SOLUTION BRIEF:
FIVE CRITICAL SECURITY CONTROLS FOR
CONTINUOUS DIAGNOSTICS AND MITIGATION

Five Critical Security Controls for Continuous Diagnostics and Mitigation

Who should read this paper

Federal Information Security executives and teams that are looking for a prioritized list of measures and controls to accomplish effective continuous diagnostics and mitigation.

Confidence in a connected world.

Content

Higher Priorities

In the waning days of 2012, the Department of Homeland Security (DHS) found itself in an unusual position – flush with cash.

Facing challenges passing a comprehensive cybersecurity bill, the 112th Congress provided DHS with a preliminary budget to begin work: $183 million to bolster implementation of a federal Continuous Diagnostics and Mitigation (CDM) program that would provide tested continuous monitoring, diagnosis, and mitigation activities designed to strengthen the security posture for civilian agencies.

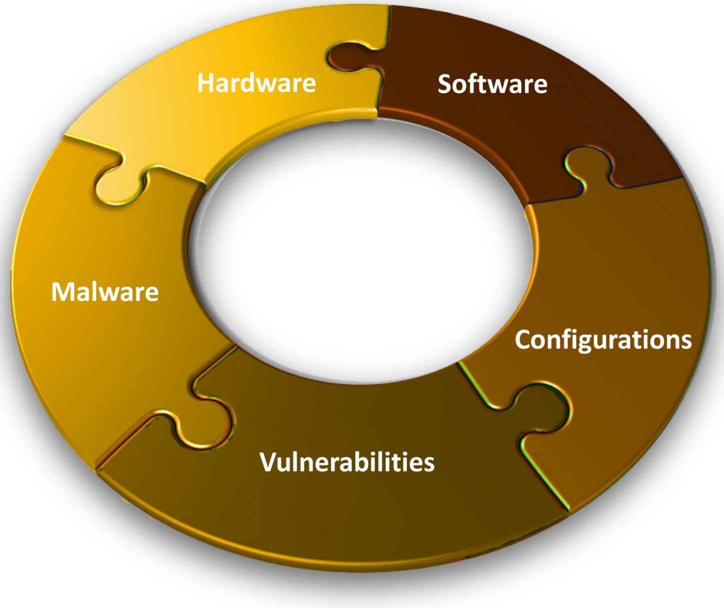
But how best to proceed? While substantial, this new funding was a mere down payment on a comprehensive FISMA compliance effort that—according to at least one DHS budget analyst—could cost $7.5 billion over the next five years.

Choices would have to be made to optimize resources: Which were the higher priority actions? Which actions could best mitigate known attacks? Which would address the widest variety of attacks? Which could identify and stop attacks earliest in the compromise cycle?

Fortunately, DHS had at its disposal a series of consensus audit guidelines—The 20 Critical Security Controls for Effective Cyber Defense—conceived by an impressive consortium of public- and private-sector cybersecurity experts, and published by the Center for Strategic and International Studies (CSIS) and the SANS Institute.

> "*The 20 Critical Controls are a reflection of the 80/20 rule at work in cybersecurity...an effort to identify the 80 percent payoff that can prevent or mitigate the bulk of the attacks against IT systems today. By automating the application and monitoring of these basic security functions, resources and manpower could be freed to address remaining challenges that are more sophisticated and require greater attention.*" --- **William Jackson, Government Computer News**

More specifically, DHS decided to focus on the first five controls, deemed the most crucial of all because they provide the highest level of protection: hardware and software asset management, configuration control, vulnerability management, and malware defense as shown in the below image.



The goal wasn't to mitigate every conceivable cyber risk, rather to solidify protections against foreseeable threats, while providing security experts with the time—and the timely intelligence—needed to focus their energies on the unforeseeable. This approach, while not the ultimate objective, is one that is gaining increasing acceptance in the federal community.

The remainder of this solution brief outlines the thinking behind the five critical controls and Symantec technologies best suited to help organizations implement them.

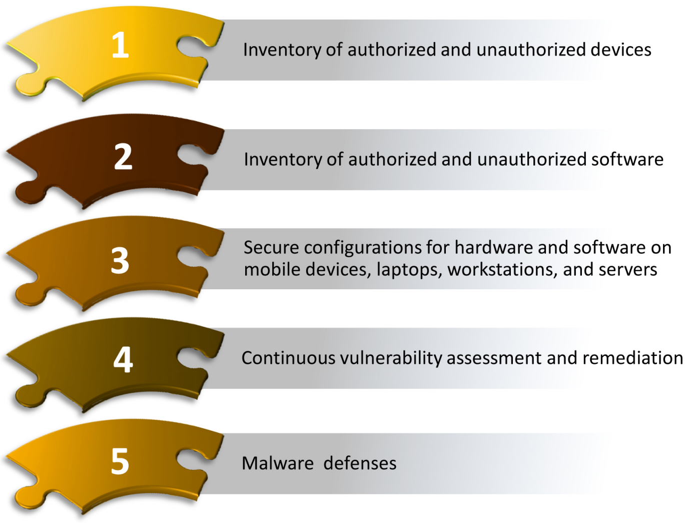
A Growing Consensus

Ever since the Office of Management and Budget (OMB) updated its FISMA guidance with continuous monitoring requirements, government agencies have been flocking to the SANS methodology—which maps closely to the continuous monitoring controls in NIST special publication 800-53.

This is not to suggest that the SANS 20 Controls are ubiquitous by any means. Some federal organizations have chosen to follow the NIST 800-53 framework directly. In doing so, they've identified hundreds of controls (one federal agency reportedly identified 256), most of which—though not all—fall generally into the categories outlined by the SANS 20. In any case, there is broad acceptance of the SANS 20 as a focal point for federal organizations limited by time, money, or manpower.

Within the SANS 20 Critical Controls, there is widespread support for prioritization of the first five as the minimum foundational requirements for continuous monitoring as shown in the image below.

The First Five Critical Security Controls for Effective Cyber Defense


1
Inventory of authorized and unauthorized devices
2
Inventory of authorized and unauthorized software
3
Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
4
Continuous vulnerability assessment and remediation
5
Malware defenses

Over time, agencies have implemented a number of disparate security tools, some of which help satisfy individual controls, but still lack a method for aggregating and analyzing the collective data for a holistic picture of their security posture.

Symantec recommends an implementation strategy that begins with data aggregation. Not only can centralization help users identify gaps and redundancies in their data collection processes, but it can provide a single, central point-of-view for better risk management and mitigation. Advanced aggregation tools, such as Symantec™ Control Compliance Suite, can ingest and analyze the multi-source data, and help organizations assess their overall risk posture. In addition, Control Compliance Suite provides a centralized risk and security asset repository with intelligent correlation, tagging, and aggregation rules. This enables prioritized alerting and remediation as well as customizable dashboards and reports.

In the following sections, we'll explore each of the first five controls and investigate the details of their implementation.

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Control 1 calls for an IT solution that identifies which devices are present on an agency's network, when those devices are connecting and disconnecting and how each of the devices are precisely configured. Implementation would enable agencies to determine authorized/ unauthorized systems and start to manage those systems.

If an agency cannot spot and monitor the full array of devices on its network, there's zero chance of achieving a secure environment. Hence, to satisfy this first control, agencies need to implement an asset management tool. Control Compliance Suite scans the network and collects security information about assets and reconciles with a known inventory of hardware to ascertain whether the assets are authorized or unauthorized. By defining the universe of hardware devices on the network, Control Compliance Suite fulfills the hardware inventory component of continuous monitoring.

It is equally important to note that these inventories must be continually assessed—lest new, unknown devices enter the environment. As Control Compliance Suite automates this process, the exercise is a painless one for security and compliance teams.

Note: Altiris™ IT Management Suite from Symantec™ is also suited to the task of scanning for devices, creating inventories and feed that data into Control Compliance Suite.

Critical Control 2: Inventory of Authorized and Unauthorized Software

Control 2 requires organizations to discover all software on their network and assess the security status of those assets. This includes application, version and vendor information across all platforms in the environment. Control Compliance Suite scans the network for software assets, and then checks that each asset is authorized and securely managed.

As with hardware scans, software inventories must be continually monitored to ensure that configuration deficiencies are detected and addressed as quickly as possible.

Note: Altiris™ Client Management Suite from Symantec™ or Altiris™ Server Management Suite from Symantec™ can scan for software assets, create detailed system inventories and feed that information into Control Compliance Suite if required.

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The crux of Control 3 is achieving hardened hardware and software configurations.

Organizations generally turn to standards bodies such as NIST, DISA or CIS for guidance on how to set this secure baseline for their assets. Hardening these configurations can include actions such as removal of unnecessary accounts, removal of unnecessary services, and applying patches.

Once an organization has achieved a satisfactorily hardened configuration, Control Compliance Suite can regularly monitor for deviations, and kick-off remediation steps as changes are discovered. As new assets are provisioned, they can also be deployed with the agreed configuration standards in place.

In most cases, continuous assessment to identify deviations from this standard configuration will be sufficient to minimize risk. For servers that house sensitive data, however, organizations may need to take an additional step to limit allowable actions on those systems. Symantec™ Critical System Protection locks down the configuration of hardware and software assets so that they cannot be changed. Furthermore, when an alteration attempt is made, Critical System Protection can immediately alert the administrator, log information about the attempt and follow-up with the offending user to ensure that they understand security policy.

Critical Control 4: Continuous Vulnerability Assessment and Remediation

Control 4 is intended to enable continuous testing for any possible weaknesses on Web servers, operating systems or network devices.

Because threat scenarios often arise as software changes (or as malicious actors discover new vulnerabilities in software that was previously deemed safe), Control Compliance Suite continuously monitors the universe of known threats, while scanning your IT systems for hardware and software assets associated with those threats.

Control Compliance Suite can apply known targeted attacks to specific exposures in your system to test how the environment responds. If any of these scans or tests produce an unacceptable level of risk, the vulnerabilities are immediately reported for tracking and remediation. For instance, if you're running a version of Windows® that isn't updated with the latest patch, Control Compliance Suite will flag the software for immediate patching.

Vulnerability data can be fed into Control Compliance Suite for centralized tracking, remediation, and reporting.

Note: Keeping up to date with the latest patches is one of the best ways to avoid vulnerabilities. Symantec offers Altiris Client Management Suite and Altiris Server Management Suite which can help automate the update process.

Critical Control 5: Malware Defenses

Custom-created, never-before-seen malware is becoming a bigger problem for agencies with each passing day.

Antivirus tools use specifically created signatures to disarm individual pieces of malware. But when attackers leverage previously unknown pieces of code (known as zero-day attacks) there's no such signature for the antivirus tools to apply.

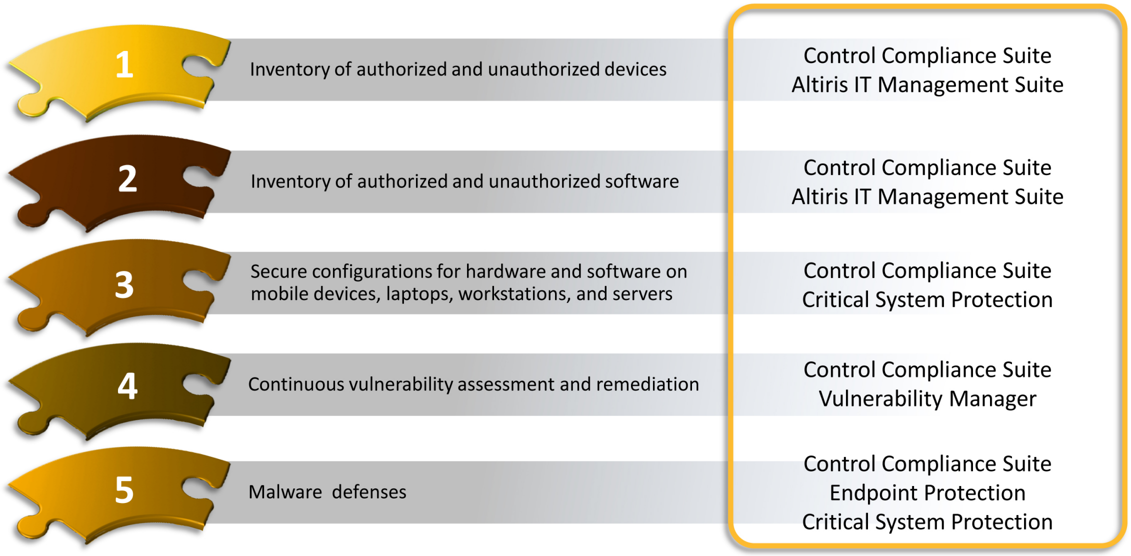
Therefore, Control 5 calls for something more than just antivirus protection. Tools that take a layered approach to endpoint security are needed to stop zero-day attacks, and unknown threats.

Symantec™ Endpoint Protection provides intrusion prevention, firewall, real-time threat reputation scoring, file behavior monitoring, application control, and device control protection. For much of an organization's infrastructure, this will be sufficient malware protection.

For mission-critical servers, Symantec Critical System Protection takes malware defense to the next level, locking down all allowable operations on your systems. Subsequently, any action that falls outside those parameters is treated as a zero-day attack. The corresponding operations are immediately quarantined, and the system administrator is instantly alerted. Better yet, Critical System Protection tricks the malware operator into thinking he's been successful. (After all, if Critical System Protection immediately rejected the malicious code, its operator might redeploy it elsewhere).

Symantec also recommends using the whitelisting capabilities of Symantec Endpoint Protection or Critical System Protection to further enhance malware defenses. Both Endpoint Protection and Critical System Protection can feed data to Control Compliance Suite. In fact, as shown in the image below, Control Compliance Suite maps precisely to each of the first five controls maps.

Symantec Solution Mapping to the First Five Critical Security Controls



1	Inventory of authorized and unauthorized devices	Control Compliance Suite Altiris IT Management Suite
2	Inventory of authorized and unauthorized software	Control Compliance Suite Altiris IT Management Suite
3	Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers	Control Compliance Suite Critical System Protection
4	Continuous vulnerability assessment and remediation	Control Compliance Suite Vulnerability Manager
5	Malware defenses	Control Compliance Suite Endpoint Protection Critical System Protection

The Bigger Picture

Having fully implemented these five essential controls (or the full 20 for that matter), government organizations will be one step closer to an effective, resilient cyber defense posture. Though it may be tempting to conclude that successful implementation and continuous monitoring of the 20 controls is the final goal for security teams, implementing security controls should not be a compliance exercise (whether to an internal or external standard). Instead, it should be part of a broader effort to advance an agency's operational mission by reducing overall risk.

Unfortunately it seems that achieving a risk management framework is still not a universally accepted target within the federal community. Ron Ross, a fellow at the National Institute of Standards and Technology, goes so far as to state that: "If you just landed here from another planet, you'd think that our entire strategy for the federal government is about continuous monitoring." There are numerous interconnected facets of a comprehensive cyber-defense strategy yet agencies view these challenges myopically at their peril.

By creating a common platform to manage risk, leveraging existing third-party technologies, and turning disparate data streams into actionable intelligence, agencies can achieve not only full implementation of the first five Critical Controls, but move more quickly towards long-term risk management maturity. And that's precisely where Symantec can help.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com