White Paper

McAfee
An Intel Company

McAfee Security Architectures for the Public Sector

End-User Device Security Framework

Table of Contents

Cabinet Office is driving a series of programmes with a view to making government ICT more streamlined, more cost effective, and less complex. One of these programmes is End User Device Strategy: Security Framework and Controls (EUD Security Framework). EUD Security Framework represents a simple set of guidelines for the security architecture for devices that will connect to government services. At its highest level, EUD Security Framework is about the use of transparent and open industry standards (for example, IPsec and SSL/TLS) along with a good deal of common sense.

In this white paper, we explain, at a strategic and tactical level, how McAfee assists customers in achieving these standards and guidelines with its portfolio of products and implementation methodology included in the Security Connected platform. We also demonstrate the results of using the Security Connected platform.

Business Value

The EUD Security Framework, produced by UK Cabinet Office, represents a set of control requirements and architecture standards that will help government agencies tangibly improve technology adoption, the user computing experience, and cyberdefense capability. Providing flexibility to use purpose-built tools, such as laptops or tablets, will improve the user experience, but that does not remove the requirement for the user to act responsibly with respect to security. Additionally, the controls framework provides consistent security capability across ministries, improving the overall cyber resilience of the government infrastructure. This white paper explains why McAfee represents the best business and technology value to implement the required security controls in the EUD Security Framework. Although the name of the framework implies device-specific security, it is actually a system-based approach to protecting those devices. The Security Connected platform yields the best value by delivering comprehensive protection and visibility across multiple device types, networks, and applications, resulting in less complexity and a more effective security architecture.

Agility

In general, agility is the capability of a system to change in response to a new condition. For resilience, agility is characterised by *integration* and *interoperability*. Integration is the ability of the system to rapidly adopt new technology or new security capability. An agile solution has the ability to easily interoperate with other technology through the adoption of open standards or an extensible management framework. The McAfee security management portfolio, specifically McAfee® ePolicy Orchestrator® (McAfee ePO™) software and McAfee Enterprise Security Manager, provides an agile foundation for an agency to comply with the EUD Security Framework through:

- Flexibility to choose multiple device types, operating systems, or suppliers and still maintain the security functions.
- A foundational platform to build new capability for a future framework or threat response requirements.
- Easy integration with existing security or management architecture to extend the value of a current investment

Assurance

In terms of cybersecurity, digital service assurance requires establishing the standards, processes, and capabilities to ensure the survivability of the system against a threat. The Security Connected platform, with integrated intelligence and real-time response actions, delivers *comprehensive security capability* to rapidly enforce policy, defend the system from both external and internal threats, and detect new threat conditions. McAfee endpoint and network security portfolios, along with McAfee Application Control and McAfee Web Gateway, provide strong assurance to prevent or detect advanced malware. The McAfee security management portfolio, specifically McAfee ePO software and McAfee Enterprise Security Manager, provide central event collection and control, enabling real-time response to detected threats. Benefits include:

- Flexibility to deliver comprehensive capability from a single security platform.
- Comprehensive solution for advanced malware across endpoint, network, and services.
- Integrated technology that delivers strong security beyond compliance.

Cost reduction

Many operating systems provide basic security controls, such as antivirus and host-based firewalls. While these features are initially attractive from a cost perspective, cost is not the only defining factor for value. In some cases, the built-in operating system tools are purpose-built. However, they often create more complexity, offer lesser or no central visibility, provide lower security functionality, and require additional investment in personal, training or integration services than originally anticipated. The Security Connected platform can yield better value by meeting the design, technology, security, and framework principles under a single platform.

Domain	Full Support	Partial Support
Assured Data in Transit	X	
Assured Data at Rest		X
Platform Integrity	X	
Incident Response	X	
Authentication	X	
Secure Boot		X
Application Whitelisting	X	
Device Update		X
Interface Protection	X	
Malware Protection	X	
Policy Enforcement	X	
Event Collection	X	

Trust

Delivering assured security products is a foundational step towards establishing a trusted digital infrastructure. As a critical supplier, McAfee leadership made the executive commitment to deliver verifiable, trusted security platforms by ensuring the integrity of our supply chain, protecting our intellectual property from theft, and finally by certifying our product security levels against international standards.

In the global economy, an *assured platform* starts well before the software development cycle. Because of our understanding of the threat landscape and close partnership with government, McAfee has established a *verifiably secure hardware supply chain*. The critical first step towards a trusted infrastructure is having the confidence that the security technology protecting the enterprise is assured.

Building confidence also means verification. McAfee has made the executive commitment to certify *all* products against the rigorous international *accreditation* standards of Common Criteria. Every product line within McAfee has the responsibility to meet and maintain Common Criteria certification through every product release.

Technology Value

The EUD Security Framework is a capability roadmap that outlines the technology and operational security requirements for a device to access government services. However, as with other guidelines, the value is achieved through operationalising the security capability. In addition to full alignment to the controls framework, the Security Connected platform offers several key elements necessary to operationalise the EUD Security Framework into real security value.

Speed

The Security Connected platform represents a faster time-to-operational value through consolidation of security operations and visibility that provides a centralised view of capability. Through integrated intelligence, centralised event analytics, and real-time response capability, the platform enables the speed of decision, response, and acquisition needed for system resilience.

Integration

The EUD Security Framework expands legacy security best practices to meet the risk to official networks today. As the new requirements are implemented, new security technology must integrate with existing infrastructures to avoid operational silos and higher costs. The Security Connected platform is open to hundreds of technology partners, allowing for immediate expansion of capability without infrastructure changes. In addition, McAfee supports and promotes the use of open technology standards such as IPsec, SSL/TLS, RESTful Web Services, and SCAP. These standards ease integration with existing architecture, expand analytical capability for incident response, and allow machine-to-machine data collection for improved visibility and decision-making.

Reference Architecture

Our reference architecture offers a guide to implementing the EUD Security Framework using the Security Connected platform. Since many of the framework controls may already be in place across the customer landscape, McAfee recommends a process to integrate additional capability for our platform.

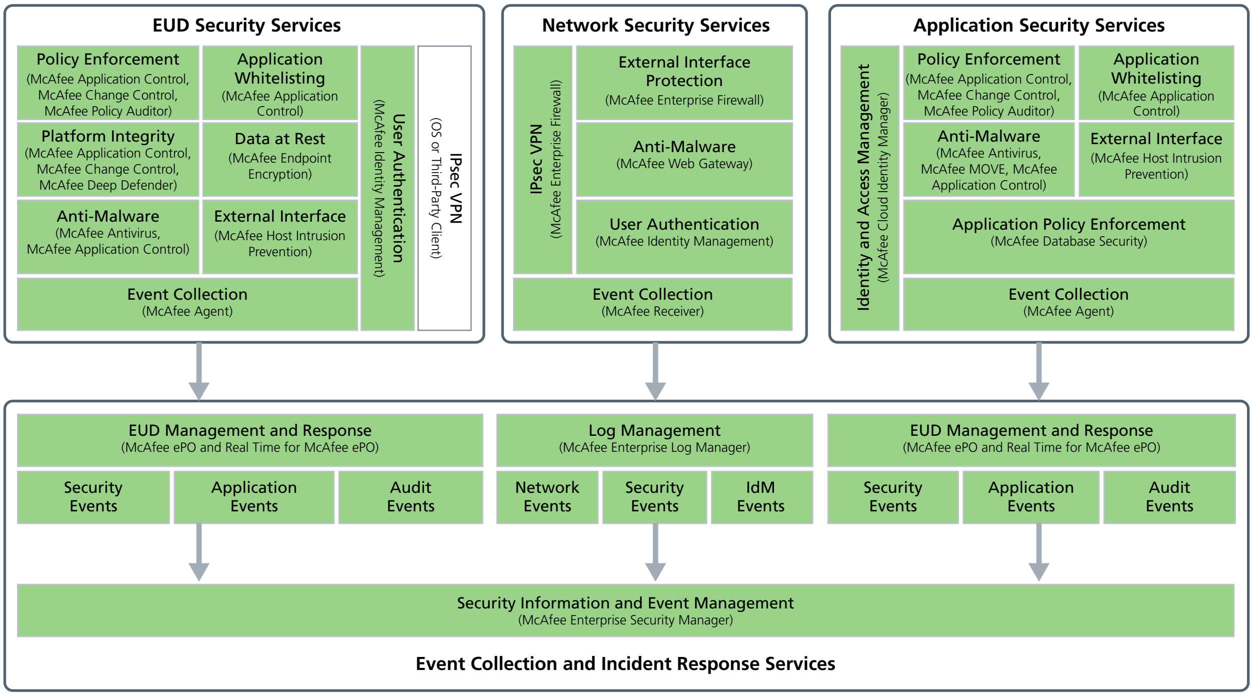
Assessment

It is important to analyse current security capability against requirements of the framework. A best practice is to divide the control framework into functional areas like security foundations, prevention, and situational awareness. This will allow for incremental integration, measurement, and implementation based on security capability.

Implementation

Implementation will vary depending on the assessment phase results. However, it will be easiest to integrate situational awareness capability first, as it generally does not have an effect on operations. For example, implementation of McAfee Enterprise Security Manager, a security information and event management (SIEM) system for event collection and incident response, will have immediate operational benefits without impact on end user experience. Additionally, implementation of audit tools, such as McAfee Policy Auditor and McAfee Vulnerability Manager, will help provide risk assessment to the current environment. Finally, prioritisation of preventative controls is key. Most malware and advanced threats use the web to both initially infect an user system and then to remotely control that system. Therefore, implementation of McAfee Web Gateway, which provides operational as well as security benefits, is strongly recommended.

The following diagram shows a representative architecture for implementation of the Security Connected platform against EUD Security Framework requirements.



EUD Security Services
Policy Enforcement (McAfee Application Control, McAfee Change Control, McAfee Policy Auditor)
Application Whitelisting (McAfee Application Control)
Platform Integrity (McAfee Application Control, McAfee Change Control, McAfee Deep Defender)
Data at Rest (McAfee Endpoint Encryption)
Anti-Malware (McAfee Antivirus, McAfee Application Control)
External Interface (McAfee Host Intrusion Prevention)
User Authentication (McAfee Identity Management)
IPsec VPN (OS or Third-Party Client)
Event Collection (McAfee Agent)
Network Security Services
IPsec VPN (McAfee Enterprise Firewall)
External Interface Protection (McAfee Enterprise Firewall)
Anti-Malware (McAfee Web Gateway)
User Authentication (McAfee Identity Management)
Event Collection (McAfee Receiver)
Application Security Services
Identity and Access Management (McAfee Cloud Identity Manager)
Policy Enforcement (McAfee Application Control, McAfee Change Control, McAfee Policy Auditor)
Application Whitelisting (McAfee Application Control)
Anti-Malware (McAfee Antivirus, McAfee MOVE, McAfee Application Control)
External Interface (McAfee Host Intrusion Prevention)
Application Policy Enforcement (McAfee Database Security)
Event Collection (McAfee Agent)
EUD Management and Response (McAfee ePO and Real Time for McAfee ePO)
Security Events
Application Events
Audit Events
Log Management (McAfee Enterprise Log Manager)
Network Events
Security Events
IdM Events
EUD Management and Response (McAfee ePO and Real Time for McAfee ePO)
Security Events
Application Events
Audit Events
Security Information and Event Management (McAfee Enterprise Security Manager)
Event Collection and Incident Response Services

Figure 1. EUD Security Framework requirements mapped to the Security Connected platform from McAfee.

The following chart maps the Security Connected Platform against EUD Security Framework domains:

Domain	McAfee Solution	McAfee Value
Assured Data in Transit	McAfee Enterprise Firewall	• High-assurance firewall specifically designed for high threat environments.
Assured Data at Rest	McAfee Endpoint Encryption	• Central management and visibility, broad platform support.
Authentication: User to service	McAfee Cloud Identity Manager	• Single sign-on improves user experience. • Support for multiple platforms. • Simplified and consolidated identity event collection.
Secure Boot	McAfee Deep Defender McAfee Application Control	• Software configuration and execution control. • Detect threats beyond the operating system.
Platform Integrity and Application Sandbox	McAfee Change Control McAfee Application Control	• Software configuration and execution control. • Supports multiple platforms.
Application Whitelisting	McAfee Application Control	• Software configuration and execution control. • Supports multiple platforms.
Malicious Code Detection and Prevention	McAfee antivirus McAfee Application Control McAfee Client Proxy McAfee Web Gateway	• Comprehensive malware protection. • Integrated file, IP, and URL reputation. • Web and EUD work together to ensure protection on and off the network.
Security Policy Enforcement	McAfee Policy Auditor	• Enterprise view of security policy.
External Interface Protection	McAfee Host Intrusion Prevention McAfee Web Gateway	• Integrated IP, URL reputation. • Malware protection for web services.
Device Update Policy	McAfee Policy Auditor McAfee Vulnerability Manager	• Centralised audit of device, server, application, and data security policy.
Event Collection and Analysis	McAfee ePO software McAfee Log Receiver McAfee Enterprise Log Manager McAfee Enterprise Security Manager	• Centralised security policy management, configuration, and event collection across multiple platforms and mobile devices. • Rapid data access to data and correlation reduces IR time.
Incident Response	McAfee Foundstone® Services	• Comprehensive programme development, forensic training, or services.

Summary

As the role of security changes from an asset-based approach to a service enabler, agencies should engage with security providers as strategic partners who can enable cyber resilience of government services. The Security Connected platform's broad portfolio of standards-based security products, services, and implementation methodologies, combined with our long-standing commitment to the UK government's extensive efforts to provide optimal technological and security assurance, reduced complexity, lower costs, and a good user experience, position it as a premier UK government supplier and partner.

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

McAfee
An Intel Company

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