UBM TechWeb

A UBM TECH WHITE PAPER

SEPTEMBER 2013

Mobile Security: How to Protect the Enterprise in the Mobile Era

3 pillars give users the flexibility and access they want and need, while providing a strong foundation to protect systems and data.

Brought to you by

DELL Software

Mobile Security: How to Protect the Enterprise in the Mobile Era

3 pillars give users the flexibility and access they want and need, while providing a strong foundation to protect systems and data.

The way people work has fundamentally changed, and mobile devices are at the forefront of this shift. Workers are no longer chained to their offices. They can work anywhere at any time — and they do.

The world's mobile worker population is expected to top the 1.3 billion mark — more than one-third of the total workforce — by 2015, according to a recent IDC study. Meanwhile, Gartner predicts that tablet sales will surpass desktop and laptop sales by 2017, and more than 1 billion smartphones will be sold this year alone. Gartner also predicts that by 2016 38 percent of companies worldwide will have stopped buying devices for their employees, opting for a bring-your-own-device (BYOD) policy instead.

The phenomenal growth of mobile and BYOD stems from convenience and habit. The ever-growing population of mobile users has become accustomed to having the Internet, as well as email and calendaring applications, at their fingertips. Today, they're also demanding mobile access to business-critical applications and the ability to choose their corporate device or use their own. And companies are finding that these capabilities provide the flexibility and access needed to increase employee productivity and spur innovation. Some companies may also find it becomes easier to attract and retain Generation Y and Z employees, who have grown up using mobile devices.

Who's Watching the Store?

As with any new strategy, there are problems and challenges that IT in particular faces when supporting a mobile or BYOD strategy. Mobile devices are often lost or stolen, which makes the data on them, as well as the corporate network, vulnerable to unauthorized access. In fact, data loss from lost, stolen and decommissioned devices is the top mobile security concern in the enterprise, according to an October 2012 Cloud Security Alliance Working Group report, "Top Mobile Threats." There are other security concerns as well. A mobile device can become a conduit for malware from rogue apps. In addition, unless data is encrypted in flight, it's susceptible to interception, especially when users are on public Wi-Fi networks.

Compliance is another obstacle. Just who owns the data created and sitting on mobile devices isn't always clear. In the BYOD world, some organizations insist that company data on employee-owned phones and tablets still belongs to the company and that it should be allowed to back up and archive that data for legal and regulatory compliance purposes. Meanwhile, companies also are grappling with the issue of advertisers and app vendors hijacking corporate data on employee- and corporate-owned devices.

Beyond the data ownership debate, it can be difficult to back up, archive and store data that

TOP FIVE MOBILE THREATS

1. Data loss from lost, stolen or decommissioned devices
2. Information-stealing mobile malware
3. Data loss and data leakage through poorly written third-party applications
4. Vulnerabilities within devices, OS, design and third-party applications
5. Insecure Wi-Fi network or rogue access points

Data: The Cloud Security Alliance Mobile Working Group, "Top Mobile Threats," October 2012

resides on a corporate-owned mobile device, and it's even more difficult to do that on an employee-owned device. Unless a device has been locked down, there's also a chance that an employee will move corporate data into the cloud or that it will be lifted directly from the device by an ad network or a cybercriminal. One technology company found 496 apps "primarily for data storage, communications and collaboration" on employee smartphones, according to *The New York Times'* article, "Where Apps Meet Work, Secret Data Is at Risk." That same story detailed a number of high-profile data losses and thefts from mobile devices.

When you look at the mobile landscape ... what's clear is that most organizations need more mobile security than existing MDM and MAM products provide.

Finally, companies that have a BYOD strategy may struggle to integrate those devices with their legacy infrastructure. Even companies that issue their own devices can have trouble finding security and management software that ties those mobile devices into the corporate network and data center. Rights management is challenging, too. IT is often hard-pressed to provide users with the appropriate level of access to files and applications to do their jobs. With budgets flat and staffing levels stagnant or down, IT must do all of the above without deploying expensive, complex or redundant mobile infrastructures.

Access Control 1.0

While policies and user education are extremely important in the mobile security world, they are only a part of an overall mobile device strategy. To date, companies are using two technologies to manage many of the above issues — mobile device management (MDM) and mobile application management (MAM). MDM functions as a single point of contact and control for the management of mobile devices. A typical MDM solution provides software distribution as well as policy, inventory, security and service management for mobile devices.

MDM lets IT track which devices have been given access to the network, push out security updates to them, and configure new and existing devices based on employees' roles and rights. The software also lets IT push out configurations, policies and apps automatically or on demand to all or some managed devices or even to a single one. Also important: MDM gives IT the ability to disable lost and stolen devices; it also can wipe data from them and decommission them entirely — functionality that's important when an employee is terminated, leaves the company or simply loses the device. There are user-facing benefits as well, since MDM can be used to troubleshoot devices. However, MDM is invasive, and it can be difficult to sell employees on the benefits of having IT control devices that employees own in a BYOD setting, and in some countries, deleting personal data presents legal issues.

Mobile application management (MAM) is designed to control, distribute and manage mobile apps. Often called mobile life-cycle app management, MAM lets IT provision secure app containers, apps and application data on any mobile device that has been given access to the corporate network. It also functions as a development tool, providing an in-house channel for developing, testing and publishing mobile apps, and it lets IT push new versions out as they move through the development life cycle.

Unfortunately, MDM and MAM tools don't address all of an organization's mobile security and management issues, something that many IT organizations fail to understand. Security aside, both MDM and MAM can be useful, but they don't always apply in a true BYOD setting, since employees usually aren't keen on making everything on their devices available to their employers. With the right alternatives, organizations implementing a BYOD strategy may not need MDM or MAM at all. These technologies provide only limited protection against mobile security threats and can be difficult to integrate with existing IT infrastructure and other third-party devices. MAM in particular lacks the security controls that are crucial in a corporate setting.

Giving IT — and the Enterprise — What's Needed

When you look at the mobile landscape and the tools available to support it, what's clear is that most organizations need more mobile security than existing MDM and MAM products provide. To make up for the missing functionality, companies must focus on three pillars of mobile security. They include the ability to:

1. Protect in-flight and corporate data. While MDM does provide some level of device-side security, experts agree that an organization is better served when IT can provide mobile users with secure connections to a secure remote access (SRA) appliance, especially when users are connecting via an uncontrolled Wi-Fi hotspot. An SRA appliance protects traffic from interception, keeping in-flight data secure from cybercriminals.

In addition, IT must provide users with one-click access to only the corporate applications and resources that they have the right to access. Both of these features can be found on Dell's SonicWALL Mobile Connect unified client app, which, in combination with a Dell E-Class Aventail Secure Remote Access appliance, authenticates users and gives network-level access to allowed organization resources over an encrypted SSL VPN. The solution also lets administrators preconfigure Web, remote desktop and virtual network computing bookmarks and Web links that are automatically downloaded by users upon authentication. When deployed with a Dell SonicWALL next-generation firewall, Mobile Connect establishes a Clean VPN, an extra layer of protection that decrypts and removes hidden threats from mobile traffic tunneled over the SSL VPN before it enters the network.

2. Enable mobile interrogation, access and denial. Any mobile device (corporate or personal) connecting to an organization's network must have its security credentials — information such as jailbreak or root status (critical to minimize the risk of malware infection), device ID, certificate status and OS version — checked before access is allowed. This feature seems simple enough, but only SRAs such as Dell's SonicWALL E-Class SRA appliances include this protection. In addition, the Dell solution is compatible with most back-end authentication systems such as LDAP, Active Directory and Radius. For increased security, IT can enable onetime password generation and easily integrate with other two-factor authentication technologies such as Dell Quest Defender.

3. Provide unified policy management. Policies work only when they can be easily rolled out and enforced across an enterprise. In fact, IT should be able to configure policies for applications, users and devices, and do so from one central location, reducing complexity. Dell's secure mobile access solution consolidates control of all Web resources, file shares and client-server resources into a single location, with central administration and a single rule set for all resources and access methods. Unlike other access control solutions, the Dell SonicWALL SRA lets IT quickly set role-based policy for mobile and laptop devices and users with a single rule across all objects. As a result, policy management takes minutes instead of hours.

Pillars Provide True Support

A mobile strategy that's supported by all three pillars of mobile security provides users, IT and the organization itself with significant benefits. Dell's secure mobile access solution, which combines the SonicWALL Mobile Connect application with Dell's Secure Remote Access, has all three pillars covered.

With Dell's solution, users finally have the ability to access permitted corporate applications and data on whatever platform they're on, whether it's a smartphone, tablet or laptop. Employees have access to exactly what they need and what they've been approved to use. This helps boost productivity, since employees don't have to struggle to find the information they need or to perform the tasks required of them. They can access a wide variety of enterprise applications and resources from a multitude of device platforms — including iOS, Mac OSX, Android, Windows, Windows Phone/RT and Linux — making BYOD easier as well. The best part: Dell's Mobile Connect makes it easy for mobile workers to connect securely to all authorized corporate apps and data via a simple home page.

IT benefits, too. Provisioning and supporting mobile access becomes simple, since everything is done from a single interface, and policies and software can be rolled out exactly the way they should be. IT gets an end-to-end solution with unified policy management. At the same time, IT can institute a secure BYOD policy, protecting the corporate network from rogue access and malware. In the end, when IT and end users alike get a secure, integrated experience that boosts productivity and reduces risk and complexity, everyone wins. ■

ABOUT DELL CONNECTED SECURITY

Dell SonicWALL products are part of Dell's Connected Security solutions for network security, ensuring that customers won't have to sacrifice performance for security. Dell Connected Security gives organizations the power to solve their biggest security and compliance challenges today, while helping them better prepare for tomorrow. From the device to the data center to the cloud, Dell helps mitigate risks to enable the business. For more information, visit **www.software.dell.com.**