A Single Approach to Anypoint Systems Management

An IT Professional’s Guide to Integrated Systems Management, including Mobile, Bring Your Own Device and other Network Endpoints
A Single Approach to Anypoint Systems Management

Introduction

Systems management isn’t what it used to be.

When you used to think about systems management, it applied primarily to personal computers. There were differences from one system to another (desktop/laptop, Windows/OS X), but because they were all nearly the same kind of animal and were issued by your organization, you pretty much knew what to expect. You could rely on your systems management tools and IT colleagues for such necessary functions as image deployment, inventory, network security, compliance and reporting. And while the task wasn’t simple, it did have boundaries.

Now, however, your users, partners and customers are taking you down a different path, one that includes not only the bring-your-own-device (BYOD) phenomenon and the explosion of mobile devices, but one in which competitive pressure is nudging your business toward the Internet of Things (IoT) and a new era of connected, intelligent devices. What used to be just cool ways to do work or get entertainment are now important competitive advantages. As the devices have gone from nice-to-have to must-have in your computing environment, you’ve realized that you need to include them in a more holistic approach to systems management. A systems management solution is now an imperative, one necessary to address the growing complexity of identifying, managing and securing a multitude of “anypoint” devices.

Are you using multiple solutions to address the complexity that BYOD, mobility and IoT bring to systems management?

Are you using multiple solutions to address the complexity that BYOD, mobility and IoT bring to systems management? If so, you’ve probably realized that they introduce their own level of complexity and resource drain: extra people, more time, additional training and manual integration of data from multiple sources.

Even if you have the resources you need to track all of the BYO and mobile devices running in your environment, you can still end up with an incomplete picture when compared to the prior management of a more homogenous and controlled environment. The potential for error from manual processes or the integration of multiple point solutions leads to network security vulnerabilities, compliance gaps and reporting problems.

This e-book explores the ways in which BYOD, mobility and the variety of new devices affect systems management and shows how you can deal with them effectively. IT professionals need as few systems management products as possible—preferably one integrated solution that can handle anypoint systems management for all devices across all platforms, regardless of operating system or form factor.

For ALL devices

Corporate issued

Bring your own device (BYOD)

Across MULTIPLE platforms

• Windows
• Mac
• Linux
• UNIX
• iOS
• Android

Figure 1: Devices x platforms = systems management complexity
A Single Approach to Anypoint Systems Management

Ready or Not, Here Come Bring Your Own Device and Mobile

To supplement the traditional war horse of computing — the desktop PC — the workforce has gradually brought personally owned smartphones, tablets and even laptops to get work done more efficiently and with more freedom, using their preferred device and user interface.

Users often prefer to have their own device for both work and personal needs than to carry separate devices; this mixed use of a single device can greatly complicate systems management. In any case, IT’s charter includes deploying, tracking, maintaining and, most important, securing all devices in the environment, whether personal or corporate issued.

Consider three different segments of the workforce and their respective needs around BYOD and mobility: business users, line-of-business managers and IT administrators.
A Single Approach to Anypoint Systems Management

Business users want empowerment

By far the largest segment, business users have evolving skill sets and a strong need for access to resources that IT should nurture (or at least not hinder) for increased productivity. No longer restricted to internal employees, this segment can now extend to outside vendors, suppliers, business partners and customers.

Employees will do what it takes to get their work done, even when it involves unapproved software and increased risk.

Users have brought three strong preferences into the mix:
1. Freedom — Four out of five workers believe that the ability to work anywhere, anytime is an advantage, and that mobile access enables a better work-life balance.* At the same time, 66 percent of employees admitted to using free file-sharing platforms that are vulnerable,† demonstrating that in the eyes of the workforce, freedom and productivity usually trump network security. Employees will do what it takes to get their work done, even when it involves unapproved software and increased risk.
2. Platform — BYO devices run Android, iOS and other operating systems. Users want to use their personal hardware/software platform at work and won’t always wait for their organization to provide it. And they would rather not deal with multiple devices (smartphones, tablets, laptop PCs, Chromebooks, Macs) when a single one suffices, even though in reality many currently are multiple device users.
3. Privacy — In the same way that users expect the organization to observe a solid line between personal life and work life, they expect segregation between personal and corporate content on the device.

Securing IT infrastructure was relatively simple when your users worked at their desks on PCs behind a firewall. With the advent of corporate-issued laptops and then mobile devices, you extended your network security beyond the firewall by wrapping security around each device. As long as you owned the device, you owned its security on your network.

Now that they own the device, how can you own the security on your network?

A Single Approach to Anypoint Systems Management

Line-of-business (LOB) managers want productivity

The watchword for LOB managers is “productive,” as in “How do I get the tools to keep my team as productive as possible?” Here, too, outside software plays a role in productivity, though not always in an approved, secure way.

These managers want to satisfy user requirements while meeting corporate standards, often more quickly and inexpensively than you and your IT team can provide. So instead of waiting for you to enroll his team’s 30 BYO tablets in the company’s mobile device management (MDM) system, a marketing director turns to an outside MDM service. Or everyone on the customer service team installs a group texting app to communicate more quickly, unaware that the app contains a known vulnerability.

Your need for network security competes with LOB managers’ demand for efficiency.

Your need for network security competes with LOB managers’ demand for efficiency. Defending the network in the face of competitive pressure, open systems and the desire for an immediate solution is no easy feat. When you can’t deliver as fast as the business wants, LOB managers start looking for quick workarounds that end-run the processes you’ve put in place for security, compliance and reporting.

Of course, the unapproved software and apps are no panacea when they offer limited functionality and integrate poorly with your overall systems management framework, or when they are manual, time consuming and subject to error. As the need for endpoint management systems grows with BYOD and mobile, so does the need for a better, more comprehensive solution across your organization or business unit.
A Single Approach to Anypoint Systems Management

You and your fellow IT administrators want network security and integration

 Traditionally, your IT duties have spanned whatever it takes to keep your network and users’ devices playing well together:

- Inventorying and tracking of all devices on the network
- Deploying operating systems and applications
- Maintaining necessary updates, for both operating systems and applications
- Ensuring continuous uptime for maximum user productivity and satisfaction
- Keeping devices in compliance with security policies
- Configuring and installing security patches
- Reporting on the status of all devices on the network

You can turn to spreadsheets and manual processes or point solutions to complete these tasks. While those may get you closer to endpoint management for all of your PCs, BYO, mobile and other connected devices, they move you deeper into complexity and new cost structures for support, infrastructure and training. Even disparate software solutions, including traditional systems management solutions coupled with MDM, can provide tenable results. But the fact remains that mobile, BYO and intelligent devices are connecting to your network in growing numbers, and that they simply must be identified, maintained and secured.

The complexity and costs associated with that are taking everybody — users, LOB managers and IT administrators — away from the ideal end game: a single solution for integrated systems management that satisfies the needs and desires of all constituents, regardless of device or operating system.
A Single Approach to Anypoint Systems Management

Current models for mobility and BYOD

In fact, integrated systems management becomes more elusive when you consider the emerging device spectrum shown in Figure 2.

From 1 to 4, the spectrum covers the four common models for enterprise mobility that IT administrators need to bring under the umbrella of systems management:

1. Corporate issued — The organization owns and issues all the devices used for business purposes.
2. Corporate owned, personally enabled (COPE) — Some countries have laws against wiping data off a device owned by another person. In this hybrid model, the organization provides employees the devices and data they desire, and employees personally enable them. The organization may wipe the device if necessary.
3. Choose your own — This model can reduce the support burden for IT. It allows employees to bring their own device, as long as it is on a list of approved devices.
4. Bring your own — Employees bring their personal devices (smartphones, tablets, laptops) into the organization and use them to access data and apps.

Over time, device choice in most organizations will continue moving toward 4, favoring user preference over centralized control. All of these models (and any that may emerge in the future) have their respective benefits, but the closer they nudge your organization to 4, the more difficult it becomes for you to integrate disparate tools to support the number and variety of devices residing on the network.

In addition, the complexity and cost mentioned above keep you from using BYO and mobile devices to their full advantage. As depicted in Figure 3, each device and PC support quadrant shares technology with the others, but by buying solutions that aren’t integrated, you simply add to complexity.
A Single Approach to Anypoint Systems Management

The IT administrator’s dilemma

In short:
• You have the means to apply systems management to your corporate-owned laptops, manually or with a software-based solution.
• You see the need to extend your systems management model to corporate-owned mobile devices.
• You can see that, as is, your model will not scale to endpoint management of personally owned BYO devices like smartphones, tablets, laptop PCs, Macs and Chromebooks.
• You need to manage BYO and mobile devices, but if you impose too much hardship on users and LOB managers, they will likely end-run your systems management model, exposing the organization to network security and compliance risks.

Meanwhile, systems management across disparate platforms and devices grows more time- and labor-intensive:
• Without interaction among tools, manual or otherwise, you have no unified solution in which to work.
• Without integration to your service desk, support becomes fragmented, negatively affecting user productivity and the organization as a whole.
• Without integrated systems management for BYO and mobile devices, you keep adding point solutions, which result in higher costs.
• And, no matter what you try for systems management, you need to reconcile device control and network security with user privacy at every turn.

Your duties — tracking, compliance, security, reporting — now extend to BYO, mobile devices and the advent of the Internet of Things. Can you still use one tool to cover all those bases?
A Single Approach to Anypoint Systems Management

Moving from more complexity to less complexity

Having to manage the entire spectrum of corporate-owned mobile and BYO devices affects your overall systems management — from the ordinary tasks you and your team spend time on every day to the workflows and processes you’ve put in place over the years. Add to that the mechanics of meeting your compliance and reporting needs and tracking all those mobile devices.

Are you being forced to use multiple point solutions or engage in manual tasks as part of your overall systems management processes? Do you have a way to keep track of everything in one place so that you’re not constantly jumping from console to console, accessing multiple screens to resolve issues, copying and pasting between applications and updating spreadsheets? How are you minimizing the day-to-day impact of systems management on your workday and your resources?

Mobility and BYOD aren’t the problem.

Mobility and BYOD aren’t the problem. The problem is the complexity of using different point solutions (or one-off, stopgap tools) for systems management across the entire device spectrum.
A Single Approach to Anypoint Systems Management

What would it take to manage mobile, BYOD and other network-connected devices just like you manage PCs?

The traditional path to simplified systems management goes through inventory, management, securing and reporting on all of the types of devices your organization owns, and focuses on corporate-owned computers and servers. The advent of mobile, BYOD and IoT requires you to manage a much broader set of devices connected to your organization’s network.

What if you could easily extend systems management to all of your network-connected devices — no matter who owned them or brought them into the network? What if you could use your regular systems management tool for inventory, management, securing and reporting of ALL devices connected to your network — traditional PCs and servers, as well as mobile, BYO and the increasing number of smart, network-connected, non-computer devices?

It only makes sense, doesn’t it?

According to a Gartner research note, “As smartphones and tablets continue to evolve into general-purpose computing devices, the need to support them in a similar way to PCs has become more apparent. This creates a natural inclination for IT administrators to use the same toolset across PCs, smartphones and tablets.”

The anypoint management model holds the promise of integrating systems management for all connected smart devices — smartphones, tablets, laptops, even non-computing endpoints — along with traditional devices.

A Single Approach to Anypoint Systems Management

Anypoint systems management with Dell KACE appliances and Dell Enterprise Mobility Management

Dell KACE offers comprehensive, easy-to-use appliances that deliver faster time to value for systems management, from initial deployment to ongoing management, support and retirement. KACE appliances also manage devices in mixed environments with multiple operating systems and device types.

The Dell KACE K1000 Systems Management Appliance (K1000) performs initial inventory and discovery, software distribution, configuration management, patch management, security vulnerability detection and remediation, asset management, service desk and reporting. The K1000 is available as an on-premises appliance (either as a physical appliance or as a virtual appliance you install in your own servers) or as a hosted software-as-a-service solution (K1000 as a Service). The K1000 improves compliance and network security for laptops, desktops, Macs, servers and virtually any other network-connected device.

Dell Enterprise Mobility Management (EMM), integrated with the K1000, helps organizations securely manage corporate-owned and personally owned smartphones and tablets. You can use it to see your entire connected environment, including mobile and BYO devices, through a single, web-based console in the K1000.

The K2000 Systems Deployment Appliance fulfills systems deployment needs like inventory assessment, systems imaging, OS and application provisioning, migration and recovery.

The Dell KACE-Dell EMM combination of anypoint management lets you secure and manage any endpoint.

Figure 4: Anypoint management with Dell KACE-Dell EMM

Table: Devices Managed by Dell KACE + EMM

- Desktops
- Laptops
- Tablets
- Smartphones
- Servers
- Virtual machines
- Non-computer devices
A Single Approach to Anypoint Systems Management

Eliminating resistance — network security with user privacy

Users want the freedom to use network resources as productively as possible, but they also want you to respect privacy on their BYO devices. When they don’t get what they want, they tend to end-run IT as a way of demonstrating resistance.

What if you could eliminate the source of resistance by clearly and securely separating business and personal use right on the device?

With Dell’s anypoint systems management, users simply download an app (Dell Mobile Workspace) to their personally owned smartphone or tablet. The app, which looks and runs like any other mobile app, creates a private, secure workspace on their personal smartphone or tablet. This private workspace is completely partitioned from their personal apps, data and settings, and allows users to get started maximizing productivity right away on their own devices without worrying that the organization can view their personal content. Similarly, Dell also allows the users to create a secure workspace on their personal laptop PCs using the Dell Desktop Workspace application.

The workspace on every BYO device offers the same layers of security you expect on your corporate-owned endpoints.

As for your IT team and its concerns about network security, the app creates on every BYO device a workspace with the same layers of security you expect on your corporate-owned endpoints: data-loss prevention (through remote wipe), encryption, secure remote access and firewall. As shown in Figure 5, your enterprise data and apps are secured through endpoint management on corporate-owned PCs and mobile devices, and through workspace management on BYO PCs and mobile devices.

Figure 5: Security of your data with Dell KACE and Dell EMM

Corporate owned

Endpoints

Workspaces

User owned (BYOD)
A Single Approach to Anypoint Systems Management

The Dell KACE K1000 Systems Management Appliance — The backbone of the Dell KACE-Dell EMM combination

The K1000 anchors the Dell KACE-Dell EMM solution, as shown in Figure 6:
1. The K1000 natively performs full systems management of corporate-owned endpoints such as desktops, laptop PCs and servers, and also provides inventory and asset management for network-connected non-computer devices.
2. Dell Mobile Management provides full systems management on corporate-owned mobile devices like smartphones and tablets, and then passes inventory data to the K1000 from corporate-owned endpoints, along with Dell Mobile Workspace data from BYO smartphones and tablets.
3. For BYO PCs, Dell Desktop Workspace creates and manages privileges for secure workspaces and lets you manage the workspaces (deploy software, patches, etc.) using the K1000.

Corporate-owned and BYO devices are listed together in a single view in the K1000 console.

Figure 6: Endpoint management and workspace management

Thus, data from all endpoints and workspaces flows into the K1000 for integrated systems management, with corporate-owned and BYO devices listed together in a single view in the K1000 console. This enables you to provide inventory, compliance reporting, alerts and service desk for all connected computers and devices (PCs, Chromebooks, servers, smartphones, tablets and connected non-computer devices) from a single solution. Additionally, the K1000 enables you to fully manage corporate-owned PCs, servers and desktop workspaces by distributing software, managing software licenses, installing patches, scanning for security vulnerabilities and enforcing security policies.

The KACE K2000 Systems Deployment Appliance complements the K1000 with automated systems provisioning and image maintenance for multiple device types and operating systems.

With the Dell KACE-Dell EMM solution for anypoint management of both corporate-owned and BYO devices, you can now provide integrated systems management to all devices in your organization without the complexity of multiple point solutions, manual processes and big infrastructure.
Conclusion

In your job managing all devices that touch the network, you have been affected by BYOD, BYOPC and now IoT. Users’ desire for privacy on their own devices and LOB managers’ desire for productivity have made systems management with traditional tools difficult. You have responded as best you can, usually with a patchwork of point solutions that still don’t give you a single overview of corporate-owned, BYO and other network-connected devices.

The Dell KACE-Dell EMM solution for anypoint management paves the way for managing user access to data from any device:

• IT can resolve problems with a single, integrated solution for mobility and systems management, instead of constantly moving among consoles, machines and sites.
• Users install a simple mobile app with a secure workspace that preserves their privacy on BYO devices, or a similar application for creating a secure desktop workspace on BYO laptop PCs.
• Data from corporate-owned and BYO devices alike becomes available for management, compliance, reporting and service desk, freeing up IT resources and making life easier for IT administrators.
• IT can now obtain accurate inventory of virtually any network-connected device, to ensure security and move closer to unified anypoint device management.

Users and LOB managers get the productivity and privacy they need, and IT gets a single integrated solution for the systems management, compliance, inventory, reporting and service desk that it needs.

See for yourself

Find out more about Dell KACE-Dell EMM and anypoint management:

• See a live web demo of the Dell KACE K1000 Management Appliance and Enterprise Mobility Management (EMM) solution.
• Take your own tour and interact with a live KACE K Series Appliance in our Demo Sandbox.
About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.Dell.com

Refer to our Web site for regional and international office information.