



SECURING MOBILE DEVICES



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.

According to a 2011 study conducted by Carnegie Mellon and McAfee, the biggest mobile security concern for organizations is sensitive data compromise. About 40 percent of the companies participating in the survey had experienced the loss or theft of mobile devices, and nearly half of those devices contained "business-critical data."

Securing the Whole Device

Challenges

There are few recent trends in technology that have had such a dramatic impact on our personal and professional lives as mobility. Mobile devices such as smartphones, tablets, and laptops have changed many aspects of our lives, such as where we can communicate and what types of information we can access. The promise of anything, anywhere, anytime, from any device has become a reality. It's because of this extensibility that mobile devices have universally become necessities for personal and professional use—from email, calendaring, and social networking, to banking, shopping, and business applications.

In addition to these devices being mobile—which introduces security management issues around access control, compliance, data protection, and so on, today's mobile devices are much more than their native hardware and software. Most are application-ready and designed to take advantage of Web 2.0 resources. Many of these capabilities are used interchangeably between personal and business use, and the number of available mobile device platforms is exploding. This combination of devices and capabilities results in greater risk to organizations in terms of lost devices, data loss, and unauthorized access.

One of the most significant areas of concern for securing mobile devices is application enablement. Consider a typical mobile device. It will include several built-in applications, such as music, web browsing, video, calendar, email, and contacts. Additionally, there are hundreds of thousands of applications for travel, entertainment, banking, health, shopping, and more. Because

organizations are taking advantage of mobile devices by allowing their employees to be more connected, enterprise and line-of-business applications are becoming increasingly popular. These applications are as varied as their consumer counterparts and include everything from CRM and virtualized desktop infrastructure, or VDI, to finance applications and solutions for provisioning and policy management.

According to IDC, in 2012, the worldwide shipments of tablets will exceed 70.8 million units.²



Facebook has more than 500 million users spending more than 750 billion minutes per month on its site. Of the hundred thousand plus applications for the Apple iPhone, Facebook is consistently in the top 10 downloads.³



There are 1,600 tweets per second; 40 percent are from mobile devices.⁴





Four is the average number of devices used interchangeably between personal and professional use.



Solutions

Securing mobile devices means securing the whole device, including the device itself and the data it contains. For IT organizations to be effective and scalable, they should be able to centrally govern all the disparate devices by setting and enforcing policies. For example, policies should be leveraged that will only allow authorized, managed, secured, and up-to-date devices to connect to the network and define where in the network access is allowed. Further, because of regulatory reporting, IT needs to be able to demonstrate and report on the compliance of all the devices on the network—mobile or otherwise.

Strong authentication should be leveraged that associates a unique identifier with the device and with the user so that policies can be applied based on the user's privileges irrespective of what device they are using. As such, for this type of authentication to be scalable, it should be associated with existing security policies and user management systems. By embracing this association, it negates the need for supporting user databases for non-mobile solutions, and another one for mobile.

From a user perspective, installing the application that enables this level of security needs to be as easy as installing the latest version of "Angry Birds." Using the iPhone as an example, a user should be able to visit the Apple App Store, download an application, enter their credentials such as their email address and password, agree to a corporate user agreement policy, and have the application automatically set up secure communication, apply policies, set privileges, and based on those privileges grant access to specific applications. From there the user should be able to use their native collaboration applications such as email, calendar, and contacts, and be automatically configured with directory services, VPN, PKI, WiFi, and the like. Finally, this process

should also set up their access to enterprise applications. Based on their user privileges they should also be granted access to specific applications relevant to their business unit. With mature solutions, this should all happen in the background within the IT environment so that the user experience consists of simply installing an application, supplying credentials, and having access to organizational resources via their mobile device.

Additional capabilities that should be considered for enhancing the security on mobile devices include: using online tools to locate lost devices, remotely locking or even wiping a device that has been lost or stolen, and information backup and restoration. Virtualization offers other capabilities. VDI offerings from companies like Citrix, VMware, Microsoft and others can allow access to network and data resources to be limited only to the VDI client installed on the mobile device. With this type of configuration limitations regarding what can be accessed, determining whether information copying and pasting are allowed, are screenshots allowed, etc, can be enforced. With VDI deployments the security controls are configured within the datacenter, and specialized security solutions, such as protection from malware, that have been optimized for virtual environments can be utilized to ensure that the VDI framework is not only secure, but efficient, and server density—the number of VDI images installed on a single physical server—can be maximized.

For a holistic approach to security and compliance it's necessary to include mobile device controls. And it's equally important that the controls integrate with other types of solutions for data, endpoints, network, and cloud. When leveraged collectively, through a centralized management platform, security is effectively optimized.

Best Practices Considerations

- Protect the device; protect the data
- Control what networks the device accesses and what data it interacts with
- Enforce policies and privileges by associating a user with the mobile device and a unique identifier
- Embrace solutions with security and scalability as well as ease of use for end users and IT staff
- Leverage mobile device security solutions synergistically with the existing security infrastructure
- Expand the demonstration of regulatory compliance to include mobile devices

Value Drivers

The right solutions for enabling your mobile devices should provide for operational value to your organization by:

- Protecting personal and application data to help decrease legal fees and fines in the event of a lost or stolen device
- Facilitating remote locking and monitoring to help ensure compliance to corporate policies and identification of devices if “misplaced”
- Decreasing overall compliance monitoring costs because of the ability to demonstrate appropriate levels of due care and due diligence in tracking and managing devices
- Empowering employees to be more agile in terms of where and how they work and thus improve productivity and the bottom line

Related Material from the Security Connected Reference Architecture

Level II

- Securely Enabling Social Media
- Enabling the Consumerization of the Workforce

Level III

- Securing and Controlling Laptops
- Securing Virtualized Desktop Infrastructure (VDI)
- Enforcing Security on Smartphones and Tablets
- Protecting Intellectual Property in Email

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

About the Author



Brian Contos, CISSP, is director of global security strategy at McAfee. He is a recognized security expert with nearly two decades of security engineering and management experience. He is the author of several books, including *Enemy at the Water Cooler* and *Physical and Logical Security Convergence*. He has worked with government organizations and Forbes Global 2000 companies throughout North, Central, and South America, Europe, the Middle East, and Asia. He is an invited speaker at leading industry events like RSA, Interop, SANS, OWASP, and SecTor and is a writer for industry and business press such as Forbes, *New York Times*, and *The Times of London*. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

¹ <http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf>

² http://www.appleinsider.com/articles/11/07/10/idc_bumps_2011_tablet_forecast_to_53m_as_apples_ipad_2_dominates.html

³ <http://www.facebook.com/facebook>

⁴ <http://techliberation.com/2011/05/18/some-metrics-regarding-the-volume-of-online-activity/>

