White Paper

# Managing Cybersecurity Risks with Confidentiality, Integrity, and Availability of Critical Data

Carina Veksler, Lee Vorthman, NetApp
January 2013 | WP-7177

## Abstract

Government agencies constantly balance the need to allow access to their data with the need to protect that data from attackers. NetApp takes a comprehensive approach to cybersecurity by providing technologies and solutions that enable agency data to be protected and trusted while still remaining accessible. Our cybersecurity technologies help protect data, know how data is being used, and minimize the risk that data will be lost in the event of an attack.

## TABLE OF CONTENTS


1 Cybercrime Threatens Everyday Life ..... 3

2 Securing Digital Assets with Cybersecurity ..... 4

2.1 Secure Access to Critical Information Is Essential ..... 4

2.2 Network Speeds Are Increasing ..... 4

2.3 Collected Data Provides Valuable Insights ..... 4

2.4 Fast Recovery Is Critical Following a Security Breach ..... 5

2.5 Data Encryption Is Key ..... 5

3 Cybersecurity Affects Storage Requirements ..... 5

3.1 Storage Requirements ..... 5

3.2 NetApp and Cybersecurity ..... 5

4 Protecting the Confidentiality, Integrity, and Availability of Your Data ..... 6

4.1 Confidentiality ..... 6

4.2 Integrity ..... 8

4.3 Availability ..... 9

5 NetApp Cyber Alliance Program ..... 10

6 Summary ..... 11


## LIST OF TABLES


Table 1) NetApp products deliver IAVA compliance. ..... 8

Table 2) NetApp disaster recovery. ..... 10


## LIST OF FIGURES


Figure 1) Cybersecurity concerns. ..... 3

Figure 2) Layers of cybersecurity technologies. ..... 4

Figure 3) Cyber reference architecture. ..... 5

Figure 4) Data security risk model. ..... 6

Figure 5) High-speed, high-fidelity packet capture. ..... 7

Figure 6) Cyberthreat analytics and monitoring. ..... 9

Figure 7) NetApp certifications. ..... 11

# 1 Cybercrime Threatens Everyday Life

Cyberspace has become an integral part of our daily activities. Everything from communications to managing finances, collaborating with peers, research, and access to government and business services now uses the Internet to streamline everyday tasks. However, as the sophistication of Internet capabilities has increased, so has the caliber of threats to Internet users. Hackers today are long past simply inconveniencing our lives and are now using sophisticated techniques to manipulate vulnerabilities in technology for financial gain. In a recent cyberthreat forecast for 2013 published by Georgia Tech, experts stated, "The bottom line, users must keep their guard up in the coming year."[1]

This sentiment is reinforced in the Symantec Internet Security Threat Report[2], summarizing 2011 cybercrime threat activity as follows:

- Symantec blocked a total of over 5.5 billion malware attacks in 2011, an 81% increase over 2010.
- Web-based attacks increased by 36%, with over 4,500 new attacks each day.
- 403 million new variants of malware were created in 2011, a 41% increase over 2010.
- 39% of malware attacks by e-mail used a link to a Web page.
- Mobile vulnerabilities continued to rise, with 315 discovered in 2011.

Cybercrime continues to be one of the fastest growing areas of crime. Due to the global nature of the Internet, criminals can easily commit illegal activity anywhere in the world. In addition to the increasing occurrences of data breaches, industrial espionage, identity theft, intelligence breaches, and denial of service, there is also a growing risk for a major attack on critical infrastructure, such as electrical grids, communications, and banking.

For the federal government, strengthening cybersecurity measures is an ongoing process. However, when attacks do occur, the time, expense, and lost productivity of recovering from the breach can cripple operations. But more important, agencies must deal with the potential threats resulting from compromised systems and lost data: the loss of personal or financial information and intelligence that affects national security.

**Figure 1) Cybersecurity concerns.**

| Theft and Espionage | Manipulation and Sabotage | Denial of Service |
|---|---|---|
| Use sophisticated attacks (advanced persistent threats) to steal intellectual property. | Gain access to and modify agency data to create adverse effect on future events. | Prevent access to tactical communications network to endanger lives of deployed military personnel. |

[1] http://www.darkreading.com/cloud-security/167901092/security/news/240142197/georgia-tech-releases-cyber-threats-forecast-for-2013.html.
[2] Symantec Internet Security Threat Report, (Volume 17, April 2012) http://www.symantec.com/threatreport/?inid=us_sr_flyout_publications_istr.

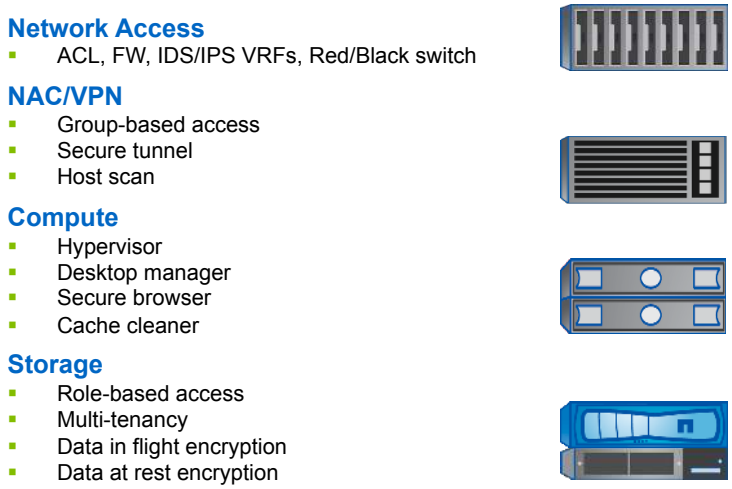
# 2 Securing Digital Assets with Cybersecurity

The White House has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cyber security.”[3]

## 2.1 Secure Access to Critical Information Is Essential

Having the right security measures in place makes it possible for both government agencies and citizens to access critical information when they need it. However, with the growing number of entry points into networks, applications, and back-end databases, such as mobile devices, virtual machines, laptops, and tablets, a broader range of security technologies is now required to provide the needed protection against penetration and disruption. In particular, with the addition of BYOD across agencies, these devices now represent a growing base for infections and compromise and can increase the potential for loss of confidential information.

**Figure 2) Layers of cybersecurity technologies.**




## 2.2 Network Speeds Are Increasing

As government agencies deploy ever-faster networks, one of the greatest challenges is enabling the network and security-monitoring infrastructure to keep up with the network itself. A key component of any monitoring infrastructure is full packet capture and storage, which enables the enterprise to go back in time, examine network performance or security incidents, and answer the question, "What happened?"

## 2.3 Collected Data Provides Valuable Insights

The information collected and stored in security logs can provide a valuable source of intelligence, in addition to the need to maintain the data for compliance reasons. Analytic tools are an excellent way for agencies to gain a better understanding of the threats, attacks, and vulnerabilities. Armed with these valuable insights, agencies are able to strengthen security policies to better safeguard systems and data from future attacks.

[3] http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.

## 2.4 Fast Recovery Is Critical Following a Security Breach

Unfortunately, security breaches are inevitable given the intricacy of attacks and technology available to hackers. The best way to respond is to have a plan in place before the incident even occurs. This means establishing an incident response plan for backing up and recovering information, as well as the policies for documenting and reporting the incident required for compliance.

## 2.5 Data Encryption Is Key

Among numerous security mechanisms, the most effective for protecting any confidential information is data encryption. If the agency's first line of defense is penetrated, data encryption will make sure that confidential data can't be viewed.

# 3 Cybersecurity Affects Storage Requirements

## 3.1 Storage Requirements

Storage represents a significant portion of IT budgets. Data retention and archiving, authentication and authorization, data loss prevention, and privacy regulations all demand appropriate security technologies within storage solutions that provide both transparency and accountability.

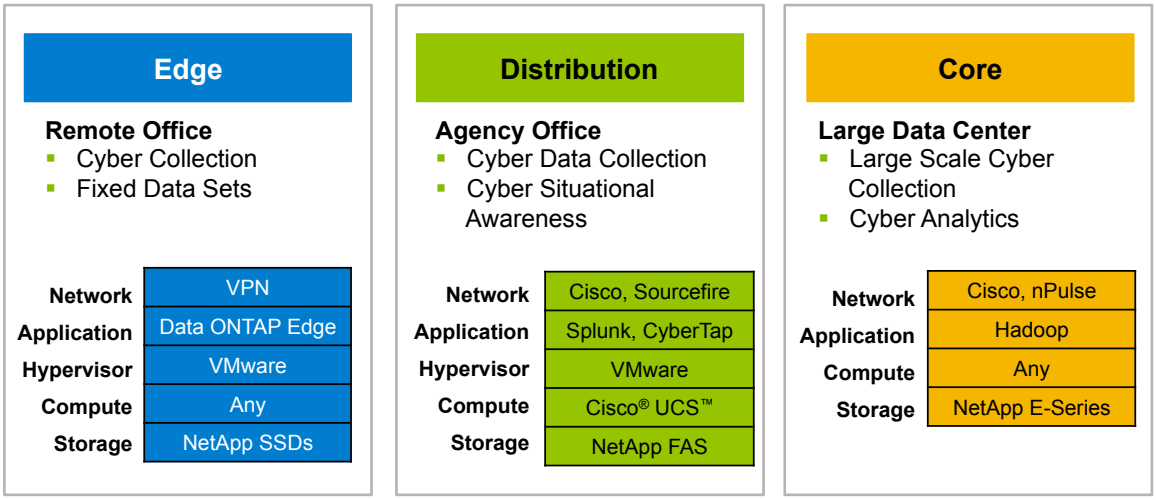
With the growing volume of security sensors across agency networks, NAS- or SAN-based storage will be required to correlate the growing data to identify and block threats, as well as to provide remediation and forensic capabilities. And as algorithms for data protection and information sharing (for both unclassified and classified information) become more complex, the ability to analyze larger datasets becomes critical.

## 3.2 NetApp and Cybersecurity

NetApp® cybersecurity technologies help government agencies protect their data, know how their data is being used, and minimize the risk that data will be lost in the event of an attack. NetApp storage solutions collect and store cyber-related information, analyze data to drive actionable intelligence, and allow agencies to quickly recover from cyber-related incidents similar to disaster recovery. The NetApp approach:

- **Is open.** Use the tools you want to access your data using standard protocols and formats.
- **Is flexible.** Adapt NetApp solutions to specific agency use cases using modular building blocks.
- **Uses best-in-class components**. Partner with leading cybercompanies to develop solutions to meet agency requirements.

**Figure 3) Cyber reference architecture.**

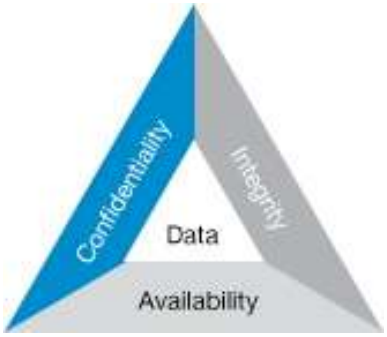


# 4 Protecting the Confidentiality, Integrity, and Availability of Your Data

The federal government relies on the exchange of data in order to be successful. However, agencies constantly balance the need to allow access to their data and the need to protect that data from attackers. NetApp takes a comprehensive approach to cybersecurity by providing technologies and solutions that enable data to be protected and trusted, while still remaining accessible. NetApp approaches cybersecurity in three areas:

- Confidentiality
- Integrity
- Availability

**Figure 4) Data security risk model.**




## 4.1 Confidentiality

The federal government has long been a prime target for hackers. Neither defense nor civilian agencies are exempt from hacker attempts to infiltrate agency infrastructures. NetApp delivers storage solutions that improve data protection for intellectual property and classified or highly regulated information. NetApp provides several ways to protect the confidentiality of your data through technologies including encryption, secure multi-tenancy, and high-speed packet transfer.

### Data Encryption

NetApp encryption solutions help protect data both at rest and in flight with AES 128-/256-bit encryption for data at rest or in flight, as well as simple, centralized key management.

- **Data at rest.** The NetApp Storage Encryption (NSE) appliance is NetApp's implementation of full-disk encryption (FDE) using self-encrypting drives from leading vendors. NSE is a nondisruptive encryption appliance that provides comprehensive, cost-effective, hardware-based security that is simple to use. This single-source solution can increase overall compliance with industry and government regulations without compromising storage efficiency.
- **Data in flight.** NetApp works with partners to offer security solutions for data in flight:
  - The NetApp SafeNet StorageSecure encryption appliance protects sensitive data in Ethernet-based network-attached storage (NAS). NetApp and SafeNet have partnered to provide advanced encryption services based on high-speed, 256-bit AES encryption and featuring redundant components and clustered failover for high reliability.
  - NetApp and Brocade have partnered to provide an advanced encryption solution for data at rest on Fibre Channel–based storage area networks (SANs). The Brocade Encryption Switch and Encryption Blade for Brocade DCX backbones help protect data from unauthorized access or modification through the use of 256-bit AES encryption.

## Secure Multi-Tenancy

NetApp's turnkey, secure multi-tenancy solution enables government agencies to logically host multiple heterogeneous functions within a single architecture of storage, network, and compute.

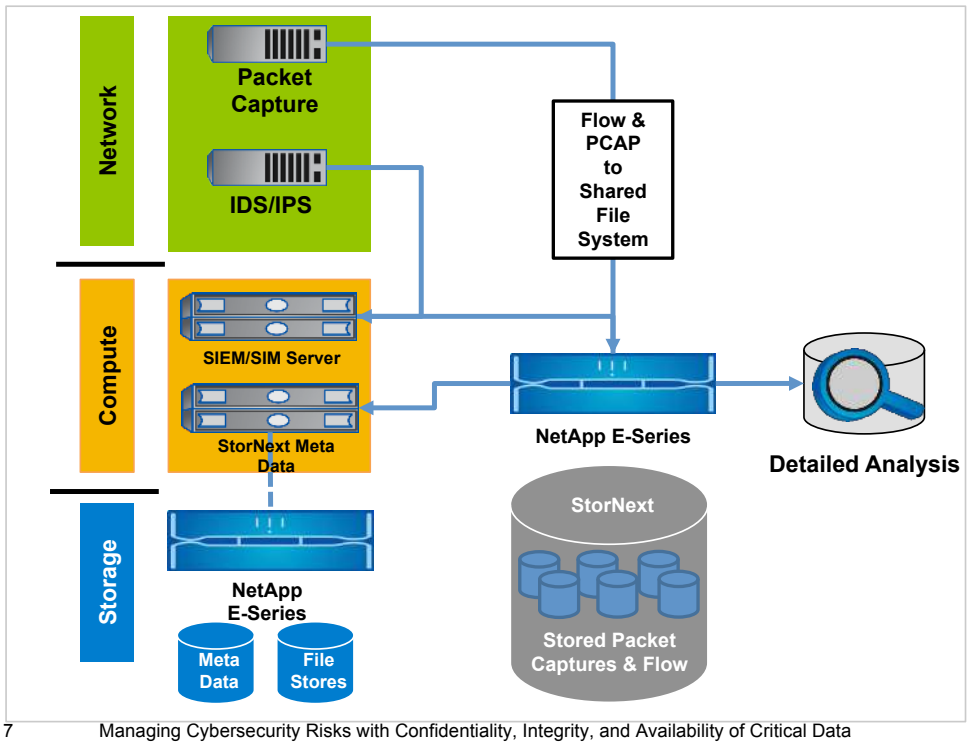
With NetApp software, agencies can share storage with maximum privacy and data security. In addition, NetApp with Cisco® and VMware® helps provide secure, end-to-end multi-tenancy across applications and data that delivers all the benefits and business advantages of a shared IT infrastructure with virtualized computing.

- **FlexPod.** The FlexPod® data center platform, jointly developed by NetApp and Cisco, provides a flexible infrastructure platform composed of presized storage, networking, and server components. Government agencies have the agility to grow their data pools only as needed with the best available security for critical data and regulatory compliance. The FlexPod solution enhances the deployment of big datastores at a fraction of the cost and with much less complexity than purchasing, installing, and maintaining traditional data silos and storage arrays. This means you can accommodate more data at less cost.
- **MultiStore.** NetApp MultiStore® software enables multiple users to share the same storage resource without compromising privacy and security. Information on one virtual storage system cannot be viewed, used, or downloaded by users on a different virtual storage system. MultiStore provides secure multi-tenancy capability to the NetApp Data ONTAP® operating system, allowing you to:
  - Host multiple customers and/or departments on a single Data ONTAP storage system
  - Consolidate many file servers, thus reducing cost and increasing staff productivity
  - Perform simple and fast data migration
  - Simplify disaster recovery strategy

## Packet Capture and Log Aggregation

Many agencies today are stuck with monitoring solutions that are "1-gigabit monitoring solutions in a 10-gigabit world." Legacy packet capture solutions with high rates of packet loss undermine the effectiveness of today's powerful cybersecurity analysis tools, producing instead the cyberequivalent of a corrupted database.

**Figure 5) High-speed, high-fidelity packet capture.**



NetApp and nPulse Technologies, the industry leader in high-performance flow and packet capture, have teamed to offer a packet capture solution that is setting new records for speed of capture and scalability of storage:

- Encrypting the packet and flow data as it is being stored at a rate of 24 gigabits per second
- Capturing multiple 24-gigabit data streams to a shared high-performance file system
- Making that data available for analytics in the open standard "pcap" format with the high performance required for exploiting the data

The nPulse and NetApp solution addresses both the bandwidth and content challenges, keeping networks protected while handling vast amounts of data in real time. Capturing data packets at the highest rates of speed without dropping any of the packets is essential to maintaining security across large, ultrafast networks.

## 4.2 Integrity

Although it is important to protect your information, it is equally important to know that you can trust your data. NetApp provides several solutions that can help businesses manage the integrity of their data, such as storage-based intrusion detection system (IDS) technology, rapid information assurance vulnerability alert (IAVA) compliance, and cyber collection and analytics.

### Information Assurance Vulnerability Alert Compliance

NetApp's storage-based IDS technology can alert businesses of any file-based event, providing granular awareness of how data is being used. Our systems also have integrated antivirus technology to keep data virus free.

Additionally, the features of the NetApp Data ONTAP operating system can simplify the process of IAVA compliance by allowing administrators to patch a single "gold disk" image instead of patching thousands of machines. This simplifies your management and ultimately reduces your window of vulnerability.

**Table 1) NetApp products deliver IAVA compliance.**

| Capability | NetApp Solution |
|---|---|
| **Storage-based IDS** | **FPolicy Engine**<br>Using Data ONTAP to enable auditing solutions at the storage level provides multiple benefits, such as the ability to:<br>• Monitor file access in NFAA exports and CIFS shares<br>• Manage persistent audit logs across system reboots<br>• Provide real-time notification to give instant alerts to storage administrators<br>The NetApp native auditing and FPolicy framework, along with the NetApp partner solutions, provides end-to-end solutions related to regulatory compliance, data protection, access monitoring, and storage analysis. |
| "**Gold disk" patching** | **FlexClone**<br>NetApp FlexClone® technology provides instant, scalable provisioning for virtual servers and desktops. Replicate data volumes, files, and LUNs as instant virtual copies without compromising performance or demanding additional storage space. |

### Cyberanalytics

Today, when a security accident occurs, the top three questions security administrators typically ask include:

- What happened?
- Why did it happen?
- What needs to be done?

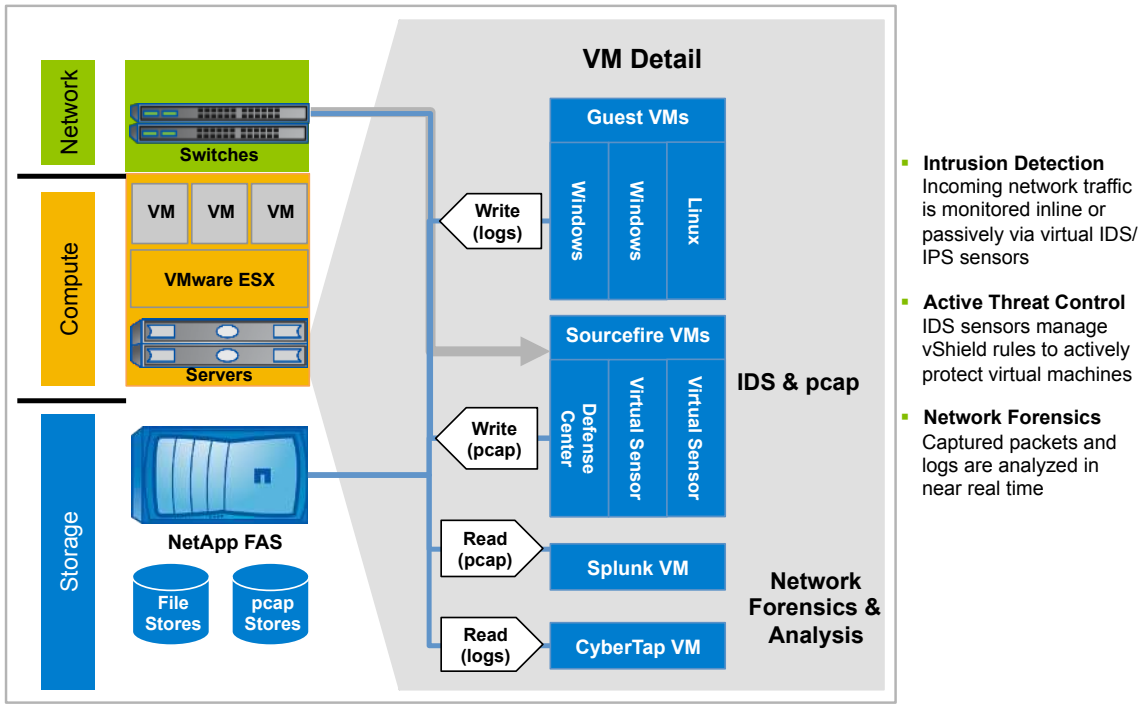
By having a cyber situation analysis process in place, security administrators can analyze both the internal and external environments to understand how the incident occurred and the necessary steps for remediation.

As described earlier, our strong partnerships with cybersecurity companies provide agencies with the ability to conduct cyber collection such as full packet capture or log aggregation. The collected cyberdata can then be analyzed to provide real-time situational awareness and long-term visibility into how the data is being used.

Increasingly, agencies are turning to Apache Hadoop to store and analyze raw, complex data and turn it into valuable business insights. NetApp provides solutions that offer government agencies breakthroughs in stability, management, and efficiency to enhance their enterprise Hadoop deployments and deliver the following benefits:

- Manage larger and more complex data with lower operating expenses and storage costs for a lower total cost of ownership
- Accelerate business processes and improve decision-making capabilities by extracting value from big data more quickly and more easily
- Increase business productivity with less downtime, higher data reliability, and faster time to recovery

**Figure 6) Cyberthreat analytics and monitoring.**




## 4.3 Availability

The NetApp Data ONTAP operating system has several integrated features, including Snapshot™ copies and cloning, that allow government agencies to create dynamic, flexible environments so they can rapidly provision resources to respond to threats or instantly recover from a logical failure.

Additionally, our clustering and compliance technologies allow agencies to create environments that make sure that data is available when it is needed.

Furthermore, when an attack or incident does occur, our disaster recovery solutions allow you to immediately revert to the last known good state.

### Rapid Cyberprovisioning

NetApp Provisioning Manager software makes it faster and easier to create new NetApp data storage resources while improving capacity management of existing resources. Storage administrators can use Provisioning Manager policy-based automation to optimize storage efficiency and capacity utilization, shrink provisioning time and costs, and increase administrator productivity—so you can store more data and achieve greater business agility with:

- Dynamic flexible environment
- Instant recovery from logical failures

### Disaster Recovery and Continuity of Operations

NetApp business continuity solutions help maintain availability across a broad spectrum of recovery point and recovery time requirements during planned as well as unplanned downtime. These solutions enable government agencies to achieve continuous availability to protect critical data:

- Leverage flexible RPO and RTO to meet service-level requirements
- Simplify administration with solutions that are easy to deploy and manage
- Reduce administrative, network, and storage costs

**Table 2) NetApp disaster recovery.**

| Capability | NetApp Solution |
|---|---|
| **Security and compliance** | **SnapLock**<br>A flexible data permanence solution, SnapLock® software, helps you comply with records retention regulations that require you to archive e-mails, documents, audit information, and other data in an unalterable state for years. At the same time, it enables rapid retrieval of unregulated yet crucial reference data that is not changed or deleted. |
| **Backups** | **Snapshot**<br>NetApp Snapshot technology enables you to create point-in-time copies of file systems, which you can use to protect data—from a single file to a complete disaster recovery solution. Snapshot copies can be created in less than a second, regardless of volume size or level of activity on your NetApp system.<br>**FlexClone**<br>FlexClone technology enables dataset replicas of entire NetApp Data ONTAP volumes to be created, as well as individual file or LUN replicas. It reduces the cost, storage footprint, and complexity of environments that support new product development, software and penetration testing, or deployment of virtual server infrastructures. |
| **Mirroring** | **SnapMirror**<br>SnapMirror® capabilities include new network compression technology to reduce bandwidth utilization; accelerated data transfers to lower RPO; and improved storage efficiency in a virtual environment using NetApp deduplication. |
| **Clustering** | **Clustered Data ONTAP**<br>Data ONTAP provides almost limitless capacity regardless of network protocol. Agencies can virtualize storage across multiple HA pairs, managed as a single logical pool, and scale to tens of petabytes. |

## 5 NetApp Cyber Alliance Program

NetApp recently announced the launch of its U.S. Public Sector Cyber Alliance Program. NetApp's Cyber Alliance Program is a collaborative program designed to establish partnerships and

interoperability of cybersolutions based on NetApp storage, virtualization, and big data technologies. The main goal of the program is to develop capabilities that enable organizations to better respond to and address the cyberthreats they face.

# 6 Summary

NetApp takes a comprehensive approach to cybersecurity by providing technology and solutions that make sure data is protected and trusted, while still remaining accessible.

Our encryption and secure multi-tenancy solutions help businesses protect data from threats. Additionally, the features of Data ONTAP help government agencies know that simplifying IAVA compliance allows them to trust their data, and our partnerships enable cyber collection and real-time situational awareness. And finally, our integrated data protection features enable data to be accessible when needed.

**Figure 7) NetApp certifications.**

| NetApp Certifications | |
|---|---|
| **Product** | **Certification** |
| Data ONTAP | EAL 2+ |
| NetApp Storage Encryption | FIPS 140-2 Level 2 |
| FlexPod | FISMA Moderate |
| FlexPod | DIACAP |

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

© 2013 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, FlexClone, FlexPod, MultiStore, SnapLock, SnapMirror, and Snapshot are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Windows is a registered trademark of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. Cisco and Cisco UCS are registered trademarks of Cisco Systems, Inc. ESX and VMware are registered trademarks of VMware, Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. WP-7177-0113

NetApp
www.netapp.com