



White Paper

Curb the Escalating Costs of Cyber Attacks with Secure Data Management Solutions

Dave Ulepich, Carina Veksler, Lee Vorthman, NetApp
July 2013 | WP-7187

Abstract

Cyber attacks continue to escalate in both volume and severity, resulting in high tangible and intangible costs to recover from a breach. Government agencies are tasked with identifying and implementing effective security controls to reduce the time from initial compromise to data exfiltration, discovery, and containment in order to protect sensitive information and systems. With the increased sophistication of techniques used in attacks, cyber data collection is now a big data problem that must be addressed by the changing role of cybersecurity. NetApp® storage and data management solutions can help government agencies effectively collect, analyze, and secure data across the enterprise.

TABLE OF CONTENTS

1	The Escalating Cost of Cyber Attacks	3
1.1	Measuring the Fallout	4
1.2	Required Security Controls	5
2	The Big Data Problem for Cybersecurity and the Impact on Storage	5
3	Close the Gap with Secure Storage	6
3.1	NetApp's Approach to Cybersecurity	6
3.2	Collect	7
3.3	Analyze	8
3.4	Secure	9
4	Summary	10

LIST OF TABLES

Table 1)	Five tenets for an effective cyber-defense system	5
Table 2)	NetApp OnCommand Management Suite	8
Table 3)	NetApp integrated data protection	9

LIST OF FIGURES

Figure 1)	Incidents reported by federal agencies in fiscal years 2006–2012	3
Figure 2)	Attack timeline	4
Figure 3)	Cyber challenges impacting storage	6
Figure 4)	NetApp's approach to cybersecurity	7

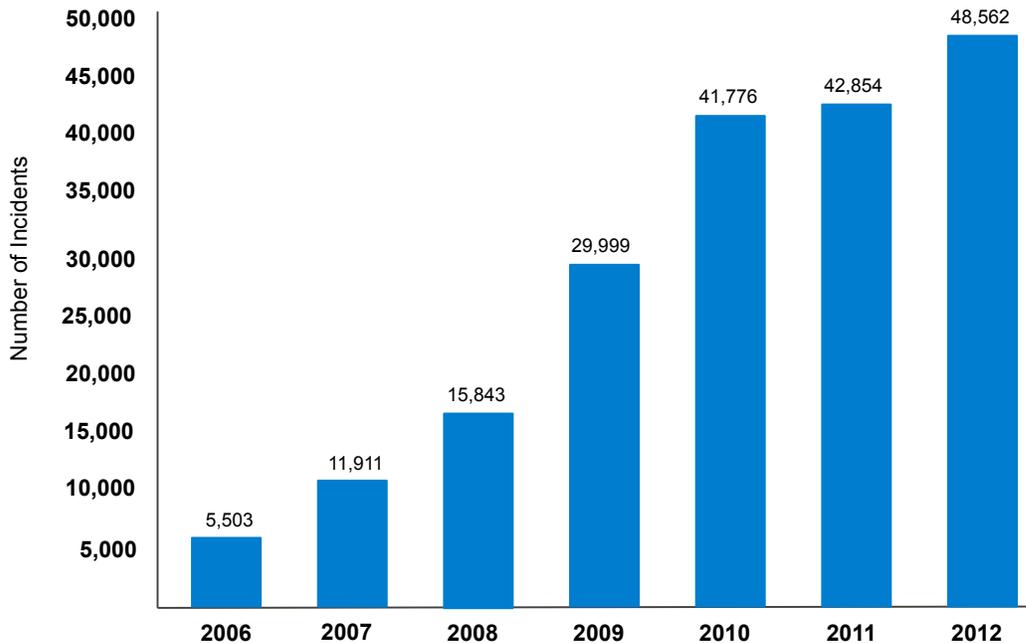
1 The Escalating Cost of Cyber Attacks

Cybersecurity is a major concern for the U.S. government. Threats to critical infrastructure and operations are becoming more sophisticated and the pace of attacks is becoming more rapid. Some of the recent high-profile headlines include:

- Edward Snowden leaked some of the United States' most sensitive secrets obtained during his employment at the NSA and he may defect to Latin America.
- The Chinese government used cyber espionage to hack into U.S. government systems, where designs for more than two dozen U.S. major weapons systems have been compromised.¹
- Jeremy Hammond, a self-described anarchist and hacker activist in the United States, pleaded guilty to charges that he illegally accessed computer systems of law enforcement agencies and government contractors.
- On January 26, 2013, anonymous hacked into a web site under the U.S. government's control: <http://www.ussc.gov/>.
- WikiLeaks continues to publish secret information, news leaks, and classified media from anonymous sources.
- Security researchers from Imperva uncovered government and military web sites on the underground auction block.²

These are just a sampling of some of the public breaches that have occurred. According to a recent GAO study,³ reported attacks on government sites increased 782% between 2006 and 2012.

Figure 1) Incidents reported by federal agencies in fiscal years 2006–2012.



Source: GAO analysis of US-CERT data for fiscal years 2006-2012

¹ http://articles.washingtonpost.com/2013-05-27/world/39554997_1_u-s-missile-defenses-weapons-combat-aircraft

² <http://blog.imperva.com/2011/01/major-websites-govmiledu-are-hacked-and-up-for-sale.html>

³ National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented: GAO, February 2013

1.1 Measuring the Fallout

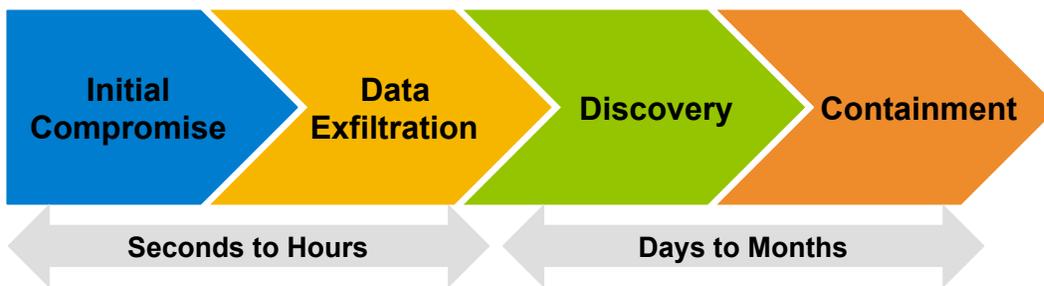
Timeline

Depending on the purpose of the attack (financial, espionage, other), initial compromise and data exfiltration can range anywhere from seconds to hours. However, discovery and containment more often take days to months to identify and implement a remediation solution. According to the Verizon Data Breach report:⁴

- Eighty-four percent of compromises occur within **hours**, and approximately 25% of compromises occur within minutes or seconds.
- Seventy percent of data exfiltration occurs within **hours**, and 23% of the data being exfiltrated occur within minutes or seconds.
- Sixty-six percent of compromises take **months** or *longer* to be discovered.

It is clear that government agencies struggle with the number of attacks and the complexity of their environments because 66% of the compromises take months or longer to be discovered. The net result? Data is gone by the time the incident is discovered.

Figure 2) Attack timeline.



Cost and Impact

As evidenced by many of the recent headlines, cyber espionage is a growing concern for government agencies. Coupled with the increasing numbers of cybersecurity incidents being reported, the exposure of sensitive information can result in serious impacts on federal and military operations, public safety, and critical infrastructure.

The most costly breaches are a result of malicious or criminal attacks, which can be caused by external hackers or criminal insiders. According to a recent Ponemon survey, U.S. organizations experienced the highest total cost of a data breach, with a cost of more than \$5.4M per incident during 2012.⁵

An expensive subset of the cybersecurity world is the ability to block identity fraud. As reported by *CNNMoney*, the IRS failed to prevent 1.5 million potentially fraudulent tax returns from being processed in 2011—resulting in refunds totaling more than \$5.2 billion, according to an audit conducted by the Treasury Inspector General for Tax Administration.⁶

How long does it take your organization to discover, contain, and remediate a cyber attack? According to the Ponemon Institute, the 2012 study identified that it took organizations an average of 24 days to

⁴ Verizon 2013 Data Breach Investigation Report

⁵ 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013

⁶ <http://money.cnn.com/2012/08/02/pf/taxes/irs-identity-theft/index.htm>

resolve a cyber attack, with an average cost of \$24,475 per day.⁷ Having the right infrastructure in place to address a cybersecurity incident not only pays for itself today, but also allows you to adapt to future incidents not even anticipated today.

1.2 Required Security Controls

In 2008, the U.S. National Security Agency (NSA) began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact on improving risk posture against real-world threats—resulting in the list of Critical Controls for Effective Cyber Defense,⁸ coordinated through the SANS Institute. The goal of the Critical Controls list is to protect critical assets, infrastructure, and information by strengthening an agency's defense posture based on five critical tenets.

Table 1) Five tenets for an effective cyber-defense system.

Tenet	Action
Offense informs defense	<ul style="list-style-type: none"> Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses.
Prioritization	<ul style="list-style-type: none"> Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in the computing environment.
Metrics	<ul style="list-style-type: none"> Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
Continuous monitoring	<ul style="list-style-type: none"> Carry out continuous monitoring to test and validate the effectiveness of current security measures.
Automation	<ul style="list-style-type: none"> Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

Using this approach, agencies have already begun to transform security by focusing their spending on the key controls that block known attacks and to find the ones that get through.

2 The Big Data Problem for Cybersecurity and the Impact on Storage

Deploying the correct security measures is a necessity for making critical information available to authorized users when they need it. However, with the growing number of devices (such as mobile devices, virtual machines, laptops, and tablets) requesting access to networks and applications, a broader range of security technologies to provide continuous diagnostics and monitoring is now required to provide protection against the growing number of attacks that result in compromised data and systems.

⁷ 2012 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2012

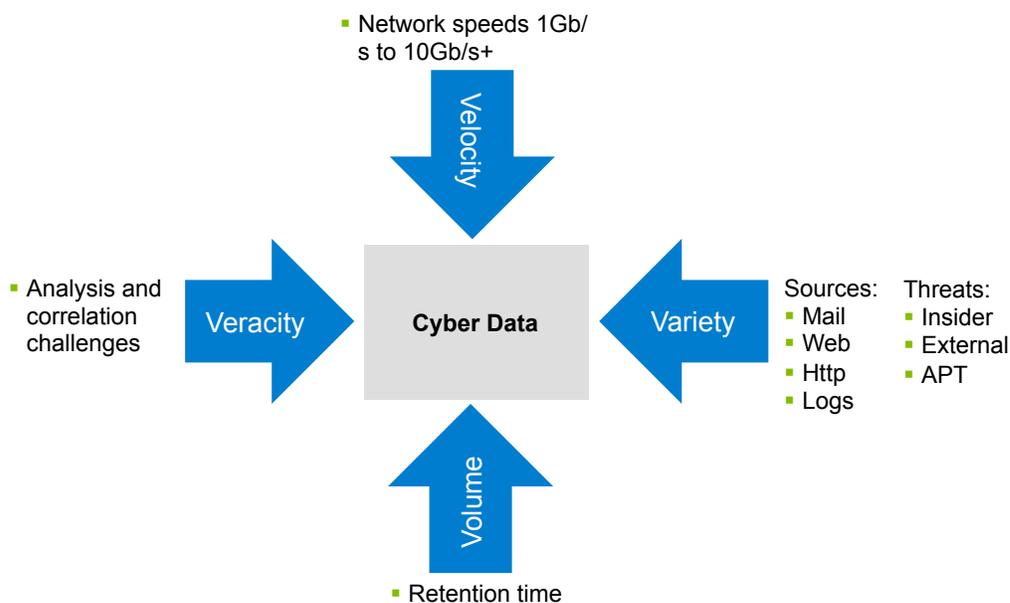
⁸ SANS Institute: <http://www.sans.org/critical-security-controls/>

With the increased sophistication of techniques used in attacks, cyber data collection is now a big data problem that must be addressed by the changing role of cybersecurity. For a typical 10GB link, storage requirements can easily reach 100TB per day to capture, analyze, and archive the data. And with retention times ranging from 1 week to 30 days, storage requirements can quickly jump from 700TB to over 3PB.

In order to protect sensitive data from compromise, data storage and data management solutions must be included as critical components to augment traditional security measures in order to protect sensitive data from compromise.

- Network speeds are increasing. Full packet capture and cyber collection involve the same challenges as big data. As network speeds increase from 1Gb/s to 10Gb/s and beyond, the velocity of data being written to storage also increases.
- There is a wide variety of sources and threats. The increasing volume of threats, infiltration points, and attackers generates significant data that needs to be captured.
- There are increased time frames for archived data. Customer requirements for longer retention times are pushing the volume of data that needs to be managed and stored.
- Analysis is critical. It is difficult to determine the accuracy of the cyber data or to extract value from it without using big data analytic techniques.

Figure 3) Cyber challenges impacting storage.



3 Close the Gap with Secure Storage

NetApp storage and data management solutions can help government agencies implement a risk-based approach with the ability to collect, analyze, and secure data across the enterprise. We have the technology and a diverse partner ecosystem that can help close the gap between compromise and discovery. We can also help agencies quickly understand what is happening within their complex environments and ultimately secure their data so that it is not stolen or destroyed by attackers.

3.1 NetApp’s Approach to Cybersecurity

NetApp helps government agencies remediate and reduce costs with storage solutions that shorten the time to discover a breach, secure the data, and minimize the impact by recovering from compromises

more quickly. NetApp approaches cybersecurity in three phases. The first step is to collect and store all of the data coming across the networks. To accomplish this, we have partnered with best-in-class companies including nPulse Technologies to build a cutting-edge packet capture solution.

The next step provides a flexible environment to analyze the data to better understand what is happening in as close to real time as possible. This means deploying a dynamic architecture that can provide virtualized and physical resources when needed to give analysts the resources they need to analyze threats. We have partnered with several best-in-class cyber companies including Splunk and Sourcefire to identify and analyze cyber events using a FlexPod® environment.

Finally, we secure the data so that it is not stolen or destroyed. This means using encryption and data security technologies such as SafeNet or Vormetric. It also means leveraging the built-in security of the clustered Data ONTAP® operating system, including Snapshot™ copies, FlexClone® volumes, and SnapMirror® technology, to quickly recover data and return to normal operations.

Figure 4) NetApp's approach to cybersecurity.



3.2 Collect

High-Speed Networks

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. The solution:

- Encrypts the packet and flow data as it is being stored at a rate of 24 gigabits per second
- Captures multiple 24-gigabit data streams to a shared high-performance file system
- Makes 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.

Storage—Performance and Scale

The NetApp E-Series storage system delivers compelling performance, extreme storage density, and exceptional uptime, and it is ideally suited for full packet capture and cyber collection. A single E5460 can collect packets from a 10Gb/s full duplex network, and it can store approximately 1 to 1.5 days of captured traffic depending on disk size. With E-Series redundant components, automated path failover, and online administration, security collection systems can be productive 24/7.

- **Optimized performance across agency infrastructure.** The solution sustains high read and write throughput, eliminating performance bottlenecks.

- **Maximum storage density.** Leading rack density saves data center floor space and lowers operational costs while accommodating the increasing volumes and file sizes of security data.
- **High reliability.** The field-proven design provides high reliability and 99.999% availability, giving care providers continuous access to stored information.
- **Robust protection.** Advanced protection technologies such as data-at-rest encryption, proactive monitoring, background repair, and extensive diagnostic features fully protect data when it reaches the storage system.

3.3 Analyze

Big data analytics provide government agencies with greater visibility, allowing them to take advantage of the entire digital data repository and turn security data into valuable intelligence. NetApp has partnered with best-in-class cyber-analytics companies, including Splunk, to collect, search, monitor, and analyze cybersecurity data across the enterprise using a FlexPod architecture. As a result of this partnership, NetApp and Splunk have developed the Splunk App for NetApp to allow real-time and historic visibility into the performance and configuration of your NetApp infrastructure.⁹

FlexPod

The FlexPod data center platform is a prevalidated solution that integrates storage, networking, and server components into a single flexible architecture. Because it provides the capability to dynamically scale and allocate resources, FlexPod is an ideal architecture for cyber analytics. This solution has been successfully and easily deployed in government facilities and provides maximum flexibility for shared storage infrastructures with secure multi-tenancy.

Cyber Analytics, Management, and Orchestration with OnCommand

The NetApp OnCommand[®] family of products helps government agencies analyze, orchestrate, manage, and report the status of their environments. This information and tool set can easily be sent to or utilized by a security operations team to report on or manage the security of the storage in their environment.

Table 2) NetApp OnCommand Management Suite.

Product	Key Features
OnCommand Systems Manager	<ul style="list-style-type: none"> • Provides simple, workflow-based wizards to automate common device management tasks. With System Manager, storage admins and IT generalists can quickly configure and manage NetApp SAN and NAS systems
OnCommand Unified Manager	<ul style="list-style-type: none"> • Integrates the functions of operations, provisioning, and protection management into a single user interface. Through a single view you can monitor your entire shared storage environment, as well as drill down to define storage service levels and policy-based workflows. OnCommand Unified Manager is designed to work with NetApp storage, including V-Series.
OnCommand Insight	<ul style="list-style-type: none"> • Delivers visibility and optimization across heterogeneous storage infrastructure. With OnCommand Insight, users can optimize performance, forecast, and Insight capacity requirements; enable chargeback and showback; and deliver to your service levels.

⁹ Splunk App for NetApp - <http://splunk-base.splunk.com/apps/67764/splunk-app-for-netapp>

Product	Key Features
OnCommand Report	<ul style="list-style-type: none"> Provides roll-up reporting for multiple instances of OnCommand Unified Manager or multiple instances of the former DataFabric® Manager product. This operational-level reporting goes beyond the basic reporting capabilities in OnCommand Unified Manager to roll up inventory and capacity reporting for multiple NetApp environments.

3.4 Secure

Integrated Data Protection

The NetApp Data ONTAP operating system has built-in data protection features that help provide instant availability to security data. With Snapshot copies, FlexClone volumes, and software integration, agencies can instantly recovery data locally: Snapshot copies provide a quick and efficient method for isolating and restoring data from cyber events that compromise the integrity of your data and FlexClone volumes allow administrators to create an instant writable copy of a dataset and then allow multiple virtual copies to be created that only store the changed data. This is ideal for secure coding, exploit development, and development/test environments that work off large datasets.

In addition, NetApp disaster recovery and continuity of operation features can help back up and restore data to/or from remote sites. Data, along with Snapshot copies and clones, is replicated between the sites to provide an exact copy of the operating environment. When faced with a security event or incident, systems seamlessly fail over to the remote site and provide agencies with the confidence that data remains in sync. Data protection solutions also work with our encryption technology so that data is not visible to anyone attempting to sniff data on agency networks. This helps minimize risk, knowing that your disaster recovery strategy works without disrupting current operations.

Table 3) NetApp integrated data protection.

Product	Key Features
Snapshot	<ul style="list-style-type: none"> Quick and efficient Built into Data ONTAP Each Snapshot copy represents a full backup Integration into third-party applications
FlexClone	<ul style="list-style-type: none"> Creates instantaneous, writable copy Stores only changes Reduces devilmnt/test costs by as much as 80%
Data ONTAP	<ul style="list-style-type: none"> Single storage namespace Simplified management and access Tiered storage You can mix SATA, SAS, and SSD and match to desired performance Nondisruptive rebalancing Improved system availability
Disaster Recovery	<ul style="list-style-type: none"> Instant recovery from attack or data failure Continuous availability
Compliance	<ul style="list-style-type: none"> Configurable data retention policies WORM volumes

Encryption Solutions

NetApp provides the ability to encrypt data in flight and at rest, allowing data to be encrypted from the moment it enters your network to where it is stored on disk or tape. Our full disk encryption works on both the FAS and E-Series product lines, and it prevents personnel with physical access to your data center from removing disks and stealing sensitive data.

- FIPS 140-2 Level 2 and 3 certified
- Centralized key management provides a single key domain for your entire enterprise
- Fast cryptographic shredding of data by simply deleting the key
- Less than 1% impact on system performance since the encryption/decryption process is offloaded to dedicated encryption modules

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. Our secure multi-tenancy architecture allows you to logically host multiple functions or tenants using a single architecture. The architecture is made up of storage, compute, network, and hypervisor components. Security is built in through the various layers and is applied end to end to enforce policies and enable secure separation of tenants. And with the capabilities built in to clustered Data ONTAP, this operating system provides the ideal secure multi-tenancy environment. It allows multiple tenants to store their data in a single namespace, and the environment provides enterprise resiliency to our government customers.

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.

4 Summary

Threats to online security continue to grow and evolve in both sophistication and volume, and the ability to use technology in a smarter way is a necessity. Agencies can now have immediate insight to ongoing cyber activity with solutions that provide continuous diagnostics and monitoring coupled with analytics to interpret the data collected. When you are armed with this knowledge, the time from compromise to remediation can be shortened and the costs minimized with the appropriate actions that protect systems, data, and national security.

NetApp takes a comprehensive, risk-based approach to cybersecurity by providing technology and solutions that enable data to be protected and trusted while still remaining accessible. By integrating data storage and data management solutions as key components of their overall cybersecurity program, agencies can now collect, analyze, and secure systems, applications, and databases from infections and compromise.

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

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, DataFabric, Data ONTAP, FlexClone, FlexPod, OnCommand, SnapMirror, and Snapshot are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and