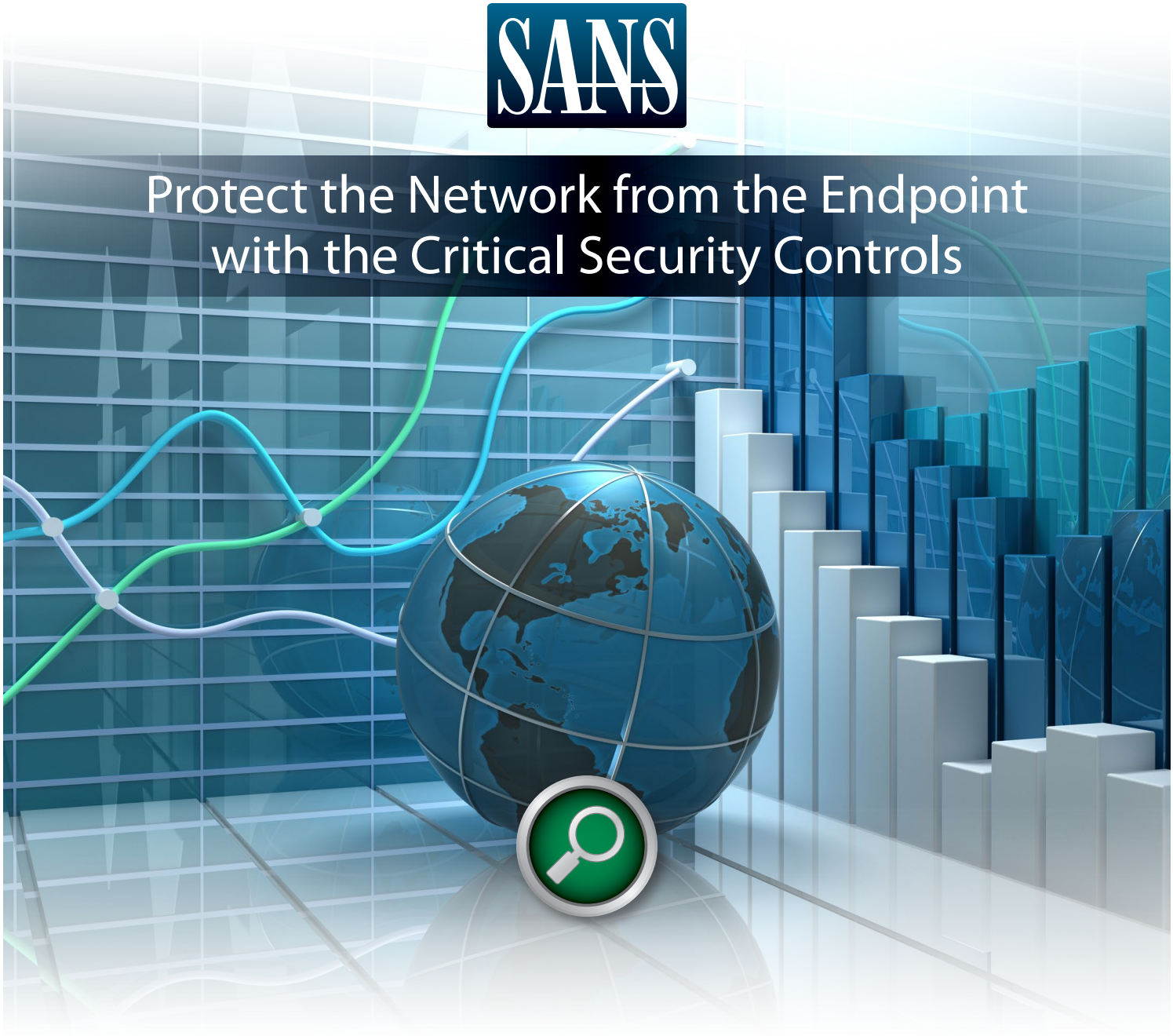
Protect the Network from the Endpoint with the Critical Security Controls

G. W. Ray Davidson, PhD



Protect the Network from the Endpoint with the Critical Security Controls

A SANS Spotlight

Written by G. W. Ray Davidson, PhD

August 2016

Sponsored by
ForeScout

The endpoint is rapidly evolving and often the first vector of attack into enterprises, according to the SANS 2016 State of Endpoint Security Survey.[1] As such, all endpoints should be considered potentially hostile.

The increased use of BYOD (bring your own device), COPE (corporate owned, personally enabled) and even IoT (Internet of Things) devices poses particularly challenging problems for organizations. Such devices do not support most conventional endpoint agents and tools, making them unusually difficult to detect and quarantine or remediate on connection to the network. The evolution of the endpoint threat is recognized in the most recent revision of the CIS Critical Security Controls (CSC)—Version 6—which includes a focus on identifying and controlling risk related to all types of endpoints, including corporate-owned devices.

Several of the CSC policies apply to assessing and detecting endpoint threats, and protecting networks from potentially hostile endpoints:

- As they connect, all types of endpoints should immediately become visible to the network, and be interrogated and treated as potentially hostile until they satisfy a set of policy rules that measure the level of trustworthiness.
- Even when an endpoint is scanned and allowed access to the network, that access should be restricted to allow only what is necessary for that endpoint. Network access management policies should allow flexible networking options, such as segmentation to secure zones for personal employee devices or contractor networks, and yet another network for remediation of infected endpoints and endpoints in violation of policy, for example.
- Access for the endpoint should also be based on the endpoint user's need to know so that users are granted access to only the resources that apply to their group or classification.
- Once connected, these devices should be continuously monitored to ensure that security, configuration and whitelisting policies are maintained while on the network.

Protecting from endpoints means controlling access to the network, as well as protecting the resources and activities made available to the endpoint after it is granted access.

[1] "Can We Say Next-Gen Yet? State of Endpoint Security," SANS, March 2016, www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827

CIS Controls and the Endpoint

The first five controls in CSC 6.0[2] constitute "foundational cyber hygiene," meaning the basic things that must be done to ensure a strong foundation for defense in an organization. Four of these controls directly concern endpoints that must be protected by the network:

CSC 1 — Inventory of Authorized and Unauthorized Devices

CSC 2 — Inventory of Authorized and Unauthorized Software

CSC 3 — Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CSC 4 — Continuous Vulnerability Assessment and Remediation

The importance of these controls is corroborated by the fact that the DHS Continuous Diagnostic and Mitigation (CDM) program[3] and the Australian Signals Directorate's "Top Four Strategies"[4] take a similar approach.

Building on this foundation, many of the remaining controls are applicable to endpoint security scanning, configuration management and controlled access as well, specifically:

CSC 7 — Email and Web Browser Protections

CSC 8 — Malware Defenses

CSC 9 — Limitation and Control of Network Ports, Protocols and Services

CSC 11 — Secure Configurations for Network Devices such as Firewalls, Routers and Switches

CSC 12 — Boundary Defense

CSC 14 — Controlled Access Based on Need to Know

CSC 15 — Wireless Access Control

CSC 16 — Account Monitoring and Control

Each control listing includes specific examples of procedures and tools that can enable implementation, integration between and among functions, and automation of critical remediation processes.

[2] www.cisecurity.org/critical-controls.cfm [Registration required for access.]

[3] "Continuous Diagnostics and Mitigation: Making it Work," SANS, August 2014, www.sans.org/reading-room/whitepapers/analyst/continuous-diagnostics-mitigation-making-work-35317

[4] "Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained," www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

Foundational Network Controls

Table 1 lists how CSC 6.0's foundation controls (1 through 4) apply to network-based protection from hostile endpoints.

Table 1. Foundational Support for Network-Based Protections from Endpoints

Control # and Title	Network-Based Controls
CSC 1: Inventory of Authorized and Unauthorized Devices	All devices should be inventoried using an automated asset inventory discovery tool. New assets should automatically be included in the inventory as they attempt access, along with distinguishing characteristics that can serve as a device fingerprint.
CSC 2: Inventory of Authorized and Unauthorized Software	When the device requests admission to the network, software on endpoints should be examined and compared with an application whitelist or other software inventory. This inventory should include software type and the version approved for each class of system. Access should be denied or the device quarantined based on violations of whitelisting policy.
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	When a device requests admission to the network, its configuration should be compared against a standard image, which includes a hardened underlying OS as well as standardized applications, including the security tools and policies configured for that endpoint. If an endpoint does not pass policy, admission should be denied or the device quarantined based on enterprise policy. Master images should be stored on a secure server and secure channels used to administer endpoints.
CSC 4: Continuous Vulnerability Assessment and Remediation	Post-admission, device configuration should be managed using standard change control and configuration management, with regular scanning of endpoints and redeployment of configuration settings as needed. This includes firewall configurations and other security devices. Vulnerability information should be regularly updated, potentially via a vulnerability intelligence service and preferably one that includes the capability to risk-rate vulnerabilities discovered on endpoints attempting access to the network. Systems should be remediated through automated workflow—such as updating patch levels on the OS and applications, in addition to the recommendations in CSC 2 and 3—and then rescanned prior to network admission to ensure vulnerabilities were addressed.

Additional Controls

A key tenet of the CIS Controls is integration among the systems used to implement the different controls, as well as automation of human tasks wherever possible. Table 2 lists additional controls as they relate to protecting the network from the potentially hostile endpoint.

Table 2. Additional Controls Related to Endpoints

Control # and Title	Network-Based Controls
CSC 6: Maintenance, Monitoring and Analysis of Audit Logs	When a device requests access to the network, it should be evaluated and only allowed access if logging is enabled (provided that the accepted network configuration requires logging). The evaluation should also determine whether the log files are configured to be stored in the correct location, whether locally or remotely. If the device is not correctly configured, it should be quarantined or refused access until it is correctly configured.
CSC 7: Email and Web Browser Protections	Patch status of email and browsers should be assessed prior to admission to the network, with access denied or the applications quarantined if appropriate based on established configuration standards. For all endpoints on the network, these applications should continue to be managed according to CSC 2 (inventory and assess software) and 4 (vulnerability assessment).
CSC 8: Malware Defenses	Endpoints attempting access should have their malware defenses deployed and updated per policy or risk being denied access or sent to a secure network for remediation. Endpoints that have missing or misconfigured defenses or, worse, are infected should be identified and potentially isolated into a separate, secure network for remediation and to control the spread. Post-admission, endpoints should be assessed and managed regularly according to CSC 3 (secure configuration of endpoint security tools) and 4 (continuous assessment).
CSC 9: Limitation and Control of Network Ports, Protocols, and Services	Endpoints attempting access to the network should be scanned for open ports, vulnerable services or misconfigured firewalls before being granted entry. Port scans should also be performed regularly on devices post-admission and the results compared with a known baseline using processes in CSC 4.
CSC 10: Data Recovery Capability	If host-based backup protection software is included as part of the standard configuration, endpoints should be queried to verify installation and patch level. Network-based queries can also be used to confirm that regular backups are being performed successfully. If the device does not conform to the specified configuration, it should be quarantined or removed from the network until it conforms to specification. Data Protection is CSC #13 in v6. The same comments as above apply.
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Network devices, including security devices, should be regularly assessed against established configuration requirements and remediated, or the device should be quarantined when out of compliance. This can help identify shadow IT/rogue WAPS, switches, hubs, etc., that may inadvertently extend the network and hence provide access to unauthorized devices. Post-admission, device configuration should be managed using standard change control and a CMDB (configuration management database).

Table 2. Additional Controls Related to Endpoints (CONTINUED)

Control # and Title	Network-Based Controls
CSC 12: Boundary Defense	Enterprise devices remotely logging in should be managed through secure access (such as a VPN). Before allowing access, boundary defenses should check configurations, installed software and patch levels. For third-party devices, subcontractors and partners must follow published security standards before gaining access to the network. Scanners should confirm these standards are met before allowing access to the network. Connecting remote endpoints (via a VPN) should be managed and assessed regularly as per CSC 3 and 4.
CSC 13: Data Protection	As devices request access to the network, network-based controls should ensure that host DLP software is installed, patched and functional, if that is part of the standard configuration. Devices should be queried regularly to ensure that the configuration conforms to specification. If the device fails to meet specifications, it should be quarantined or removed from the network until it does conform to specification.
CSC 14: Controlled Access Based on Need to Know	Endpoints attempting access should be allowed to access only those resources for which they have permissions. This highlights the importance of network zones for secure, unknown and potentially hostile endpoints, for example. Some endpoints, such as employee devices, may access only a guest network, whereas company-owned computers have access to departmental servers. Access to resources should also be controlled based on need to know. Information stored on systems should be protected with file system, network share, claims, application or database-specific access control lists (ACLs). The validity of these ACLs should be reviewed regularly using a network-based tool, and access logs should be kept by and be accessible to appropriate operations and security personnel.
CSC 15: Wireless Access Control	Wireless endpoints, including end-user devices and access points, should conform to an authorized configuration and security profile, with a documented owner of the connection and defined business need to access. Also, insecure peer-to-peer applications should be disabled before granting access, unless approved for documented business need. And separate virtual LANs should be created for user-owned systems and other untrusted devices.
CSC 16: Account Monitoring and Control	All account access configuration should be performed through a local directory or LDAP. Typical user access (time of day, duration, etc.) and the user's authentication methods should be profiled and unusual activity (users accessing resources from endpoints that have not been profiled as belonging to the user) flagged for follow-up. All account use on endpoints should be monitored and users logged off automatically after a standard period of inactivity. Endpoints should also be monitored for attempted usage by deactivated accounts.
CSC 19: Incident Response and Management	In the event of an incident, responders can use analysis of log and other data collected on the endpoint's activities, security status, access records, patch level, installed applications and other information to provide context to the event, and to determine appropriate IR activities, including remediation and follow-up. Interoperability among the organization's IR tools and good communication among IR personnel is key for this activity.

Final Thoughts

Networks are connecting to an increasing variety of endpoint devices[5] and will require a variety of approaches for protection. These protections will need to keep up with the diversity of endpoints, as well as their applications and uses.

Protection is possible only with deep visibility into *all* the endpoints attempting access on the network, enforceable policies that restrict access to different secure zones based on the state of those endpoints, and orchestration and automation of response processes. The newest version of the CIS Controls provides an excellent base of information for accomplishing these and other tasks related to protecting the network from potentially hostile endpoints.

[5] www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827

About the Author

G. W. Ray Davidson, PhD, is the former dean of academic affairs for the SANS Technology Institute. He continues to serve as a mentor, subject matter expert and technical reviewer for the SANS Institute and holds several GIAC certifications. Ray started his career as a research scientist and subsequently led global security projects for a major pharmaceutical company. He has taught at the college level and worked at a security startup. Ray currently works with clients to develop and implement network security monitoring and threat intelligence capabilities. He is also active in the leadership of the Michigan Cyber Civilian Corps.

Sponsor

SANS would like to thank this survey's sponsor:

ForeScout®