AN ORACLE WHITE PAPER | APRIL 2014

The New Perimeter: Keeping Corporate Data Secure in the Mobility Era

IEEE computer society

ORACLE

next page

Contents

Introduction

The corporate enterprise is moving deeper into the mobile realm. This evolution, well underway, is accelerating in the mobile app economy as companies enable employees to conduct more of their business activities via smart phones and tablets and to access cloud and on-premise services via mobile apps.

The motivation for this shift is clear: mobility removes many barriers inherent in traditional business, enabling companies to reshape their organizations and processes for the digital data economy. The shift substantially improves efficiencies and productivities and it enables companies to optimize real-time decision-making at all levels in their organizations, introducing cost savings as it creates these new opportunities. But while mobility enables companies to transcend previous limitations, it makes the traditional security perimeter appear brittle as data can now move unrestricted to a mobile device from resources that were previously secured behind the firewall. This change in computing is visibly pushing the perimeter away from the corporate domain and out to the device. The change is introducing new risks and it is also prompting new questions about ownership and control of digitized information.

Today and in the future, IT organizations need to secure this new perimeter if they want to fully exploit mobility's benefits. The purpose of this paper is to describe the transformation of the corporate perimeter; explore the challenges it presents to corporations as they externalize their data for employees, partners and customers; suggest new and emerging solutions that will help organizations protect their data assets; and offer practical guidance for companies that want to take steps now to reduce security risks.

Contents

The Traditional Perimeter for Web Computing

In the era of web computing, the corporate perimeter has been defined by the firewall on the corporate network and for the last couple decades, firewall technologies* have protected company information for all types of businesses. Generally in this environment, a browser installed on a user's desktop or a laptop provides a thin client and access to data from a server, conveniently enabling the user to consume web pages and data at the presentation and application layers of the network. Companies have invested substantial amounts of time, money and resources on firewall technologies to protect data accessed via the browser and they've employed the necessary network security tools to help secure the transmission and exchange of company information.

The firewall facilitated a paradigm shift from the pre-Internet era, when computing systems were interconnected over private connections, to the Internet era in which computing could take place in "trusted" and "untrusted" environments and firewalls enforced access policies to keep backend databases and servers secure. And now, as organizations increase their reliance on mobility solutions, another paradigm shift is occurring. Today, mobile applications are pulling data out of the brick-and-mortar establishment's firewall-protected data center and transmitting data to and from hybrid computing infrastructures that are accessible by the corporation, partners and customers on any mobile devices that these entities and individuals might use. Because a user's identity is affiliated with their mobile devices, companies can now extend user entitlements to the mobile device, extending access privileges to company data via mobile platforms. In this context, the notion of the firewall as corporate perimeter is no longer applicable. Businesses need to understand this new paradigm shift and prepare their organizations to protect the evolving and increasingly complicated perimeter that mobility creates.

* The reference to firewall technologies is for the larger category of products and network infrastructure deployed at the edge of a corporate network. This could include a traditional firewall, a VPN gateway, an NAC appliance, etc.

Contents

The New Perimeter in the Mobility Era

The new perimeter is defined as the end point where data consumption occurs. The perimeter is influenced by all the people, devices, and data that access the network. It is a diverse and always-changing environment. People accessing the network can include company employees, contractors, customers and partners. Devices can include a wide range of smart phones, servers, laptops, tablets, and even connected components in the "Internet of Things" that provide remote data-gathering and communications functions for businesses. The data can include structured information from corporate databases and other company-controlled resources as well as unstructured data such as access credentials, documents, files, and local copies of intranet websites.

The new perimeter is enabled by the broad market adoption of mobile device platforms, cloud services and mobile applications.

Smartphone adoption is contributing significantly to this new perimeter. Smartphone adoption has advanced so rapidly that in 2016 there will be more subscriptions globally for smartphones than basic mobile phones subscriptions, according to Ericsson. The telecommunications infrastructure vendor estimates that in 2019, worldwide smartphone subscriptions will reach 5.6 billion, up from 1.9 billion in 2013. It expects the number of mobile PCs, tablets and mobile routers affiliated with cellular subscriptions to reach 800 billion in 2019, up from 300 million in 2013. The connected device segment does not include Wi-Fi-only devices, which is another sizeable segment.[1]

The new perimeter is defined as the end point where data consumption occurs. The perimeter is influenced by all the people, devices, and data that access the network. It is a diverse and always-changing environment.

Contents

These types of mobility trends are pervading the corporate environment. In particular, the bring-your-own-device (BYOD) phenomenon, created by employees who are using their own devices in the workplace, is becoming increasingly common. The research firm Gartner says that 38% of CIOs will stop providing devices to their employees by 2016 and 45% will stop by 2020.[2]

A variety of web services enabled by application programming interfaces (APIs) are used to deliver data on demand from servers to native apps that function like thick clients on the mobile device. Because of the advanced computing capabilities of today's mobile devices, data that previously resided only in the data center can now be manipulated and stored locally on the device. An end user can view and analyze data on the device, online or offline, and in rich formats that are comparable to the formats offered by desktop computers. Employees, business partners and customers appreciate mobile-accessible services because the approach can offer practical features and apps and an effective user interface and the conveniences improve productivity and efficiencies. With APIs, IT is able to fully manage services so that employees and customers can have access to appropriate applications and data, yet the service costs are substantially lower than the costs associated with traditional IT infrastructure.

The prolific app economy is helping fuel the use of private and public cloud services and native apps. Gartner expects that by 2016, there will be more than 300 billion app downloads annually from mobile app stores.[3] By 2017, the firm expects that 25% of enterprises will have enterprise app stores for managing corporate-sanctioned apps on mobile devices and PCs.[4]

Contents

Extending the Perimeter to Enter the Digital Data Economy

To succeed in today's extremely competitive business markets, companies need to function and make decisions in a real-time context. They must free their businesses from traditional processes that are relics of a paper-based economy and convert to digital data capture technologies. Mobility platforms and applications that operate on smart phones, tablets and other devices are enabling companies to transition to this more dynamic and better-informed environment. Industry segments that have begun the transition are already exhibiting its value.

In healthcare, for example, the recent industry-wide shift to electronic medical records (EMRs) is now enabling providers to capture patient data on mobile devices for both mobile and routine, on-site tasks. CDW Healthcare, citing various studies, reported that 66% of doctors already use tablets for medical purposes and 70% of healthcare provider organizations use mobile devices to access EMRs.[5] Yet another study, conducted by Float Mobile Learning, found that 56% of doctors who use mobile devices say it expedites decision making.[6]

Retailers and manufacturers have found that mobility improves the supply chain. A survey conducted by IDC, for example, found that mobility creates collaboration capabilities and introduces new innovation opportunities across retail and manufacturing. The firm reported that new data collection tools, mobile apps and smart devices improve core processes and functions in these sectors. It noted that manufacturers are using mobility to improve fulfillment functions and strengthen visibility of products throughout the supply chain and that retailers are using apps for mobile commerce and improved productivity.[7] Another study, reported by IHS Technology, found that increasing numbers of manufacturing employees are using smartphones and tablets to remotely manage equipment and observe processes, whether the employees are working offsite or monitoring equipment from various locations within a facility.[8]

Contents

The Extended Perimeter's Challenges and Risks

Companies must find ways to keep the extended perimeter secured as the point of data consumption moves farther and farther away from the corporate intranet and firewall to the device. This new business requirement is not without challenges.

The perimeter is evolving constantly and rapidly because the device market is constantly changing. It is very difficult in this environment for security technologies and tools to keep pace. On any given day, a corporation might confront the introduction of new devices on the market, new form factors that influence how company data is accessed or viewed, operating system upgrades, and software updates. The expansive app ecosystem is populated with products that are vulnerable to malware and other attacks and the devices themselves can be lost or stolen.

BYOD exacerbates many of these risks. Many companies have learned that they can't prevent employees from using their own devices, yet companies can be exposed to new vulnerabilities when employees use apps and access corporate data for work from their personal devices. For example, the mobile apps employees use might have security flaws or provide exposure to malware. Employees might use weak passwords (or no passwords at all) and they might make extensive use of unsecured networks, like public Wi-Fi hotspots, when working from airports, hotels or other venues. Additionally, employees might use apps that store passwords to corporate applications; this practice, while convenient, can introduce a vulnerability to Single Sign-on tools.

In recent years, companies have used a variety

The perimeter is evolving constantly and rapidly because the device market is constantly changing. It is very difficult in this environment for security technologies and tools to keep pace.

Contents

of methods to manage BYOD as well as corporate-owned, personally enabled (COPE) devices, but first-generation approaches have not been able to effectively satisfy both IT and employee priorities. Preventing the comingling of corporate and personal data on these devices has become a fundamental issue. Companies have tried simply limiting the use of personal features on devices, but this strategy is not friendly to employees who want to use their devices for personal email, applications and features during non-work hours. Virtual desktop infrastructure (VDI), which gives employees remote access to business apps, has enabled companies to remotely control what their employees use on their devices, but the approach is expensive and does not facilitate use of corporate apps locally, nor does it facilitate use of data offline. Dual-boot or dual-persona access tools can separate corporate and personal content by requiring employees to log in and out of each environment on their devices. But this approach has drawbacks too because it is not available on all devices and OSes and it is a significant inconvenience to the users. Such strategies can actually become counterproductive for companies if the security methods present a barrier to use and dissuade employees from taking full advantage of mobile enterprise applications and tools.

As the industry has pursued improved strategies to address mobile perimeter challenges and risks, a variety of discrete products has emerged that companies can choose from, adopt, and deploy, as desired, to manage access to corporate applications and data. These include mobile device management (MDM) and mobile application management (MAM) tools, among others.

MDM has been widely adopted by companies seeking to manage the hardware accessing their networks. With MDM, the IT department can control which apps employees can install and which Wi-Fi access points can be used. IT can also require users to employ PINs to access their devices. But MDM software can be intrusive and cumbersome for users and it does not prevent data leakage, which can occur during some routine processes. Many

In recent years, companies have used a variety of methods to manage BYOD as well as corporate-owned, personally enabled (COPE) devices, but first-generation approaches have not been able to effectively satisfy both IT and employee priorities. Preventing the comingling of corporate and personal data on these devices has become a fundamental issue.

Contents

corporations are now looking at MAM to control corporate and employee applications and services in a way that satisfies both IT and employee priorities. MAM goes beyond device-centric strategies by enabling companies to provision and manage apps on a very granular level to form a secure boundary between corporate and personal data.

MDM, MAM, and other more specific techniques such as identity management, secure containers, secure-access and Single Sign-on tools are gaining traction among corporations, but crafting a coherent security strategy with a variety of discrete products can be problematic for many companies and often is not viable for the long term. The fragmented market supplying individual solutions adds costs and complexity for enterprises that seek to integrate security functions to optimize mobility's business benefits. Fragmentation increases costs because companies must purchase multiple products and the expenses required to support, manage and maintain multiple management tools increase accordingly. Fragmentation also produces mobile security data silos, which generate fragmented views of data and services to the enterprise and create associated challenges for security auditing and compliance activities.

Contents

Data Ownership and Data Sprawl

As companies strive to minimize mobility's challenges and risks, they should also pay attention to two additional and very important concerns: who owns the data and where is the data?

Data ownership questions arise when corporate data is delivered on devices or infrastructure that is not owned by the corporation and when an employee's identity-based corporate credentials facilitate access to corporate data yet the data is still controlled by IT. Data sprawl questions are created when corporations lose the ability to know precisely where their data is and who is using it. This is an increasingly challenging problem for companies today because smart phones, tablets and mobile apps make it extremely easy for employees to use and share data on their devices and the devices can store any type of data, from emails to proprietary materials to large graphics and video files.

The IT industry is focused on developing new innovations that will help the enterprise better understand data ownership and data sprawl. Two important problems must be solved to effectively address these issues.

First, now that the corporate perimeter is extended to the end point where data consumption occurs, companies must have the ability to connect an identity to every piece of data that is stored, used and transmitted. This capability must extend to all data even as the data is transmitted to and from users in different departments and different companies, across systems and geographies and even as the data reaches out to remote and embedded devices that make up the Internet of Things.

Attaching an identity to all data will benefit companies because it puts identity at the heart of all solutions. In its most basic implementation, a company could use the identity associated with a device to assign a policy to data used by the device. This would give the company the ability to control the data as it is stored and transmitted and the capability to allow or prevent access to the data. Many types of business processes and proprietary information could be protected by this capability. For example, if a company is issuing an RFP to vendors, the company could attach an identity to the RFP and track the RFP's access as it is transmitted to

Contents

and from various users such as the RFP originator, a vendor's sales manager, and the company's lawyer. Certainly, this can be done to a certain extent today, but an architecture has yet to emerge that can fully facilitate this capability across systems and track the destiny of corporate information to the farthest edges of the perimeter. This is an important area of development in the industry today.

Secondly, corporations must have the ability to securely shred any data that belongs to the company. In the world of traditional physical documents, companies have ongoing needs to eliminate business records and shredding services are widely available to provide this function. The industry must better develop this capability for the distributed computing environment and particularly as corporate data moves out to the new perimeter. Appropriate architectures must be developed to ensure that data can be permanently deleted by IT. This represents another measure of control over data sprawl and it is another important area of development in the industry today. Emerging solutions will likely leverage identity solutions to enable this capability.

Contents

The Need for Next-Generation Mobile Security Solutions

Security is a business enabler. Because mobile security minimizes risks, it gives corporations the confidence they need to exploit the many benefits mobility offers to their businesses. Analyst firms are noting the correlation between mobile security and business improvements and the impact can be substantial. PricewaterhouseCoopers, for example, asserts that companies can realize 25% improvements in business performance if they carefully prepare their businesses to address mobile security vulnerabilities.

"To balance data safeguards against the productivity and employee satisfaction that portable devices enable, organizations must implement a rigorous, comprehensive framework for security. Correctly developed and deployed, an effective mobility strategy can produce productivity gains as high as 25 percent across an organization," the firm reported.[9]

The next generation of mobile security strategies now emerging should enable enterprises to provide a comprehensive framework while minimizing the fragmentation challenges associated with

"To balance data safeguards against the productivity and employee satisfaction that portable devices enable, organizations must implement a rigorous, comprehensive framework for security. Correctly developed and deployed, an effective mobility strategy can produce productivity gains as high as 25 percent across an organization." — PricewaterhouseCoopers

Contents

earlier technologies. Gartner, for example, is emphasizing this shift. The analyst firm has stopped tracking MDM as a product category and is advocating that enterprises focus instead on integrated enterprise mobility management solutions.[10] Integrated solutions can include all necessary security capabilities in one system and enable companies to select and implement the technologies as part of a larger platform to secure their apps and content.

The IT industry is architecting next-generation approaches that will yield a comprehensive framework while providing better options for corporations. Among other advantages, these new solutions will give companies the ability to balance the needs of both IT and users in the rapidly changing mobile environment; allow corporate and personal applications and data to coexist on a device independently from one another; and help break down existing mobile security silos. The solutions will help businesses pursue the many business efficiencies, productivity, and decision-making benefits that mobility offers. The most effective solutions will address the new perimeter's three end points: people, devices and data.

Contents

Take Steps Now to Secure the New Perimeter

As industry innovates to craft new architectures to address new and emerging security concerns, enterprises can take fundamentally important steps today to reduce the security risks associated with the evolving perimeter.

Step 1: Associate an identity with anything that connects to data that is owned or curated by the corporation

Many companies overlook the importance of identity and as a result identity is often a gap in business IT security practices. But identity is a powerful tool. It can be applied to people, devices as well as data and therefore plays a vital role in securing the new perimeter.

Companies should leverage identity management tools so they have the visibility to see any time a company employee connects to an organization's web site, downloads a corporate document, sends or receives a business email, or uses online resources. These capabilities will also help companies address nagging data ownership and data sprawl issues by tracking who has access to data, who uses it, which devices company data resides on, and how it has been shared. Identity-based tools also give individual employees a better understanding of the implications of their data consumption, which can help foster increasingly responsible data usage.

As the central enabler of numerous security tools, identity is also used to centralize and streamline device provisioning, apply policies and entitlements and manage accounts. It facilitates secure access solutions, including Single Sign-on capabilities that streamline access for users. It is also a key ingredient in fraud-detection programs ensuring that entities

Identity is a powerful tool. It can be applied to people, devices as well as data and therefore plays a vital role in securing the new perimeter.

Contents

and individuals attempting network-based transactions are, in fact, who they claim to be.

Step 2: Create a clean boundary between corporate and personal data

Companies must isolate corporate applications and data from within personal devices and they must maintain a secure separation between the two in order to prevent the comingling of corporate and personal data. This is vitally important in today's environment, where employees use BYOD or COPE devices for work as well as personal and family applications.

The most effective approach for creating and managing this boundary is to implement mobile application management in conjunction with secure containers.

MAM is a welcome capability for corporations and employees alike because it focuses on the control of data that is transmitted to and from smart phones and tablets via the applications that are installed on these devices. MAM separates personal and corporate apps, allowing personal and corporate information to coexist independently on the same device while preventing the intermingling of data. It achieves this by facilitating and managing a secure container for corporate apps and data.

MAM is beneficial to both companies and employees because it enables IT to control corporate data while ensuring that employees have flexibility to use their single, preferred device for both business and personal applications and services. At the same time, it ensures corporate data is secure by leveraging identity tools and enforcing PIN and password protections for corporate data access. An employee's personal apps and data are kept out of the container; personal information is not subject to these controls and cannot be accessed by IT.

The container itself is a highly specialized app that runs on a device. It establishes a secure sandbox, or workspace, where all of a company's authorized applications and data are housed. These applications, which can be hosted on the corporate app store, can include business software tools, corporate email and calendar programs, and documents. The container is not dependent on the device OS and can be installed on Android, iOS and other platforms. Employees must securely sign into the

Mobile application management (MAM) separates personal and corporate apps, allowing personal and corporate information to coexist independently on the same device while preventing the intermingling of data.

Contents

container on their devices in order to access corporate apps and data.

Containers are also convenient for companies. The technologies give IT a centralized console that can be used to apply identity-driven security rules to control and manage data access in accordance with company policies. IT can also use the console to enforce and push policies to employees and provision and de-provision all users. IT can track the location of each container and wipe it clean without interfering with the user's personal content. These capabilities are employee-friendly, enabling employees to keep their personal apps and data when they leave a company even though the corporate workspace is deleted.

Step 3: Make sure your security controls do not distract from the user experience

Many of today's tensions at the new perimeter are driven by conflicting needs of IT and end users. IT wants and needs to control company data accessed from mobile devices, but employees want the flexibility to use devices they prefer and enjoy and they want uninhibited freedom to use personal apps and features. The industry is developing strategies to help resolve this tension. In the meantime, companies can take some specific, practical steps to balance these needs.

In particular, companies should make sure the security solutions they adopt are frictionless to the end user and that all application policies and entitlements are clear to users. Companies must also recognize that today's employees, and especially younger generations who will make up the future workforce, will not tolerate cumbersome processes that adversely affect the user experience. IT must anticipate and be able to accommodate these types of workplace trends.

Step 4: Make sure the hardware accessing your network complies with your security policies

Corporations need to know which devices their employees are using and make sure that all devices comply with company security policies.

When provisioning devices for use in the network, IT should make sure it can secure each supported device as well as the applications and services that will operate on the device. IT should also make sure it has capability to block access from any device that is vulnerable, compromised or not supported by the IT organization.

A COPE device environment—in which the devices are physical assets purchased and owned by the company—places a particular responsibility on IT to track and manage each asset. In COPE scenarios, the IT department can employ MDM to enroll and provision each device and enforce corporate policies governing access to software, apps and features.

Contents

A Next-Generation Model: Identity-Based Mobility Management and Oracle's Role

More and more corporations are using mobility solutions, cloud services and mobile applications to succeed in the digital data economy. As these companies look for improved security solutions, they will need next-generation, unified approaches that can effectively secure the corporate perimeter by managing all people, devices and data that interact with the network.

A flexible, integrated platform that puts identity at the heart of its solutions will give companies powerful new capabilities to address near-term mobile security challenges while positioning their organizations to confidently address future mobile security needs. In particular, an identity-based security model that incorporates mobile application management and containerization tools will provide the rigorous, comprehensive framework needed to

A flexible, integrated platform that puts identity at the heart of its solutions will give companies powerful new capabilities to address near-term mobile security challenges while positioning their organizations to confidently address future mobile security needs.

Contents

address key vulnerabilities while alleviating many of the challenges and fragmentation issues associated with traditional, device-centric strategies.

Identity management, MAM and containerization are fundamental to Oracle's mobile security strategy and the solutions it offers to help companies secure the new perimeter. From a single console, IT can employ this family of tools to clarify the ownership of company data, understand data sprawl, create a clear separation of corporate and personal data on employee devices, and balance IT and employee needs.

The three components in Oracle's unified strategy include the following: 1) identity-based management tools that extend enterprise credential-level access onto the mobile platform, allowing users to self-service their accounts and enjoy Single Sign-on features and adding support to company fraud detection solutions; 2) MAM tools that allow corporate and personal data to coexist independently on a device, ensure separation of the data, and secure corporate data that is transmitted to and from corporate applications; and 3) containers or secure workspaces that separate corporate data from personal information on a device and allow companies to remotely wipe corporate information from a device without interfering with personal content.

Contents

Conclusion

The corporate enterprise is becoming increasingly mobile, as companies enable employees to conduct business via smart phones and tablets and access private and public cloud services via mobile apps. Mobility gives companies very real and exciting new opportunities to compete in the digital data economy but to benefit from these opportunities companies must be able to secure corporate data at its farthest reaches: the end points where data consumption occurs. Securing this new perimeter is particularly challenging because it must address BYOD trends and resolve increasingly important data ownership and data sprawl issues, among other concerns. Next-generation security solutions are emerging that enable companies to integrate rigorous, identity-based mobile application management and containerization capabilities to control and protect corporate data while ensuring that employees have private access to the personal apps and services they enjoy. Companies can take practical steps today to put effective, comprehensive mobile security precautions in place.

Learn More

Oracle looks forward to helping enterprises employ the latest mobile security solutions and best practices to secure the new corporate perimeter and fully embrace mobility's benefits.

For more information about Oracle's mobile security strategy, please contact your Oracle account manager or visit the following sites:

ORACLE www.oracle.com/MobileSecurity

www.facebook.com/OracleSecurity

www.twitter.com/OracleIDM

blogs.oracle.com/OracleIDM

Contents

References

1 Ericsson Mobility Report on the Pulse of the Networked Society, Nov. 2013, page 7. http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf

2 Managing Enterprise Mobility, a Gartner presentation by Monica Basso and Rob Smith, 2013.

3 Ibid.

4 "Gartner Says that by 2017, 25 Percent of Enterprises will have an Enterprise App Store," Gartner press release, Feb. 12, 2013. http://www.gartner.com/newsroom/id/2334015

5 "Healthcare Mobility Trends," by CDW Healthcare, August 2013. http://industryview.cdwcommunit.com/index.php/2013/08/15/healthcare-mobility-infographic/

6 "Float Mobile Learning Research Report Suggests mHealth is Poised to Explode in Next Decade," press release, March 13, 2012. http://www.prweb.com/releases/2012/3/prweb9276198.htm

7 "Mobile Technology Trends in Retail and Manufacturing: More Portable and Accessible Information Will Fuel the Supply Chain," by Simon Ellis, practice director, manufacturing insights, IDC, published on the AT&T Networking Exchange Blog, Jan. 20, 2014. http://networkingexchangeblog.att.com/enterprise-business/mobile-technology-trends-retail-manufacturing/

8 "Mobile Devices Invade Factory Floor as BYOD Trend Spreads," IHS press release, Jan. 21, 2014. https://technology.ihs.com/483340/mobile-devices-invade-factory-floor-as-byod-trend-spreads

9 Managing Security in a Mobile World, report published by PricewaterhouseCoopers, 2012, page 5. http://www.pwc.com/en_us/us/it-risk-security/assets/managing-security-in-a-mobile-world.pdf

10 Managing Enterprise Mobility, a Gartner presentation by Monica Basso and Rob Smith, 2013.