

Addressing the SANS Top 20 Critical Security Controls for Effective Cyber Defense

How Trend Micro Deep Security Can Help:
A Mapping to the SANS Top 20 Critical Security Controls

-
- » Addressing the SANS Top 20 Critical Controls can be a daunting task. With a comprehensive range of security controls, Trend Micro Deep Security can help organizations streamline the security of servers across hybrid cloud deployments



INTRODUCTION

In the face of increasing reports of data losses, intellectual property theft, credit card breaches, and threats to user privacy, organizations today are faced with a great deal of pressure to ensure that their corporate and user data remains secure. They are also obligated to address compliance with a wide range of industry regulations and laws, making it challenging to understand how best to approach the problem. Finally, with the advent of widespread cloud usage and the shifting to a shared security responsibility model for cloud workloads, organizations are forced to apply security in new ways that often don't fit with traditional approaches.

\$400 M

The estimated financial loss from 700 million compromised records

2,122

Confirmed data breaches across 61 countries

Source: Verizon 2015 Data Breach Investigations Report

CRITICAL CONTROLS FOR EFFECTIVE CYBER DEFENSE

*“...the Center for Internet Security’s Critical Security Controls identify **a minimum level of information security** that all organizations that collect or maintain personal information should meet. The **failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.**”*

California Attorney General,
California Dept. of Justice,
[California Data Breach Report, Feb. 2016](#)

In order to help, the SANS Institute, working in concert with the Center for Internet Security (CIS), has created a comprehensive security framework—the Critical Security Controls (CSC) for Effective Cyber Defense (often referred to as the SANS Top 20)¹—that provides organizations with a prioritized, highly focused set of actions that are implementable, usable, scalable, and compliant with global industry & government security requirements. These recommended security controls also serve as the foundation for many regulations & compliance frameworks, including NIST 800-53, PCI DSS 3.1, ISO 27002, CSA, HIPAA, and many others².

There are several reasons that businesses, regulatory bodies and governments have embraced the Top 20 CSC as the foundation for security strategies and frameworks:

- Implementation of the controls can reduce the potential impact of known high risk attacks as well as attacks expected in the future.
- The controls are comprehensive and address the most important areas of concern.
- The controls were generated by experts in both the federal government and private industry.
- The controls are well written, approachable and make common security requirements easy to understand and implement.

HOW TREND MICRO DEEP SECURITY CAN HELP

As organizations implement a security framework like the SANS Top 20 Critical Security Controls to address their needs, Trend Micro Deep Security can play a significant role in addressing many of the critical requirements. Delivered from the market leader in server security³, Deep Security is a

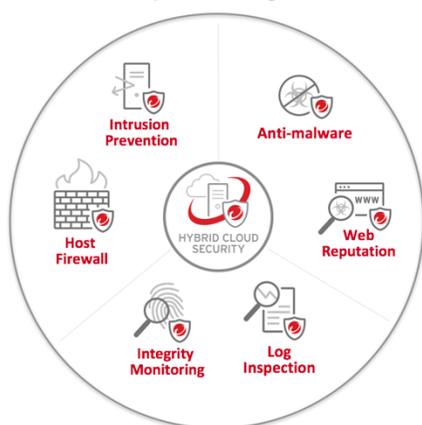
¹ [The CIS Critical Security Controls for Effective Cyber Defense Version 6.0. October 2015](#)

² [Mapping to the CIS Critical Security Controls. January 2016](#)

³ [IDC, Worldwide Endpoint Security Market Shares: Success of Midsize Vendors, #US40546915, Figure 5, Dec 2015](#)

comprehensive platform for security that can address server security across physical, virtual, cloud & hybrid environments. Available as software, service, or via the AWS and Azure marketplaces, it can help organizations streamline the purchasing and implementation of the essential security elements recommended by the CIS.

Trend Micro Deep Security is a host-based security control platform that secures millions of servers across thousands of customers around the world. It includes a comprehensive set of security controls for protecting servers, including:



- **Network security** enabling virtual patching through Intrusion Detection & Protection (IDS/IPS) and a host-based firewall
- **Anti-malware** with Web reputation to protect vulnerable systems from the latest in threats
- **System security** through integrity monitoring & log inspection, enabling the discovery of unplanned or malicious changes to registry and key system files, as well as discovering anomalies in critical log files.

With these controls, Deep Security can help organizations:

- **Defend against network and application threats**, leveraging proven host-based network security controls like Intrusion Detection & Protection
- **Protect against vulnerabilities**, instantly shielding vulnerable applications and servers with a ‘virtual patch’ until a workload can be patched or updated
- **Keep malware of workloads**, ensuring that servers and applications are protected.
- **Identify suspicious changes** on servers, including flagging things like registry settings, system folders, and application files that shouldn’t change—when they do.
- **Accelerate compliance** with key frameworks like the SANS/CIS Critical Security Controls, as well as key regulations like PCI and HIPAA, delivering multiple security controls, central control, and easy reporting in a single product.

At a summary level, **Deep Security can help with 14 of 20** of the Top 20 Critical Security Controls:

SANS TOP 20 CRITICAL SECURITY CONTROLS	
1. Inventory of Authorized & Unauthorized Devices	11. Secure Configurations for Network Devices
2. Inventory of Authorized & Unauthorized Software	12. Boundary Defense
3. Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers	13. Data Protection
4. Continuous Vulnerability Assessment & Remediation	14. Controlled Access Base on the Need to Know
5. Controlled Use of Administrative Privileges	15. Wireless Access Control
6. Maintenance, Monitoring, & Analysis of Audit Logs	16. Account Monitoring & Control
7. Email and Web Browser Protections	17. Security Skills Assessment & Appropriate Training to Fill Gaps
8. Malware Defenses	18. Application Software Security
9. Limitation and Control of Network Ports, Protocols, and Services	19. Incident Response Management
10. Data Recovery Capability	20. Penetration Tests & Red Team Exercises

MAPPING THE TOP 20 CRITICAL SECURITY CONTROLS

This table below provides a high-level mapping of Deep Security’s security controls to the SANS/CIS Top 20 Critical Security Controls, and also provides commentary on where cloud service providers (CSPs) like AWS, Microsoft Azure, and others have a roll to play.

CIS CRITICAL SECURITY CONTROL	CLOUD SERVICE PROVIDER ROLE	APPLICATION OF SECURITY CONTROLS
<p>1. Inventory of Authorized & Unauthorized Devices: <i>Actively manage (inventory, track & correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized & unmanaged devices are found and prevented from gaining access.</i></p>	<p>Will typically be able to generate asset lists via an API</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Change management • Source control • Restrict access to APIs • Automated server discovery across physical, virtual, & cloud 
<p>2. Inventory of Authorized & Unauthorized Software: <i>Actively manage (inventory, track & correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized & unmanaged software is found and prevented from installation or execution.</i></p>	<p>No controls</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Change management • Source control • Integrity monitoring 
<p>3. Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers: <i>Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.</i></p>	<p>Change control of the IaaS layer</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Change management • Source control • Integrity monitoring 
<p>4. Continuous Vulnerability Assessment & Remediation: <i>Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, & minimize the window of opportunity for attackers.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • Routing tables • Network access control lists • Security groups 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Scans as part of deployment • Intrusion prevention • Strong patch management 



CIS CRITICAL SECURITY CONTROL	CLOUD SERVICE PROVIDER ROLE	APPLICATION OF SECURITY CONTROLS
<p>5. Controlled Use of Administrative Privileges: <i>The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • IAM (Identity & Access Management) • Granular policy support 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Principle of least privilege • Regular review of access • Log inspection 
<p>6. Maintenance, Monitoring, & Analysis of Audit Logs: <i>Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • Storage • Logging at the IaaS level • Netflow logs 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Centralized logging • SIEM (<i>Deep Security supports the leaders, including HP ArcSight, IBM QRadar, and Splunk</i>) • Log inspection 
<p>7. Email and Web Browser Protections: <i>Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers & email systems.</i></p>	<p>No controls</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Regular endpoint patching • Anti-malware protection • Web reputation services • Intrusion prevention 
<p>8. Malware Defenses: <i>Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, & corrective action.</i></p>	<p>No controls</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Change management • Anti-malware scans • File integrity monitoring • Web reputation services 
<p>9. Limitation and Control of Network Ports, Protocols, and Services: <i>Manage (track/control/ correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • Security groups 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Application control • Secure OS configuration • Intrusion prevention • Firewall 
<p>10. Data Recovery Capability: <i>The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • Snapshots for workloads • Snapshots for databases • Simple high availability 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Regular automated snapshots • Test restoration
<p>11. Secure Configurations for Network Devices: <i>Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process.</i></p>	<p>They implement & enforce:</p> <ul style="list-style-type: none"> • Configuration of network fabric • Separation of virtual private clouds 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Route tables • Network access control lists • Security groups



CIS CRITICAL SECURITY CONTROL	CLOUD SERVICE PROVIDER ROLE	APPLICATION OF SECURITY CONTROLS
<p>12. Boundary Defense: <i>Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • Routing tables • Network access control lists • Security groups 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Good network design • Intrusion prevention • Firewall 
<p>13. Data Protection: <i>The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • IAM (Identity & Access Management) 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Strict access control • Intrusion prevention <i>(Enabling lateral movement detection)</i> 
<p>14. Controlled Access Base on the Need to Know: <i>The processes and tools used to track/control/prevent/correct secure access to critical assets according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • Routing tables • Network access control lists • Security groups 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Good network design • Change management • Asset management • Log inspection • Firewall 
<p>15. Wireless Access Control: <i>The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.</i></p>	<p>Not applicable</p>	<p>Not applicable</p>
<p>16. Account Monitoring & Control: <i>Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.</i></p>	<p>They provide:</p> <ul style="list-style-type: none"> • IAM (Identity & Access Management) 	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • No shared accounts • Log inspection 
<p>17. Security Skills Assessment & Appropriate Training to Fill Gaps: <i>For all functional roles in the organization, identify the specific knowledge, skills, and abilities needed to support defense of the enterprise.</i></p>	<p>Not applicable</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • A culture of security that spans all functions • A business strategy that is secure by design
<p>18. Application Software Security: <i>Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.</i></p>	<p>No controls</p>	<p>Organizations should implement & enforce:</p> <ul style="list-style-type: none"> • Change management • Robust SDLC • Intrusion prevention (virtual patching) 



CIS CRITICAL SECURITY CONTROL	CLOUD SERVICE PROVIDER ROLE	APPLICATION OF SECURITY CONTROLS
19. Incident Response Management: <i>Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.</i>	No controls	Organizations should implement & enforce: <ul style="list-style-type: none"> • Clear, easy-to-follow process • Simple communications flow • Repeatable procedures
20. Penetration Tests & Red Team Exercises: <i>Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.</i>	No controls	Organizations should provide: <ul style="list-style-type: none"> • Scope of engagement • Permission from CSP

Find out more about how Trend Micro Deep Security can help you more effectively and efficiently implement the SANS Top 20 Critical Security Controls for an effective cyber defense on our web site at www.trendmicro.com/hybridcloud.



Securing Your Journey
to the Cloud

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

..... **TREND MICRO INC.**
 U.S. toll free: +1 800.228.5651
 phone: +1 408.257.1500
 fax: +1408.257.2003

