Technology Blueprint

McAfee
An Intel Company

ENFORCING SECURITY ON SMARTPHONES AND TABLETS

Protecting the business while allowing personally-owned devices to access the network

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL 1 2 **3** 4 5

Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. 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 Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Protecting the business while allowing personally-owned devices to access the network

The Situation

As IT security, do you cringe when you see your employees—or worse yet your executive team—bring in the latest smartphones or tablets and demand email access on them? What if you see them browsing confidential presentations? As employees utilize personally-owned smartphones and tablets to access more than just email, cybercriminals are responding with creative, modern ways to exploit the trend with mobile device-specific threats.

Today, smartphones and tablets are both key business enablers and a critical business risk. They enable productivity while opening the network and corporate data sources to threats, including the risk of noncompliance with regulations and governance requirements.

Driving Concerns

In your company, mobile devices are becoming just another endpoint. The twist is that a growing percentage of these smartphones and tablets will be employee-owned—and each employee may have more than one. The number of devices may triple overnight.

Protecting these devices means balancing flexibility and risk in areas where most companies don't have policies or programs. Organizations must decide: how to deal with personal data vs. corporate data; how to educate users on the safety (and dangers) of the thousands of apps in the marketplace; and how to minimize exposure when these devices disappear.

Because of the diversity and refresh rate of smartphones and tablets, security architectures must move the focus from device-specific policies to network-based enforcement of corporate policies. Broad enforcement must enable end-to-end protection of the new mobile perimeter.

In order to bring smartphones and tablets safely into the enterprise, mobile device policies and enforcement must tackle three areas: enabling access, protecting data, and demonstrating compliance.

Enabling access

- **Broad device support.** The "standard" corporate device platform ended with the Blackberry. Few companies can narrowly dictate specific devices or operating systems, and the refresh and update cycle of consumer devices is much faster than traditional endpoints like PCs.
- **Fast, easy policy and application provisioning.** A complex and painful process will deter users from allowing their personally-owned devices to be governed
- **Enterprise integration.** Enterprises already struggle to maintain access privileges as employees join, migrate around, and leave the organization. Mobile devices must not add more user management cost or complexity.
- **Strong authentication.** Access must be limited to users that the organization recognizes and trusts
- **Support costs.** Enterprises fear that complex implementations, password resets, jailbroken phones, and unexplained misbehavior on devices will burden either IT or the help desk with lengthy, costly interventions.

Protecting Data from Malware and Loss

- **Protecting devices from malicious apps and files.** The number of apps on a smartphone or tablet can be ten times higher than that of standard desktops. Users can choose from a mix of games, productivity, finance, social networking, and thousands of other apps. The chance of installing an app containing malware is higher than with a standard desktop, because of the lack of network or device protection as well as the sheer simplicity of searching for and installing a risky application. Users may be trained or prevented from installing personal apps on corporate-owned computers, but IT can't dictate app downloads on a personally-owned device. Malware can also be introduced to the device from multiple sources besides applications: emails, photos, text messages, even a PC used to top up power. The device needs to be secured against being compromised or spreading infection if it connects to other computers.
- **Protecting intellectual property and regulated data.** Smartphones and tablets contain organizational contacts, corporate email, confidential spreadsheets, presentations, and documents that thieves value and regulators demand you control. Due to the small form factor of these devices, they are more likely to be misplaced, lost, or stolen. When this happens, companies must prove that regulated data was encrypted at the time of loss.
- **Delineation of corporate data vs. personal data.** Users will have personal email, photos, music, video, and content shared with friends and family—all intertwined with corporate data. The challenge becomes how to protect corporate data while ensuring integrity of the user's personal data. There are also privacy and legal issues that could require policies for selective backup, or selective wipe in the event of device loss.
- **Support for safe browsing.** As more and more websites can identify access from a mobile device, malicious content is migrating to this vector. Most of these devices will operate off the corporate network, so extra protections are needed to ensure that a user's browsing experience remains safe.

Demonstrating Compliance

- **Visibility.** Auditors and risk management require IT to quickly and accurately show the compliance status of devices that have access to corporate assets
- **Enforcement.** To prevent compliance violations, enterprises must show they have the ability to deny access to unencrypted, jailbroken, or otherwise insecure devices
- **Compliance reporting.** Enterprises resent the existing costs of compliance, so any mobile device solution should minimize the incremental burden of reporting on these devices

Solution Description

An effective solution integrates secure mobile application access, antimalware, strong authentication, high availability, a scalable architecture, and compliance reporting in a seamless system. Comprehensive and robust management features should enable IT to effectively manage the mobile lifecycle: secure the mobile workforce, ensure that policies and configurations are persistent, protect devices and the corporate network from malware threats and lost data, and deliver automatic and real-time compliance management. The solutions should also help minimize support costs and overall TCO by leveraging the native capabilities of your enterprise's existing data center infrastructure and IT network, including directory services, Wi-Fi, VPN, and PKI.

Enabling access

- **Broad device support.** Since personally-owned devices can come in any form, you may need to restrict the approved access list to certain configurations that meet minimum standards (such as on-board encryption or remote wipe support). You should expect to offer support for multiple vendors and multiple operating systems, such as iPhone, Android, Microsoft, and Blackberry, as well as the many flavors of hardware from smartphone to tablet.
- **Fast, easy policy and application provisioning.** The solution must make it straightforward to deploy and decommission devices and applications over the air (or tethered to a managed PC) based on the device's compliance. IT's effort should be minimal after policies and approved users are defined; users should have options and parameters for self-service provisioning as well as updates.

Decision Elements

These factors could influence your architecture:

- Will your organization provide smartphones or tablets to your employees?
- Will you restrict or recommend approved apps or allow users full access?
- How will you ensure that your policies are consistent across your entire infrastructure including your mobile workforce?
- How will you provide automatic security updates to your mobile workforce?

- **Enterprise integration.** The solution should hook into and stay synchronized with existing enterprise infrastructure, such as user directories (Active Directory), network access (Wi-Fi and VPN), and authentication systems (such as PKI). Users and policies should be manageable as groups or as individuals to allow role-based access to applications.
- **Strong authentication.** Policies (and enforcement) should have the flexibility to allow or disallow access based on tiered levels of authentication, with the minimum of a password and the option for stronger authentication such as PKI or two factor
- **Support costs.** The solution should minimize mobile device support efforts through web self-service and integration with existing help desk and support workflows

Protecting Data from Malware and Loss

- **Protecting devices from malicious apps and files.** Antimalware should scan any content being downloaded to the device over any connection type or communication path, prevent installation of malicious content, and block access to download sites and app stores that carry risky content. The solution must be able to scan all possible ways that malware can infect your mobile device, including files, compressed files, applications, SD cards, and text messages. Access to real time threat intelligence will also be crucial to protect against the latest malware that can spread quickly today via social networks.
- **Protecting intellectual property and regulated data.** Two capabilities are critical: encryption and remote lock and wipe. You should make native encryption support a base requirement for device access to corporate networks. The solution should be able to validate encryption before connection and show that encryption was active at the time of loss, especially if the data is stored on a removable SD card that could be switched to another device. Remote data wipe can reduce data loss risk if the device is lost or stolen.
- **Delineation of corporate data vs. personal data.** As these devices blur the line between work and personal use, your organization will need the ability to provide selective wipe capabilities of corporate data (such as email) while preserving personal data. Not only does this provide peace of mind for your users, but it also can help with legal and privacy issues.

Demonstrating Compliance

- **Visibility.** IT should be able to aggregate and present dashboards and logs showing device usage, device status, compliance status, and recent application activity
- **Enforcement.** The solution should test for and deny access to devices that are not compliant with policies; tests should reveal and block access by rogue, unencrypted, and jailbroken devices
- **Compliance reporting.** Both real-time audits and custom reports should be available to support different organizational communication requirements

Technologies Used in the McAfee Solution

McAfee® Enterprise Mobility solutions respect both IT and user requirements for control and convenience. Our scalable offerings respond to users' needs as those users shift from consumers to corporate employees—and back again. IT gains governance over users' devices, regardless of ownership, to ensure that enterprises can protect the device, the data on the device, and the corporate network, while offering options that help respect the employee's privacy when the device is used for personal purposes.

The McAfee solution for enterprises includes McAfee Enterprise Mobility Management (McAfee EMM) for secure management of mobile devices and McAfee VirusScan® Mobile for active protection against malicious code.

McAfee Enterprise Mobility Management

The McAfee EMM platform blends mobile device management with policy-managed endpoint security, network access control, and compliance reporting in a seamless system. This platform integrates smartphones and tablets into enterprise networks and security management with the same level of security protection, convenience, and scale enjoyed by laptops and desktops.

With McAfee EMM, system administrators have the tools and capabilities needed to effectively secure a broad range of mobile devices in the enterprise network, seamlessly manage them in a scalable architecture, and efficiently assist users when problems arise.

McAfee EMM protects sensitive data with policy-based security, support for native encryption, remote lock and wipe, and optional PKI and two-factor authentication. We can detect and block devices that are not using encryption, as well as those without approved versions of the firmware and unauthorized or modified devices like jailbroken iPhones and rooted Android devices. In addition to remote lock, McAfee EMM supports two kinds of wipe: full and selective wipe. Full wipe takes the device back to factory settings for firmware and applications. It is ideal when the user loses a device. It works even if encryption is active. Selective wipe allows IT to manage enterprise data (email, contacts, and calendars) on the phone, but leaves intact the user's personal information and content (such as an iTunes library and photos).

McAfee EMM supports PKI and strong authentication options using provisioning tokens and Enrollment Agents, as well as two-factor authentication such as RSA SecurID. Before a user can access the enterprise network, you can require user authentication: through standards-based certificates (McAfee EMM integrates with the Microsoft Certificate Authority so every device being provisioned has a unique device certificate to enable strong authentication), VPN on demand, or SSL VPN. In addition, to sync email, you can require strong authentication—username and password plus the device certificate.

McAfee EMM is managed by McAfee® ePolicy Orchestrator® (McAfee ePO™), so it can be rolled out and managed efficiently alongside other McAfee and third party solutions. During configuration of the McAfee EMM server, the administrator can set up a roles-based console to use Active Directory (AD) or Domino LDAP credentials and leverage directory security groups. PKI users set up Enrollment Agents and Certificate Authorities based on existing PKI infrastructure. You can define policies for each user based on the type of device used and the security appropriate to each user's role. Policies can also define the types of connections and services users/groups can access, including VPN, Wi-Fi, messaging, and line of business applications.

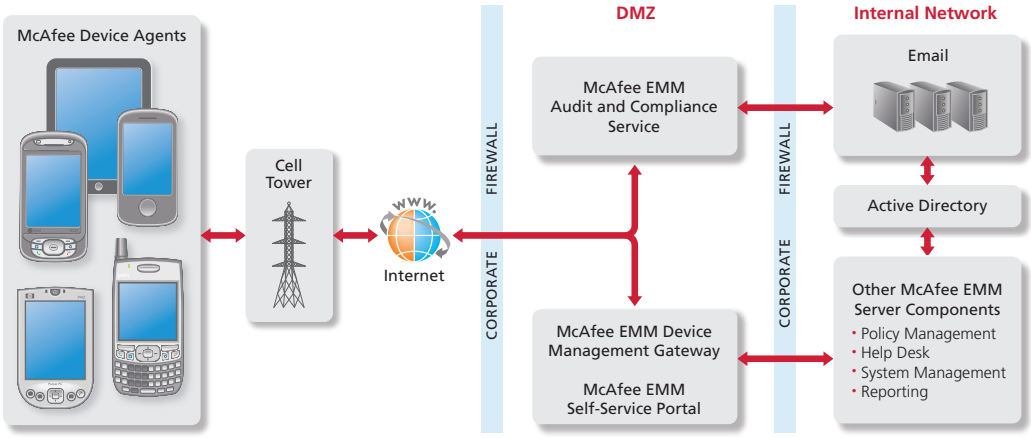
After the administrator installs McAfee EMM on a server and defines policies, devices, and authorized users (based on Active Directory or LDAP entries), users can provision their own devices over-the-air from a self-service interface. McAfee EMM allows employees their choice of devices with support for Apple iOS, Google Android, Microsoft Windows Mobile, Windows Phone, and RIM BlackBerry smartphones and tablets. Several app store options allow easy downloads, and updates to security policies and configurations are pushed in real time to the device over the air to keep the device updated with minimal user effort. A self-service portal option helps users find answers and resolve their own problems.

In addition to real-time visibility into device compliance status, you can generate reports that cover specific policy violations, application inventory, compliance status tracking, and lost devices. These statistics can roll up with other McAfee ePO results into custom reports. For example, McAfee EMM Device Agent data can be presented with data from other McAfee-secured endpoints and mobile devices within a McAfee ePO dashboard for enterprise-wide visibility, with direct drill down for more details, such as audit logs, device status, and pending actions.

McAfee VirusScan Mobile

McAfee VirusScan Mobile scans and cleans mobile data, preventing corruption from viruses, worms, dialers, Trojans, and other malicious code. VirusScan Mobile protects mobile devices at the most critical points of exposure, including inbound and outbound emails, text messages, photos, videos, email attachments, and Internet downloads. Comprehensive antimalware technology protects data transmitted via wireless carrier data networks, Bluetooth, Wi-Fi, and infrared communications. McAfee VirusScan Mobile runs with minimal memory resources, avoiding any service interruptions while protecting against malware.

These solutions work together to meet the requirements of enabling smartphones and tablets in the enterprise.



The centralized McAfee EMM architecture efficiently supports device diversity

Impact of the Solution

Using McAfee mobility solutions, enterprises can confirm compliance and deny network access to compromised devices that could allow malicious applications to steal corporate data. This control with flexibility lets you move quickly to allow employees to bring their own devices to work, yet enforce appropriate standards for security and policy compliance. You both reduce risk and trim costs.

By leveraging McAfee Mobile Security solutions in your environment, you gain visibility into and control. You also set up a scalable infrastructure that will help reduce risks in the following ways:

- Secure user-owned technologies on the corporate network
- Protect against data loss and malware infection
- Enforce policy compliance automatically regardless of technology ownership
- Remotely lock and wipe missing devices, reducing the risk of data loss if a device is lost
- Ensure all data transmitted between mobile devices and servers is encrypted

Centralized policy management reduces the burden on IT and other support systems throughout the mobile device lifecycle. Our integrated approach allows you to:

- Say yes to user-owned technologies to save procurement costs
- Centrally manage user-owned technologies for full visibility and control
- Set policies, but have users self-provision and self-manage using a portal that helps users find answers and resolve their own problems
- Take advantage of the Microsoft REST services implementation to automate help desk functions such as decommissioning a mobile user
- Scale as an increasing number of users bring their devices to work

Q&A

Why shouldn't I use Microsoft Exchange, Apple iPCU, or other device management solutions?

Enterprise-class support requires control across the entire lifecycle of the device, not just password/PIN unlock and remote wipe. We provide features that allow you to scale to the service levels and devices your users require and enforce the policies your business demands:

- Self-service device activation, including a user agreement process
- Group-based policy configuration (tied to Microsoft Active Directory or Lotus Domino LDAP)
- Automatic and personalized configuration of enterprise services, including VPN, email, and Wi-Fi
- Strong authentication
- Encryption management
- Over-the-air push updates of security policies and configurations

Exchange and other device-specific management tools offer subsets of these functions for specific applications and devices. We offer a comparable minimum feature set—pin unlock and remote wipe—for all supported platforms, plus more capability where feasible.

What control do I have over the firmware and applications on the device?

You can block devices that are noncompliant with your policies, including those without approved versions of the firmware, and exert some control over the resources and applications on the device, such as turning off the camera or Bluetooth. On Apple devices you can ban certain native applications such as YouTube, Safari, and iTunes. Once the device is active, you can block installation of any additional applications, leaving existing applications and personal data in place.

What happens if the SIM is removed before a device is wiped?

Even if the SIM is removed, the device is protected with the PIN. If the password is entered too many times, the device can be set to auto-wipe. However, if you do not use encryption, then the SD card itself might be read before the wipe is performed, allowing a thief access to sensitive information on the SD card.

Can I control who can provision devices?

You can pre-populate (whitelist) selected users that are allowed to provision, or you can allow all users.

Can I blacklist certain applications?

On Apple devices you can ban (blacklist) certain native applications such as YouTube, Safari, and iTunes explicitly.

How can I provide access to in-house developed applications?

To distribute your own application, you have two options: place it on the Apple iTunes store, or physically tether the device and download the application directly to each device, then configure it with the platform utility, such as the iPhone Configuration Utility (iPCU).

What if the device already has personal content and applications installed?

Once the device is active, you can "secure the image" to block installation of any additional applications, leaving existing applications in place.

What assistance do you offer to help us ensure and maintain device compliance?

- You can manage policies and devices and get reports through any Silverlight-enabled web browser. Our console allows you to monitor who is trying to connect.
- You can use automatic policy enforcement to ensure that only authorized devices from authorized users can connect to enterprise applications and services
- You can require that devices are registered, secured, and up to date with respect to policies, configurations, and operating system versions before allowing a connection
- When you update a policy (usually per user or group), the policy is applied to the device when the device checks in
- Windows Mobile users can limit exposure using a policy that declares "if a device has not logged on for 15 days, it should automatically wipe"

Are there any compliance-specific reports?

We provide some audit reports to get you started, including device status, noncompliant device list, and an audit log that notes changes in the console, pending actions, and device health. You can see device details, such as user, email, phone number, security policy applied, and device state.

Additional Resources

www.mcafee.com/emm
www.mcafee.com/virusscan-mobile
www.mcafee.com/epo

Androids in the Enterprise Solution Brief
www.mcafee.com/us/resources/solution-briefs/sb-androids-in-the-enterprise.pdf

Employee Use of Personal Devices Brief
www.mcafee.com/us/resources/solution-briefs/sb-employee-use-of-personal-devices.pdf

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Authors

Dean Dyche is the director of the northeast sales engineering team at McAfee. He is responsible for ensuring his team has the skills and resources necessary to sell McAfee solutions into the Northeast Fortune 100 accounts including Citibank, JPMC, GE, and many others. Dean brings over fourteen years of experience as an industry leader, with a background in sales engineering, management, and military service. Prior to McAfee, he led the northeast sales engineering team for Secure Computing, which was acquired by McAfee in 2008. Prior to Secure Computing, Dean was a senior sales engineer with CipherTrust, the leading provider of email appliance security, which was acquired by Secure Computing in 2006. Prior to CipherTrust he spent 4 years with Elron Software selling mail and web solutions to Fortune 100 companies and the United States Government. Dean served in the United States Coast Guard as a telecommunications specialist and has a degree in network engineering and management.

David Johnston, director of the southeast engineering team at McAfee, brings over twenty years of experience in development, consulting, sales engineering and management to his role. His organization supports Fortune 100 accounts including Bank of America, FedEx, and Time Warner Cable. Prior to McAfee, David was the assistant vice president of sales engineering for Blueprint Systems, a requirements definition software company. Prior to Blueprint, David spent 6 years with Mercury Interactive as a sales engineer and manager. He studied computer science at the Georgia Institute of Technology.

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee, McAfee Enterprise Mobility Management, McAfee EMM, McAfee ePolicy Orchestrator, McAfee ePO, McAfee Global Threat Intelligence, VirusScan and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied.
Copyright © 2011 McAfee, Inc.
37904bp_compliance-smartphones-L3_1011

McAfee
An Intel Company

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