

Automating Security Control & Compliance Enforcement for Financial Services

Understanding the Value of Catbird vSecurity for Security and Multi-Regulatory Compliance in a Private Cloud

EXECUTIVE SUMMARY

For financial institutions using virtual IT infrastructure, it's difficult if not impossible to effectively monitor those components and control the security of sensitive data with traditional physical security that is usually deployed at the network edge. A major pitfall is the inability to enforce compliance with laws and regulations governing security of sensitive data, such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), Payment Card Industry (PCI) Data Security Standard (DSS) and Health Insurance Portability and Accountability Act (HIPAA). Catbird vSecurity® is a unique solution engineered to automate seamless, comprehensive network security and compliance of virtualized IT and data. Catbird vSecurity can address the security and compliance requirements facing data centers as they migrate from physical to virtual, whether on or off premise, in a private or hybrid cloud configuration. Benefits extend to all key IT stakeholders in a financial institution, including Data Center & Network Operations, Security Operations and Compliance Operations. This paper describes Catbird vSecurity's five value propositions for financial institutions by meeting the full complement of auditor-required network security controls for a virtualized data center.

ASSESSING THE CHALLENGES OF VIRTUAL SECURITY

Virtualization is not just an operational change in IT; it also affects how financial institutions enforce and document compliance for a range of regulatory requirements including SOX, GLBA, the PCI DSS, and HIPAA.

Securing cardholder data (CHD), Personally Identifiable Information (PII) and other sensitive information in the cloud is a challenge because traditional network security technology, which is deployed at the edge, is unable to easily and comprehensively protect the virtualized network components inside the cloud. Particular issues include data segmentation, IT asset management and policy enforcement.

With these issues comes the challenge of enforcing and documenting compliance. Without the use of controls that are specifically engineered for cloud, a financial institution will be unable to have continuous visibility on sensitive data traversing the network in the cloud, nor the technical capability to protect it and prove to auditors that the organization is compliant with regulatory requirements.

Some financial institutions are attempting to adapt traditional physical network security tools, but this process is complex, highly manual and ill-suited to the nature of dynamic cloud environments.

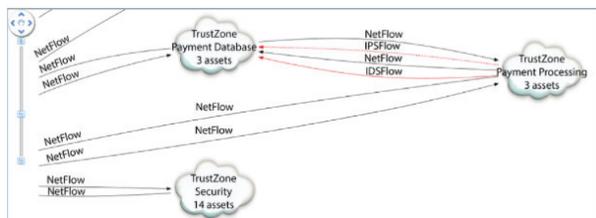
Financial institutions can immediately reap many benefits by using Catbird vSecurity, the industry's only software-defined multifunctional tool expressly designed to control and enforce security for networks in virtual environments, and provide the ability to demonstrate/prove compliance for auditors.

1. AUTOMATED, LOGICAL SEGMENTATION

Segmenting, or isolating critical IT assets and sensitive data in a virtualized environment is the bedrock strategy for reducing the scope and cost of audits, lowering the cost and complexity of implementing and maintaining controls, and reducing risk.

Proper segmentation requires that even if the out-of-scope system component was compromised, it could not impact the security of sensitive data.

Catbird vSecurity enables easy segmentation of assets and sensitive data in a virtual environment with its logical policy container called a TrustZone™. By dragging and dropping virtual assets on the data plane into TrustZones, the assets automatically inherit security policies set for the containers (similar to how Microsoft Active Directory assigns policies to its objects).



Catbird vSecurity logically organizes all sensitive assets into TrustZones, assigns and enforces security policies, and automatically maps Net Flow for compliance.

2. PERFECT INVENTORY OF ALL VIRTUAL ASSETS

Segmentation enabled with TrustZones provides precise visibility and management of all virtual networks, network devices, system components and sensitive data in the cloud.

Control includes a perfect inventory of all assets as they are turned on or off in the dynamic virtual environment. The automation around creating this perfect inventory provides a crucial benefit, for manual tracking is nearly impossible due to rapid, continuous changes in virtual infrastructure.

Inventory mapping also enables the benefit of automatically producing diagrams that show Net Flow across all systems and networks. Manually mapping accurate Net Flow is impractical if not impossible.

3. CONTINUOUS MONITORING

Catbird vSecurity provides the positive assurance of control with continuous monitoring for network components in the entire virtual environment.

Monitoring includes all virtual assets and network activity, plus automatic enforcement of access controls and network configurations.

The benefit of continuous monitoring is the ability to immediately spot changes that may compromise the security and compliance posture. Alerts for security policy violations may be followed by manual or automatic policy-based enforcement actions to mitigate and maintain compliance.

An additional component of continuous monitoring is vulnerability management, which includes network-based checks on the Virtual Machine and hypervisor configuration, such as credentialed checks against file format.

4. COMPREHENSIVE SECURITY, COMPLIANCE & POLICY ENFORCEMENT

Catbird vSecurity automatically maps its security and enforcement policies to frameworks relevant to financial institutions, including:

- Control Objectives for Information Related Technology (COBIT) used for Sarbanes-Oxley Act (SOX) and Gramm-Leach-Bliley Act (GLBA) compliance.
- Payment Card Industry (PCI) Data Security Standard (DSS) v.3.0 used for PCI compliance.
- The U.S. Dept. of Health and Human Services Privacy and Security Framework used for Health Insurance Portability and Accountability Act (HIPAA) compliance.

These policies are automatically assigned by Catbird vSecurity to all virtual assets placed in TrustZones, which enables the solution to automatically and deterministically enforce those policies to protect sensitive data wherever it may be processed, stored or transmitted in the virtual environment.

Catbird vSecurity uses the same control frameworks as auditors, so its virtual network diagrams, Net Flow maps and operational reports instantly provide “audit ready” documentation whenever you need it.

5. OPERATIONAL EFFICIENCIES

The Catbird solution is deployed and managed from a single processing hub and interface, so it provides financial institutions with significant operational efficiencies – beginning with a simplified hardware infrastructure to support security controls and compliance for the virtual environment.

The solution is 100% software-based with a minimal processing footprint, so financial organizations can easily use existing IT platforms to host Catbird vSecurity.

Being a multifunction solution, financial institutions get systematic and maximum coverage without having to deploy and manage multiple tools.

Automation of inventory tracking, monitoring and real-time reporting provides these resources on demand when needed for management, forensics and interfacing with auditors.

With Catbird vSecurity, Data Center, Security and Compliance professionals can focus on a single interface, which streamlines their efforts and makes them more efficient – freeing time to deal with other important responsibilities.

ABOUT THE SOLUTION

COMPONENTS

Catbird vSecurity provides a 100% software-defined security solution that is deployed on virtual infrastructure servers such as VCE vBlock. It includes:

- Catbird Control Center, a Linux-based virtual appliance with web management console for vSecurity and central processing hub for all security and compliance operations.
- Virtual Machine Appliances (VMAs), which are deployed on the virtual network itself – one per virtual switch or hypervisor – not on the Virtual Machines.

FEATURES

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

- VMAs execute best-practice technical security controls mapped to specific frameworks:
- Firewall orchestration
- Network Access Control (NAC)
- Intrusion Detection and Protection (IDS/IPS)
- Net Flow
- Vulnerability monitoring
- Virtual Infrastructure Monitoring, which is integrated with hypervisor APIs for network configuration, access control, auditing, monitoring and policy enforcement

CONCLUSION

Catbird vSecurity 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 environment

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

We invite you to learn more about how your enterprise can automate security and enable compliance for your virtual IT infrastructure with Catbird vSecurity. To learn more, please visit contact us or visit www.catbird.com.

CATBIRD

866.682.0080
info@catbird.com

Catbird is a global leader in the virtualization and cloud security market. The Catbird vSecurity solution is based on logical zoning — TrustZones — a location-independent network-based policy enforcement capability. vSecurity policies apply a broad set of network security technical controls to TrustZones to monitor and enforce security for virtualized network components. Of particular value to Catbird partners and customers is the ability to deliver near real-time compliance visualization, workflow and reporting against the leading standards to ensure a positive assurance of control necessary for audits. Catbird partners have accelerated their time to market for compliant services, enabling them to focus on core differentiation while avoiding the risk and complexity of a "build-your-own" strategy.

