



Mobilizing Business Applications with McAfee

Table of Contents

Mobilizing Business Applications	3
Understanding the Scope	3
Foundational Requirements	4
Security	4
Connectivity	5
Personalization	5
Integration	6
Scale	7
Summary	7

As the world's largest dedicated security company, McAfee has long been a leader in mobile phone security, providing encryption and anti-malware solutions for Microsoft Windows Mobile smartphones. McAfee extends its mobile security portfolio with data and device protection for today's most popular smartphone operating systems and device types, including the Apple iPhone and Android devices. McAfee helps enterprises offer their employees mobile device choice and ownership with secure and easy access to corporate applications in a scalable manner. Enterprises of all sizes look to McAfee for comprehensive end-to-end security and management across all endpoints and all users, regardless of how or where they do business.

Mobilizing Business Applications

Today, organizations are intent on mobilizing business applications to increase productivity, drive top-line growth, and improve customer satisfaction—in short, to improve business performance.

This may mean mobilizing existing applications or developing and deploying applications that are purpose-built for the mobile worker. The need for a mobilized application is normally identified and driven by a departmental line or business project owner, such as a vice president of sales or general manager of a product line or market segment, to persuade the IT organization to satisfy their need for real-time access to business data while on the go. Common categories of mobilized line of business applications include business intelligence, sales force automation, point-of-sale, and document sharing, among others.

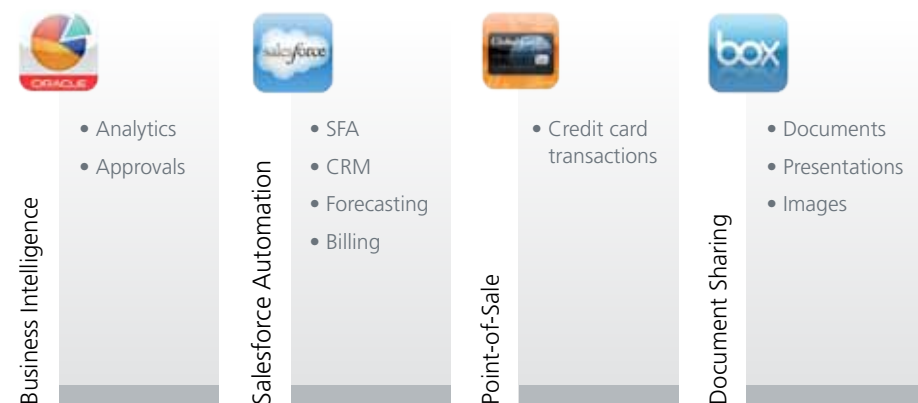


Figure 1: Commonly mobilized business applications.

Understanding the Scope

Before corporate IT can begin mobilizing an application effectively, several questions must be answered:

- How is the data that will be accessed and used by the application protected?
- How will applications running on mobile devices connect to back-end data services?
- Who will use these applications?
- How will mobile endpoints integrate into the existing IT environment?
- How will IT scale the introduction of mobile applications?

McAfee addresses each of these questions and provides the management platform to:

- Ensure integrity, confidentiality, and authenticity of all corporate data
- Enable secure, real-time access to business application data and IT services
- Configure mobile devices appropriately for disparate end users
- Seamlessly integrate mobile devices into the enterprise
- Meet all of these requirements on a large-scale deployment

The McAfee® Enterprise Mobility Management (McAfee EMM®) solution provides the foundational underpinnings necessary for an organization to succeed with their application mobilization initiatives. It reassures enterprises that their data is protected and their mobile workforce is productive by enabling them to connect to enterprise applications securely while providing a scalable architecture that can seamlessly manage up to thousands of mobile users.

Foundational Requirements

There are five key foundational requirements that an IT organization must address when mobilizing business applications, specifically security, connectivity, personalization, integration, and scale.

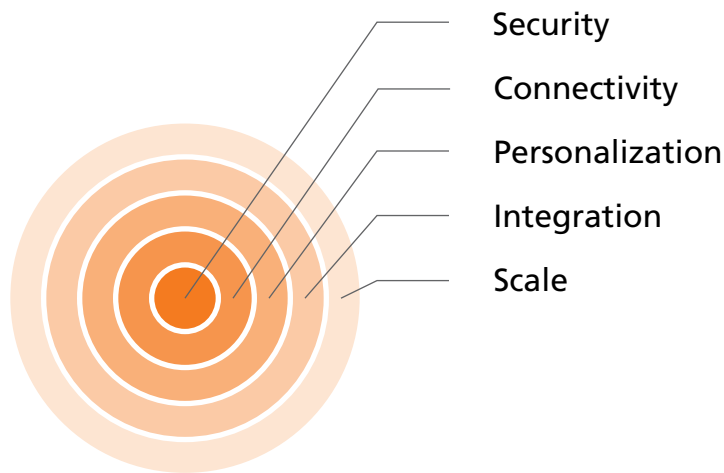


Figure 2: Enterprise mobility management foundational requirements.

Security

The McAfee EMM solution protects all enterprise data on supported mobile endpoints, including business application data, user credentials, shared credentials, email, and personal information management (PIM). This comprehensive approach reduces risks associated with violations of the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley (SOX) Act, Basel II, the Federal Information Security Management Act (FISMA), the U.S. Food and Drug Administration (FDA) requirements, and the Payment Card Industry Data Security Standard (PCI DSS) while enforcing compliance with corporate IT security policies.

The McAfee EMM architecture leverages native security—for example PIN/password, encryption, local and remote wipe—and management features built into enterprise-class mobile devices. By properly configuring those mobile devices to connect into an existing IT infrastructure, as laptops do today, data services can be delivered to mobile endpoints while maximizing infrastructure investment and offering the best possible experience to end users. By following this architecture, IT provides the necessary security controls, yet remains seamless and unobtrusive to end users and does not negatively affect device performance or battery life. The McAfee EMM solution also eliminates help desk calls that commonly result from using poorly integrated third-party security “add-ons.”

Simply put, McAfee addresses the foundational requirements around security without impacting productivity.



Figure 3: Easy, secure, and automated self-service provisioning.

Connectivity

Mobile applications are most powerful when they can efficiently connect to back-end data services.

Current generation mobile devices are powerful productivity tools, in part, because they provide an array of connectivity options. Devices can access data over carrier networks via WiFi, 2G, 3G, and now 4G. In addition, enterprise-class devices provide powerful VPN capabilities which, when combined with wireless connectivity, provide secure remote access to enterprise data. These networking capabilities enable a new world of transaction-oriented applications in addition to the important and well-supported enterprise email application.

The McAfee EMM solution automates the configuration of secure WiFi, VPN, and native email sync. By properly configuring mobile devices to connect into your existing IT infrastructure, as laptops do today, data and services can be delivered to mobile endpoints—which maximizes infrastructure investments—while providing the best possible experience to end users.

Personalization

In the mobile environment, as in traditional computing, there is no “one size fits all.”

- Each user requires a set of unique credentials—username and password digital certificate, or both—to access network resources
- Users located in various campuses or buildings connect to local wireless access points
- Users in different geographic regions often connect to regionally deployed VPN access servers or front-end messaging servers
- Users may require different security policies or access privileges, depending on their role within the organization



Figure 4: Securely connect to enterprise services.



The McAfee EMM solution enables users to connect to the services needed while maintaining the level of data protection the organization requires.

When an authorized user connects his or her mobile device to work via the easy-to-use McAfee self-service facilities, the system automatically:

- Provisions the device with the user’s unique credentials
- Connects the device to the network and user-specific application services based on the security policy established for that individual user
- And secures all data on that device according to policies appropriate to the user’s role within the organization

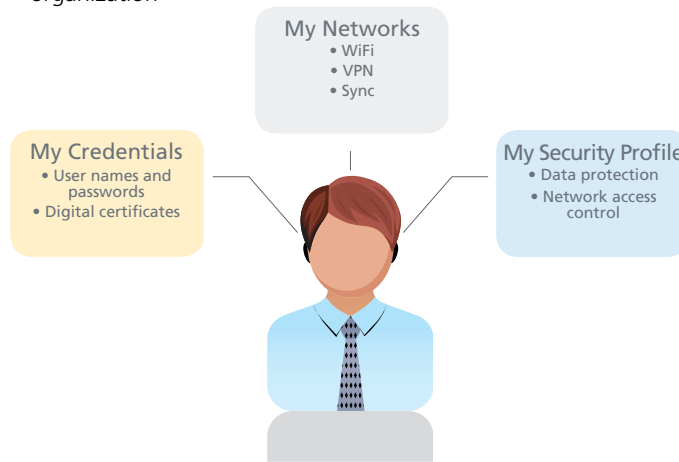


Figure 5: EMM delivers personalization.

Integration

The McAfee EMM solution mobilizes the enterprise application architecture by connecting mobile devices to enterprise applications via an organization’s current infrastructure—Sync, WiFi, VPN, and PKI (future). It bridges mobile users, applications, and devices to the data services those entities need to access.

The McAfee EMM solution integrates deeply into existing systems. The platform is a pure software overlay that is part of the IT datacenter environment and architected to avoid inefficiencies, poor scalability, and interoperability problems caused by closed or appliance-based IT silos. Our solution integrates with Microsoft Active Directory, Lotus Domino Directory, Microsoft Windows Server, SQL Server, Microsoft Exchange ActiveSync— Microsoft Exchange, Lotus Domino, Google Apps, and enterprise public key infrastructure (future)—thereby reducing total cost of ownership by leveraging the IT organization’s intrinsic skills.

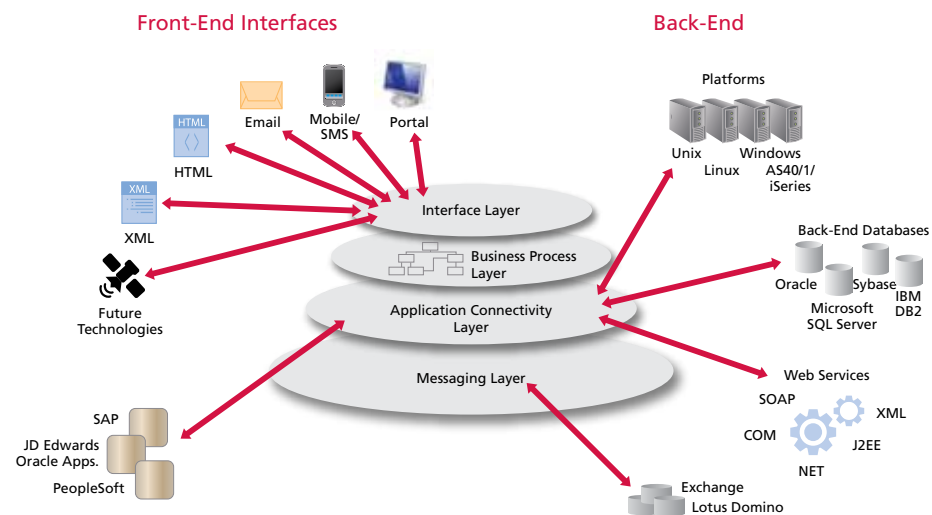


Figure 6: EMM leverages your native IT infrastructure and network.



Scale

Scaling the introduction of mobile business applications to an organization's mobile users is both critically important and challenging, particularly as scale allows the organization to truly improve operational efficiencies and top-line growth. As expected, an organization will face challenges that are both labor and time intensive when enabling data access and protection for hundreds or even thousands of mobile workers. This fundamental requirement—scale—can be cost prohibitive without the proper tools.

The McAfee EMM solution enables all of the fundamental requirements—security, connectivity, personalization, and integration—at scale, meaning it centralizes and automates the implementation of all of these requirements within a single system.

The McAfee EMM solution allows mobility to be scaled:

- To thousands of mobile users
- For multiple business applications
- Over a geographically dispersed data network
- While protecting mobile data



Figure 6: Scalable security anytime, anywhere.

Summary

Mobility has moved beyond email. Today, an assortment of applications that solve real business problems are commercially available; or, where no commercial solutions exist, development tools are readily available to allow organizations to build custom, enterprise-specific applications. Only after an IT organization has fully digested the scope of mobilizing business applications and laid the foundational requirements—security, connectivity, personalization, integration, and scale—will they be able to deliver tangible business value, increase top-line growth, and improve operational efficiencies.

Organizations intent on mobilizing their workforce can rely on the McAfee EMM solution.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>

