White Paper

Conquer the Top 20 Critical Security Controls

Build on McAfee coverage for the "Quick Wins" in the Top 5

Table of Contents

"The strength of the Critical Controls is that they reflect the combined knowledge of actual attacks and effective defenses of experts in the many organizations that have exclusive and deep knowledge about current threats. These experts come from multiple agencies of the US Department of Defense, Nuclear Laboratories of the US Department of Energy, the US Computer Emergency Readiness Team of the US Department of Homeland Security, the United Kingdom's Centre for the Protection of Critical Infrastructure, the FBI and other law enforcement agencies, the Australian Defence Signals Directorate and government, and civilian penetration testers and incident handlers.

Top experts from all these organizations pooled their extensive firsthand knowledge of actual cyberattacks and developed a consensus list of the best defensive techniques to stop them. This has ensured that the Critical Controls are the most effective and specific set of technical measures available to detect, prevent, and mitigate damage from the most common and damaging of those attacks."[1]

"The US State Department has previously demonstrated more than 94% reduction in 'measured' security risk through the rigorous automation and measurement of the Top 20 Controls."[2]

Introduction

Many CISOs wonder where they should optimize processes and focus their resources to reduce security risk most effectively. They know that threats are moving more quickly than protections and regulatory initiatives have yielded security that isn't effective against real-world threats. Even heavily regulated enterprises and critical infrastructure sectors that have already adopted risk management practices and frameworks must consistently reassess the effectiveness of their efforts.

Wherever you are in your risk management maturity, validating your security controls and processes against the recommendations of the Council on CyberSecurity Top 20 Critical Security Controls (previously known as the SANS Top 20) can help secure your organization's assets, infrastructure, and information.

The Top 20 Critical Security Controls strengthen your organization's security posture through continuous, automated protection and monitoring of your infrastructure to reduce compromises. The authors used an "offense must inform defense" approach to select and prioritize the list of controls that would have the greatest impact on improving risk management against real-world threats.

The Value of the Critical Security Controls

The strength of the Critical Security Controls (CSCs) is that they reflect the consensus of successful experiences captured and refined over multiple revisions. The CSCs help organizations break down operational silos by providing a pragmatic blueprint detailing where to focus efforts to achieve the greatest results.

"The Critical Security Controls effort focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works"—security controls where products, processes, architectures, and services are in use that have demonstrated real-world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness."[3]

While the CSCs are broken down into 20 separate controls, the authors recognize that organizations need a place to start. The control sequence reflects their impact, from one to 20. Within each control, sub-levels provide further guidance so that every organization can experience "quick wins," gain "visibility and attribution" of assets in their infrastructure, and improve "configuration and hygiene" of assets to reduce exposure to threats. This range of detail makes the CSCs relevant to any organization, even if solely as a means to validate that existing efforts meet "due care" expectations for cybersecurity.

As validation of the merit of these baseline steps, according to the Australian Government Department of Defense, at least 85% of the targeted cyberintrusions to which the Defence Signals Directorate (DSD) responds could be prevented through application whitelisting; patching of applications, browsers, and operating systems; and minimizing the number of users with administrative privileges.[4] These controls are all encompassed by the CSC Top Five.

Top 5 Critical Security Controls

Critical Control 1	**Inventory of Authorized and Unauthorized Devices** Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
Critical Control 2	**Inventory of Authorized and Unauthorized Software** Actively manager (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
Critical Control 3	**Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** Establish and implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Critical Control 4	**Continuous Vulnerability Assessment and Remediation** Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
Critical Control 5	**Malware Defenses** 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, and corrective action.[5]

"At least 85% of the targeted cyberintrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies listed in our Strategies to Mitigate Targeted Cyber Intrusions:

- Use application whitelisting to help prevent malicious software and other unapproved programs from running.
- Patch applications such as PDF readers, Microsoft Office, Java, Flash player, and web browsers.
- Patch operating system vulnerabilities.
- Minimize the number of users with administrative privileges.

The Strategies to Mitigate Targeted Cyber Intrusion are ranked in order of overall effectiveness. Rankings are based on ASD's analysis of reported security incidents and vulnerabilities detected by ASD in testing the security of Australian government networks."[6]

McAfee Integrated Security for the Top Five CSCs

The CSC emphasis on integration and automation makes it align very well with the Security Connected approach from McAfee. The Security Connected framework enables you to establish a robust risk management process with integrated solutions and management that protect your infrastructure—including IT and incident command systems (ICS) without impairing system availability. Because McAfee and partner solutions share a unified, policy-based management platform and real-time threat intelligence, organizations can move easily to adopt incremental controls as part of a consistent, efficient process.

Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives.

The following list maps the quick wins within Critical Controls 1 through 5 to associated McAfee products, services, and partner solution capabilities—all part of the Security Connected platform. In this paper, we cover the quick wins in the controls that matter most, the initial five controls. Once you have embraced these core controls, you can use the same McAfee® security management foundation to expand your security foundation to support CSC Controls 6 through 20. Note that the individual products listed may be available as part of integrated suites.

Critical Control 1: Inventory of Authorized and Unauthorized Devices

McAfee and Partner Products	CC-ID	Implementation	McAfee Offering
McAfee Vulnerability Manager **McAfee Real Time** **McAfee Enterprise Security Manager (SIEM)** **McAfee® ePolicy Orchestrator® Rogue System Detection** **McAfee Asset Manager (part of McAfee Vulnerability Manager)**	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	McAfee provides two solutions for *active* scanning of network devices. McAfee Vulnerability Manager provides asset-based discovery, management, scanning, and reporting. McAfee Vulnerability Manager supports LDAP integration to import systems from existing asset repositories. McAfee Real Time provides on-demand asset discovery of managed and unmanaged devices by running real-time queries. McAfee provides two solutions for *passive* scanning of the network with real-time identification of assets on the network. McAfee Rogue System Detection, a feature of McAfee ePolicy Orchestrator software, provides real-time detection of unknown and unmanaged systems by means of a sensor placed on at least one system within each network broadcast segment (typically a subnet). McAfee Asset Manager will passively monitor network assets and provides real-time identification of devices and device types, including mobile devices. Furthermore, McAfee Enterprise Security Manager provides a centralized location that allows you to discover, manually create, and import assets.

McAfee Enterprise Security Manager McAfee ePolicy Orchestrator Rogue System Detection McAfee Asset Manager	1.2	Deploy dynamic host configuration protocol (DHCP) server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.	McAfee Enterprise Security Manager is the central consolidation point for logs collected from network devices, including DHCP server logs. McAfee Rogue System Detection, a feature of McAfee ePolicy Orchestrator software, provides real-time detection of unknown and unmanaged systems by passively analyzing DHCP response packets within each network broadcast segment (typically a subnet).
McAfee Vulnerability Manager/McAfee Asset Manager McAfee ePolicy Orchestrator Rogue System Detection	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	McAfee Vulnerability Manager provides McAfee Asset Manager, a passive network inventory monitoring function that automatically populates the McAfee ePolicy Orchestrator software software's asset database in real time. McAfee Asset Manager automatically updates its inventory module with newly discovered devices. Once here, they can be marked as "authorized" or "unauthorized." Offline devices may be removed from the inventory list. McAfee ePolicy Orchestrator Rogue System Detection can send alerts when unmanaged devices are discovered on the network.

CCS Critical Control 2: Inventory of Authorized and Unauthorized Software

McAfee and Partner Products	CC-ID	Implementation	McAfee Offering
McAfee Application Control McAfee Network Security Platform Endpoint Intelligence Agent	2.1	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (isolating the custom software in a virtual operating system that does not retain infections).	McAfee Application Control uses dynamic whitelisting to ensure that only trusted applications run on servers and endpoints. Unlike simple whitelisting, a dynamic trust model eliminates the need for tedious manual updates to approved lists. The McAfee Network Security Platform Endpoint Intelligence Agent gathers MD5 hash values of all applications installed on an endpoint and sends them to the McAfee Network Security Platform, where the application can be stopped or added to a whitelist or blacklist for network communications.
McAfee Application Control	2.2	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	McAfee Application Control can inventory a system for software and then authorize such software to be run or not run on the system. McAfee Application Control allows you to derive each endpoint's whitelist from the endpoint itself. In this way the whitelist can be gathered in minutes, not weeks, and is always able to capture uncommon applications or non-standard versions that are specific to individual user communities. Image deviation helps administrators track inventory present on a client system; if any changes occur, they can be brought to the administrator's attention immediately.
McAfee Application Control McAfee Policy Auditor McAfee Change Control	2.3	Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system. A strict change-control process should also be implemented to control any changes or installation of software to any systems on the network. This includes alerting when unrecognized binaries (executable files, DLLs, other libraries, etc.) are found on a system, even inside of compressed archives. This includes checking for unrecognized or altered versions of software by comparing file hash values (attackers often utilize altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software components).	McAfee Application Control can alert administrators when software that is not whitelisted attempts to install/ launch. McAfee Policy Auditor can be configured to run custom audits to check for the existence of any software that is not included in an approved list. McAfee Change Control enables administrators to: monitor the integrity of program executables, configuration files, or registry keys and changes to file content or attributes to detect, block, and evaluate attempted changes to see if they are malicious or benign. You can control individuals and services that can change systems and align change control policies to company change windows.

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

McAfee and Partner Products	CC-ID	Implementation	McAfee Offering
McAfee Policy Auditor McAfee Application Control McAfee Vulnerability Manager	3.1	Establish and ensure the use of standard secure configurations of your operating systems. Standardized images should represent hardened versions of the underlying operating system, and the applications installed on the system. Hardening typically includes: removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, configuring non-executable stacks and heaps, applying patches closing open and unused network ports, implementing intrusion detections systems and/or intrusion prevention systems, and use of host-based firewalls. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	McAfee Policy Auditor helps you report consistently and accurately against a variety of compliance mandates, including PCI DSS, SOX, GLBA, HIPAA, FISMA, and the best practice frameworks ISO 27001 and COBiT—and you can download authoritative benchmark content in minutes. McAfee Vulnerability Manager allows administrators to run baseline policy scans for systems configurations, as well as run compliance scans for PCI DSS, SOX, GLBA, HIPAA, FISMA, and the best practice frameworks ISO 27001 and COBiT. McAfee Application Control provides the ability to configure and capture a gold standard baseline for systems and compare that gold standard baseline against all systems in the environment. Administrators can run a report and view deviations between the gold standard baseline and systems in the environment.
Partner Solution: Autonomic Network and System Administration	3.2	Implement automated patching tools and processes for both applications and for operating systems software. When outdated systems can no longer be patched, update to the latest version of application software. Remove outdated, older, and unused software from the system.	McAfee Security Innovation Alliance Partner Autonomic Software provides a patching solution fully integrated to McAfee ePolicy Orchestrator software. McAfee ePolicy Orchestrator software is required. See the McAfee Security Innovation Alliance Public Directory Listing http://www.mcafee.com/apps/partners/partnerlisting.aspx?region=us#autonomicsoftware. Company website: http://www.autonomic-software.com.
Partner Solution: Avecto Privilege Guard	3.3	Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help prevent installation of unauthorized software and other abuses of administrator privileges.	McAfee Security Innovation Alliance Partner Avecto uses McAfee ePolicy Orchestrator software as its console and provides Microsoft Windows privilege management (controls software installation without requiring administrator privilege). The solution complements McAfee Application Control whitelisting. See the McAfee Security Innovation Alliance Public Directory Listing: http://www.mcafee.com/apps/partners/partnerlisting.aspx?region=us#avecto. Additional resource: http://www.mcafee.com/apps/partners/partnerlisting.aspx?region=us#foxt Company website: http://www.avecto.com
Not Applicable	3.4	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	This control relates to policies or processes required by organizations. McAfee does not currently offer a solution here.
Not Applicable	3.5	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	This control relates to policies or processes required by organizations. McAfee does not currently offer a solution here.

CCS Critical Control 4: Continuous Vulnerability Assessment and Remediation

McAfee Products	CC-ID	Implementation	McAfee Offering
McAfee Vulnerability Manager	4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with the risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	McAfee Vulnerability Manager quickly and accurately finds and prioritizes vulnerabilities and policy violations on networked systems. It lets you balance asset value, vulnerability severity, threat criticality, and countermeasures to focus protection on your most important assets.
McAfee Enterprise Security Manager (SIEM)	4.2	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. Second, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	McAfee Enterprise Security Manager (SIEM) normalizes all events from hundreds of third-party sources to provide advanced correlation. All major vulnerability scanners are also supported. Events can be tied to exploitable threats, so, security personnel can be quickly alerted and begin remediation. McAfee Enterprise Security Manager also maintains granular historical data to facilitate forensics and historical correlation against older events with new threat information. McAfee Enterprise Security Manager gets feeds from the McAfee Global Threat Intelligence cloud on all external IP addresses and their reputation to alert if any known external bad actor is (or has been) active on the private network.
Not Applicable	4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	This control relates to policies or processes required by organizations. McAfee does not currently offer a solution here. However, both McAfee Vulnerability Manager and McAfee Asset Manager can be configured to use a dedicated account for authenticated vulnerability scans. The account credentials can be stored and encrypted so that unauthorized employees cannot view them. The management interface for both systems can be locked down with the same or separate credentials to ensure that the security and privacy of the vulnerability scans are only visible to authorized individuals.
McAfee Vulnerability Manager/McAfee Asset Manager McAfee Policy Auditor McAfee Vulnerability Manager for Databases	4.4	Subscribe to vulnerability intelligence services to stay aware of emerging exposures and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.	McAfee risk and compliance products receive updated information about new and current threats from millions of collection points, delivered by our renowned research organization, McAfee Labs. In addition to threat descriptions and analyses, the threat feed supplies recommended remediation, links to threat discussion groups and notices, various risk scoring methods, a list of applications affected, and insight into how threats affect regulatory mandates.

CCS Critical Control 5: Malware Defenses

McAfee Products	CC-ID	Implementation	McAfee Offering
McAfee Complete Endpoint Protection—Enterprise **McAfee Complete Endpoint Protection—Business**	5.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with antivirus, antispyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	McAfee Endpoint Protection suites include layered protections to block advanced malware and protect against emerging threats. Advanced anti-malware, host intrusion prevention, device control, host-based firewall, dynamic application control, and more, tackle malware, zero-day threats, and evasion attacks at every vector—mobile, data, web, email, and network. McAfee anti-malware leverages real-time global threat intelligence to quarantine or block viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs. Behavioral intrusion prevention with a stateful desktop firewall allows you to control desktop applications that can access the network to stop network-borne attacks and downtime. Used to define policies and manage all McAfee endpoint malware detection and compliance solutions, McAfee ePolicy Orchestrator software provides a single point of reference for deploying, managing, and maintaining security for endpoints, data, networks, and compliance solutions from McAfee and McAfee Security Innovation Alliance portfolios. It provides instant visibility into security status and events and direct access to management for unified control of all your security and compliance tools.
McAfee VirusScan® Enterprise/ McAfee ePolicy Orchestrator	5.2	Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations, or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.	McAfee VirusScan Enterprise proactively stops and removes malicious software, extends coverage against new security risks, and reduces the cost of responding to outbreaks. You can use policies to schedule automated updates to .DAT files as often as you prefer and use compliance reports and tasks to make sure that systems are up to date. All content that is updated frequently, for example patches and signature files, can also be checked in manually or checked in using an automated server task. In addition, McAfee offers a heuristic network check feature that looks for suspicious programs and DLLs running on McAfee VirusScan Enterprise-protected client systems. This feature catches malware before the regular .DATs are deployed.
McAfee Device Control	5.3	Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens ("thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares.	McAfee Device Control monitors and regulates how your employees transfer data to removable media such as USB drives, MP3 players, CDs, DVDs, and Bluetooth devices—even when users are not connected to the corporate network.
McAfee VirusScan Enterprise	5.4	Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.	McAfee VirusScan Enterprise provides on-access scanning for files when any read or write action is taken from removable media.
McAfee Email Protection	5.5	Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering.	McAfee provides email security onsite, in the cloud, or an integrated hybrid of both. Going beyond antispam and malware protection, McAfee Email Protection integrates data loss prevention technology, content-based policy enforcement, click-time link scanning, and continuity services to ensure email access during server outages.
McAfee Advanced Threat Defense	5.6	Enable anti-exploitation features such as data execution prevention (DEP), address space layout randomization (ASLR), virtualization/ containerization, and more. For increased protection, deploy capabilities such as enhanced mitigation experience toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.	McAfee Advanced Threat Defense detects today's stealthy, zero-day malware with an innovative, layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic, malware analysis (sandboxing) to analyze the actual behavior of malware. When combined, this represents the strongest advanced anti-malware technology in the market, and effectively balances the need for both security and performance. McAfee Advanced Threat Defense integrates with McAfee endpoint and network security products for comprehensive malware protection.
McAfee Device Control	5.7	Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices.	McAfee Device Control protects your data from falling into the wrong hands via removable storage devices and media, such as USB drives, MP3 players, CDs, and DVDs. It enables you to specify and categorize which devices may or may not be used and enforce what data can and cannot be transferred to these devices—at the office, at home, or on the move.

Case Study: Top 20 and the State of Colorado

The Colorado Governor's Office of Information Technology (OIT) adopted the CSC/SANS Institute Top 20 Critical Security Controls as its new structure for 90% of the state's IT security, starting with the first five controls. The McAfee team inventoried the technologies they already had, then made a grid showing gaps and what needed to be done to move the project towards the customer's goal. A deal was struck—a 50/50 combo of products and three years of on-site professional consultation. The contract also included flexible McAfee product licensing. The state of Colorado selected technology comprised 15 products to address the SANS Top 20 Critical Security Controls and its security project goals. OIT was not ready to implement and/or use all of the tools on day one, but the deal structured by McAfee made the decision easy, and OIT knew all of the tools would eventually be needed as the project progressed.

"From my position, what I seek more than anything is situational awareness in real time. I want to know the current state of my systems, who's attacking them, how and what their level of compliance is with our security configuration. What I needed was a way to roll up that collected information into one pane of glass.

Honestly, the only product I found that met all of my criteria and allowed that data to seamlessly integrate into one dashboard was McAfee.

We went full in with McAfee to implement the first five SANS Institute controls, which are heavy lifts in themselves. I wanted to ensure that we were in this together. The goal was to achieve the five controls within the timeframe we wanted—to really get the ball rolling, get the hardware and networking installed and build the human processes into these tools. I pushed them hard. The timeline was very, very difficult, but it worked."

—Jonathan Trull, CISO, Governor's Office of Information Technology, State of Colorado

From Top 5 to Top 20 and Beyond

Anyone reviewing baseline security and minimum standards can be confident that the Top 5 CCS controls provide a robust foundation for safeguarding core organizational assets. A focus on the quick wins is a useful starting point, a platform on which to build, not a checklist to fill out and file.

Using the Security Connected platform, the basic protections described in this white paper can be extended for more visibility, better protection, and more efficiency, resulting in an effective operational model for supporting each of the Top 20 Controls and adapting as threats and technologies require.

Comprehensive Threat Protection Built for Operational Excellence

The Security Connected platform from McAfee provides a unified framework for hundreds of products, services, and partners to learn from each other, share context-specific data in real time, and act as a team to keep information and networks safe. Any organization can reduce risk and response time and lower overhead and operational staff costs through the platform's innovative concepts, optimized processes, and practical recommendations.

- *Innovative*—The platform leverages a real-time data exchange layer, collective threat intelligence, high-performance analytics, and open security management to make endpoint, network, and cloud countermeasures protect as one.
- *Optimized*—Actionable intelligence and situational awareness enable prioritization and balance of risk mitigation, resources, and operational value.
- *Practical*—Automation and integration cut costs and improve security. The Security Connected Reference Architecture shows how to adapt the Security Connected vision to your unique risks, infrastructure, and business objectives.

To learn more about McAfee coverage of the Top 20 controls and review a reference architecture for the Security Connected platform, visit mcafee.com/securityconnected.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

[1] http://www.sans.org/critical-security-controls/guidelines.php
[2] http://www.sans.org/critical-security-controls/
[3] http://www.sans.org/critical-security-controls/
[4] http://www.asd.gov.au/infosec/top35mitigationstrategies.htm
[5] For detailed descriptions see http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf
[6] http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60958wp_ccs-20-sec-controls_0414_ETMG