



ENABLING CONSUMERIZATION OF THE WORKFORCE



According to Gigaom, one in two Americans will have a smartphone by the end of 2011¹

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.

Ninety-six percent of Generation Y (individuals born between the mid-1970s and early 2000s) use social networks, and social networking has overtaken pornography as the number one Internet activity.²

Securing Personal Devices at Work

Challenges

The division has blurred between end-user devices being supplied by corporate IT and consumer electronics that employees feel they need to conduct business. Users are finding that the laptops, tablets, and smartphones they purchase for personal use, along with their applications and integration with Web 2.0 services, are generally more powerful, capable, and all around “sexier” than what is supplied by their employers. From techies to business executives, this has resulted in explosive growth in the use of personal technology for business. At the top of the list for justifying these consumer devices is mobility.

Mobile applications are becoming increasingly customer facing. It was once big news to have customer self-service web portals accessible via a desktop or laptop computer; those are now evolving into sites optimized for mobile devices to check account statuses, receive updates, transfer funds, trade stocks, and more.

There are several business advantages to the consumerization of IT, such as enhanced productivity, lower organizational procurement costs brought upon by “bring your own PC or Mac,” and less demand on IT for endpoint support. These advantages also bring risk. The mobility of these devices introduces security management issues around access control, compliance, data protection, and so on. And 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

The challenges are rooted in two key areas: protecting how data is being manipulated and controlling network access across mobile devices, laptops and desktops, and virtualized desktops. Tasks that have been rudimentary for traditional corporate-owned end-user devices such as provisioning and revocation, are now opaque because it’s not always clear who owns the device, and further, who owns the data on that device.

“The desktop Internet ramp was just a warm-up act for what we’re seeing happen on the mobile Internet. The pace of mobile innovation is unprecedented, I think, in world history.”

—Mary Meeker
Morgan Stanley
April 2010

55 PERCENT

Fifty-five percent of companies believe employees accidentally brought in malware or were involved in careless data loss.



Solutions

Solutions for enabling the consumerization should encompass and connect controls for mobile devices, laptops and desktops, and virtualized desktops.

Mobile devices require scalable solutions that help IT secure and manage the entire device and the data. IT needs a centralized way to enable easy, self-service provisioning to include access mechanisms like VPN and Wi-Fi, to set and enforce policies independent of the ever-growing endpoint types, and to do so in a way that is persistent and can't be undone by users through careless or intentional acts. There also has to be accountability for the employee device. During the initial authentication process, when accessing the corporate network, each device needs a unique ID that is associated with a particular user, and, as such, that user's groups, roles, and permissions. With these dots connected to determine appropriate network access and access to enterprise and line-of-business applications, risk can be mitigated.

Other important features for securing mobile devices include allowing IT to perform full or partial data wipes. Partial wipes are critical for employee-owned devices where only corporate data should be removed, thus preserving photos, music, applications, and other non-corporate resources. Remotely tracking the phone's location, locking it, and performing backups and restoration are also important mobile device security capabilities.

Mac and PC laptops and desktops should be controlled by leveraging network access control (NAC) or NAC with multiple zones based on access criteria. For example, a visitor with an unmanaged device may get Internet access via an untrusted guest network but no internal access—much like Internet access from a coffee shop or hotel. Old antivirus .DATs or unpatched operating systems may still get a device on the trusted network

based on how policies were set but deny access to sensitive business assets. Only when a system can be fully evaluated to ensure that it complies with organizational policies will it receive the greatest access. Even in this case, that access will remain limited based on the user's identity and role. Thus, regardless of the device, access can be managed.

Virtualized desktops are a common mechanism for mitigating risks surrounding the consumerization of IT. A virtualized image can be installed atop a smartphone, tablet, laptop, or other mobile device. A user leveraging a virtualized image can interact with the corporate network and sensitive data based on policies and permissions that might limit the ability to download data, take screen captures, and access certain applications. While it's a powerful control, the virtualization promise of any device anywhere has historically been limited by traditional security controls. For example, installing antivirus on every virtualized image is a network, system, and virtualized image density drain. Virtualized images should be used in conjunction with specialized security solutions designed to optimize virtualized environments and maximize virtualized image density without sacrificing security.

The consumerization of IT is rapidly being embraced. Saying "no" won't scale, and it could lead to missed business opportunities. By focusing on mobile devices, laptops and desktops, and virtualized desktops, it is possible to mount an effective risk mitigation strategy built atop mobile device management, NAC, and security for virtualized images that also yields operational efficiencies. Users need easy and secure solutions. IT needs centralized, scalable, and integrated solutions that address security and compliance across networks, endpoints, and data security controls.

Best Practices Considerations

- Accept that consumer devices will be brought in by users and provided by IT
- Deploy solutions that maintain the consumer IT experience without degrading organizational security
- Implement accountability by associating devices with users and as such their permissions and roles
- Take advantage of NAC to enforce access policies
- Use the virtualized desktop infrastructure for greater security together with specialized security controls optimized for virtualization
- Centralize controls for network and data with endpoint controls for smartphones, tablets, laptops, and other devices

According to CIO Magazine's Enterprise Desktop Alliance survey, two out of every three companies are buying Macs, and this is introducing integration challenges for IT administrators.³

Consumerization will force more IT change over the next 10 years than any other trend.
(Source: Gartner 2009)

Value Drivers

The value points are similar to those for social media—with a few key differences.

- Operationally, organizations have to work more progressively. New ways of provisioning application access could bring efficiency to the organization, and additional efforts for network segmentation and management could help reduce operational impacts (bandwidth, control requirements) in other areas.
- Security concerns are overcome with access reviews, better social media policies, and traditional network firewalling and URL filtering
- Direct cost savings will be seen over time with capital expenditure reduction of hardware and freedom (from the help desk side) from managing non-strategic assets
- Indirectly, the IT staff could be more focused on high-value, high ROI projects; the workplace may be more attractive to new hires, and one could argue that employees will be more productive (from work and from home). As you get buy-in from legal, HR, and IT to take on this type of effort, the focus on data loss prevention (DLP) and review of contingency plans for rapid application and access control should make the organization more aware and responsive in the event of a data issue (for example, a lost device).

Related Material from the Security Connected Reference Architecture

Level II

- Securing Mobile Devices
- Protecting the Data Center
- Securely Enabling Social Media

Level III

- Enabling Bring Your Own PC (BYOPC)
- Securing Virtualized Desktop Infrastructure (VDI)
- Enforcing Compliance on Smartphones and Tablets
- Enforcing Endpoint Compliance

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://gigaom.com/2010/03/26/1-in-2-americans-will-have-a-smartphone-by-christmas-2011/>

² <http://www.informationweek.com/news/197006474>

³ http://www.cio.com/article/552263/More_Macs_in_the_Enterprise_Survey_Says

