CATBIRD® WHITE PAPER

VIRTUAL SECURITY FOR HIGHER EDUCATION

Catbird protects private clouds with multiple security controls and produces proof of compliance easily and efficiently.

Compliance and information security demands are top concerns for America's higher education institutions. The regulations and compliance requirements are growing and continue to challenge colleges and universities capabilities to meet these demands. With technology advancements in the virtual compute space and ever changing vulnerability complexities, producing a record of compliance and supporting those strategies and methods of a secure and stable environment are a mind-boggling challenge.

SOLUTION BENEFITS

- Change control via Network Access Control
- Continuous monitoring and policy enforcement via IDS/IPS
- Logical segmentation of assets via TrustZones™
- Data flow diagrams to prove segmentation
- Automated mapping of security controls to compliance frameworks (FISMA, HIPAA, PCI and more)
- Firewall orchestration of VMware® vCNS® (vShield®) enabling dynamic updates to firewall controls

OCTOBER 2013

INTRODUCTION

In order for an educational institution to be able to utilize government grants for research and fund certain programs they are often subject to FISMA and/or HIPAA oversight by way of their Federal contract obligations. Many education institutions continue to offer more and more payment options for student faculty, and others, forcing the institution to manage more complex amounts of payment card information. With this development in credit card technology, the risk profile puts the institutions in scope for Payment Card Industry's Data Security Standard (PCI DSS).

WHAT DOES THIS MEAN?

1. Education institutions will need to assess their information security posture as well as their compliance initiatives.
2. Inconsistent security controls across departments and schools can result in multiple security regimes and a lack of standardization, which affects the ability to consolidate and manage a compliance program for campus and online-based e-commerce.
3. Institutions will need to be cognizant of the changing rules and regulations pertaining to the compliance measures that are applicable to their specific guidelines.
4. The impact of these rules and guidelines often can cause unease and the sense of distrust or "big brother." Examples of issues in need of attention but not limited to are:

- Liberal access rights to systems (lack of network segmentation)
- Improper storage of cardholder data
- Insufficient data asset inventory/classification
- Categories of protected information
- Minimum baseline controls
- Refinement of controls using a risk assessment procedure
- Documenting the controls in the system security plan
- Implementing security controls in appropriate information systems
- Assessing the effectiveness of the security controls once they have been implemented
- Authorizing the information system for processing
- Monitoring the security controls on a continuous basis

WHERE TO BEGIN?

Universities and colleges throughout America are the center of free thought and the incubator for innovative ideas and concepts. To support an intellectual environment, a key consideration is the capability of sharing knowledge. In order to accomplish the ability to meet your compliance and security requirements and not dilute the perspective and needs of the broader campus, a few simple steps can be taken to avoid disaster in either direction.

1. Determine if you need to comply (check contracts, talk to researchers, talk to agency IG)
2. Perform a risk assessment
3. Categorize government information and systems in use
4. Perform a gap analysis between requirements and current state of your organization
5. Develop plan to remediate gaps
6. Test design and effectiveness of controls
7. Remediate control issues
8. Re-test design and effectiveness of controls
9. Report on compliance

SIMPLE RIGHT?

For most organizations the previous list is a monumental task that requires an organization-wide concerted effort drawing key resources away from mission critical focus. In addition to stay in tune with regulatory updates and then assess those against the ever-changing environment, the task

of asset management and policy enforcement poses a significant challenge. Up until very recently this has been an uphill battle that has required endless hours of focus and effort.

In addition to increasing compliance requirements, most organizations have started if not completely migrated to virtualized infrastructures. Traditional physical data center architectures are rigid and complex. Hardware-defined network security has limitations that become acute in a virtualized infrastructure, which is characterized by transience and mobility. Physical devices deployed on the perimeter of the data center have no visibility to security-related activity occurring within the virtual infrastructure.

As virtualization expands to sensitive and mission critical systems, security professionals must ensure that the virtualized systems they oversee remain secure and compliant. As with any significant technological change, virtualization and cloud computing bring new security challenges, but also the unique opportunity to apply security in better ways.

VERY SIMPLE!

Catbird® vSecurity® is the industry's first network security solution architected for virtualized infrastructure. As software-defined security, vSecurity delivers security that is adaptive, automated, accurate and scalable while also providing continuous compliance monitoring and reporting. vSecurity introduces simplicity to the world of network security, providing protection based on logical policies not tied to any server or specialized security device.

Just as virtualization abstracts computing away from physical hardware, Catbird vSecurity untethers security from expensive single-purpose security appliances. This decoupling of security from a particular vendor's hardware device or APIs is at the root of software-defined security. Reconstituted as software only, security is flexible and automated—and able to become part of the network itself.

Catbird vSecurity addresses the list of regulatory requirements that historically required hundreds of man-hours. vSecurity consolidates the most critical network security controls into a single software-based product enabling a secure and compliant virtual or private cloud infrastructure. The controls encompass all the areas common to defense-in-depth and ensure IT can meet the full complement of auditor-required network security controls, including:

Auditing: vSecurity captures a rich event stream from its broad offering of technical controls to confirm security posture, generate alerts and trigger workflow.

Inventory Management: vSecurity automatically detects VMs and enforces policy, including optional automatic quarantine

Access Control: vSecurity ensures VMs are appropriately managed and isolated, irrespective of changes in VM or virtual network configuration.

Configuration Management: Monitors network activity and enforces network configurations.

Change Management: Monitors for changes that may compromise security and compliance posture. Provides manual and policy-based enforcement actions.

Incident Response: Alerts for security policy violations and takes enforcement actions to mitigate and maintain compliance.

Vulnerability Management: Provides network-based checks on the VM and hypervisor configuration, including credentialed checks against file formats.

THE BENEFIT TO UNIVERSITIES

The benefits of virtualization are apparent. Virtual and cloud data centers promise significant cost savings, improved operating efficiencies, increased performance and dynamic and flexible data management. As data centers become virtualized, it is imperative to virtualize security as well. Physical security devices were not

designed to protect the new virtual components architecture of virtualization and will pose a significant security risk.

In recognition of these changes, independent 3rd party standards bodies, such as PCI, HIPAA, and FISMA, have modified their own regulations. Their updated specifications acknowledge that without appropriate technology and training, virtualization and cloud systems will introduce significant security and compliance gaps.

Virtualization improves security by making it automated, more fluid and context-aware. This means security is more accurate, easier to manage and less expensive to deploy than traditional physical security. Catbird vSecurity protects from within the virtual network, addressing these security and compliance gaps while reducing cost and complexity.

Catbird vSecurity is 100% software and utilizes the pioneering technology of TrustZones™ along with orchestrating Policy and Compliance, which enables IT security and networking personnel to: detect everything; virtualize everything (even critical apps); attain, maintain, monitor and enforce compliance; and accelerate VMware deployment. With the right technology and processes, virtualization has the power to make University cloud environments even more secure and compliant than the physical data centers they replace.

A University's prime objective is to build and develop the future of bright students. Catbird's objective is to simplify their effort to meet compliance requirements by integrating multiple security controls and boost efficiencies by mapping the security controls to regulatory frameworks, enabling real-time proof of compliance graphics and reports. By supporting Universities in the effort to secure their revenue stream with grant funding, Catbird also supports their effort in educating students and building a stronger tomorrow.

Visit **www.catbird.com** to learn more about our virtual security solution for **Higher Education** including compliance data sheets with detailed descriptions of FISMA, HIPAA, and PCI controls that are addressed by Catbird vSecurity.

CATBIRD

1800 Green Hills Road, Suite 113
Scotts Valley, CA 95066 U.S.
Tel 866.682.0080
catbird-sales@catbird.com