Best Ways to Extend Endpoint Management and Security to Mobile Devices

Combining endpoint protection and Mobile Device Management (MDM)

By Dana Ragsdill, Product Manager, Quest

Does endpoint management extend all the way to management of your mobile devices, like smartphones and tablets?

It makes sense for IT administrators to think of mobile devices as simply another category of endpoints. Just like the traditional endpoints of PCs, printers and network devices, mobile devices carry data, they are vulnerable, and employees depend on them to accomplish their tasks. Yet while most organizations have well-developed strategies for endpoint management, many have not yet taken the logical step of moving mobile devices into that fold.

This paper examines the reasons for incorporating mobile device management (MDM) into endpoint management. It explores how IT admins can execute four administrative functions – enroll, take inventory, configure and secure – for mobile devices as they do for traditional devices. Readers will take away a better understanding of how to fit enterprise mobile management into their existing strategies for endpoint management.

MANAGING ENDPOINTS MEANS MANAGING MOBILE DEVICES

The main argument for bringing mobile devices into endpoint management is that they play too big a role to ignore when employees are trying to get their work done. That has an upside and a downside.

Upside

In smart companies, IT admins willingly support all devices allowed onto the network, even if the employees personally own them (BYOD). When it comes to boosting employee productivity on mobile devices, they support innovations like VoIP communication, cloud storage apps, workplace flexibility and essential company software applications. One study points to a 16-percent gap in productivity – amounting to more than six hours per week – between “pioneer” employers that make good use of mobile technology and those that make poor use of it.[1]

Figure 1: Mobile device management extending endpoint management

> Small wonder, then, that 72 percent of cybersecurity professionals report data leakage/loss as their main concern related to BYOD.

Downside

But that path to greater productivity is not lined entirely with roses. Undeniably, mobile devices are an entry point for security threats, which means that endpoint security has to cover mobile device security. Nokia reports that, in general, mobile device infection rates grew 63% from the first half of 2016 to the second half and the infection rate for smartphones in particular grew 83 percent in that time period.[2]

Small wonder, then, that 72 percent of cybersecurity professionals report data leakage/loss as their main concern related to BYOD.[3] Any mobile device large enough to be useful is small enough to be easily lost or stolen and, despite anti-theft measures built into smartphones, the devices remain irresistibly tempting to thieves. An unprotected stolen device can quickly become a back door to a network.

While the sheer volume of mobile devices is daunting – Gartner estimates about 1.9 billion will be shipped worldwide in 2017[4] – the greater impact on IT is that mobile devices bring more complexity into the enterprise. Heterogeneous IT environments are expanding across device types and operating systems. Adding to the traditional platforms of Chrome OS, Linux, macOS and Windows come iOS, Android and other mobile operating systems, with associated apps and architecture. They, in turn, can lead to multiple consoles and different views of endpoints that access network resources.

When the move to support mobile devices results in a scramble to manage them easily and securely, the downside

[1] *"Mobility, performance and engagement," The Economist, May 2016, http://www.arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf*

[2] *"Nokia Threat Intelligence Report," 2017, https://pages.nokia.com/8859.Threat.Intelligence.Report.html*

[3] *"BYOD and Mobile Security – 2016 Spotlight Report," Crowd Research Partners, March 2016, http://crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf*

[4] *"Gartner Forecasts Flat Worldwide Device Shipments Until 2018," Gartner, January 2017, http://www.gartner.com/newsroom/id/3560517*

can overshadow the upside. Productivity can rise for users even as it plummets for admins.

MOBILE DEVICE MANAGEMENT: 4 MAIN CONSIDERATIONS

Properly extending endpoint management to include mobile devices entails four administrative functions:

1. Enroll
2. Inventory
3. Configure
4. Secure

For mobile devices, different considerations and practices apply to each of these functions.

Enroll

First, unlike the typical endpoints of PCs and other devices attached to the network, IT knows that smartphones and tablets do not run agents. So, how can IT ensure that the hardware and software used to manage endpoints can locate and connect to mobile devices?

The simplest way is with an app built for the respective operating system. If the organization provides the device, it can install the app before giving it to the user. In the case of BYOD, the user should be able to install the app as easily as from an app store or internal portal. In either event, smooth, uniform enrollment is important enough to ensure that users have no excuse for not installing the app and that IT does not need to intervene for each installation.

Inventory

Once the devices are enrolled, admins should be able to see and report on every mobile device connected to the network.

In many environments, endpoint inventories may not include mobile devices (especially personally owned devices), putting admins at a disadvantage in several ways:

- Mobile devices could be accessing wireless networks or corporate resources. Every admin would want the ability to ascertain that, and seeing the devices in the inventory is a fast, efficient way to do so.
- Every organization should be able to quickly and satisfactorily answer the question “How many mobile devices do we own and who has them?” An inventory of endpoints that includes all owned mobile devices is useful in tracking them down.
- A full endpoint inventory shows not only the traditional characteristics like make, model, OS version and update status, but also mobile-specific attributes like IMEI, secured status and whether the device has been rooted.

Collecting that information in a report is instrumental as admins try to determine which platforms to support, which mobile devices are non-compliant and whether any are vulnerable.

Configure

Managing endpoints includes being able to configure devices over the network. Even in the heterogeneous environment of multiple operating systems and mixed ownership, admins in smart companies maintain as much homogeneity as possible within platforms (OS version, patches) and across platforms (enterprise applications) for several reasons:

- The ability to configure helps admins install certificates for access to corporate resources.
- Admins can uniformly install and maintain the applications or apps employees need to do their job.
- They can configure basic parameters for access to the network, email and global address lists.
- Policies govern access based on employee attributes and need to be enforced on all devices.
- Platforms and applications are continually due for updates that plug up vulnerabilities.
- Admins should be able to set automated plans that roll out whenever attributes or circumstances change, without having to touch each device.

The main goal of configuration is to manage mobile devices as just another kind of endpoint, regardless of the manufacturer.

Secure

No device should be on a network unless it is secure. The same endpoint management features that enforce security policies, like requiring a passcode, should extend to any mobile device that needs access to corporate resources.

> Every organization should be able to answer the question “How many mobile devices do we own and who has them?”

Of course, some policies work only with mobile devices owned by the organization. Users are less likely to allow the installation of necessary software on a device they own and less inclined to risk corporate access to personal data on the device. But if circumstances warrant, admins should retain the prerogative to lock a device, remotely wipe it, locate a lost device and reset it to factory settings to protect company data and assets. Endpoint management should enable MDM down to that level.

FITTING MDM INTO EXISTING ENDPOINT MANAGEMENT

Given the need to extend endpoint management to MDM, organizations face three options :

1. The ideal option would be a single product to manage all devices everywhere on the network. Such products are still rare, large, complex and cumbersome.
2. At the other end of the spectrum is the least desirable option of a dedicated MDM product. It would enroll, inventory, configure and secure all mobile devices perfectly, but it would manage them specifically as mobile devices rather than broadly as endpoints, and it would live alongside and separate from the existing endpoint management system.

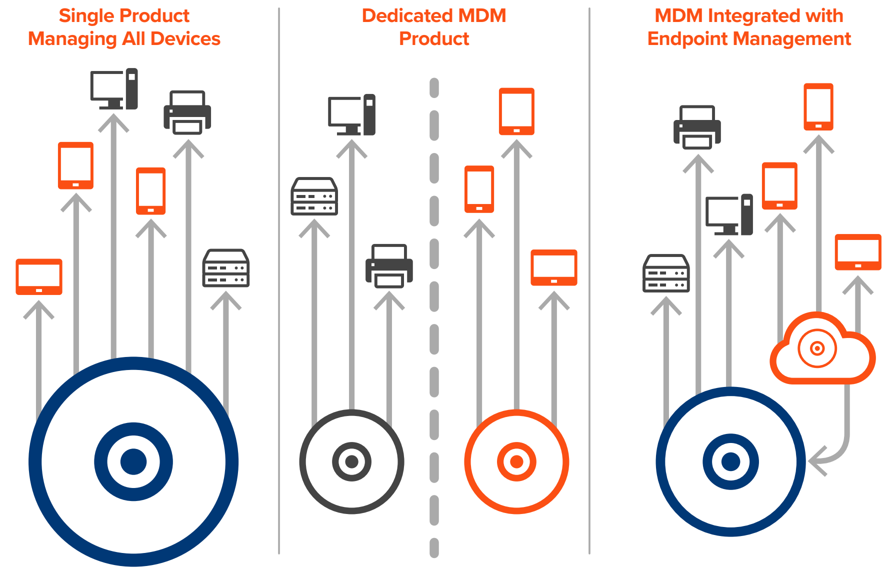

Figure 2: Three options for MDM management

Admins should retain the prerogative to lock a device, remotely wipe it, locate a lost device and reset it to factory settings to protect company data and assets.

3. The happy medium is a product designed to integrate with a traditional endpoint management system, fitting MDM into full endpoint management.

In the third option, the lowest level of integration would allow inventory from one console. The next level up would allow inventory and control of devices from a single console. The highest level of integration would allow the organization to purchase any quantity of mobile devices it needed to manage, separately from traditional devices. But it would allow the full enroll-inventory-configure-secure suite of functions through a single pane of glass, maximizing the productivity of IT admins.

That highest level applies to all endpoints: PCs, laptops, smartphones, tablets, servers, printers and network devices. Complete endpoint management plugs the vulnerabilities that jeopardize security and give IT admins headaches.

ABOUT KACE CLOUD MOBILE DEVICE MANAGER

With KACE Cloud Mobile Device Manager, IT admins can protect their network from BYOD and mobile security threats. They can enroll, inventory, configure and secure mobile devices on the most common platforms. The SaaS-hosted product allows admins to take inventory, manage passwords, and locate, erase and reset mobile devices easily.

The KACE Cloud Mobile Device Manager integrated with the KACE Systems Management appliance offers a comprehensive inventory of all network endpoints – traditional and mobile – from a single console. This helps customers transition smoothly to unified endpoint management of all the devices used by employees.

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.

WhitePaper-ExtendEndpointMgmt-MDM-US-KJ-29019