PCI Compliance with Catbird

Automating Security & Compliance in a Private Cloud

All merchants and financial institutions 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). Virtualization technology and the use of private clouds are addressed by PCI DSS 3.0. Traditional physical security components that are usually deployed at the network edge are difficult if not impossible to effectively monitor and control virtual components, so it is vital for organizations using virtual technology in the Cardholder Data Environment to adopt tools that protect cardholder data. Catbird® is a unique solution engineered to automate seamless, comprehensive security and PCI DSS compliance for organizations with a virtual CDE.

SEGMENTING THE CARDHOLDER DATA ENVIRONMENT

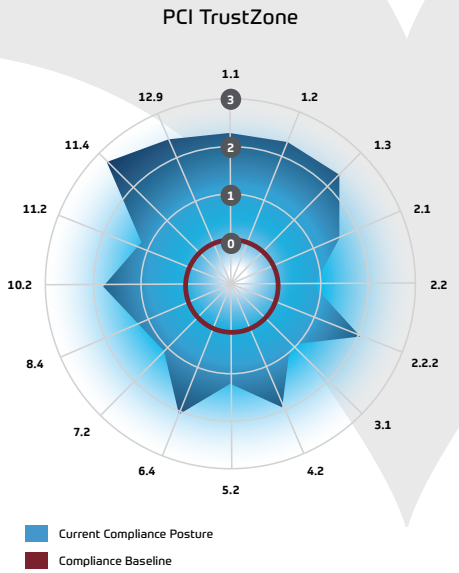
Segmenting, or isolating the CDE is "strongly recommended" by PCI DSS 3.0 to reduce the scope and cost of an assessment, lower the cost and complexity of implementing and maintaining controls, and reduce risk. Proper segmentation requires that even if the out-of-scope system component was compromised it could not impact the security of the CDE. Catbird enables easy segmentation of CDE in a virtual environment with its logical zoning container called Catbird TrustZones®. By dragging and dropping virtual assets on the data plane into TrustZones, the assets automatically inherit PCI DSS security policies set for the containers (similar to how Microsoft Active Directory assigns policies to its objects).

MAPPING AND MANAGING ALL VIRTUAL ASSETS IN THE CDE

Segmentation enabled with TrustZones is the bedrock of software-defined security in the virtual CDE. It provides precise visibility and management of all virtual networks, network devices and system components. This includes a perfect inventory of all assets as they are turned on or off in the dynamic virtual environment – including mapping capability that diagrams all cardholder data flows across systems and networks. These are new requirements in PCI DSS 3.0 (1.1.3 and 2.4) and are fulfilled automatically by Catbird.

ENFORCING & DOCUMENTING PCI DSS POLICIES

PCI DSS policies are automatically assigned by Catbird to all virtual assets placed in TrustZones, which enables the solution to automatically and deterministically enforce those policies to protect cardholder data wherever it may be processed, stored or transmitted in the virtual CDE. For example, Catbird automatically executes virtual firewall policies such as blocking, alerting and quarantining according to PCI DSS requirements. Catbird uses the same control framework as PCI Qualified Security Assessors, so its virtual network diagrams, Net Flow maps and operational reports instantly provide "audit-ready" documentation whenever you need it.



Catbird maps the compliance posture of a virtual data center to PCI DSS security controls producing real-time audit diagrams.

Solution Benefits

Catbird provides clear visibility into the virtualized Cardholder Data Environment and puts control into the hands of your organization's key stakeholders:

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 entire lifecycle
- Event and policy alerts integrated with 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 environment

COMPLIANCE OPERATIONS

- Reduces audit scope by providing evidence of control and automatically applying and enforcing PCI DSS 3.0 in the virtual environment
- Reduces compliance cost by simplifying the PCI DSS 3.0 compliance process through automatic generation of near real-time audit-ready reports
- Reduces risk of compliance failure through audit enforcement actions

CATBIRD®

HOW CATBIRD ADDRESSES CONTROLS IN PCI DSS 3.0*

The PCI Security Standards Council's Virtualization Special Interest Group has published its Information Supplement: PCI DSS Virtualization Guidelines. It contains an overview of virtualization issues related to securing cardholder data, including risks for virtualized environments and recommendations. For details, please visit www.pcisecuritystandards.org. The table provides a summary of how Catbird addresses requirements in PCI DSS 3.0.

REQ. 1 – firewall configuration	Catbird's logical zoning of virtual assets into security groups is combined with firewall management and automated visualization and updating of Net Flow maps.
REQ. 2 – network & system configurations	Catbird enables automated enforcement of secure network configurations and the ability to passively detect incorrect or weak system configurations.
REQ. 3 – protecting stored cardholder data	Catbird's logical zoning ensures continuous protection of stored data in the virtual CDE – including data stores connected to VMs that are powered off and on by system operators.
REQ. 4 – encryption	Zone access and IDS controls may limit services to encrypted ports and detect unencrypted traffic on any port.
REQ. 5 – anti-virus protection	Catbird provides continuous agent-less scanning of virtual system configuration and host-based anti-virus status in the CDE.
REQ. 6 – securing applications	Zone access and network traffic controls may separate development and test environments from the production CDE and segment privileged user access to these environments.
REQ. 7 – access control	Catbird automates firewall and network access controls, detects unprotected virtual machines, and reports and alerts when default deny-all settings are not in place.
REQ. 8 – authentication	Catbird enforces restricting access by devices to the hypervisor and prevents use of vulnerable services.
REQ. 10 – access tracking & monitoring	Catbird zone access, net flow, and common event format audit controls may be used to: Validate that NTP is deployed and used according to policy; and/or protect and audit network access to audit and log aggregation servers.
REQ. 11 – testing security	Catbird deploys IDS/IPS and net flow probes on virtual hosts and virtual switches. It automatically detects a failure of IDS/IPS coverage for any CDE asset and triggers corresponding alerts to designated personnel.
REQ. 12 – managing policies	Catbird continuously monitors compliance of all virtual assets in the CDE and applies operator-defined security policy. Control failures trigger compliance alerts to designated personnel and a trouble ticket system.

ABOUT THE SOLUTION

Catbird is a 100 percent software solution that is deployed on virtual and cloud infrastructure.

COMPONENTS

- Catbird Control Center, a web management console and central processing hub for all security and PCI DSS compliance operations.
- Virtual Machine Appliances (VMAs) deployed on the virtual network itself — one per virtual switch or hypervisor.

FEATURES

The Catbird Control Center is the policy definition point, providing visualization, workflow, and reporting for TrustZones policy and virtual compliance.

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 PCI DSS policy enforcement.

SYSTEM REQUIREMENTS

Catbird supports all releases of VMware vSphere and ESX 4.0 and above and Microsoft Hyper-V Server 2012, SP1, and R2. VMware NSX will be supported upon release.

TEST DRIVE CATBIRD

Catbird has built a demonstration environment that provides a full function product experience. We invite you to test drive Catbird by visiting www.catbird.com/demo.

Copyright © 2014 Catbird Networks, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Catbird products are covered by one or more patents. Catbird and vSecurity are registered trademarks of Catbird Networks, Inc. in the U.S. and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

www.catbird.com

Catbird 1800 Green Hills Road Suite 113
Scotts Valley CA 95066 USA
Tel 866.682.0080

PCI COMPLIANCE WITH CATBIRD DS | US-042114