An Oracle White Paper
April 2014

The Oracle Mobile Security Suite: Secure Adoption of BYOD

Executive Overview

BYOD (Bring Your Own Device) is the new mobile security imperative and every organization will need to adopt internal policies to allow employees the flexibility to use personal devices for work purposes.

By 2015 there will be as many as 6.7 billion personal smartphones used globally for both work and personal purposes. The proliferation of personal devices has caught many IT organizations un-prepared for the new security requirements and regulatory challenges.[1] In fact, 89% of employees are using smartphone devices for work, and nearly half of them are doing so without the permission of their employer. [2]

The proliferation is complicated by the variety of platforms and operating system versions that make it difficult for security teams to adapt consistent policy and enforcement across devices.

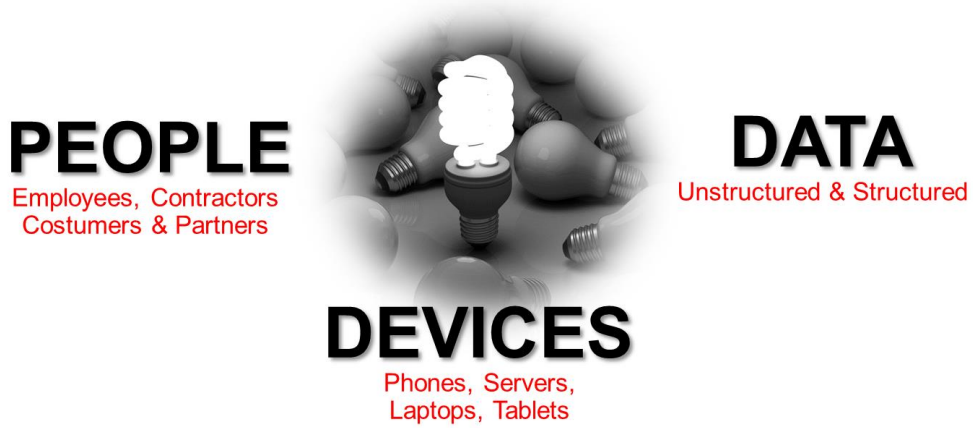
The rules have changed:

- Mobile devices have redefined perimeter security
- The network is no longer the main point of control
- The new security perimeter is users, devices, and data

The new security model must incorporate controls around users, enterprise data, and all of the devices that access corporate resources. New business transformation requirements are re-defining the boundary of the network perimeter; examples include use of cloud storage and applications, access portals for partners and customers, and employee collaboration on mobile and social networks.

[1] Gartner, (2012)

[2] http://www.csoonline.com/article/706335/companies-slow-to-react-to-mobile-security-threat



All of this means IT organizations must transform in order to address the new security requirements of a BYOD economy that enables new paths to market and empowers employee productivity.

Pressures to Adopt BYOD

Lines of business are driving IT to adopt mobile platform support for employees so they may have greater access to near real-time information. According to a recent CIO Mobility Survey, 67% of CIOs and IT leaders feel mobility will impact their business as much, or more, than the Internet did in the 90's.[3] They realize an opportunity to gain employee efficiencies because of real-time availability and extended 24x7 collaboration.

However, employees are combining work and pleasure, and enterprise data is exposed alongside personal data. How do you manage personal and corporate devices under a unified security policy that protects organizational assets, while providing flexibility for personal use? To accomplish this, IT organizations must incorporate tighter security controls around people, devices, and data. Since identity is central to the issue, organizations must simplify device provisioning and lifecycle management.

[3] http://www.ciosummits.com/Tangoe_WhitePaper_-_The_Dos_and_Donts_of_Mobile_Application_Management.pdf

Mobile Device Risk

Recent data shows that the single greatest target for the mobile platform is credential theft. Today, 76% of all enterprise data breaches are the result of weak or stolen credentials.[4] If a cybercriminal gains access to a privileged user's mobile device, they can potentially find privileged credentials to further penetrate the organization. Though indispensable, mobile devices face several vulnerabilities that organizations must contend with to get started in support of BYOD initiatives.

Mobile Malware

Mobile malware has increased 58% from 2011 to 2012. In addition, out of all known malware, 59% target mobile platforms.[5] The most common activity carried out by malware today is stealing sensitive data on the device, including but not limited to the theft of device and application credentials.[4] In 2012, nearly a quarter of all attacks targeted the manufacturing industry with a goal of stealing trade secrets.[6] Half of all attacks target organizations of 2,500 employees or more.[4] It's no surprise that mobile devices are a key target for cybercriminals, because gaining access to the device potentially provides access to employee credentials used in these targeted attacks.

Lost or Stolen Devices

In the US alone, 113 cell phones are lost or stolen every minute.[7] Today 84% of organizations have a firm policy that departing employees must surrender their personal devices.[8] Organizations should consider what might the end user delete, or retain, before turning their devices in. Often there are no consistent and common policies across mobile devices, whether personal or corporate owned. This makes onboarding and off boarding difficult and jeopardizes corporate data and access.

Application Management

Applications have quickly become the greatest enabler for businesses to empower their employees with real time data. Unfortunately, applications can be a conduit for privileged access abuse, misuse, and data theft; often through secondary applications and malicious code that steals credentials or leverages unauthorized connections. Therefore, IT organizations are deploying their own enterprise application catalogs to distribute secure and vetted applications. It is predicted that 25% of enterprises will have

[4] 2013 Verizon Data Breach Investigations Report

[5] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[6] https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov16986&S_TACT=102PW63W

[7] http://us.protectyourbubble.com/

[8] http://mobileenterprise.edgl.com/news/Surprising-Stats-About-Mobile-Security84688

their own application stores by 2017, enabling organizations to provision multiple corporate applications for employees, customers, and partners.[9]

The New Security Requirements

There must be a balance between securing enterprise application data and maintaining employee privacy. Many solutions today follow a device-centric approach (Mobile Device Management) that is intrusive and does not meet requirements for secure adoption of BYOD. MDM solutions treat all data on the device as property of the corporation, without respecting the boundaries between corporate and personal application data. This has given rise to a new set of customer expectations.

Identity Management

IT recognizes the key to managing people, data and devices, is through identity. Identity is the central component of how mobile devices will access content, applications, secured communications and more. Therefore, it is critical to leverage an identity management infrastracture to enable a mobility platform.

Secure Container

The key to a next generation mobile security policy is being able to separate the business application data from the personal application data. Containers are used to create a secure workspace environment where authorized applications and data reside. This provides the benefit of applying identity-driven security policies that can easily be provisioned and deprovisioned, without third-party application interference.

Single Sign-on

To reduce mobile device credential theft organizations need stronger authentication methods using a certificate-based approach, strong passwords, and unified Single Sign-on. This allows one set of credentials to authenticate many different applications and services, each with their own unique credentials. Employees no longer need to remember complex and unique credentials for each account.

Application Management

Appropriate application management supports provisioning and deprovisioning of approved and secured applications for mobile devices. Many organizations are establishing requirements for their own enterprise application stores for sourcing approved and secured applications for their mobile platforms in an effort to reduce risk and exposure. This is also an enablement platform that allows

[9] http://www.gartner.com/newsroom/id/2334015

organizations to simplify a workflow process of procuring standardized sets of applications to employees.

VPN Independent

As organizations move to the mobile platform, there is a shift from session-level encryption, such as VPN, to application-specific encryption that reduces exposure and risk to the organization. Session-level encryption is a doorway that allows malware, or unauthorized connections, to share VPN sessions. This potentially provides cybercriminals direct and unfettered access to sensitive enterprise data and systems. By eliminating VPN, organizations can reduce bandwidth costs associated with non-business related Internet traffic passing through corporate networks.

Device Provisioning

Provisioning a device shouldn't be a multi-step process anymore. This should be part of a new-hire automated workflow that sets up the accounts associated with a new user. As part of new device ordering, the workflow must tie the device order to the new user's "identity." A new policy can be provisioned, along with all associated applications, before the user is granted access to the device.

Multi-user Devices

One of the newest, and arguably most difficult to address, requirements is to provide secure access to applications and resources on shared devices, while retaining the privacy of patients, customers, and employees. This is often found in environments, such as healthcare and manufacturing, where shared devices are common.

Lost & Stolen Devices

Rather than wipe entire devices if they are lost or stolen, organizations can use secure containers to selectively delete only corporate applications, and data. This enables employees the added flexibility of using personal devices and content, without interference by, or to, enterprise data and applications.

Oracle's Mobile Security Strategy

Oracle's mobile security strategy separates corporate application data from personal data to allow employees the freedom of using personal devices at work, without compromising corporate security.

Containers

Using a technique called containerization, the Oracle Mobile Security Suite creates a secure workspace in which corporate applications, email, and data are stored. Only authenticated users can access the secure workspace to run the applications and access data, and only applications provisioned or approved by corporate IT can be installed and executed from within this secure workspace. All personal applications, photos, and content are managed and accessible by the employee and controlled through data policies that limit how the content can be shared, viewed, printed and more. If the device is lost or stolen, corporate IT can remotely wipe the secure workspace without affecting any personal data.

Controls

With Oracle Mobile Security Suite, application policies and entitlements are provisioned based on role, location, time, or other context variables. Organizations can automatically provision and de-provision applications to mobile users as they depart or enter new countries that may have restrictive policies. Policies are not hard-coded, but enforced at run-time when an application is executed in the container, or an authenticated user accesses the container. Because of this, a secure workspace always has the latest access policies and application entitlements. New applications can be added to the corporate application store to extend approved, in-house or 3rd party, applications based on user roles.

Experience

With capabilities like role-based user access, Oracle Mobile Security Suite can extend the same credential level access from within the enterprise to the mobile platform, leveraging the same identity and policy framework. This greatly reduces complexity and cost by using self-service for account management, including password resets and support issues. Additionally, by using Oracle Single Sign-On users can authenticate once, with a strong set of credentials, and gain access to all of their applications and services within the secure workspace.

SUPERVALU Strengthens Customer Relationships

SUPERVALU is a US-based grocery retail and food logistics organization with over 4,700 company and franchised owned locations servicing 130,000 employees. One of their objectives was to provide store managers with Apple iPads, so they may have immediate access to store data. Key requirements included simplified iPad provisioning with associated policies, risk-based authentication, and secure access to real-time inventory data.

Using Oracle Mobile Security Suite, SUPERVALU's store directors are now able to securely access back office applications using iPads to manage their respective SUPERVALU retail locations from anywhere on the store floor. This has resulted in increased productivity and the ability to spend more face-to-face time with customers.

In Summary

Oracle Mobile Security Suite is helping organizations face the transformation of the network perimeter to mobile devices. Oracle Mobile Security Suite achieves the goal of securing People, Data and Devices with a multi-layered approach to securing the mobile device. Oracle does this by containing the risks through application containers, then by controlling the risks through application and policy controls. Last, Oracle manages the overall experience by extending the identity management frameworks onto the mobile device providing capabilities such as Single Sign-on the mobile platform.

Oracle provides the structured architecture that separates both personal and corporate applications and data on the same device, and applies policies independent of one another, so corporate data is always secured, and personal flexibilities are maintained. Oracle is driven by the core belief that mobile security should not be driven by a policy of device control at the cost of personal freedoms, nor should personal freedoms over-ride corporate security needs.

For more information on Oracle's Mobile Security Strategy, please visit:
www.Oracle.com/MobileSecurity

Oracle Mobile Security Suite
2014

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0113

Hardware and Software, Engineered to Work Together