White Paper

A Business-Driven Approach to Mobile Enterprise Security

By Jon Oltsik, Senior Principal Analyst

May 2012

This ESG White Paper was commissioned by Juniper Networks and is distributed under license from ESG.

Contents

Executive Summary

IT consumerization and the massive influx of mobile devices is affecting many large organizations. CEOs want immediate network access on Monday after buying the latest iPad version over the weekend. Young employees think nothing of using work PCs for updating their Facebook status or using Dropbox to move documents to their home computers. Sales managers are demanding that the global sales force be provided with access to cloud-based CRM applications on their smart phones so they can access and update records from the road.

How should enterprises handle IT consumerization? While some Chief Information Security Officers (CISOs) would prefer to simply prohibit and block these activities, industry research indicates that only about one-third of organizations take this type of extreme position. Why? Because mobile devices and cloud services may lead to new types of business process productivity gains and even revenue opportunities. Before organizations implement Bring Your Own Device (BYOD) policies or let employees access social networking sites from the corporate network, however, they must prepare the business and IT infrastructure to support these decisions, enable operational benefits, and address added risk.

This white paper concludes:

- **The mobile enterprise is a cooperative venture.** Few companies have the right oversight or security controls in place to handle a multitude of new security policies and enforcement rules for the mobile enterprise. Business, IT, and security managers must think in granular terms: Who needs access to cloud-based applications and services and how to integrate that with single sign-on enablement? Which users in which roles should be allowed to use mobile devices to access the network and which applications should they be allowed to access? What should and shouldn't these users be allowed to do? What device types and OS versions should be allowed? How will managers measure mobile enterprise activities to gauge their success? Should a security policy do double duty, by not only customizing access to the user's role, location, and type of device….but also adjusting policy dynamically when needed, to isolate users under attack and prevent the attack from spreading? To get ahead of the mobile enterprise, smart business, IT, and security managers will take the time to answer these questions.
- **Existing security controls are no match for mobile enterprise demands.** Answers to the questions posed above turn into security policies and these policies need to be monitored and enforced. Unfortunately, today's assortment of tactical security tools and network access controls aren't designed for mobile enterprise security requirements like central policy management, coordinated distributed enforcement, or end-to-end monitoring.
- **Large organizations need a tailored mobile enterprise strategy.** The mobile enterprise changes a number of requirements for campus networks, including network access controls, security controls, and monitoring/reporting. What's needed here is a new type of integrated network/security architecture built specifically for central command-and-control, distributed security enforcement, comprehensive monitoring capabilities, and real-time automation to support critical business processes or block attacks in progress. Businesses need to consider the scale and resiliency of the network as a core requirement, since the mobile enterprise is moving to enable business-critical functions on mobile devices.

Just What Is The Mobile Enterprise?

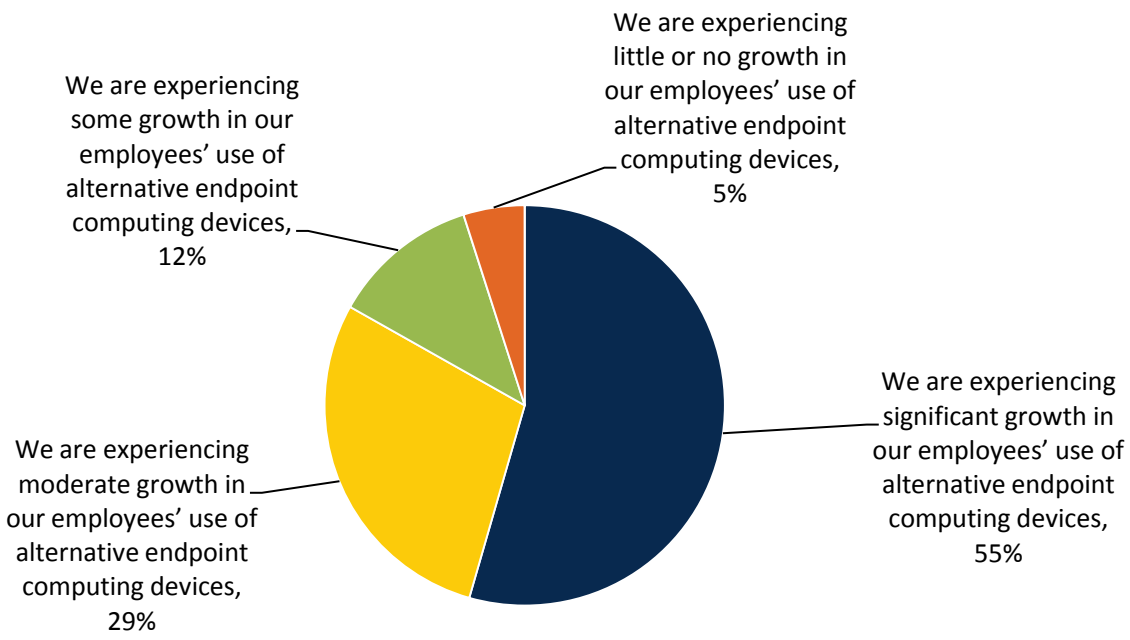
In ancient times (i.e., 10 to 15 years ago), corporate IT was tightly controlled. User devices were typically limited to Windows PCs. Business applications were controlled by IT and either run locally on endpoints or on physical servers in data centers. Network security was based upon clearly defined perimeters that separated trusted internal networks from the untrusted Internet.

Fast forward to today and you'll see massive changes in each of these assumptions. Now, corporate networks must accommodate:

- **A growing array of new devices.** According to ESG research, 55% of enterprise organizations are experiencing significant growth in employee use of alternative endpoint computing devices like Apple Macintosh PCs, tablet PCs, and smartphones (see Figure 1)[1]. In many cases, employees are allowed to use a combination of endpoint devices as part of their day-to-day activities.

Figure 1. Organizations are Experiencing Growing Use of Alternative Endpoint Devices

Which of the following statements best describes the changes your organization is experiencing with respect to alternative endpoint computing devices? (Percent of respondents, N=221)



Source: Enterprise Strategy Group, 2012.

- **Cloud-based applications.** Applications no longer run solely on physical servers in corporate data centers. Quite the opposite, applications can run anywhere—on traditional physical servers, mobile virtual servers, or in the cloud as Infrastructure as a Service (IAAS), Platform as a Service (PaaS), or Software as a Service (SaaS). As if this wasn't enough, end-users can now take advantage of a wide variety of cloud-based applications and IT services for personal and professional use. Facebook can be used for an employee's personal profiles or as a component of a corporate marketing campaign. Employees depend upon Skype to speak with friends abroad or for legitimate business video conferencing. Dropbox can be used to distribute documents between corporate and personal devices for mobility and user productivity.
- **De-perimeterization.** Given new device proliferation, application mobility, and cloud-based consumer and corporate services, the notion of a static network perimeter is all but gone. Now there are a multitude of network perimeters around devices, applications, users, and data. These perimeters have also become quite dynamic as they must adapt to various environmental conditions such as user role, device type, server virtualization mobility, network location, and time-of-day.

All of these factors have transformed traditional enterprise IT into a new model called the mobile enterprise. To be clear, however, the ramifications associated with mobile enterprises aren't limited to internal issues like BYOD, iPads, and cloud computing for employees. Rather, the mobile enterprise must also address external business

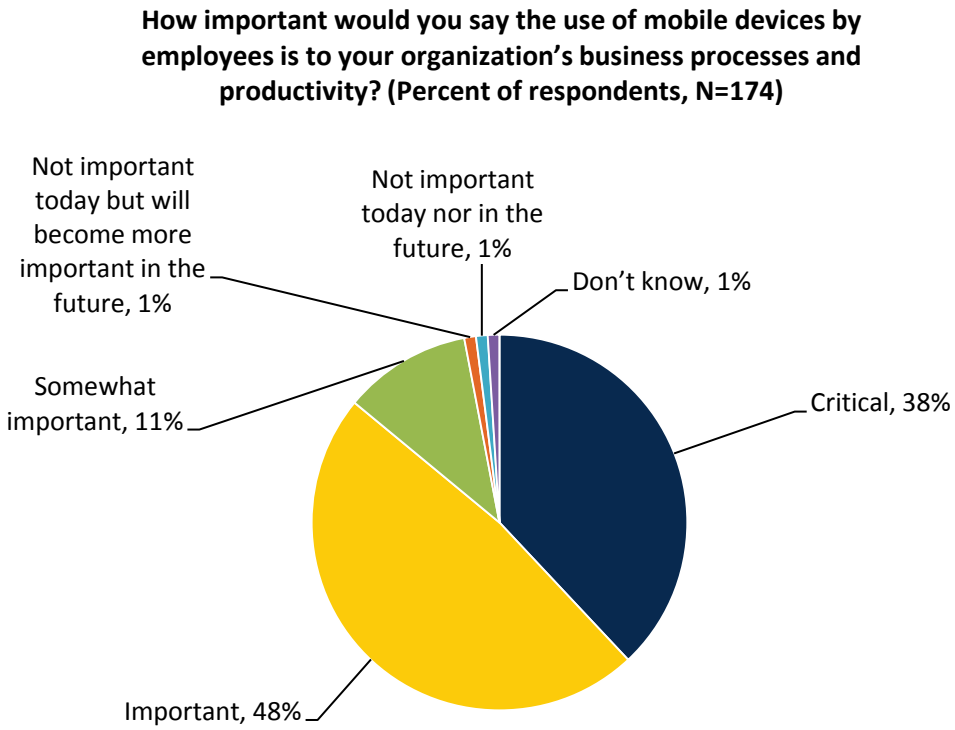
[1] Source: ESG Research Brief, *Corporate Endpoint Device Type Trends*, May 2011.

realities like providing guests, third-party contractors, and business partners network access using various devices from a multitude of locations. To accomplish this, the mobile enterprise must be flexible, adaptable, resilient, scalable, and always on.

Mobile Enterprise Momentum Is Driven by Business Needs

The mobile enterprise transition has another unique aspect. In the past, business managers were fairly impartial to IT technology and infrastructure decisions but this is no longer the case. Forward-thinking technology executives were at the forefront of pushing IT to provide network access for iPhones when they first appeared in 2007. The same thing happened with the iPad introduction in 2010. CEOs are not alone. HR managers champion mobile device support to CIOs as a means to recruit techno-savvy employees. Sales executives want to provide CRM access to the sales team from any location and any device. This business-centric push is on the rise. According to *Datamation*, iPads had penetrated 50% of Fortune 100 companies within 90 days of its first release. Previously conducted ESG research indicates that, far from technology toys, most organizations consider mobile devices either critical or very important for their business processes and overall productivity (see Figure 2)[2].

Figure 2. Mobile Devices are Considered Critical or Important for Business Processes and Productivity



Source: Enterprise Strategy Group, 2012.

The Mobile Enterprise Presents Numerous IT Security Challenges

Given the business value of greater connectivity, productivity, and application flexibility, the mobile enterprise has become an unstoppable force. Unfortunately however, the existing IT infrastructure was designed and built for a more genteel style of business computing. This is leading to a growing gap between mobile enterprise requirements and corporate IT capabilities as a whole but the discontinuity is most acute with regard to IT security. Mobile enterprises present unique security challenges because:

[2] Source: ESG Research Brief, *Mobile Device Security: It's All About the Data*, April 2010.

- **Mobile device security is a work-in-progress.** Large organizations have been battling endpoint security issues for years—antivirus signature distribution, vulnerability scanning, patch management, etc. As bad as this situation is already, mobile device security makes current PC protection seem like child's play. Why? These devices come in many flavors so IT and security teams must learn the platform, software, and security idiosyncrasies of multiple systems. Consumer-focused mobile device applications are notoriously insecure and known to perform blatant security policy violations like harvesting user contacts for vendor marketing campaigns. Mobile devices are often lost or stolen, in some cases while containing sensitive or regulated data. Finally, mobile device malware is on the rise, especially for the open source Android operating system. Enterprises are quickly learning that managing and securing these devices is bound to test their existing IT capabilities.
- **Network access isn't black and white.** Obviously, mobile devices are portable which means they can access the network from any WiFi access point or insecure Internet hotspot. Yes, this may bolster convenience and productivity but it can also violate corporate governance or regulatory compliance policies. Security best practices suggest a granular approach, where mobile device network access policies are enforced according to who wants access, the type of device they are using, where they are located, and what they want to do. In other words, network access privileges for mobile devices are based on a set of decision criteria. This type of access control structure should be consistent and able to support, for instance, employees with mobile devices or contractors using PCs from the corporate network. While granular and contextual access controls can support business and security requirements, many existing network and security point tools lack the integration or network coverage to provide this type of tailored security policy enforcement across the enterprise.
- **Web-based applications open new threat vectors.** As described above, business applications have also become highly mobile with the proliferation of cloud-based applications. Combined with laptops, tablets, and smartphones, however, cloud-based applications represent a potentially toxic security mix. New endpoint applications can open easily exploitable system vulnerabilities. Social networking sites like Facebook can act as malware distribution vectors. Online file sharing programs like Dropbox could easily become vehicles for accidental or malicious data leakage. Since most organizations are unwilling to block all cloud-based application traffic, CISOs are forced to try to monitor and manage cloud-based application activities without alienating employees or violating corporate security policies. Given the limitations of existing network and security controls, this is extremely difficult to do.
- **Security credential provisioning.** Mobile devices are notoriously hard to handle with regard to the credential provisioning to truly enable secure connections on the wireless network. Some verticals such as education and hospitality prefer a non-intrusive clientless approach to credential provisioning while the enterprise lends itself to a managed security provisioning approach.

These challenges are not trivial IT details as they represent a potential increase in risk to the business. Mobile enterprise benefits must be aligned with proper management and security or it is fairly easy to lose visibility and control of valuable IT assets and sensitive data. Lacking the right network infrastructure and security controls, CIOs and CISOs face a losing battle here.

A Business-Driven Approach to Mobile Enterprise Security

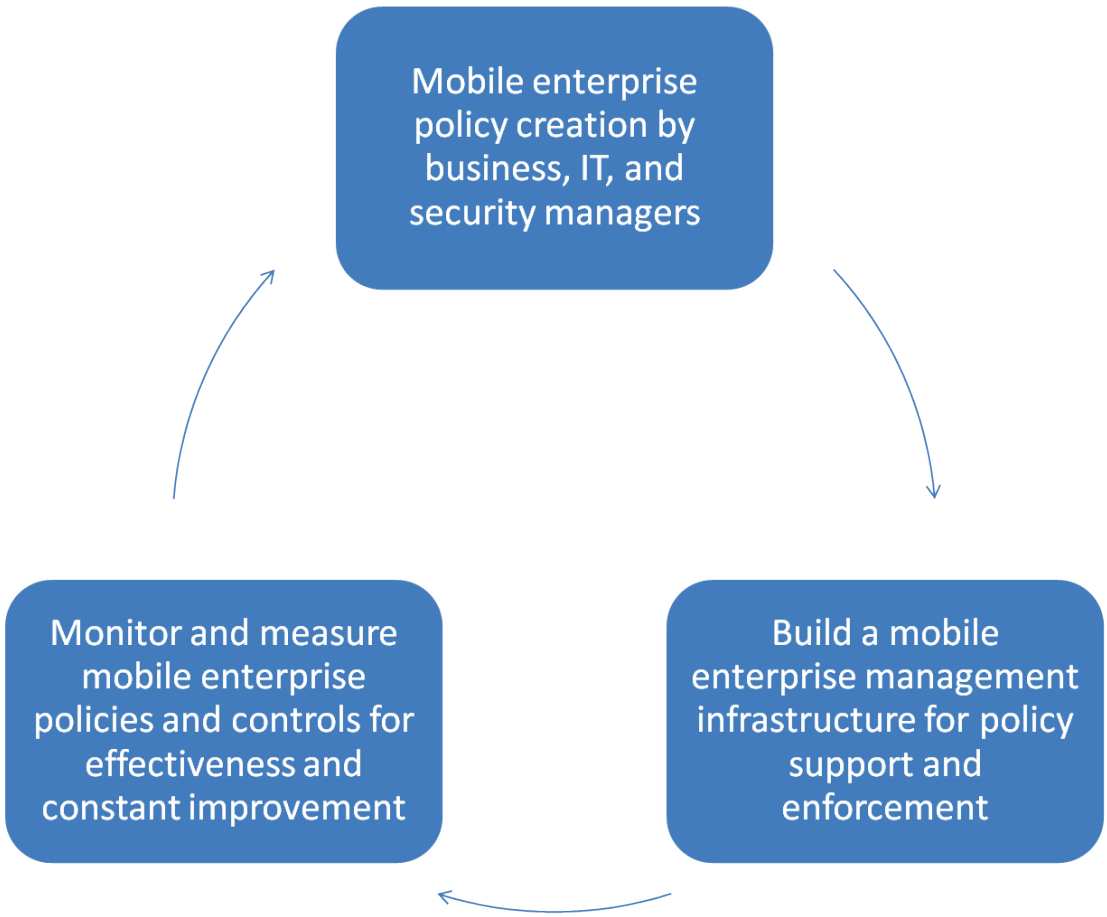
Large organizations must make policy changes and security technology investments to adequately manage and monitor new risks posed by the mobile enterprise. That said, ESG sees too many firms addressing mobile enterprise security issues haphazardly by implementing standalone security policies, investing in tactical security controls, or relying on incomplete monitoring. This may be reactionary. CISOs feel like they need to do something, but incomplete measures provide marginal results, leaving organizations exposed.

ESG recommends a more strategic, comprehensive, and business-driven approach to mobile enterprise security composed of three related activities:

1. Create mobile enterprise security policies as a collaborative effort between business and IT.
2. Build the right network, security, and management infrastructure for the mobile enterprise policy support and enforcement.
3. Monitor and measure mobile enterprise security for IT audits, policy and controls effectiveness, and constant improvement

These three processes complement each other, creating a mobile enterprise security lifecycle that can be modified as business, IT, and security requirements change (see Figure 3).

Figure 3. Cooperative Cycle for Mobile Enterprise Policy Creation, Management, and Security



Source: Enterprise Strategy Group, 2012.

Mobile Enterprise Policy Creation

ESG sees several common mistakes with current policy implementations in the marketplace. First, security managers often create policies without input from their business peers. This tends to lead to guidelines that are either overly liberal, adding risk, or excessively draconian, which disaffects users. It is imperative for organizations to bridge this gap by crafting mobile enterprise security policies as a collaborative effort between business, IT, and security. Business managers should come prepared with a list of objectives in terms of desired user behavior and success metrics while IT and security executives should be equipped to point out risks and any technical limitations. Both groups should also fully understand and adhere to the organization's governance statutes and compliance obligations.

Detail-orientation is very important with regard to all security policies, so it behooves business and IT executives to do their homework and craft mobile enterprise policies that include:

- **Device and configuration support.** BYOD cannot become an "open door" to any device from any user. Business managers should be ready to make a case for popular consumer devices like Macintosh PCs, iPhones/iPads, and Androids, and clearly propose why supporting these devices could benefit the business. Some firms may also need support for Blackberries and Windows Mobile, but since support equates to investment, each device type must have a clear and measurable business justification.

  Once devices are selected, it is important to define what "support" means. As part of security best practices, IT managers should be able to inspect each device before allowing network access. IT will want to establish configuration guidelines for operating systems and applications. For example, "rooted" or "jail-broken" devices are not permitted on the network, and mobile devices cannot store corporate contacts on local storage. As part of configuration management, IT should ensure that all devices are PIN protected with a 4-digit password as a minimum standard and those passwords are changed at least 4 times per year. IT will also likely want to install management and/or security software such as digital certificates, VPN clients, anti-malware protection, and remote wiping capabilities on each device in case they are lost or stolen. In verticals that don't lend themselves to installing IT-managed software on the mobile device, a clientless self provisioning approach to device on-boarding should be offered. Business managers will want to get a commitment from IT, defining what type of support users can expect when they call the help desk or show up in the IT lab with a brand new iPhone S5 smartphone.

- **User access privileges and restrictions.** This is the true nexus between the business, IT, and security, so it needs careful attention. The fundamental question to answer here is: Which mobile enterprise services do users need and through which type of devices do they need to access them? These questions seem straightforward but are often difficult to answer in practice because they really require a thorough review of job descriptions and business processes. Some of these appraisals are easy—remote salespeople can be more productive if they can access Salesforce using smartphones, while iPad access to health care records makes sense for physicians visiting patients at hospitals. Others aren't as clear cut: Should all or just some employees have access to social networking sites? Are there social networking functions like gaming or video upload that should be blocked in all cases? What about device type and network location—should access decisions be based upon considerations like these? Where should corporate governance or regulatory compliance concerns dictate mobile enterprise policies?

  To work through this complex series of decisions, ESG recommends a matrix approach that aligns organizational groups (or subgroups) with mobile enterprise activities in order to craft specific policies and provide the IT security team with an enforcement template (see Table 1).

Table 1. Sample Matrix for Mobile Enterprise Policies

Organization	Group/Role	Endpoint Device	Location	Activity	Permit/Deny/Limit
Marketing	Marketing Communications	PC, tablet, smartphone	Corporate network	Access Facebook	Permit access; block gaming, video upload, and content posting; monitor activity
HR	Recruiter	PC, tablet, smartphone	Corporate network, public network	Access LinkedIn	Permit access; block posting; monitor activity
Finance	Accounting	PC, tablet, smartphone	Corporate network, public network	Access general ledger	Permit on all devices from corporate network; monitor activity; deny access from public network

Mobile enterprise policies should be thoroughly vetted by business and IT stakeholders before execution. Once completed, employees should be required to read and sign off on the policy (along with their managers) before submitting their devices to IT and gaining network access. After this step is completed, it is incumbent upon IT to provide employees with the self-service tools they need for network access and policy enforcement henceforth.

Finally, it is important to recognize the sweeping impact mobile devices have on network access. Given their mobility, laptops, tablets, and smartphone policy enforcement is subject to constant change. A legitimate network session may be terminated suddenly when security tools detect the presence of unknown network protocols. A CEO's laptop that worked fine at the office may be blocked from network access due to a software vulnerability alert that took place during her commute home. As a result of these dynamic conditions, it is crucial that business, IT, and security leaders thoroughly assess the risks, craft policies to address these risks, and build the right controls and metrics to gauge policy and controls effectiveness.

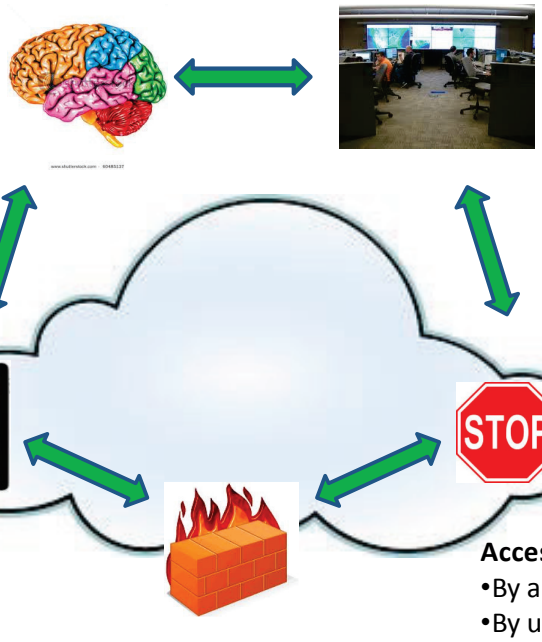
Mobile Enterprise Management, Network, and Security Infrastructure

Once again, many organizations approach mobile enterprise security in a piecemeal fashion by implementing tactical controls arbitrarily in response to their most pressing issues. This leads to "islands of security" rather than enterprise coverage.

ESG believes it is worthwhile to create a more strategic plan that encompasses the entire network and security infrastructure. This strategy should include a comprehensive networking and security architecture designed specifically for the mobile enterprise (see Figure 4).

Figure 4. Mobile Enterprise Architecture

Central command-and-control
- Policy management
- Configuration management
- Monitoring/reporting



Security Intelligence
- Situational awareness
- Threat management
- Log management
- Automated response

On-boarding and Device management
- VPN
- Auto-provision access policies
- Remote device management
- Remote device security
- Remote wipe, backup, and restore

Access Controls
- By application
- By user, role, device and location
- Authentication
- Device inspection
- Wired/wireless
- Local and remote access

Source: Enterprise Strategy Group, 2012.

This architecture includes:

- **Central command and control.** Network configuration and security controls must "report" to an authoritative central command and control for all management functions. This includes policy management, configuration management, and all reporting. The word "central" is somewhat relative here as some organizations will want to delegate oversight to business units or departments. Of course, this type of entrustment is fine but the architecture should support a management hierarchy where lines of business have authority over their domains while "C-level" executives retain oversight over the entire enterprise.
- **End-to-end security controls.** There are three goals here: 1) Layered defense, 2) Distributed policy enforcement, and 3) Comprehensive visibility. As such, security controls must be present throughout the enterprise: on endpoint devices, at the network access layer, in the network core, and even in the cloud. These controls are far from static security signatures and filtering rules. Rather, they provide the muscle for granular and flexible mobile device security enforcement like access policy, device configuration policy, and application controls. Furthermore, enforcement controls should also take on the role of network sentry, monitoring and reporting activities to central command and control in order to fine-tune risk management strategies, detect security events, and respond to attacks as soon as possible to minimize damages.
- **Automation.** Mobile enterprise security must be designed to respond to real-time detection and remediation. This means that central management and distributed controls must be instrumented for security automation. When a new vulnerability is discovered, mobile enterprise security controls should be able to assess which assets are vulnerable, monitor these systems for anomalous or suspicious behavior, and create "virtual patching" enforcement rules as soon as possible. Furthermore, each component has local and systemic responsibilities. Endpoint security software can protect mobile devices from a malware attack and then communicate details of the attack to cloud resources to generate new rules to safeguard all other devices. Application controls can open the network to social networking traffic but block suspicious executables upon network ingress and then pass new rules to firewalls and IPSs. In this way, network defenses are fine-tuned constantly to protect each individual user and all of IT.

In the mobile enterprise, historical organizational and technology boundaries between wired, wireless, and remote network access disappear. This demands common management of wired and wireless network infrastructure and wide-ranging security integration. This will not only require a mobile enterprise-friendly campus network but also new network and security skills within the IT organization.

Mobile Enterprise Security Monitoring

As the old business saying goes, "you can't manage what you can't measure." Since the mobile enterprise is relatively new and includes a multitude of technology elements, it is essential that security policies and controls be observed and reviewed constantly to assess their effectiveness. This will require a contextual view of all endpoint, user, device, network and application activities. This seems logical but many monitoring tools are anchored in the technology realm of IP addresses, MAC addresses, and network protocols. By taking this information to a more user-friendly level, mobile enterprise monitoring can help in a multitude of ways. Security analysts can isolate suspicious traffic to specific users and initiate investigations, looking for behavioral patterns that may indicate a malicious insider attack. Network managers can study traffic patterns of individual groups to improve performance and SLAs. Business managers can review employee mobile device use to improve business processes.

Mobile enterprise monitoring is anchored by information collection and sharing amongst all security enforcement points as well as tight integration with SIEM systems. Armed with a contextual view, SIEM can provide added value for analyzing behavior by user, location, device-type, application, or traffic patterns.

The Juniper Networks Mobile Enterprise Strategy

Mobile enterprises demand network and security designed for scale, resilience, intelligence, integration, and enterprise-wide coverage. Juniper Networks is one of the few vendors with the combination of experience,

architecture, and products to address these new requirements. Best known for high-performance in the network core, Juniper has introduced networking and security products, acquired new technologies, and gained tremendous enterprise experience over the past few years. Juniper can now combine these individual products to form a comprehensive mobile enterprise architecture that includes:

- **Scalable and resilient wireless LAN and wired network**. Juniper Networks offer a wireless LAN (WLAN) solution that can profile the device types and apply device-type-aware policy. The wireless LAN solution is designed for resilience and scale to meet the mission-critical needs of a growing mobile enterprise.

  The Juniper EX Series switching product family addresses the access, aggregation, and core layer switching requirements of micro branch, branch office, campus, and data center environments, providing a foundation for the fast, secure, and reliable delivery of applications that support strategic business processes in a mobile enterprise**.** The manageability and resiliency of the Juniper EX Virtual Chassis technology, which allows multiple interconnected EX Series switches to operate as a single, logical device, is an important element of a mobile enterprise.

- **Simplified user on-boarding**. One of the fundamental challenges of a mobile enterprise is the ability for IT to scale, by letting users self provision and on-board their mobile devices to the wireless network. Juniper's SmartPass Guest management application and Junos Pulse solution, including secure remote access and on-device mobile security, enable user self provisioning on to guest and secure networks.

- **Mobile device management and security.** When Juniper Networks acquired mobile device security and management vendor SMobile in 2009, it greatly expanded its footprint in the mobile enterprise. Juniper now combines this endpoint security, mobile device management software with a VPN and wireless config provisioning client, as part of its Junos Pulse solution for secure connectivity, network acceleration, and on-device mobile security and management**.**

- **An integrated network access control layer**. Juniper offers a number of other technologies to enforce granular network access policies for the LAN. For example, Juniper's Junos Pulse Access Control Service on MAG Series solutions or the IC Series Unified Access Control (UAC) appliance can authenticate wired and wireless devices using standard technologies like RADIUS, 802.1X, or MACauth. By integrating with Active Directory or other LDAP repositories, UAC can also push role-based ACLs to wireless LAN controller, EX Series Ethernet switches and SRX Series firewalls to enforce access policies for mobile devices and users whether they reside on campus or connect through public networks via VPN. Juniper's Junos Pulse Secure Access and Access Control services also support single sign-on based on SAML, further extending the access security to the cloud for the Mobile Enterprise. Finally, Juniper SRX Series secure services gateways offers application controls to block or limit access to social networking sites like Facebook or online services like Dropbox.

- **Central management.** Juniper mobile enterprise command-and-control comes together through its JUNOS Space and Ringmaster network management platforms. This is where business, IT, and security teams can create and deploy global network and security policies for enforcement across the enterprise.

- **Security intelligence.** In a Juniper-based network, security monitoring and reporting takes place in its Security Threat Response Manager (STRM) product. STRM collects log and flow data for network security and provides more granular knowledge of user/device identity and applications. STRM is designed to detect suspicious behavior and security incidents and is integrated with other Juniper products like the SRX Series and IDP for automated security remediation.

Juniper has also embraced the Interface for Metadata Access Points (IF-MAP) standard from the Trusted Computing Group (TCG). IF-MAP servers act as a database repository for security information and objects. While somewhat esoteric, ESG believes IF-MAP can be extremely helpful for providing granular data objects that can enhance security monitoring, analysis, and forensic investigations for mobile enterprises. Juniper's implementation of IF-MAP for wireless LAN users helps tie the mobile device user policy with unified policy enforcement from Junos Pulse Access Control/UAC service.

Finally, the Juniper mobile enterprise architecture can be deployed as a layered solution over time. For example, large organizations can start with Junos Pulse for mobile device security, UAC for network access policy enforcement, and wireless LAN, switching, or SRX Series for policy enforcement. This can help enterprises protect their existing investments as they transform static campus networks into a mobile enterprise architecture.

The Bigger Truth

It's time that business managers, CIOs, and CISOs move beyond hyperbolic terminology like mobility, social networking, and BYOD to truly understand how these consumer technologies impact their businesses. There is little doubt that this will happen in most cases. Smart companies will get ahead of these technologies to assess where they create opportunities and where they increase risk.

It is important to start with a thorough assessment of business goals. In other words, what are the objectives for providing users (i.e., employees, contractors, business partners, etc.) with mobile enterprise technologies like mobile devices and cloud-based services and how will success be measured? By performing this analysis up front, managers can then transpose business enablement into granular policies for network access, application controls, and security protection.

For IT professionals, the mobile enterprise is the next step in a progression that started years ago with the introduction of laptop PCs, enterprise wireless access points (APs), and mobile storage devices. There are important distinctions however. The growing use of consumer technologies and cloud-based services makes mobile enterprise policy management and enforcement more granular and complex— few organizations are simply willing to ban the use of iPads or block all employees from Facebook. As soon as these technologies are accepted, decisions on who can use which technology at what time and for what purpose become more difficult to create and enforce.

Ultimately, large organizations need to think of the mobile enterprise as a new model and act accordingly. This is already happening in some industries. For example, hospitals use wireless technology and RFID tags to locate mobile equipment and roaming physicians while private health care practices are eschewing in-house servers and applications for cloud-based alternatives. At a high-level, mobile enterprise guidelines are fairly simple: create and enforce policies to enable productive behavior and minimize risk. At the same time, constantly monitor activities to measure success. Finally, use technology to automate fixes when possible.

While some vendors will take time to adjust to mobile enterprise requirements, Juniper Networks has already developed a comprehensive architecture that enables automated granular policy creation and enforcement spanning from mobile wired/wireless endpoints to the network core. As such, large organizations would be well served to evaluate Juniper Networks as they develop mobile enterprise strategies.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com