White Paper

McAfee Guide to Implementing the *10 Steps to Cyber Security*

Security by default—enabling transformation through cyber resilience

Table of Contents

Government is undergoing a transformation. The global economic condition, coupled with explosion of IT capability, and an evolving, persistent threat landscape, has forced a reinvention of the service delivery and business model of the government. This change in business requirements is also forcing a change in how security is perceived and implemented throughout the enterprise.

In order for the government to realise the value it can achieve through digital services, the resilience of systems must be assured and enterprises must improve their capability to defend against continuous cyber assaults. The *10 Steps to Cyber Security* guidance, produced by Communications-Electronics Security Group (CESG), the information security arm of the UK Government Communications Headquarters (GCHQ), represents a template for threat prevention capabilities that will help enterprises tangibly improve their cyber defence capacity and the resilience of their digital systems. This white paper describes the five measures McAfee believes will help an organisation successfully implement the CESG guidance to improve their cyber resilience and security posture.

1. Develop an Information Security and Risk-Management Regime

A successful information risk management programme starts at the top of the organisation. Establishing a culture of risk management and accountability ensures that security becomes part of the business and not an afterthought. Secondly, articulating the information assurance policy framework formally anchors the security programme. This framework will include the policies and processes that form a secure, high-assurance foundation for the organisation. The *10 Steps to Cyber Security* policy framework, recommended by CESG, should include some of the following key components:

- Home and mobile worker.
- Acceptable use of government systems.
- Malware prevention.
- Privileged account management.
- Removable media.

An associated *10 Steps* process framework will include some of the following key components:

- Training, certification, and awareness programme for users, operators, and security specialists.
- Secure configuration development and patch management.
- Incident management programme that includes monitoring and incident response processes.
- Penetration testing to assess security processes and control readiness.

Finally, incorporating cyber risk factors into business decisions regarding service assurance or new service deployment ensures that security becomes operational in the business.

McAfee® Foundstone Strategic Consulting Services, as part of strategic security engagement, can assess the current security programme and guide an organisation through the essential elements of developing an effective Information Security and Risk Management Regime.

2. Secure System Configuration Management Strategy

Employing baseline secure configurations of system architecture is an essential component of cyber risk management. However, secure configurations are not static elements. They must be continually reviewed to keep up with threat conditions, new business functionality, or policy requirements. A process of *Design, Test, Monitor, and Control* will enable a secure configuration management process. Typically, the process starts with a system assessment to Design the baseline configuration, added security functionality, and change management process. Baseline configurations are usually available for commercial off-the-shelf operating systems and applications. However, custom web applications and databases may need further testing to develop a secure configuration.

McAfee Foundstone Services, as part of a strategic security engagement, can assess the current security configurations, conduct additional penetration testing, and conduct code review for the custom applications.

Once deployed, the system should be continually tested for new vulnerabilities and monitored for unauthorised changes to the baseline and any potential intrusions. The *10 Steps to Cyber Security* recommends conducting regular scans to assess vulnerabilities using automated tools that support open standards like the Security Content Automation Protocol (SCAP). *McAfee Vulnerability Manager* and *McAfee Policy Auditor* solutions support these open standards and facilitate configuration monitoring through the *McAfee ePolicy Orchestrator® (McAfee ePO™)* security management platform. In addition to operating system vulnerabilities, it is important to test web applications and databases. These applications form a critical backbone of most digital government systems but are usually not tested nor monitored regularly as part of this process. Through the same management platform, organisations can also use *McAfee Web Application Assessment Module* and *McAfee Vulnerability Manager for Databases* to scan and test these critical applications and systems.

Although not mentioned directly in the *10 Steps* guide, it is a good practice to identify and label these critical assets within the security information and event management system. This information on the criticality of systems provides essential context during incident response.

Although the *10 Steps* guide requires managing and monitoring privileged users' accounts, it is very challenging for organisations to get granular control and visibility over the use of administrative accounts. Through the *McAfee ePO* security management platform and *McAfee Security Innovation Alliance (SIA)* partner Avecto, McAfee makes it easy for government organisations to meet this requirement. Check the McAfee SIA website for more information on the McAfee-AVECTO integration.

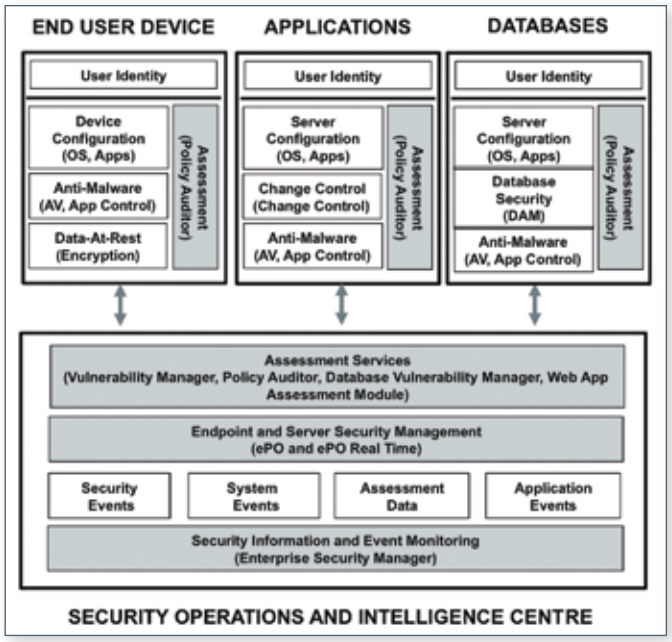

Figure 1: Basic secure configuration management reference architecture.

One of the most important functions in this process is selecting the additional security controls that will harden the system against a variety of threat vectors. According to the *10 Steps to Cyber Security,* the baseline security controls must include the capabilities to restrict removable media devices, conduct regular antivirus scans, and implement data-at-rest encryption. The McAfee ePO security management platform, first employed to conduct vulnerability and configuration assessments, can be now be used to easily deploy those additional baseline security controls.

3. Establish an Anti-Malware Strategy

Malware is the tool of choice for any cyberattacker and has many potential vectors into an organisation. However, most organisations mistakenly equate anti-malware with antivirus. As malware has become increasingly sophisticated and the attack surface increasingly diverse, a successful anti-malware strategy must include a dynamic capability to *Prevent, Detect, and Respond* in order to limit the impact of malware as an attack vector.

McAfee Application Control also enables the organisation to meet other controls recommended by the *10 Steps to Cyber Security,* such as locking down operating systems and software. McAfee Application Control can also be extended to include real-time file integrity checking for monitoring changes to critical systems. The additional data provided by Application Control can be monitored within the McAfee Enterprise Security Manager. This will improve the incident management programme by enabling more effective detection of breach attempts.

McAfee Application Control can also be deployed on embedded operating systems.

McAfee Web Gateway also meets the requirement in the *10 Steps to Cyber Security* guide for a proxy at the network perimeter. By extending the web security to include identity controls, an organisation could develop a fuller picture of user behaviour and more effective policy enforcement.

A layered defence to malware starts with the user. Although layered defences most often addresses technology, users must be trained to recognise attack methods, such as phishing, and understand where to report suspicious activity. Since many successful attacks often target a specific user, training is an essential anti-malware control. McAfee Foundstone services, as part of a strategic engagement, will design a recurring and accountable user security awareness programme. This programme ensures that both users and specialists become the first and last line of defence against malware. In addition, McAfee Foundstone can provide specialist security training, such as *Forensic and Malware Analysis,* for the Security Operations and Intelligence Centre (SOIC) analysts.

Protecting the user device is the next stage in the strategy. The end-user device baseline security configuration recommended by CESG already includes antivirus as a first layer of defence. Hardening the end-user devices or servers with additional security capability beyond antivirus, such as application whitelisting and reputation intelligence, will provide an effective defence at the host layer, even against malware that uses zero-day exploits. Security and change events generated at the host should be centrally collected, monitored, and analysed by the SOIC to detect potential incidents. Through the McAfee ePO security management platform, McAfee makes it simple to deploy application controls and enable extended behavioural-based security functions, such as reputation intelligence within *McAfee VirusScan® Enterprise* software already deployed at the endpoint. Security events are also collected through the McAfee ePO platform and reported to the *McAfee Enterprise Security Manager,* the McAfee Security Information and Event Management (SIEM) system, for correlation and incident response services.

Although application whitelisting and antivirus are effective prevention tools, malware is a multi-stage attack utilising several vectors into and out of the protected network. A comprehensive anti-malware strategy must include a network capability to recognise malware behaviours on the network and to protect end-user devices that may not support host-based security controls, such as smartphones or tablets. Since the most common delivery and command vector for malware is via the web, it is recommended to deploy web content anti-malware inspection at the Internet perimeter to better protect end-user devices or detect behavioural evidence of malware already inside the network. By employing the *McAfee Web Gateway* with its strong anti-malware capability—including sophisticated content emulation, a gateway anti-malware engine, botnet identification, and reputation intelligence—organisations not only increase their resilience against malware but also their agility to adopt new enabling technologies. As with host-security events, events from McAfee Web Gateway should be centrally collected, monitored, and analysed by the SOIC to detect potential incidents.

As mentioned, a comprehensive anti-malware strategy involves a people, process, and technology approach. One of the key processes is a breach response strategy that will Identify, Validate, Contain, and Respond to security incidents. When a suspicious event is identified, security analysts in the SOIC must rapidly validate the malware, uncover its characteristics, and find affected hosts in order to contain the impact, such as data loss or further compromise. Having direct access to automated malware analysis tools and real-time data sources will greatly increase the speed of analysis and reduce the impact of malicious cyber activity. The McAfee advanced sensor grid, including the *McAfee Network Security Platform* and McAfee Web Gateway, will identify malware in motion.

Today, McAfee uses the *McAfee Global Threat Intelligence™ (McAfee GTI™)* network to quickly share detections of emerging malware threats. The McAfee host and network products detect a suspicious file and contact the McAfee Global Threat Intelligence network to see if it has a reputation. Based on that reputation, as well as network connection reputation, and other factors, the McAfee products can make a decision to block the file.

McAfee is also developing a new integrated, advanced malware detection appliance, called McAfee Advanced Threat Defense. If the content cannot be validated immediately, it will be automatically sent to the Advanced Threat Defense system for behaviour deconstruction and analysis. Advanced Threat Defense will assign a fingerprint to the malicious file and distribute this threat intelligence locally—to McAfee-protected endpoints and network gateways—and, if you permit, that DAT will also be sent to the McAfee Global Threat Intelligence network. Through this intelligence exchange, McAfee products on your site and at other customer sites will be able to protect against this newly identified malware.

- The new DAT will allow any infected system to be identified and cleaned by McAfee VirusScan (the scanning engine inside McAfee endpoint protections).
- The network security products will block transmission of that content over the network to prevent reinfection within your infrastructure.
- The web and email gateways will block inbound reinfections.
- The endpoint protections will block infection directly on the host (through an infected USB stick, for example.)
- *Real Time for McAfee ePO* can be used to ensure all endpoints have pulled down the new DAT and run a scan to see if the malware is present.

This combination of sensor, analysis, and automated response is unique in the industry and will greatly reduce the impact of malware on the environment.

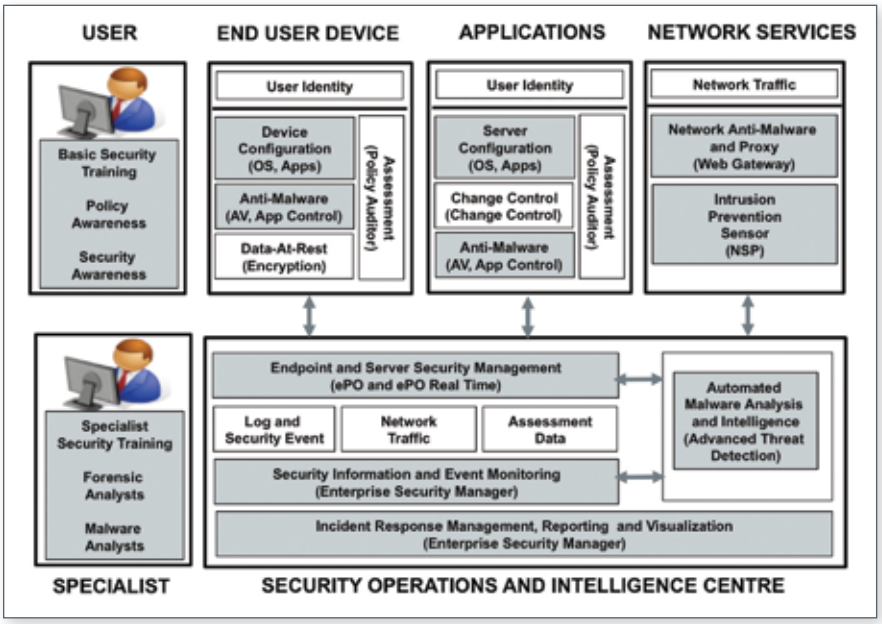

Figure 2: Basic anti-malware reference architecture.

4. Network Security Strategy

The role of network security is expanding and changing with the expansion of digital services in government. Traditionally, network security devices functioned as traffic cops governing which network addresses can pass or which protocols can traverse the Internet perimeter. While still providing that function, the goal of the network security strategy is to *Deny, Delay, and Disrupt* the ability of an attacker to get in and move around on the protected network systems.

To enable this strategy, network security devices have evolved from controlling addresses to identifying and controlling application access across multiple security zones within the enterprise. This is aligned with the *10 Steps to Cyber Security* recommendations to protect both the internal and external network boundaries.

Dividing the network into logical security zones requires different checkpoints for an attacker. Typically, one of the internal security zones is the consolidated or shared-services datacentre. An effective datacentre network security strategy requires an application layer firewall for controlling application access and an intrusion prevention sensor to protect the sensitive applications from vulnerability exploitation. Other potential network security zones include partner and cross-domain network interconnections. Each of those connections requires an application firewall to control access, although the risk of vulnerability or malware exploitation is low across these perimeters. The greater concern is the access to, or loss of, sensitive data to unauthorised business or coalition partners. Best practice recommends a network data loss prevention solution be deployed and monitored at these perimeter locations.

The adoption of cloud services presents unique challenges for traditional perimeter security solutions. While an application layer firewall provides granular traffic control at the Internet perimeter, many applications are exposed to external cloud services through application programme interfaces. Today, on-premises deployment of a centralised service gateway is recognised as the best practice deployment pattern for the application-to-application, web-based service interaction models. A service gateway enables the organisation to develop a standards-based policy enforcement point that is integrated with internal identity management and auditing/monitoring infrastructure.

5. Security Monitoring Strategy

With the sophistication and persistence of malicious cyber activity combined with the complexity of security information, detecting or anticipating a security breach requires an organisational monitoring and intelligence strategy, trained specialists, and a 24/7 SOIC. Developing a monitoring strategy starts with an understanding of attack methods. Using threat intelligence will determine the data sources that are most effective to identify and validate an incident. The monitoring strategy must also reflect other requirements from regulations such as GPG13. Once requirements are established, the data collection architecture can be built to support the various breach response or other monitoring use cases.

McAfee Foundstone Services can design an incident-management programme from policy development, to process employment through specialised training in malware analysis and attacker techniques.

The *10 Steps to Cyber Security* recommends collecting various data types such as network traffic, security events, server and device events, and user behaviour, as the foundation of the monitoring capability. Centralising this data inside McAfee Enterprise Security Manager will facilitate rapid data mining for both identification and validation. The McAfee Enterprise Security Manager easily scales to handle high-volume data sources while still enabling rapid data retrieval for reporting and analysis.

One of the key processes of the SOIC is Incident or Breach Response. This is the process of *Identifying, Validating, Containing, and Mitigating* a cyber incident. A successful strategy also starts with threat intelligence of attack methods to determine what are the most effective indicators. For example, identifying an insider attack usually requires identity and database activity monitoring since these provide the most likely indicators. Identifying an attempted breach from an outside attacker usually requires network and host sensors and automated malware intelligence as described in the anti-malware section. Designing the sensor grid that will expose the right indicators is one of the key foundations to this strategy. Existing McAfee ePO infrastructure can easily be extended to include *McAfee Database Activity Monitoring* and *Privileged Identity* data that supports insider monitoring use cases. McAfee Advanced Threat Defense and McAfee Web Gateway will reveal indications of remote attackers using malware as the entry vector. Centralising this data and incident workflow within the McAfee Enterprise Security Manager allows for rapid identification and validation of malicious activity.

The SIA partner, TITUS, can monitor user behaviour related to data and data policy. TITUS is fully integrated with the McAfee ePO security management platform for deployment and management. TITUS events can also be sent to McAfee Enterprise Security Manager for user behaviour trending and further user-related correlation scenarios

Once a breach is identified, speed of response is critical. McAfee Enterprise Security Manager is a central command and control platform that can adjust policy on the McAfee Network Security Platform to rapidly block malicious files or update security policy through McAfee ePO software to contain an incident at the host level.

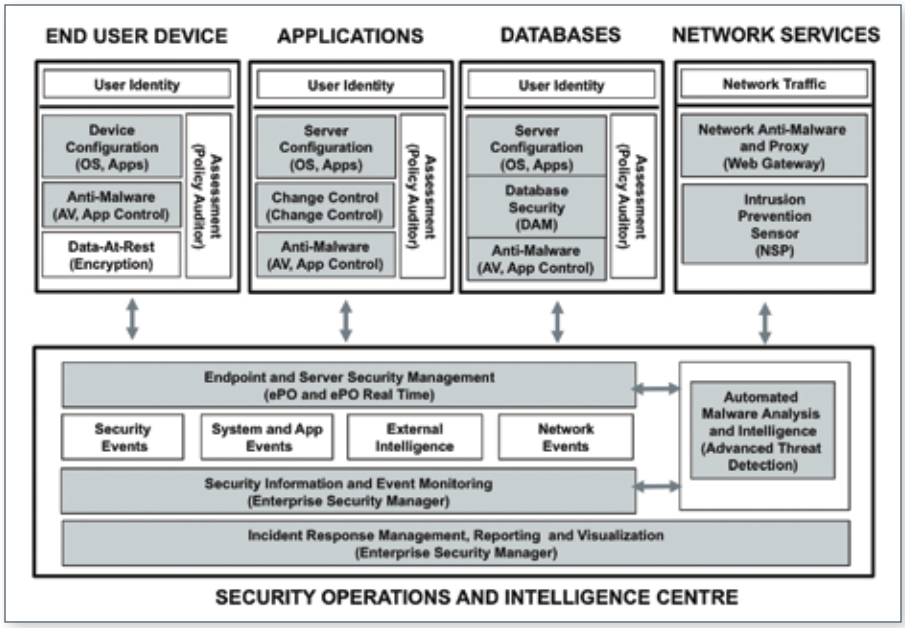

Figure 3: Basic monitoring reference architecture.

Summary

This solution brief represents McAfee ideas for improving cyber resilience and security posture through implementation of the CESG's *10 Steps to Cyber Security.* While this guide does not address all areas of security or cyber defence requirements, it does provide proven cyber risk reduction steps that could allow an organisation to withstand a cyber threat. For further information and consultation, please contact your local McAfee representative or visit www.mcafee.com.

McAfee
An Intel Company

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

60245wp_10-steps-cyber-security_0513_fnl_ASD