FOR: Security & Risk Professionals

Prepare For Anywhere, Anytime, Any-Device Engagement With A Stateless Mobile Architecture

by Chenxi Wang, Ph.D., June 29, 2012

KEY TAKEAWAYS

Prepare For The Future With A Stateless Mobile Architecture

To deliver enterprise mobility successfully, security and operations professionals should adopt a stateless mobile security and operations architecture that delivers simplicity, modularity, and portability.

A Stateless Mobile Architecture Supports Simplicity, Modularity, And Portability

Fundamental principles of a stateless mobile architecture include decoupling protection from the infrastructure, always deriving trust dynamically, and avoiding costly new investment of in-house applications and infrastructure.

Follow Four Steps To Build A Stateless Mobile Architecture

For anywhere, anytime, any-device mobile engagement, implementing a stateless architecture calls for building protection in the application layer, moving from device management to risk-based device inspection, performing real-time threat detection and mitigation, and leveraging cloud technologies.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

Prepare For Anywhere, Anytime, Any-Device Engagement With A Stateless Mobile Architecture

Future Look: The Mobile Security And Operations Playbook

by Chenxi Wang, Ph.D.
with Christopher Voce, Ted Schadler, Stephanie Balaouras, and Eric Chi

WHY READ THIS REPORT

This report outlines Forrester's future look for mobile security and operations. We designed this report to help security and risk (S&R) and infrastructure and operations (I&O) executives understand and navigate the major business and IT trends that will affect the development of a future-proof mobile support strategy. Mobility holds the promise of fostering new innovations, reaching new audiences, and most importantly, creating never-before-seen user experiences and business opportunities. To stay ahead of constantly evolving mobile business requirements, S&R and I&O pros can't rely on the old approach of end-to-end control over the data path, device, and applications. Instead, they must embrace a "stateless" architecture where IT decouples security controls from the devices and the infrastructure, derives trust dynamically, and avoids costly new investment of in-house applications and infrastructure. A stateless architecture will engender big changes in IT operations and expectations of control, but the end result will be a coherent strategy that allows IT to provision services to any device dynamically but with the controls needed to operate safely and in compliance. In this report, we will outline four steps that S&R and I&O pros must follow to build a stateless architecture and to prepare for a future that supports anywhere, anytime, any-device engagement.

Table Of Contents

Notes & Resources

To develop this report, Forrester drew from a wealth of analyst experience, insight, and discussions with end users. We also interviewed Accellion, Arxan Technologies, EMC, NVidia, Taptera, WatchDox, and several end user organizations.

Related Research Documents

Address Complexity With Mobile Security And Operations
May 21, 2012

Define A Road Map For Mobile Security And Operations
May 16, 2012

MOBILE DEMANDS UPEND ENTRENCHED MODELS OF IT SECURITY AND OPS

According to Forrester surveys, 91% of US consumers and 86% of European consumers have at least one connected device.[1] It's therefore not surprising that over a three-year period starting in 2007, mobile carriers such as AT&T saw wireless data traffic on their network increase by 5,000%. Mobility promises fresh delivery channels, more user-friendly services, and more importantly, a fundamentally new way of doing business. Consumer-facing organizations race to embrace mobile apps to meet customer expectations and to foster new business opportunities. At the same time, business users demand that internal IT deliver mobile-enabled functions for anytime, anywhere, any-device access to information. All of this creates a new reality for both S&R professionals and I&O professionals charged with securing and managing enterprise technology. Consider that:

- **Mobile apps and devices are exploding in popularity.** Forrester predicts that by 2015 one in every three US adults will own a tablet, a statistic that is both astounding in its number and in its implications.[2] This means that the number of knowledge workers in your organization as well as consumers demanding mobile-enabled services is growing by leaps and bounds — rapidly turning mobile support from a "nice-to-have" to a "must-have" investment.

- **Unmanaged devices are a fact of life.** Gone are the days when IT can demand to manage devices on the corporate network and rely on being heard. According to our surveys, nearly 60% of companies say that they support a bring-your-own-device (BYOD) program in some fashion.[3] Even if you don't have a BYOD initiative today, your knowledge workers will increasingly expect mobile-friendly content and services. Most enterprises must eventually learn to incorporate unmanaged user devices as part of their ongoing business strategy. In fact, Forrester believes that distinguishing between managed and unmanaged devices will only serve short-term purposes — a more prudent and future-proof practice is to treat everything as though it is unmanaged and thereby eliminate design vulnerabilities due to unsound trust assumptions.[4]

- **Mobile workers flock to cloud or cloud-connected apps.** Cloud is now an established enterprise technology.[5] Mobile workers who demand anywhere, anytime access have helped to fuel its popularity. The rapid rise of cloud collaboration technologies with a mobile front end such as Dropbox, Box, and Chatter is a strong testament to how today's workforce favors no-fuss technologies that deliver instant results. The combination of mobile and cloud is a rich ground for innovation for enterprise technologies.

- **Mobility will drive never-before-seen customer engagement models.** An example is augmented reality (AR), a new form of technology that helps users extract personal and relevant information from a visual display of reality.[6] The Commonwealth Bank of Australia incorporated AR in its mobile app to deliver pertinent real estate information directly to users.[7] Interested buyers of a property can hold up the phone to a house and the app will show the sales price and other relevant information about the property. The user can also pan to the left or right of the house and the app will show the sales prices of the neighboring properties centered on the phone. These types of customer engagement models will require S&R and I&O pros to develop advanced mobile security and operations capabilities well beyond their comfort zone.

Current IT Security And Ops Strategies Are Ill-Suited For The Extended Enterprise

These trends, along with other, broader IT consumerization initiatives, give rise to what Forrester refers to as the "extended enterprise," where the enterprise routinely leverages innovations happening outside the confines of the company to accomplish core business tasks.[8] In the setting of an extended enterprise, you must still control access to critical resources, but now you must do it regardless of: 1) the device that initiates the access; 2) the network the data must traverse; and 3) the server that stores the resources. This is a fundamentally new requirement that challenges existing assumptions and entrenched operational models for enterprise IT. Unfortunately, today's IT operational model is the product of decades of efforts to close off the enterprise environment from the external world. This model breaks down when you begin to incorporate mobile delivery requirements. Why? Because IT professionals:

- **Designed models and processes based on the assumption of managed endpoints . . .** The assumption that IT knows of and completely manages all endpoints is deeply entrenched in many aspects of enterprise IT. For example, with a few clicks, an admin can change the configuration settings on a user laptop or desktop to enforce an enterprise policy such as how often the endpoint receives antivirus updates. IT has built enterprise security models on the belief that uniform controls are available at the device level and that therefore there is no need to enforce security at the application or the data layer. When you extend such applications to a mobile environment with untrusted and unmanaged devices, you lose the safety net of infrastructure-level protection, and the security posture breaks down.

- **. . . as well as a managed network.** Both S&R and I&O pros are accustomed to having complete control over the enterprise network — they can set firewall rules, zone the network, and monitor traffic that goes in and out of the network if they wish. In the smartphone and tablet world, not only does much of the communication happen outside the corporate infrastructure, but also IT may not be able to filter, monitor, and archive protocols such as SMS and MMS.[9] This can present a compliance risk to those who must log and archive all business communications with external parties.

- **Developed apps without remote access in mind.** Over time, enterprises accumulate legacy applications and infrastructure components, many of which IT did not design with remote access in mind, let alone for the accommodation of mobile access. For example, back-office applications that require VPN for remote access are poor candidates for mobility: Not only is the mobile VPN cumbersome, IT did not design the interface of these applications for the screen real estate of mobile devices. To enable proper mobile access to these legacy applications, IT must often custom-develop native mobile apps or a middleware layer to provide the translation of credentials and interfaces from legacy applications to mobile-enabled apps. These implementation efforts are not a trivial undertaking.

- **Did not account for the increased traffic demands of an empowered workforce.** Increased mobility taxes both internal wireless networks and external Internet links. Most enterprises today cannot support everything their users would like to do on their wireless-capable devices. The same is true with the mobile carrier networks: AT&T, one of the world's largest mobile carriers, saw traffic on its mobile network increase by 5,000% from 2007 to 2010. Simply put, the appetite for wireless communication is accelerating faster than the ability of wireless networks to keep up. To make matters worse, unlike wired networks, upgrading wireless capacity would require replacement of most of the capital equipment, a significant investment.

PREPARE FOR THE FUTURE WITH A STATELESS MOBILE ARCHITECTURE

Enterprise mobility provides an opportunity to enhance the level of customer engagement for both external and internal customers. IT infrastructure operations and security provide the fundamental enabling fabric for that engagement to happen.[10] To successfully establish this enabling fabric, S&R and I&O professionals need to adopt a stateless mobile security architecture.

Forrester defines a stateless mobile security architecture as:

> *One in which controls are dynamically assessed and implemented at the point of access and delivery rather than statically in the infrastructure, on the device, or in the network.*

Conceptually, to implement the stateless architecture, you should follow these principles:

- **Decouple protection from the infrastructure.** In a mobile environment where access is anytime and from anywhere, protection and security logic must follow in similar fashion. A good design principle, therefore, is to avoid tight binding of protection with the infrastructure layer. For example, implementing endpoint traffic filtering logic in a fixed corporate point (e.g., firewall, web gateways) means either that you are not filtering mobile endpoints or you have to invest in expensive traffic backhauling. A far better approach is to embed the filtering in an application on the endpoint or use application-level virtualization on top of the mobile network.

- **Infer trust dynamically rather than relying on statically determined factors.** This principle states that trust, which underlies permission to perform an operation or a transaction, is always assessed at the point of request, as opposed to relying on previously established secrets such as a cookie or certificate. Dynamic factors, such as environment and context, are taken into account when assessing trust. Some of the e-banking and eCommerce mobile apps already do this: A large consumer bank in UK checks every mobile app transaction to determine whether the device is jailbroken or rooted before the transaction is allowed to proceed. This also allows the server the agility to dynamically change the trust evaluation logic to take into account new threats without having to change the system altogether.

- **Avoid costly new investments in in-house applications and infrastructure.** Instead, look externally for suitable options first. It's likely that someone has already built this function somewhere and you can leverage their experiences. More fundamentally, this allows the beginning of a *declarative* way of approaching system operations — you specify "what" needs to be done but decouple yourself from "how" it is done. Being declarative is another fundamental principle of stateless. Declarative security, where you simply specify a security policy and the system employs different abstraction layers to get the job done is already beginning to emerge in the mobile field. Good Technology's Good Dynamics product and Mocana's automatic app wrapping are two examples of declarative security implementation in the mobile space.

A Stateless Mobile Architecture Supports Simplicity, Modularity, And Portability

Statelessness is particularly relevant to mobile computing, because "stateless" implies simplicity, modularity, and portability. You can easily swap out a component in the mobile infrastructure and not worry about how it will affect the rest as long as it conforms to a standard interface for integration. In a world where you don't control all the pieces — consider the increasingly popular BYOD movement — achieving statelessness is particularly appealing. At a more practical level, the stateless principle provides the ability for S&R and I&O pros to:

1. **Leverage cloud and cloud-connected applications.** In the spirit of avoiding costly new investment in in-house applications and infrastructure, explore cloud-delivered or cloud-connected functions. Many cloud applications come with a mobile front end or APIs so you can build your own mobile apps. Explore these APIs for single sign-on (SSO) and data integration. You should look for providers that support the access management and federation languages that you speak, such as SAML, OpenID, or OAuth.[11]

   In addition, to support the rapid growth of mobility and remote access, many enterprises must upgrade the corporate infrastructure to handle the mobile last mile. This includes significantly increasing DMZ and VPN gateway capacity and bandwidth and ensuring that they are optimized for large volumes of object data transfers as opposed to low volumes of large communications. For many, this upgrade will be prohibitively expensive. The economics of supporting mobile access will drive more and more enterprises toward cloud or cloud-connected capabilities.

2. **Migrate from device management to device inspection.** Instead of managing devices, consider answering the question, "Is it safe to run this enterprise application on this device at this time?" The answer to this question would depend on dynamic device inspection, rather than on statically known factors such as cookies, passwords, or certificates. This is what being stateless

is about — decisions are made dynamically with real-time information. Device inspection is an effective way of handling mobile risk without managing the device directly, an approach that is increasingly popular in a BYOD environment. Inspection operations can range from lightweight checking of OS version and device configuration settings to extensive data-gathering, such as device reputation, OS fingerprinting, and jailbreak detection. Depending on the result of the inspection, you can allow access to increasingly critical business functions (see Figure 1).

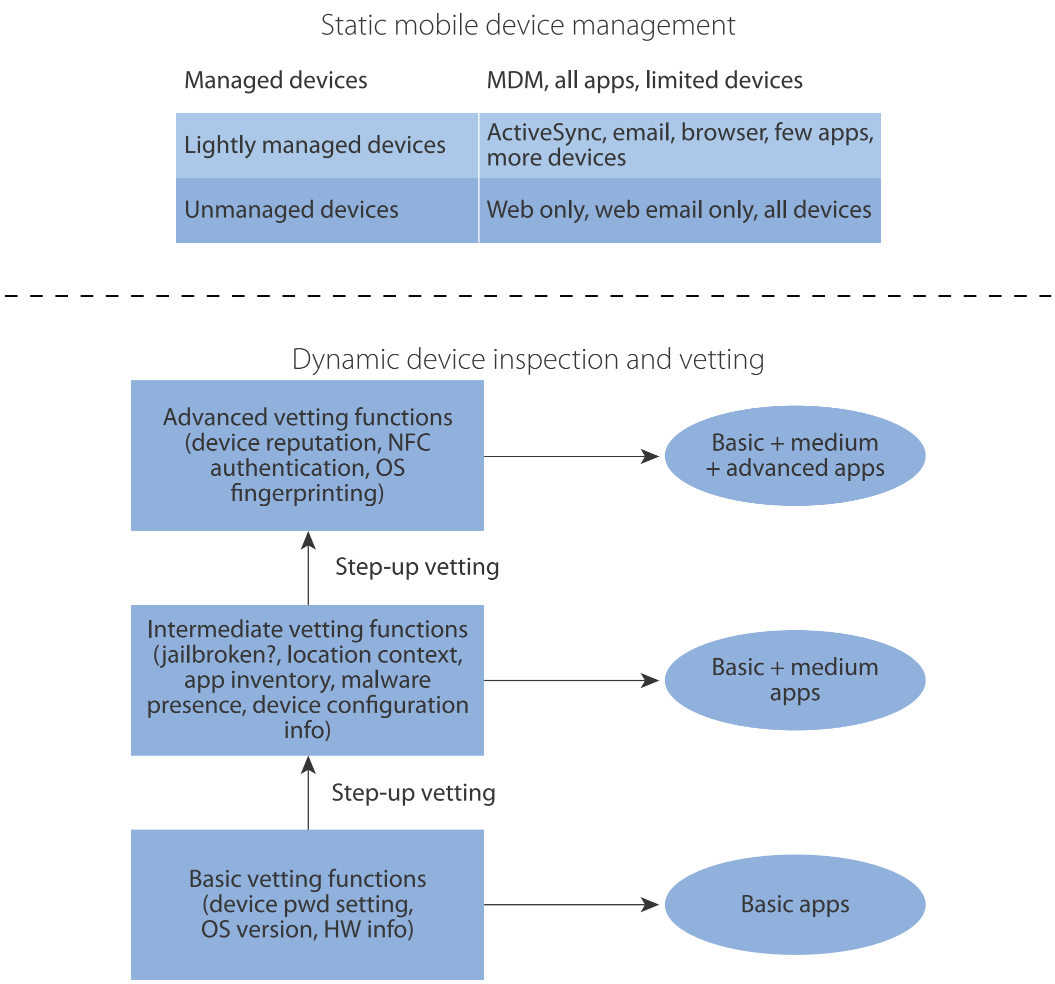
For example, if the user is using the standard features of a payment app, a set of standard inspection steps would take place, but the minute the user invokes the funds transfer feature to a third-party account, a much more rigorous device inspection logic, along with more rigorous user authentication steps, would kick in for risk mitigation purposes. For apps that require a server component to function, as with most transactional apps, the server can reject communication from the client if device inspection fails. For apps that operate in an offline mode, the app itself must perform inspection and policy enforcement.

3. **Perform real-time threat detection and mitigation.** One of the core principles of employing a stateless approach is to reduce the number of static trust points in the system. This is what Forrester calls Zero Trust.[12] To implement Zero Trust, you need real-time data-gathering and threat analytics. In the mobile environment, a native app on the device can collect a wide range of sensory data, including the unique device ID, GPS, NFC (whenever available), and jailbreak information. On the server side, you have traffic and activity pattern data. Combining these information sources provides powerful and contextual real-time threat analytics that S&R pros can use for fraud and threat mitigation purposes.

   A UK-based consumer bank, after experimenting with e-banking apps that support mundane tasks such as "view account balance," upgraded its app to include a set of jailbreak detection logic and sophisticated server-side fraud detection before allowing customers to perform transactions with mobile apps. This was the result of extensive threat modeling performed with the first version of the banking app. The jailbreak detection and fraud monitoring logic have now become the underpinning of a threat analytics layer that the bank is baking into all future mobile apps.

4. **Build protection logic into the application layer.** To decouple protection from the infrastructure, you need to investigate ways to implement protection logic into the application. S&R pros should work with the app dev team to design protection and threat mitigation logic into mobile applications. For native apps, it may involve some form of application wrapping or the old fashioned way of coding security functions directly into the application itself. For web and HTML5 applications, dynamic behavior-based detection, such as technologies by Silver Tail Systems and Mykonos (now owned by Juniper Networks), provide a potential means for just-in-time threat detection and policy enforcement.

Figure 1 Moving From Static Device Management To Dynamic Device Inspection



61569 Source: Forrester Research, Inc.

5. **Help your CIOs reinvent and phase out the internal system of record.** As organizations increasingly use cloud-hosted or cloud-connected functions, some CIOs see this as an opportunity to reinvent their IT infrastructure, with the end goal of eventually replacing much of their internal legacy system of record with cloud deployments. In the short term, this manifests in wrapping many of the existing legacy applications with APIs that are accessible by mobile devices.[13] S&R and I&O pros can help your organization realize this vision by providing guidance on API wrapping and cloud migration. In the near future, it means that many enterprise applications will be wrapped and accessed through APIs.

A good place to start is enterprise collaboration systems. Instead of restricting or blocking the use of Dropbox or other consumer-grade cloud collaboration services, IT security can identify compensating controls to secure your content or help establish a secure alternative to Dropbox.[14] A large financial institution did just that. After evaluating many cloud file-sharing services, it selected WatchDox, a secure cloud-connected mobile file-sharing service, to allow top executives to share confidential documents. The CIO uses this deployment as an experiment before rolling out the service to the entire firm, with a potential goal of using the WatchDox platform as their official file system of record in the future.

FOUR STEPS TO BUILD A STATELESS MOBILE SECURITY AND OPS ARCHITECTURE

To build a stateless mobile architecture, S&R and I&O professionals must look beyond delivering isolated mobile experiences for business needs that arise separately, and keep your eyes on the ultimate prize — a fully mobilized enterprise where mobile use cases are fulfilled by a concerted IT approach. To that end, Forrester recommends that you adopt these steps: 1) Craft a coherent and future-proof mobile strategy; 2) externalize your applications in a phased approach; 3) transition from device management to risk-based device inspection; and 4) extend your stateless strategy to other IT transformation initiatives.

Step 1: Craft A Coherent And Future-Proof Mobile Strategy

The first order of business for S&R and I&O pros is to develop a concerted IT strategy for the extended enterprise. This has two important requirements: 1) Treat enterprise mobility as a central goal of your IT development strategy for the next five years; and 2) stop crafting standalone mobile capabilities for different business use cases and start developing an enterprisewide mobility strategy and road map.[15]

Many organizations rush to develop applications and network capabilities to support business mobility needs without thinking through the implications to the corporate IT strategy. One of the national retail store chains experienced this recently. As a result of an overzealous business group's decision to hurry out mobile apps in an effort to beat competition, the IT steering committee had to pull the plug on a few operational mobile apps when they found that the apps cached primary user credentials in a server in the DMZ. To craft an enterprisewide IT strategy that has a core mobile focus, Forrester recommends these specific steps:

1. **Study your mobile use cases.** Understand from your employees, customers, and partners the desired mobile use cases. Choose four to five apps as your test cases to study the common infrastructure and security requirements. The best use cases to start with are common functions that have a visible productivity or business impact but are not overly complex to take to mobile. Genentech tested the waters with a people finder app, and EMC started with a conference room finder app. Both are popular tools within their respective businesses but are not mission-critical business functions.[16]

2. **Extract common operations and security requirements from the use cases.** From the test cases, S&R and I&O professionals must extract common requirements such as: 1) authentication and credential management; 2) bandwidth and throughput requirements; 3) infrastructure requirements to externalize applications; and 4) threat modeling and data protection (see Figure 2). Some of these components will become the fundamental building blocks for enterprise mobility. Your job is to identify these building blocks, regardless of the application itself, and determine the most efficient ways to implement and support them.

Figure 2 Common Infrastructure And Security Requirements For Enterprise Mobility

Authentication and credential management	How do we authenticate the app, the user, the device? How are user credentials handled? Do we need additional infrastructure (e.g., PKI) and protocols (e.g., OAuth, OpenID) to accommodate authentication and credentialing? Do we store credentials on the client? If so, where and how are they protected?
Bandwidth and throughput	What's the average bandwidth and throughput requirements? Do we have sufficient infrastructure capacity to deal with the requirements? What's the capacity requirement for the component in the DMZ? What's the bandwidth requirement for the last mile between DMZ and the server?
Externalizing server applications	What mechanism would we use to deliver business functions to mobile devices: native, HTML5, hybrid, or virtual applications? What burden will it put on the network infrastructure? What communication protocol will we support between the client and the server? Does this require opening up new sockets or ports on the firewall? What lives in DMZ versus internal network?
Threat modeling and data protection	Is device jailbreak a relevant threat? What about malware? What about other consumer apps? Should threat detection be done on the mobile client or on the server side? Do we need to tamper-proof the threat detection function? What application data will the mobile client handle? How is data processed, stored, and protected?

61569 Source: Forrester Research, Inc.

Step 2: Externalize Your Applications With A Phased Approach

Once you have identified the building blocks, put them in a phased rollout plan. To accomplish this:

1. **Establish an enterprise app store to enable a delivery channel.** Your mobile enterprise needs a channel to publish, distribute, and manage applications for its users. An enterprise app store is one such channel. A good enterprise app store must offer the same user experience as the consumer-facing app stores, and, in addition, must enforce enterprise user or group-based app access policies. A number of products, such as Apperian, AppCentral, and OpenPeak, provide such app stores. Note that your enterprise app store can serve more than your own employees; you can easily extend the scope of users to include business partners, contractors, and customers.

2. **Consider building or sourcing an enterprise mobile middleware solution.** Whichever mechanism you choose to make your applications mobile accessible, be it native, HTML5, or hybrid apps, there are a few common utility functions you would need. The list includes: 1) access management and credential translation; 2) externalizing, rationalizing, and consolidating interfaces; 3) access monitoring and logging; and 4) session management and secure communication. Rather than building these functions directly into the mobile application (either as part of the client or the server application), it's much more efficient if you implement them in a middleware layer from which multiple applications can benefit. An added benefit of the middleware approach is that the server-side application will be stateless with respect to mobile access, as the application itself does not have to manage session data.

   For example, UBS uses Framehawk to consolidate hundreds of legacy applications into a consistent interface, which it then uses to manage and monitor access centrally. A global oil and gas company has a similar middleware deployment to handle identity and access management between end user devices and enterprise applications, including the many use cases where the back end application supports standard access tokens (e.g., OAuth tokens) and where they do not.

3. **Build threat protection and policy enforcement directly into your applications.** A hardware manufacturer of a mobile credit card reader for iPhones and iPads discovered that fraudsters were targeting its services by interjecting between the OS and the reader. Responding to the threat, the company built several data-gathering functions into its app. Prior to every transaction, real-time data is shipped from the device to a server for advanced jailbreak and fraud detection. In addition, the company uses a layer of software hardening technologies by Arxan to prevent tampering of the threat detection logic. Coding threat protection and policy enforcement directly into the app is the only way to consistently enforce security policies across different platforms and devices.

2. **Use stopgap measures sparingly.** Because mobile computing is a maturing field, you may need to employ stopgap measures in the short term to fulfill some of the requirements. Make a list of stopgap measures as opposed to those needed to support long-term initiatives. Prioritize the latter whenever possible, and revisit the list of short-term measures every 12 to 18 months for better alternatives.

   A mobile VPN, for instance, may be a stopgap measure before you fully mobilize your applications. Some may consider virtual desktop infrastructure (VDI) a stopgap technology also — one that you employ before you can deliver a native mobile experience. Chuck Hillis, CTO of global marketing for EMC, believes exactly that. He said: "Mobility is about delivering immediate user experiences with native apps, not about building fancy browser and server applications." He believes that EMC will eventually phase out its VDI deployment in favor of a secure, native mobile experience.

Step 3: Transition From Device Management To Risk-Based Device Inspection

Because corporate-owned devices are likely to remain in enterprises for some time to come, and because most IT shops are still stuck in the mindset of managing devices rather than managing the risk of mobile operations, mobile device management will continue as an area of investment in the near future.

The aforementioned mobile credit card reader manufacturer is one example of tiered device inspection. The application's inspection operation includes jailbreak detection as well as other deeper inspection to flush out issues such as an invalid checksum for OS library routines (e.g., Android License Verification Library) as needed. For example, if the inspection algorithm finds evidence of jailbreaking, a more detailed and rigorous inspection routine will kick in to check for the presence of malware and other signs of tampering. The goal is to identify evidence that suggests a risky environment for the physical reader — such as a "man-in-the-mobile" attack. If device inspection indicates possible transaction risks, the server side may proceed to put a limit on the dollar amount of transactions, engage in a second-channel verification (e. g., a call will be dispatched to the credit card owner to check the validity of the transaction), or in some cases, completely disable the payment app. To move from device management to stateless device inspection, S&R and I&O pros should:

- **Lightly manage your devices with ActiveSync.** As much as you can, go light on device management, and use native platform tools. Microsoft shops may want to leverage their investment in Exchange ActiveSync to enforce a security and policy baseline, such as device password, remote wipe, and automatic device lock. IBM Lotus users can do the same with the MDM functions in the Lotus product.

- **Use an application-level container if you must, but know that it's disposable.** For firms with a strong data protection and leak prevention requirement, ActiveSync management won't do the job. You may want to consider a container-based approach today to enforce encryption and crude DLP policies, but expect to replace that within the next 18 months or so with more fine-grained, data-aware control technologies built directly in the application.

- **Define your device inspection framework based on risk assessment.** What level of device inspection do you need for protecting your applications and data? Do you want to perform step-up inspection? If so, what are the different tiers of inspection rigor and how should you handle the inspection result for each tier? You must answer these questions before you implement device inspection. For example, the risk profile for a mobile payment application is very different from a corporate email application. Thus, the treatment of device inspection for the two should employ very different levels of rigor as a result. S&R and I&O pros should work with business owners of the applications to put together a device inspection framework that accurately reflects business risks.

- **Identify technologies and ecosystem partners to implement device inspection.** To gather the appropriate information for device inspection, you may have to use third-party technologies or services, such as device reputation information like those supplied by iovation, and behavior analytics by vendors like Silver Tail Systems. To ensure the integrity of device inspection and other security operations embedded in the application, look to software hardening and anti-tampering technologies such as those by Arxan and PreEmptive Solutions. IT security and ops professionals should proactively identify technologies and services that help to implement device inspection and determine how to incorporate the technologies in your mobile infrastructure.

Step 4: Extend Your Stateless Strategy To Other IT Transformation Initiatives

Don't confine your strategy solely to mobile efforts. Investigate how you could leverage your mobility investments for other IT initiatives. Some immediate areas of synergy are to:

- **Extend the mobile access middleware to support cloud use cases.** The oil and gas company that built an identity and access management middleware for mobile access quickly realized that cloud access is another viable use case for the middleware. As a result, they decided to build cloud access management into the architecture design. The middleware implementation is nearly complete and can now handle mobile access to any SAML-compatible application, whether it is hosted on-premises or in the cloud. It just so happens that the company is considering moving from an internal CRM implementation to a public CRM cloud. The existence of this access management layer will dramatically simplify the task of migration to the cloud — a big win for IT and the company.

- **Implement the mobile access middleware with cloud technologies.** Organizations are finding out that the mobile last mile, from the access middleware to the internal application, is a capacity planning headache: As access volume increases, the middleware layer can become a bottleneck. This is a perfect place for cloud to step in. Putting the middleware layer in a cloud is the only viable way for good bandwidth and capacity management. In this way, cloud provides the opportunity to support mobility and really is the ideal platform to deliver the anywhere, anytime vision. S&R and I&O pros supporting mobility should collaborate with other IT transformation efforts such as cloud migration to drive synergy and optimize investments.

- **Bake the stateless approach into client management beyond mobility.** With the mobile transformation, the old approach of driving absolute efficiency into managing a single device image across the enterprise is breaking down. I&O professionals must deal with various forms of consumer technology burrowing into the workplace, including employee-owned PCs. By employing the principles of a stateless approach, I&O pros have the opportunity to evolve their workforce computing strategy to enable emerging business demands, such as supporting BYOPC programs.

RECOMMENDATIONS

PROVIDING THE ANYWHERE, ANYTIME, ANY-DEVICE MOBILE VISION IS A JOURNEY

Depending on your organization's size, industry, and strategic business objectives, your company will mobilize at a different pace. However, whatever pace you take, you will soon face many of the same challenges as other organizations that have embarked on the mobile journey. You don't have to be close to the anywhere, anytime, any-device vision to feel the pain of accommodating your device-wielding, technology-adept mobile user population. To make your journey smoother:

- **Put together a mobility council — you'll need it.** A good mobility council should consist of representatives from app dev, networking, client management, security, and business. Because most likely there is not a solution out there that will provide everything that you want, the mobile team will have to craft compensating controls, deliver stop-gap measures wherever necessary, and work with the rest of the IT to ensure the success of mobile delivery. But most importantly, the mobility council serves as a central governance function to help create order out of the mobile chaos.[17]

- **Draw innovation inspiration from the mobile experiments.** Start your experiments with non-mission-critical but productivity-enhancing applications such as a people finder or lightweight collaboration. Learn from the experience, and deduce from it the essential layers of operational and security services that you will need for mobile expansion, like the building blocks described previously. Try to distinguish those that you need for short-term measures and those that will stay for the long haul.

- **Choose your trust points strategically, and protect them appropriately.** Even with a stateless architecture, you will still rely on a few components to function properly to deliver business functions and services. These trust points include services that you depend on to supply information for security decisions, such as device inspection and data collection, or those places where you conduct policy enforcement. S&R pros should perform threat modeling and choose appropriate protection mechanisms to preserve their integrity. In addition, I&O pros should treat these trust points as critical services and take appropriate steps, such as providing failover capabilities with redundant servers, to guarantee service continuity. Together, even if some of the components or data points fail, you can still reliably assess trust and security.

WHAT IT MEANS

ENTERPRISE MOBILITY GOES FAR BEYOND MOBILIZING EXISTING EXPERIENCES

If what we implement in the mobile sphere is simply replicating functions that already exist as a web application or other classic forms of enterprise application, we would have missed the point. Mobility holds the promise of fostering new innovations, reaching new audiences, and most importantly, creating never-before-seen user experiences and business opportunities that are either impossible or prohibitively expensive to deliver in traditional environments.

Augmented reality is one of those technologies that is impossible to deliver without advanced mobility. In the future, AR may become the norm for how we experience the world around us; firms with a sound mobile architecture blueprint today will be in a better position to leverage new and emerging technologies like AR. Bearing this in mind, S&R and I&O pros would serve their organizations better by prioritizing infrastructure and technology investments that enable new experiences and business transformation rather than a strict replication of existing functions for the mobile channel. Enterprises that are able to grasp this concept and adapt quickly will have the competitive advantage.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Report

Accellion

Arxan Technologies

EMC

NVidia

Taptera

WatchDox

ENDNOTES

[1] With computing devices becoming increasingly affordable, many consumers today own more than one device to access the Internet, such as a tablet, smartphone, laptop, desktop, or netbook. See the June 12, 2012, "Global PC And Broadband Penetration" report.

[2] With 55 million iPads sold through December 2011, and an estimated 5.5 million Amazon Kindle Fires sold in their first quarter on the market, tablets have gained unstoppable momentum. Forrester forecasts that tablets will reach 112.5 million US consumers — one-third of the US adult population — by 2016. See the March 6, 2012, "US Consumer Tablet Forecast Update, 2011 To 2016" report.

[3] Source: Forrsights Networks And Telecommunications Survey, Q1 2011. We asked, "What is your firm's official IT policy for supporting employee personally owned mobile devices (cell phones, smartphones and tablets) (does not include laptops)?" Fifty-nine percent of the respondents say their companies support BYOD to a certain extent: Some provide 100% support, others provide limited support. Ten percent say they do not officially allow personally owned devices, and 26% say they do not support personally owned devices.

[4] There is a simple philosophy at the core of Zero Trust: Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network)

and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted. See the September 14, 2010, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" report.

5 Long term, enterprises will have a hybrid portfolio of cloud and non-cloud workload deployments that uses this breadth of options to optimize resource and agility requirements. In this future state, the majority of systems of engagement workloads will be cloud-resident while your systems of record evolve to cloud at a slower but deliberate pace. The end result will be a mixed environment managed through a decision tree and series of workload automation systems that ensure governance and regulatory compliance across this portfolio. See the June 1, 2012, "Make The Cloud Enterprise Ready" report.

6 Triggered by a visual cue, AR can deliver dynamically generated content, including sound, 2D information, or 3D animation, laying on top of the physical object image seen in the device display. Futurists imagine a world not too far in the future where AR becomes the new norm for how we experience the world around us. AR can enhance our world by personalizing it. A 10-year-old child visiting a history museum will experience content matched to his age and interests as will a 75-year-old World War II history buff. Initial AR scenarios relied on dedicated eye- or headgear but the devices and the experience were expensive to create. Today, mobile phones offer the potential of a more economical though less immersive experience but one that is available to the masses given the ubiquity of these powerful devices. AR will enable consumers to experience products before they purchase them and simplify the discovery and consumption of highly relevant content. See the December 22, 2011, "Augmented Reality: Emerging Tools To Explore" report.

7 Commonwealth Bank of Australia is generating 1% of its overall mortgage leads by using mobile augmented reality (AR) within a homebuyer's research application to enhance its home-buying service. This implementation delivers content in a richly relevant, intuitive, and convenient way and has fostered more than 212,000 downloads of the application. A significant part of Commonwealth's overall strategic approach, the mobile service allows the bank to connect with consumers very early in the purchase cycle. The app offers licensed information of actual selling prices and closing dates as well as estimated current values. See the December 22, 2011, "Case Study: Home Buying With Mobile Augmented Reality" report.

8 Successful businesses don't work in isolation. Today's businesses must constantly create new products and services, expand their geographic presence, streamline operations, and deliver top-notch customer services. To do this, your business will increasingly use third-party and cloud services to reduce cost and increase speed-to-market. Your business will unleash the creativity of your employees and customers with mobile, social, and rich media technologies. More and more devices come equipped with microprocessors, which means cameras, cars, home electronics, and even musical instruments will all become conduits for businesses to deliver services and engage customers. To stay relevant, your enterprise must continuously extend itself to include new peripherals and meet new business scenarios. See the November 9, 2011, "The Extended Enterprise: A Security Journey" report.

9 iOS does not allow any third-party application to intercept SMS and MMS message streams, while it is possible to do so on BlackBerry and Android devices.

[10] Mobile devices and apps (and mobile websites — we call them all "apps" here) are powerful tools that firms can harness to engage customers, serve partners, and empower employees. But mobile is not merely another chapter in the smaller, faster, cheaper device story. And it's not tiny web or screen-scraped PC applications. Instead, mobile is the flash point for a much more holistic, far-reaching change. Your app is in your customer's pocket. Now what are you going to do? Forrester believes that mobile apps are the front end and first stage of what Geoffrey Moore has termed new systems of engagement that empower customers, employees, and partners with context-rich apps and smart products to help them decide and act immediately in their moments of need. See the February 13, 2012, "Mobile Is The New Face Of Engagement" report.

[11] The SAML 2.0 assertion format and corresponding web SSO protocol are the most robust, future-proof, and interoperable choice for enterprise federation scenarios. OAuth's lightweight and flexible API security mechanism makes it an ideal tool for mobile needs. And OpenID is important because of its dynamic partnering capabilities. See the June 3, 2011, "The 'Venn' Of Federated Identity" report.

[12] One of our goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. We call this "designing from the inside out." If we begin to do all those things together we can have a much more strategic infrastructure. If we look at everything from a data-centric perspective, we can design networks from the inside out and make them more efficient, more elegant, simpler, and more cost-effective. See the November 5, 2010, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" report.

[13] Apigee, Framehawk, and many other companies will help you develop this API layer.

[14] Since 2008, the Palo Alto Networks Application Usage and Risk Report has monitored browser-based file-sharing as an application category. It has steadily increased to the point where it is now found in 92% of all participating organizations, while P2P file-sharing has slowed to where it is used in 82% of the participating organizations. Only client/server related file transfer applications (FTP, etc.) are more commonly found. Source: "The Application Usage And Risk Report," Palo Alto Networks, December 2011 (http://media.paloaltonetworks.com/documents/Application_Usage_Risk_Report_2011-12.pdf).

[15] When planning for the future, I&O and S&R professionals must develop a road map to link their mobile strategy to business needs, shape future capital requirements, and guide product selection. To understand business requirements, you should engage executives and line-of-business owners to understand what business functions they want to mobilize; you will also need to survey employees to determine their expectations and the most common use scenarios. See the May 16, 2012, "Define A Road Map For Mobile Security And Operations" report.

[16] Corporate mobility momentum today is fueled by employee bring-your-own-device (BYOD) programs and increased demand for a wide range of mobile applications and services to address the needs of employees, partners, suppliers, and customers. This increasingly fragmented and complex mobility landscape is forcing many corporate IT departments to develop and communicate a corporate mobility strategy. In fact, 35% of surveyed North American and European enterprises identified developing a comprehensive corporate

mobility strategy as a top mobile priority in the coming year. See the May 21, 2012, "Address Complexity With Mobile Security And Operations" report.

[17] The mobility council must have the horsepower to define strategy, make decisions, establish policies, secure funding, and get things done. This is not an advisory group; it is a decision-making group. The leader — and either an S&R or an I&O pro can play this role — should carry a VP title to send the message that mobility matters. The council must have representatives from every discipline, function, and business. Cisco is taking this approach with a cross-organizational mobility council led by Sheila Jordan, senior vice president of communication and collaboration. See the May 7, 2012, "Charter A Mobility Council With Seven Tasks" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On
Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals