Executive Summary

Federal agencies must bolster IT security systems and practices to combat increasingly sophisticated cyber threats. SimpliVity Hyperconverged Infrastructure can help agencies shore up defenses by minimizing attack surfaces and encrypting data at rest. In addition, the product’s built-in data protection capabilities and accelerated data efficiencies let IT administrators quickly restore critical applications and services in the event of malware attacks or other service-impairing incidents.

This paper reviews cybersecurity trends and threats, and explains how SimpliVity Hyperconverged infrastructure can help agencies mitigate security risks and improve compliance with Government security initiatives.

Introduction

Cybersecurity is a top concern for IT professionals. Across the world, cyberattacks continue to grow in frequency, complexity and severity. A global PricewaterhouseCoopers study reveals global security incidents increased by 38% from 2014 to 2015, and corresponding intellectual property theft grew by 56%.¹

When it comes to cybersecurity threats, the U.S. Federal Government is certainly not immune. According to a November 2015 Government Accountability Office report, the number of reported information security incidents affecting federal systems has steadily increased from about 5,500 in fiscal year 2006 to almost 67,200 in fiscal year 2014.² And security events involving personally identifiable information such as social security numbers have more than doubled in recent years to over 27,600 incidents in 2014.

“The federal government faces an evolving array of cyber-based threats, as illustrated by recently reported data breaches at federal agencies, which have affected millions of current and former federal employees. Such incidents underscore the urgent need for effective implementation of information security controls at federal agencies.”

– 2015 GAO Report

¹ The Global State of Information Security® Survey 2016. © 2015 PricewaterhouseCoopers LLP
² GAO -16-228T, November 2015
Introduction

Security breaches can tarnish an agency’s reputation, erode public confidence and have serious consequences for the Government and its citizens, including:

- Disclosure or modification of confidential data including personally identifiable information and classified information
- Disruption of essential Government functions including emergency services and national defense operations
- Theft of information technology resources or financial assets
- Loss of Government worker productivity and taxpayer dollars
- Hijacking of information technology systems for fraud, impersonation or abuse
- Damage to applications, data, networks or equipment
- High remediation costs

Recognizing the enormous risks posed by cyberattacks, Congress has enacted a series of laws such as the 2014 Federal Information Security Modernization Act (FISMA) requiring agencies to improve the protection of Government IT systems and data. To that end, in 2015 the Federal CIO office issued a Cybersecurity Strategy and Implementation Plan (CSIP) to strengthen cybersecurity measures within the Federal Government.
SimpliVity Hyperconverged Infrastructure Mitigates Cybersecurity Risks

SimpliVity hyperconverged infrastructure delivers cloud economics and agility while satisfying stringent Government performance, resiliency and security requirements. Designed from the ground up to support today’s data intensive, highly-virtualized IT environments, the SimpliVity solution provides a scalable, modular 2U building block of x86 resources that offers all the functionality of traditional IT infrastructure—including hypervisor, compute, storage, and data protection capabilities—in a single device, with a unified, VM-centric administrative interface.

The SimpliVity solution features a number of unique capabilities and attributes that help Government CIOs and security officers support the CSIP initiative and improve FISMA compliance. Specifically, the SimpliVity solution can help Government agencies:

• Reduce security vulnerabilities by minimizing potential points of attack
• Protect data at rest with self-encrypting storage technology
• Improve remediation by accelerating data backup and restoration efforts

Minimizing Attack Surface to Reduce Cyber Risks

Security threats can take a variety of forms and can originate from inside or outside an agency. The National Security Agency recommends a layered “defense-in-depth” approach to security to protect against the widest range of threats. A complete strategy incorporates a wide range of security solutions and technologies including firewalls, intrusion detection/prevention systems, and virus and malware protection solutions. By implementing comprehensive security measures across the entire IT landscape—from the network perimeter to the applications running in the data center—agencies can improve their security posture and mitigate risks.

When formulating a defense-in-depth plan it is important to minimize points of attack for would-be intruders. Potential attack points include:

• Open ports on external-facing servers
• Services available inside of a firewall
• Applications running on agency servers
• Application interfaces (APIs, SQL queries, web forms, etc.)
• IT infrastructure administrative interfaces and code (servers, storage, networking, etc.)

By reducing network, software and other attack surfaces, agencies can narrow security threats and limit exposure. Traditional IT implementations composed of discrete compute, storage and SAN/NAS solutions with distinct administrative interfaces are inherently difficult to secure. Each technology platform and management interface represents a potential attack point—the more devices and administrative interfaces, the greater the attack surface.

“Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and the actions of careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees and other organizational insiders, foreign nations engaged in espionage and information warfare and terrorists.”

– 2015 GAO Report
SimpliVity hyperconverged infrastructure provides a single, shared x86 resource pool across the entire IT stack, eliminating siloed data center architectures with multiple technology platforms and broad attack surfaces. The solution limits potential points of attack and reduces security vulnerabilities by consolidating all the functionality of traditional IT infrastructure onto one device with a single administrative interface.

![Diagram](Image)

**Figure 2: SimpliVity Hyperconverged Infrastructure Mitigates Risks by Reducing Potential Attack Points**

**Protecting Data at Rest with Self-Encrypting Storage Technology**

A complete defense-in-depth strategy must protect not only data in motion but also data at rest on disk. Confidential data can be lost or stolen due to a physical security breach or if a disk leaves the secure confines of the data center for repair, retirement or relocation. SimpliVity hyperconverged infrastructure supports optional self-encrypting drives (SEDs) that help Government agencies protect data at rest on disk. SimpliVity SEDs employ Advanced Encryption Standard (AES) encryption, recommended by the National Institute of Standards and Technology (NIST SP800-111) and approved for Federal Information Processing Standard 140-2 Level 2 usage, including sensitive or classified national security data.

SimpliVity SEDs are easy to deploy and administer, with set and forget simplicity. And they are fully transparent to other IT infrastructure elements and applications. Once security is enabled, data is automatically encrypted and decrypted as it is written to and read from disk. A misappropriated disk cannot be unlocked without the secure encryption key embedded into the drive and the corresponding administrative passphrase.

SEDs provide strong security without impairing application or system performance. Data is encrypted and decrypted on the disk itself, so system compute resources remain fully available for mission-critical applications and services.

**Improving Resiliency by Accelerating Data Backup and Restoration Functions**

SimpliVity hyperconverged infrastructure provides efficient data backup and restoration capabilities that help IT organizations quickly recover from malware or ransomware programs that evade threat protection solutions. SimpliVity’s native data protection functionality enables rapid business continuity and disaster recovery, while eliminating the need for special-purpose backup solutions or WAN optimization appliances.
The SimpliVity solution performs inline deduplication, compression and optimization on all data at inception across all phases of the data lifecycle (primary, backup, WAN, archive, and in the cloud), across all tiers within a system (DRAM, Flash/SSD, and HDD), all handled with fine data granularity of just 4KB-8KB. By driving efficiencies at the point of origin and by offloading processor-intensive functions onto purpose-built data acceleration hardware, the solution conserves storage capacity and minimizes disk I/O and network traffic, accelerating data replication and workload mobility and freeing up compute cycles for business-critical applications.

The product’s inherent data efficiencies enable more frequent backups, longer retention periods, and faster recovery. With SimpliVity, terabyte-sized VMs can be backed up and restored in just seconds—even over bandwidth-constrained WAN links. In the event of malware or ransomware attacks, applications can be restored to previous-working versions in a matter of seconds or minutes. And SimpliVity’s global unified management capabilities simplify routine data protection administrative tasks. IT generalists can clone, move, backup and restore VMs with just two or three mouse clicks using familiar tools like VMware vCenter.

Conclusion

Government IT organizations must safeguard information systems and data against increasingly sophisticated attacks. SimpliVity Hyperconverged Infrastructure helps lower security risks and safeguard confidential information by minimizing potential points of attack and encrypting data stored on disk. And SimpliVity’s built-in data protection capabilities and accelerated data efficiencies enable rapid recovery from malware and ransomware programs and other service-impacting attacks. As part of a complete defense-in-depth strategy, the SimpliVity solution helps agencies improve FISMA compliance and support the CSIP directive.

For more information, visit:
www.simplivity.com

© 2016, SimpliVity. All rights reserved. Information described herein is furnished for informational use only, is subject to change without notice. SimpliVity, the SimpliVity logo, OmniCube, OmniStack, and Data Virtualization Platform are trademarks or registered trademarks of SimpliVity Corporation in the United States and certain other countries. All other trademarks are the property of their respective owners.