The Future of Mobile Enterprise Security

Gearing Up for Ubiquitous Computing

PIQUE SOLUTIONS

August 2014

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | Fax: 415.373.3892

Contents

Introduction

As enterprise adoption of mobility moves forward, the growth of the Internet of Things (IoT) presents the next evolution in computing. The impact of these trends in terms of increased risk to the business is straining existing security infrastructures. Enterprises need a dynamic and flexible security framework to balance risk and trust. This need has led to the rapid expansion and growth in enterprise security technologies for mobility. To balance costs with needs, however, the enterprise needs to know which technologies to invest in. It also needs to know whether to rely on one, a combination of technologies, or to take a unified approach. While making these decisions, the biggest challenge for the enterprise is balancing user needs with enterprise requirements and regulations. In this whitepaper, we will review the current state of the mobile enterprise, lessons learned with existing tools, and how a unified approach to application and access management balances the needs of the end user and the enterprise.

State of the Mobile Enterprise

IT and User Needs Are Not Always Aligned

Mobile devices blur the lines between work and personal life. The applications, services, and device functions that people find useful in their personal lives are just as empowering in the enterprise. Where in the past a camera, cloud storage, and third party applications might have been considered suitable for personal use only, these same functions now contribute to work life as well. In this scenario, it is the way the applications are used that defines the need for controls.

Initial adoption of personal devices in the enterprise was easy to achieve due to the commonly understood value of having happier, accessible, and more productive employees. Now it is about growth through business transformation. All of these benefits are achieved on low-cost hardware, many times with the cost deferred to the user, creating immediate savings for the enterprise. Yet, it did not take long for IT to realize that short-term savings on hardware eventually led to longer-term costs for management and control. There is also the downside of risk to the organization's security posture and potential data loss. The greatest need of information security is the awareness of how and where enterprise information exists and is used on mobile devices. Users need efficient, easy access to information. As a result, the role of IT has evolved to that of a content facilitator and business enabler tasked with providing appropriate services and resources.

Methods for restricting use of enterprise data need to be increasingly transparent to the user.

For devices on which users spend an inordinate amount of time, methods for restricting use of enterprise data need to be increasingly transparent to the user. Approaches such as mandating complex passwords for the entire device are giving way to more user-friendly approaches, such as transparently encrypting enterprise data, adding authentication for enterprise access only, and single sign-on. As mobility management vendors approach IT, they must provide tools that appeal to all levels of risk tolerance, while keeping in mind the needs of users.

Rapid Change Contrasts with Slow Enterprise Technology Adoption Models

Enterprises practice a process-oriented method when evaluating and deploying new technology and software. This is to ensure that new functionality does not impact operational capabilities and that the organization is prepared to support any potential problems that might occur.

Microsoft, the dominant desktop OS provider for the past 30 years, achieved only 18% adoption of its Windows 7 release in its first 10 months. Most enterprises have not even begun to look at or adopt its latest version, Windows 8.

In comparison, mobile technology operating systems are updated annually, if not faster. Consumer, not enterprise, demand for new features drives this approach. Apple introduced the first iPhone in 2007. Over the course of the next seven years, Apple released seven new versions of the iPhone and eight versions of iOS. Apple has introduced a new updated version of both the hardware and operating system on a yearly cycle. Even more incredible is the rate of adoption of each new update by the end user community. iOS 7, which launched on September 18, 2013, was loaded onto more than 26% of iOS devices in only the first three days.

When comparing enterprise adoption of technology to consumer adoption of mobile platforms, it is clear that end-user expectations have changed. For a number of reasons, IT goals (primarily for security) are generally not aligned with these user expectations.

Rise of Ubiquitous Computing – Everywhere All the Time Information Access

The technology landscape has experienced a transition from desktop systems to pocket-friendly devices. These portable devices provide organizations with opportunities for growth through business transformation. Yet these devices only represent the tip of the iceberg. Moore's law continues to prove true as computing power grows at a rate that allows for everything to become a computing device.

Connected smart devices represent the next phase in computing. Also known as machine-to-machine (M2M) or the Internet of Things (IoT), smart devices contain specialized functions, monitors, and sensors that communicate with their surrounding ecosystems (humans, machines, applications, or other smart devices). Smart meters, smart appliances, smart cars, and smart homes represent tremendous opportunities for organizations. According to Gartner, Inc., the Internet of Things' installed base will have grown to 26 billion units by 2020.

Computing is becoming ubiquitous, with a world of "everywhere, all the time" access to company information from any device, whether it is a desktop, laptop, tablet, mobile phone, or smart device. Computing devices may be company-issued, may be part of the Bring Your Own Device (BYOD) movement, or both. Regardless of device, people transition from device to device to access the same information. To meet the demands of "everywhere, all the time" computing, the enterprise needs to manage and secure large, complex, distributed, and changing environments both within the traditional perimeter and/or in public facilities, with limited visibility into controls. In this new model, trust at the endpoint no longer exists.

There are many hurdles before "everywhere, all the time" computing becomes a reality. IT needs to test, revise, and develop applications and networks. Applications must be cross-platform. Security controls need to provide a unified approach to every device type. Authentication must offer a single, consistent method of access to all devices.

In this new model, trust at the endpoint no longer exists.

Disparate Approaches to Managing the Mobile Landscape

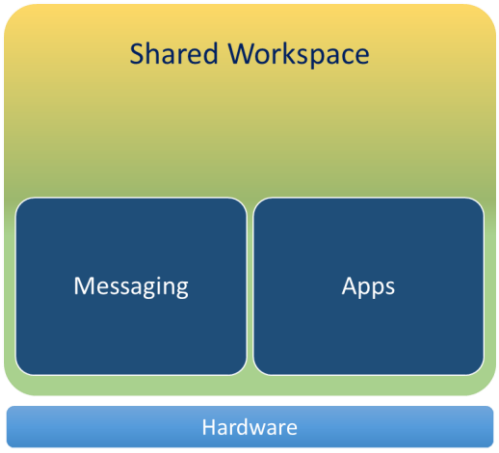
There are various approaches to mobile management. While these technologies are somewhat easy to define, the vendors that provide these tools are constantly evolving. This evolution makes it difficult to define their role in the market. It also highlights the convergence of many technologies within a single

enterprise technology provider. The approaches described in this paper are ordered from the least to the most effective methods for securing the environment on mobile devices.

Mobile Device Management (MDM)

MDM was the industry's first attempt to control the proliferation of mobile devices in the enterprise. MDM leverages an installed client on the device—or semi-private APIs on iOS—to provision, manage, and de-provision mobile devices over the air. For example, MDM allows IT to on-board large populations of devices by pushing the client or profile to the device via email, SMS, or a website. During the provisioning process, MDM sets up corporate email, pin/password access to the device, Wi-Fi access point credentials, and VPNs. In addition, during the life of the device, MDM allows IT to track the device location and inventory-installed applications and monitor health statistics. If a device is lost or stolen, IT can wipe the device, removing both corporate and personal data. In the case of employee-owned devices, MDM enables IT to remove corporate email and applications installed through a corporate application store when necessary.

Figure 1. MDM Approach



MDM first appealed to enterprises because it provided an almost Blackberry-like environment in the era of non-Blackberry devices. Blackberry set a standard for control over mobile devices but was limited to managing its own devices. At the core of MDM is a set of authentication and certificate enrollment and configuration processes that allow the device and the server to trust each other. MDM solutions enable behind-the-scenes remote management of a mobile device through a central server. Hence, tasks such as policy enforcement, device configuration setting, and remote wipe or lock do not require end-user interaction.

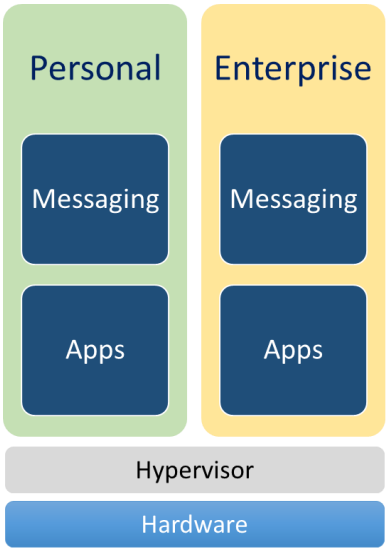
However, Mobile Device Management is, per the name, focused only on the mobile device. It is a management tool and not a strong security tool. It does not segregate personal and enterprise environments for messaging and applications. MDM is a good solution for device configuration, provisioning, awareness, support, or controlling physical aspects, such as a camera, within a controlled facility. It is not a good solution for managing the flow of information. In this same context, security controls are device-centric, in particular authentication. Mobile device vendors do not provide key management beyond device key storage. Alternatively, Microsoft ActiveSync provides the same level of authentication and encryption configuration. Weaknesses become apparent in MDM when the enterprise needs a stronger set of controls for applications and information. The impact MDM has on user experience is negligible. MDM does not change or impact how the device functions.

Mobile Virtualization

Mobile virtualization divides a device into two distinct operating environments. Referred to as dual-persona, one environment is for personal use and the second is for enterprise use. This division creates a separation of information and applications for a strong data-loss prevention strategy.

Comparable to Virtual Desktop Infrastructure (VDI), mobile virtualization has remained low-key to date. The key benefit of virtualization is that the OS build can be centrally managed and distributed, reducing overhead for IT and demarcating ownership of information and applications.

Figure 2. Virtualization

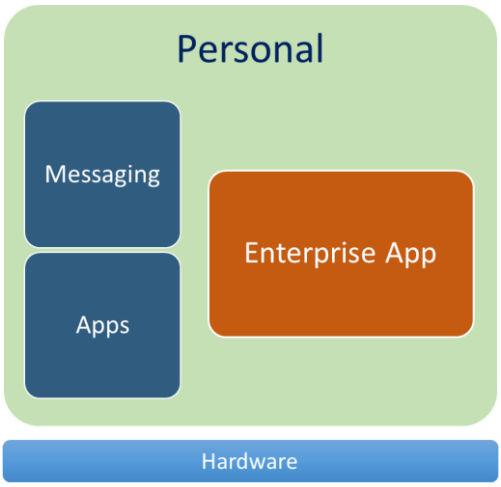


Mobile virtualization has the appearance of being a strong technology for supporting personal devices in an enterprise environment, but the reality of developing for hardware has become its largest limitation. Apple has not allowed any of the virtualization vendors to develop for their hardware. This is because doing so requires inserting a layer between the hardware and the software. While there are significant limitations on iOS, Android and Windows 8/RT do support mobile virtualization. It is possible to have two competing OSs on the same device. But, for Android, the diversity of hardware platforms and chipset providers means virtualization technology must be developed for each specific configuration. In addition, mobile virtualization is memory-dependent and negatively impacts battery life. This means the mobile virtualization vendors must decide what they will support, forcing the enterprise to follow suit. Lastly, the idea of swapping between operating systems can be cumbersome to the user, going against the core themes of user ease of use.

Mobile Application Management (MAM)

MAM evolved out of MDM as a way to enforce control around enterprise applications. Basic levels of MAM include an application catalog, app provisioning, and update management. Security controls include application-based encryption, authentication, app-level VPN access, device integrity checks, and API controls. These controls are useful particularly where application developers have not provided this capability natively to their application. Vendors provide developers a software development kit (SDK) to recompile custom, in-house, or third-party applications. Alternatively, some MAM vendors allow IT administrators to wrap custom, in-house, or third-party applications at the management layer.

Figure 3. MAM Approach



MAM is considered a lightweight approach to managing applications. Enterprise applications appear within the same operating environment as personal applications. While MAM does not provide visibility or control of the operating system, it does offer policy management for enterprise applications without impacting personal applications. With an application focus, MAM works well for enterprises that want to avoid legal and privacy issues without compromising their information security requirements.

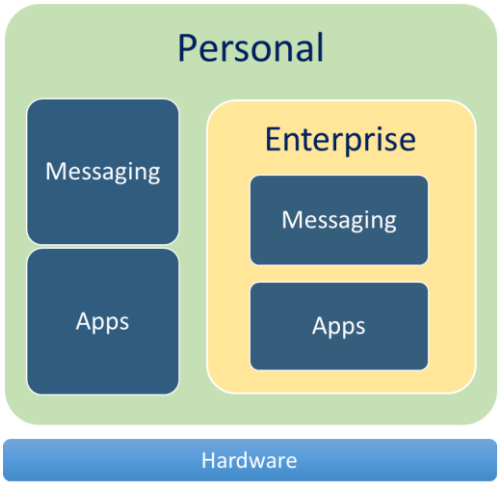
The biggest limitation for MAM is the lack of enterprise mobile applications. The market for mobile enterprise applications is still in its infancy. Most enterprise applications are still legacy Windows or web-based, which are typically out of scope for MAM. It also does nothing for the native messaging environment, which has been the early primary driver around mobile device adoption. The reason MAM cannot protect native messaging environments is that mobile OS vendors, in particular Apple, have not permitted interference with their native mail,

contacts, or calendar applications. MAM also does nothing for document management, as it only protects the data related to the applications it can control.

Mobile Container

Mobile containers offer separate workspaces on mobile devices for enterprise and personal use. This divided workspace offers secure management of enterprise applications and information and facilitates collaboration. The grouping of enterprise applications in a shared container is the key distinction of containerization compared to the other discussed methods. MDM focuses on the device, while virtualization essentially creates two devices. MAM applies controls directly to the applications. Mobile containers apply application management, provisioning, authentication, and encryption to the secure workspace. Secure communication is also managed at the container level.

Figure 4. Mobile Container Approach



Mobile containers can simulate the same set of provisioning and configuration options as MDM, but at the container level. They also offer the same divided workspace as mobile virtualization, but with none of the hardware limitations. Finally, mobile containers support the same methods of application control as MAM, but with the ability to extend support beyond just mobile applications to include legacy windows and web applications. An additional benefit of the mobile container approach is the ability to provide productivity applications such as messaging, contacts, calendar, and documents.

The impact of containerization on usability depends on the design of the mobile container and its associated applications. Early mobile containers diverged from the core OS design and provided their own look and feel. In general, today's containers inherit the usability, look, and feel of the native operating system so as not to impact the user experience.

Lessons Learned from a Device-Centric Approach

Physical Ownership Limits Device Control

Because users carry mobile devices – particularly smartphones – day and night, there are real concerns about employers knowing the location of a device and how the device is used. Even when corporate-issued, the personal nature of mobile devices creates an expectation for privacy. There are valid use cases where the location of a device will determine device or application access. Geolocation even provides for stronger authentication. But for most workers, having IT know where they are at all times feels invasive and unacceptable. Policy enforcement points must therefore consider the context of the situation.

For users concerned about privacy, it is easy to bypass device-based security measures, even on company-issued devices with locked down environments. This results in a huge blind spot for the enterprise. Bypassing security controls in a restrictive environment is damaging to the organization's security and risk posture. A better approach would be to implement an open and accepting device usage policy that seeks to limit security controls to enterprise information and applications only.

Not All Mobile Operating Systems are Created Equal

Mobile OSs differ from structured desktop operating systems. Legacy Windows files are accessible to any process given the proper credentials. In theory, mobile devices are inherently more secure when it comes to application and process management. This is because mobile OSs use a sandbox approach to limit access to information through application-based APIs, controlling access rights.

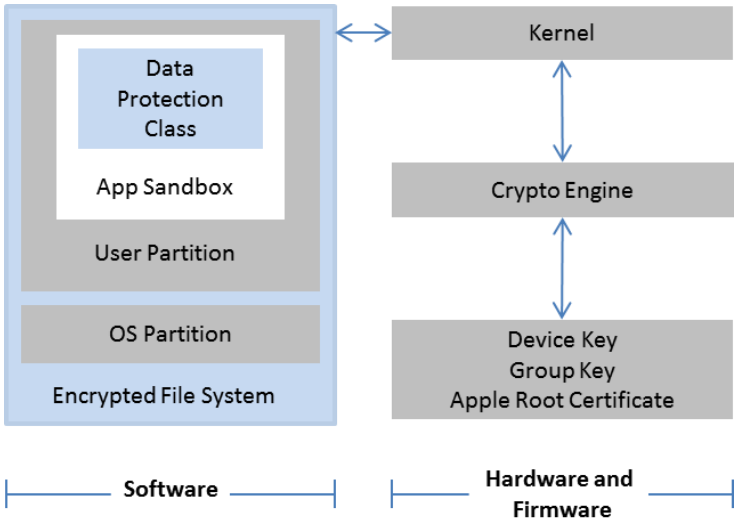
A primary security concern for mobile devices is the use of specific APIs that result in information access. Many applications, malicious or not, allow liberal access rights, and unfortunately most users do not know exactly what they are permitting when they install apps.

Each mobile operating system vendor defines their API for advanced configuration controls. This differentiation results in a variance in the level of capabilities between platforms, complicating the ability for IT to establish a consistent set of controls across disparate platforms. For example, for email, Microsoft provides a limited set of controls consistent across all mobile operating systems, while IBM offers their own set of controls for Lotus Notes.

Apple

As **Figure 5** portrays, Apple has created a strict set of controls and processes for application access to the underlying operating systems and hardware. iOS is designed to allow only applications that have been validated and digitally signed by Apple to install and execute on iOS devices. This, in theory, makes it impossible for malicious code to present itself on a system unknowingly. It also impedes the ability of security vendors to gain access to the underlying kernel, limiting both malware scanners and virtualization technology in particular.

Figure 5. iOS Architecture - Apple



Google

In comparison to iOS, Android does not require the same strict level of adherence. It also has not fared as well against malware with its open application store and ability to side-load applications from untrusted sources. While Android's application execution environment is stricter, the device still has the larger security problem. Despite Google's efforts to check all the applications in Google Play for viruses, many malicious applications go undetected. It appears that Android OS limitations are the weakest link in the security chain. But in reality, user decisions represent the largest attack surface. Users approve

permissions for all applications. So, to launch a virus, an attacker only needs an application to be approved with trusting information access. Malicious applications for Android usually request permissions for unlimited Internet access, access to contacts and browsing history, and rights to send SMS/dialing phone numbers.

Placing responsibility for access and authentication rights on a user group lacking security expertise is a fundamental flaw in information security. This leads to a balancing act between user experience and system restrictions where the user will more often choose access over security.

Microsoft

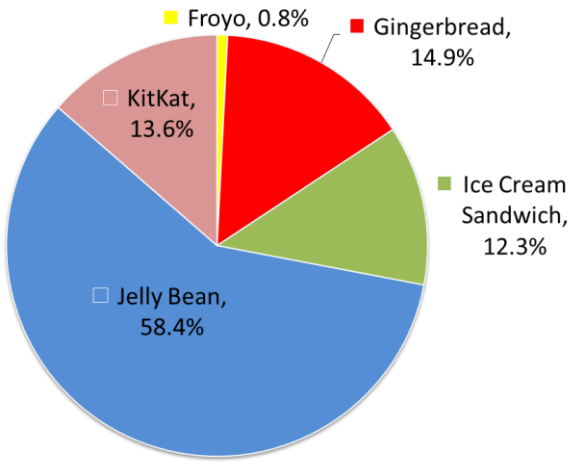
For Windows Phone, Microsoft has sought to provide a balance in the iOS and Android OS architecture. Microsoft implements both application compartmentalization and application store validation. Yet, Windows Phone lacks some of the extensive capabilities provided by Android and does not exercise the same level of strict control sought by Apple.

In any case, no two mobile operating systems are the same. Enterprises must be aware of the strengths and flaws of each when considering a device-centric approach. All of this means that when it comes to Mobile Device Management, the enterprise must choose between diverse management capabilities or the lowest common denominator. Some MDM vendors are doing a great job supporting as many different OEM MDM APIs as possible, but device management capabilities are still limited to the APIs provided by the device manufacturer.

Fragmentation is the Rule, not the Exception

The rate of mobile operating system development is rapid. Each new version of the various operating systems introduces new security capabilities. But, as Figure 6 portrays, Android is becoming more fragmented with each new version, as older devices are incapable of supporting newer versions of Android. Now, not only do organizations have to manage several different mobile operating systems with varying capabilities, but they also have to deal with the fact that just in Android alone, devices from different manufacturers will have different management APIs.

Figure 6. Android Platform Distribution - Google



The introduction of third-party vendors who can modify Android for their specific platforms only exacerbates the issue. For example, Samsung SAFE has some of the most prominent OEM MDM APIs, and was recently adopted platform-wide by Google, but there are also special management APIs for

devices from HTC and Motorola, and even the Amazon Kindle Fire tablet and phone have their own set of management APIs. There is a clear need for a third party unified platform here.

For Samsung and the other vendors, all of these OEM MDM APIs are predicated on the idea that a single platform will be provisioned by the company. However, these will not help to manage diverse personal devices, regardless of the corporate policy. No matter what, users will want to work from all manner of devices. It will only get worse with the Internet of Things.

Evolving Need for Secure Application Delivery

If a device-centric approach taught any lessons, it is that there are no certainties beyond an enterprise's ability to trust its own applications and services. Endpoint and network controls are becoming less able to reduce the risk posture of an organization. Every device is becoming part of the untrusted network. Applications need to be the trusted provider for confidential information. Devices become a part of a larger contextual definition of what levels of access and trust to provide for user to application mapping.

In contrast to device-centric approaches, the enterprise can insert security controls at the application and service level. This removes device dependencies to create an application-centric security model, or security through application delivery. An application-centric security model removes the user or system access at the network level and applies authentication and auditing at the application level. The primary goal is to replicate the trust that exists inside a corporate network and extend it to foreign devices.

The primary goal is to replicate the trust that exists inside a corporate network and extend it to foreign devices.

An application-centric trust model includes the following components:

- An application container manages access to information that resides on the endpoint. This is the boundary within which to apply authentication, encryption, and data controls. Access is mapped to the device, user, and contextual data, such as location.
- Delivery of applications from a centralized form of gateway. This layer controls delivery through an encrypted channel along with establishing approved access to backend systems.
- An application store, or an alternate verified application repository for application provisioning and verification.
- The ability to natively embed security that is integrated with enterprise access management controls into apps for situations when a container approach doesn't make sense, such as access for customers and business partners to their accounts or other sensitive information.

While several options allow for the control and management of applications on a device, application delivery is the main consideration for enabling secure enterprise information architecture. Secure communication and authentication is established with the application, not the device. This is critical for eliminating threats presented by devices and users. The goal is to block unnecessary exposure inside the trusted network, while still providing the required access to applications.

In an application-centric security model, an application establishes its own self-contained, encrypted communication channel at the application level or within the enclosed environment where the application exists, without reliance on the operating system or device. This provides a buffer between

the personal and the enterprise space. It also enables the delivery of applications in a format digestible by smaller, touch-based devices that might not be able to handle the inputs of a legacy application.

Segregation of enterprise applications from the personal space achieves several key functions:

- It preserves the user experience with no modification to the device and no controls on personal applications.
- It provides the necessary level of access control for enterprise applications with the ability to exceed current standards.
- It reduces the risk posture of the enterprise by eliminating the use of endpoints for entry to the trusted network.

Historically, companies would have used a device-level mobile VPN to extend remote access to mobile devices. However, mobile device VPNs have several flaws. First, device-level VPNs expose the corporate network to nefarious applications, malware, and viruses that may have been downloaded by the user. Also, use of constrained delegation in the demilitarized zone (DMZ) creates a proverbial "man-in-the-middle" between the mobile device and the trusted active directory in the enterprise. Finally, PKI certificates stored in device keychains are accessible to any device user; without a proper PIN there is no "two-factor" authentication.

Moreover, mobile devices don't contain native support for enterprise authentication standards. Each mobile OS has its own peculiarities regarding security and authentication, making the consistent deployment of security standards nearly impossible.

For security-minded organizations — those using strong security methods to authenticate users trying to access confidential information and data (smart cards or Kerberos with PKI certificates) — numerous security concerns emerge when enterprise access is extended to and from smartphones and tablets.

Encryption is implemented along with access control to ensure that only authorized users have access to critical data when and where they are authorized. Three areas that should be addressed with encryption include the endpoint, the transmission period, and stored data—both structured and unstructured. Most products today provide AES-256 level encryption, key management, and some form of access control integration with existing LDAP or access control models. These are features that any good encryption product should provide at a minimum.

Key management is a fundamental piece of any encryption strategy. A centralized, easy way to manage keys and separated access controls to ensure the integrity of the data is imperative. This management must consider that the same users responsible for managing the infrastructure are not the same users that should have access to the data being protected. Any authentication and encryption strategy that lacks proper key management separate from the device is questionable. Considerations should also be made, as for any access control strategy, for key strength, scheduled rotation, controlled access, availability, and security of the centralized infrastructure.

An organization could be invested significantly in implementing secure Kerberos/X.509 authentication, both inside the enterprise and for laptop remote access; however, the complexity of authentication challenges is exacerbated with mobility, consumer devices, and especially BYOD programs. Security-conscious IT professionals must look beyond current technologies to those designed for the new challenges that accompany changing realities.

Looking at the Big Picture: Unified Identity and Access

As the use of mobile, cloud computing, and IoT continues its rapid expansion, enterprises are finding that existing implementations of Identity and Access Management are not always able to provide the level of access and trust required. It is becoming necessary to know a person's digital identity across all multiple devices, cloud services, and roles relating to that person.

Ubiquitous computing will succeed or fail on the strength of its identity capabilities.

Digital identity is the data that uniquely describes a person or a thing and contains information about the subject's relationships. Identity management is focused on the management of digital identities and using these identities to enable secure online interchange between some combination of people and systems. Digital identity *claims* or *assertions* are the basis of establishing such trusting relationships between digital subjects.

The most common form of digital identity has been the tried and true user name and password. However, this is an imprecise method to determine the identity of a person in the digital space. Although these attributes are associated with a person's digital identity, they can be easily replicated by others who simply know the credentials. Combined with this simple-to-acquire knowledge is the fact that there are many authentication systems and digital identifiers for every system, device, and application, creating a need for a unified and verified identification system. Thus, there are numerous issues of privacy and security related to digital identity.

A flexible, unified approach that puts identity at the heart of its strategy will allow companies to address near-term mobile security challenges, while positioning their organizations to address future ubiquitous computing security needs. In particular, an identity-based security model that incorporates secure application delivery, mobile application management, and containerization will offer the framework to address key vulnerabilities while alleviating many of the challenges and fragmentation issues associated with device-centric strategies. Identity management, secure application delivery, MAM, and containerization are fundamental to a mobile security strategy and platforms designed to empower ubiquitous environments.

Modular: With a set of new access demands, a security strategy needs to take into account the complexity caused by multiple users, devices, access points, and privileges to company data. At the same time, the strategy needs to protect legacy applications and services. While addressing immediate needs around mobile access management, organizations should consider a solution that also enables modular expansion for new and changing requirements over time.

Scalable: The number of users can expand exponentially from thousands of users to millions of users in a short period of time and over several geographic locations. An identity system needs to be scalable and dynamic enough to handle these changes and serve content regardless of location.

Borderless: With the Internet of Things, everywhere, all the time ubiquitous computing is occurring. Companies need to provide “borderless” and secure access to applications that are not only stored on premises, but also in the cloud and accessed from any Internet-connected device.

Context: Traditional IAM dealt with a set of specific tasks and static data, but IAM can also help companies better engage with stakeholders based on context and behavior. As such, it must be intelligent enough to evaluate different circumstances and make the best judgment, for example using adaptive and two-factor authentication when a user logs in from an atypical device.

Along with identity, authentication remains at the core of information security. Once authentication is compromised, security controls are ineffective. Strong authentication controls must be balanced with usability. By mapping authentication to applications, the enterprise can implement a complex identity management strategy that does not impede usability. Authentication extends beyond user name (who the user is) and password (what the user knows), and in many instances the access token (what the user has), by adding location (where the user is) and transaction (what the user wants) information. Where tokens are widely used to describe what a user has, the device becomes the token. With the addition of these types of specific mappings, it becomes considerably more difficult to successfully exfiltrate enterprise information. It is important that authentication shares a single identity across a wide spectrum of devices. This simplifies the user experience with a consistent authentication method regardless of the device in use.

Enterprises need to address the needs of internal employees, business partners, contract workers, and customers when providing identity and access directly to applications, information, and services. Every person, regardless of his or her associations, is provided specific access on an as-needed basis. The level of control of permissions and usage of the information within the application is defined with each application itself.

Ubiquitous Computing Requires Dynamic Trust

Segmented networks still rely on flat trust models. With the extension of the enterprise perimeter beyond traditional architecture to enable the sharing of information beyond employees to partners, customers, and devices, trust must become dynamic. The trust level of a user is dynamic, and depends on the security posture of the device in use at a given point in time. In this case, trust is not static. It is contextual.

Trust Is Not Static. It Is Contextual.

Ubiquitous computing environments serve resources to individuals based on what is appropriate for each individual in a particular context. They mediate identity, relations, public and private spaces, and ability. They should be designed with a critical awareness of the politics of visibility. First, do the environments permit individuals to claim a particular identity in a particular context? They should facilitate separable contexts and separable identifiers. A person should be allowed the appropriate level of access to the appropriate resources at the appropriate time. Second, do the environments provide a context from which to produce knowledge, and permit the formation of trusted groups able to share information and collaborate with one another? Finally, do the environments permit the claiming of their resources? They should make their own workings controllable and facilitate control of the knowledge produced by their members.

In a heterogeneous environment imposed by mobility and the Internet of Things, it is very difficult, if not impossible, to build a one-size-fits-all approach that accommodates all diverse requirements without context. Adaptation is required to address the mismatch problem between multiple clients, users, and servers. For secure access, there are two requirements. On the user side, different configurations, such as device profiles, location, and device state, must be considered. On the service side, there exist different data formats, security requirements, and so on. Hence, we have to adapt access control policies to such diverse situations.

Adaptive access requires an extensive set of capabilities, including device fingerprinting, real-time behavioral profiling, and risk analytics. This approach requires risk-based authentication methods, taking into account the dynamic environment in which the devices reside. Adaptive access must balance

the level of authentication required of a digital identity on a continuous basis with the ability to adapt and enhance the level of challenge response based on current conditions.

With adaptive access, corporations can protect themselves and their online users against potent fraudulent attacks—such as phishing, malware, transaction, and insider fraud—in a cost-effective manner.

Security policies should dynamically adjust when user access originates from a mobile device. This improves the range of analysis and accuracy of the risk evaluation, which reduces false positives. For example, IP geolocation velocity rules behave differently if the access request is via a cell connection rather than a WIFI connection. The goal is to provide device fingerprinting, registration, risk analysis, and risk-based challenge mechanisms, as well as lost and stolen device management. With risk-awareness, the enterprise can enable new business opportunities that otherwise wouldn't be possible. Employees can work from anywhere with any device because they have secure communication. Partners can directly access inventory; customers can access support data. There are many possibilities.

Conclusions and Guidance

The world has changed, and end-users are in control. They demand a simplified user experience and will not tolerate barriers or hurdles in the name of security. This ubiquitous computing has numerous business benefits, enabling productivity and interaction with partners and customers at an unparalleled level. In this new model of ubiquitous computing, trust at the endpoint no longer exists. The challenge is to enable trusted connectivity from untrusted devices. And the approach needs to be smart and contextual.

Mobile security is no longer about managing the device. It is about enabling secure access to data on unmanaged devices. It is also about ensuring a consistent experience for a single digital identity across multiple devices. Security policies for mobile should be consistent with other points of access. Access via mobile should be a part of overall enterprise access: a single point of management and a single point of audit.

Mobile security is no longer about managing a device. It is about enabling secure access to data on unmanaged devices.

The future of mobile security requires a unified approach to access management across any device and any application. Mobile-only security solutions make no sense because there is no context, no intelligence, and no unified view of a user's access.

Enterprises must provide tiered levels of service, authentication, and access for the disparate populations of users and devices within their organization. The challenge is to provide this tiered level of service, authentication, and access for groups of users, and to ensure that critical data is only shared among users that have gained the appropriate level of access from their devices – or else it is all for naught.

This white paper was sponsored by:

Oracle understands that in a world of ubiquitous computing, context is a necessary component of trust. Organizations can no longer rely on the device itself to be secure and solutions that attempt to reduce risk by more strictly inserting roadblocks into the user experience will only serve to divert activity through other, less secure channels. Context allows organizations to provide a seamless experience that matches user expectations for a mobile computing environment while still elevating assurance for high-risk activity.

Oracle provides a unified, risk-aware approach to access management across enterprise, cloud, social, and mobile environments that includes: 1) secure mobile apps for Oracle applications, 2) in-app security integrated with Oracle enterprise Access Management solutions, and 3) management and security for third party apps supporting an employee-centric BYOD strategy. Oracle mobile security solutions serve both enterprise and public-facing consumer scenarios.

For more information on the Oracle Access Management platform and Oracle Mobile Security, please visit Oracle's website at http://www.oracle.com/identity