement 11 – Regularly test security systems and processes.

PCI DSS	Catbird
11.2 requires running internal and external network vulnerability scans at least quarterly and after any significant changes in the network. 11.4 requires using IDS/IPS to prevent intrusions to the virtual CDE by monitoring all traffic at the perimeter of the CDE and at critical points within. Significant related issues for a virtualized CDE include: ■ Scanning and testing may be required across multiple virtual layers: all virtual endpoints, hosts, hypervisor interfaces and management consoles. ■ Additional scans may need to address dormant/off-line VMs. ■ Virtualization-specific vulnerabilities may not be detected by traditional scanning tools. ■ Specialized tools may be required scan virtual components from within the virtualized CDE. ■ Specialized IDS/IPS solutions may be required to monitor traffic over virtual networks and between virtual systems. ■ Specialized tools may be required to monitor critical files within the virtualized CDE. ■ Controls for monitoring traffic and CHD in the virtual CDE may need to encompass dormant and off-line VM images.	Catbird's SCAP validated configuration scan and vulnerability scan functions are fully integrated with virtual infrastructure audit and inventory management assuring coverage of the virtualized CDE. The solution also enables deployment of IDS/IPS and net flow probes on a per virtual host or per virtual switch basis providing real time threat detection and flow auditing. All scanner and IPS events trigger a corresponding alert to authorized personnel assuring that changes in the vulnerability threat surface are identified and addressed for all CDE components.

Requirement 12 – Maintain a policy that addresses information security for all personnel.

PCI DSS	Catbird
Requirement 12 mandates a security policy and risk assessment process to protect the virtual CDE, operational security procedures, and an incident response plan. Specific policies and procedures must address unique aspects of virtual environments: ■ The risk profile of a virtual CDE will be different from a physical environment. ■ Usage policies must address proper use of virtualization-based technologies. ■ Additional user training may be needed to ensure understanding of the security implications and proper use of virtualized technologies. ■ Specialized training may be needed for personnel responsible for monitoring and responding to security incidents in a virtualized CDE.	Catbird performs continuous compliance monitoring of the CDE. Any control policy change that results in a lack of coverage of CDE components will generate an easily identifiable change in compliance levels for the PCI DSS. Catbird continually inventories and monitors all virtual infrastructure assets in the CDE and applies security policy for Firewall, IPS, Vulnerability Scanning, Configuration Scanning, Layer 2 connectivity monitoring, network flow auditing, dynamically changing policies in response to configuration changes of virtualized CDE components. Catbird's multi-functional virtualized security controls provide the most comprehensive and most verifiable application of security policies that are required by the PCI DSS making virtualized CDE more secure and easier to audit than their physical counterparts. The combined virtualization aware controls of Catbird enable security and compliance teams to easily apply more controls with a single solution greatly reducing training costs for network based security controls in the virtualized CDE. .

SOLUTION BENEFITS

Catbird provides clear, continuous visibility into the virtualized IT environment and puts automated control of network security and compliance into the hands of your organization's key stakeholders. A summary of benefits by stakeholder includes:

DATA CENTER & NETWORK OPERATIONS

- Perfect inventory ensures control through automatic mapping of all virtual assets
- Automatic application of security controls based on logical zoning of all virtual assets through the entire lifecycle
- Event and policy alerts integrated with Security Information and Event Management (SIEM) and trouble ticketing systems

SECURITY OPERATIONS

- Automatic and consistent application of security policy with all virtual assets
- Automatic enforcement through optional mitigation actions, including quarantine
- Simplified management of security in a complex virtual environmen

COMPLIANCE OPERATIONS

- Reduces audit scope by providing evidence of control for network security requirements through the entire lifecycle of the virtual machine assets, automatically applies and enforces relevant controls to the virtual environment
- Reduces compliance cost by simplifying the compliance process with SOX, GLBA, PCI DSS, HIPAA and other regulations through automatic generation of near real-time audit-ready virtual network diagrams, Net Flow, and compliance posture documentation
- Reduces risk of compliance failure through audit enforcement by automatically mitigating against policy violations

LEARN MORE

With the accelerating adoption of virtualization technology for payment card processing, it's vital for organizations to recognize the limitations of physical security components in providing adequate visibility and protection of cardholder data in this environment. Catbird is a unique solution engineered to automate seamless, comprehensive security and PCI DSS compliance for organizations with a virtual CDE. We invite you to learn more about how your enterprise can use Catbird to automate virtual security and enable PCI DSS 3.0 compliance for your virtual Cardholder Data Environment. To learn more, please visit contact us or visit www.catbird.com.

CATBIRD

866.682.0080
info@catbird.com

Catbird brings the power, agility and automation of the cloud to security policy and compliance, with a solution that automates, instruments and enforces policy while providing proof of continuous compliance. Customers rely on Catbird for managing cloud and virtualized infrastructure subject to compliance requirements including HIPAA, PCI-DSS, FISMA and SOX. The company is a winner of four Best of Show Finalist Awards at VMworld, CRN's 2013 Virtualization 50 and SC Magazine's "Innovator of the Year" for virtualization security. For more information please visit http://www.catbird.com.