

Highlights from a recent webcast on KACE Endpoint management

PREDICTING THE FUTURE OF ENDPOINT MANAGEMENT IN A MOBILE WORLD

A Digital Dialogue based on a webcast featuring Timothy Warner of Pluralsight and Nick Morea of Quest Software.

Information technology professionals face device and data management problems that were basically unheard of just 10 years ago. Gone are the days when the majority of an organization's end users sat in cubicles working on PCs hardwired into a LAN. The proliferation of smart phones, tablets and other mobile devices allow an increasing number of employees to work from home offices, coffee shops, airport terminals, and almost anywhere else that a wifi connection can be made. It is in many ways an unruly environment that IT is now being asked to manage.

"Given this huge number of different endpoint possibilities," Timothy Warner

of Pluralsight asked Nick Morea of Quest Software, "what are challenges you've heard from your customers in terms of managing and wrangling all these things?"

"It certainly is a challenge," Morea acknowledged. "When you look at the different operating systems, you've got Windows, Linux, Mac OS, tablets, Chromebooks coming into the organizations. Some IT administrators have little or no experience with some of these other operating systems, yet they still need to track, and manage, and report on them the same way they do with their existing devices, devices they've had for years. The numbers are increasing so

rapidly, especially with users sometimes bringing their own devices onto corporate networks."

Managing BYOD and COPE Devices

There are two categories of devices that mobile workers are using in corporate environments, Warner explained. They are known by the acronyms BYOD and COPE. BYOD, which stands for Bring Your Own Device, has become a well-known term for devices that fall under a workplace policy where employees are allowed to use personally owned devices in the workplace as well as on the road. Those devices are allowed to access privileged company information and applications.

For example, employees use the Outlook app on their iPhone to check their company email and send responses from wherever they happen to be.

COPE is a newer acronym, which stands for Company Owned, Personally Enabled.

"Here we try to do the best of both worlds," Warner explained, where the company purchases the hardware so the business IT has the last word on the device's usage but we're still relaxing the security in that the user can do some personal use."

COPE devices, where the company owns them and IT does the provisioning, offers a better level of control for



compliance and security, Morea said. But whether it's COPE or BYOD, IT needs to secure its network and the backend infrastructure and the applications and systems being accessed.

Another new wrinkle that's developed in the past 10 years is the cloud. Everything from old fashioned desktop PCs to smart phones access applications and data in cloud environments. There are hybrid environments where some data and systems are on the corporate network and some are in the cloud. And IT is being asked to make all this workable and secure.

Endpoint Device Confetti

With the cloud, Warner said, IT is facing "endpoint device confetti."

"What I call endpoint device confetti is when we have a user with a BYOD, COPE scenario, where he or she will have a Windows 10 desktop computer. They may have a Mac OS company issued laptop they're allowed to take on the road with them, or to take home. We have smartphones and tablets running Apple iOS or Google Android. What makes this more complex even yet, is you have different operating systems versions. You may have a number of different employees with potentially different versions of Android, which suffers from huge hardware and operating system fragmentation."

Endpoint device confetti creates a nightmare scenario for IT when they are asked to manage the complexities of so much hardware and so many operating systems.

"I would submit that any business without solutions – a service desk solu-

"I would submit that any business without solutions – a service desk solution, endpoint management solution – is going to be dead in the water." —Timothy Warner, Pluralsight

tion, endpoint management solution – is going to be dead in the water, given all these complexities," Warner concluded.

This brings up the question of how IT is going to handle help tickets coming from the endpoint device confetti. Or what happens when a regulatory requirement or legal issue mandates reporting and tracking of data from a hodge-podge of mobile hardware?

KACE Endpoint Management

KACE Endpoint Management, the industry's most comprehensive endpoint systems management solution, meets these challenges. It allows IT to replace manual processes for non-integrated point solutions, or overly complex software. KACE fast-to-implement, easy-to-use systems management and deployment appliances provision, manage, secure, and service your growing organization's network-connected devices, including Windows PCs, Macs, Chromebooks, tablets, Linux, UNIX, and Windows Servers, printers, storage and the internet of things (IoT).

"We start with provisioning the device," Morea explained. "We have solutions that allow you to not only capture an image of the operating system that you need to deploy but provide you with the capability to do zero touch operating system deployment. This can be done on multiple systems simultaneously, leveraging multicasting."

KACE Endpoint Management handles maintaining end user data through an

automated user state migration. Remote site support gives IT a single pane of glass, a single console, for supporting those remote locations. Beyond provisioning it inventories every device over the course of its lifecycle. It automates distributing software, reporting and compliance as well as security patches, configuration maintenance and policy enforcement.

With smartphones and tablets knocking around on the road and even at employee's homes, things will inevitably go wrong. Here too the KACE Systems Management Appliance can help IT provide end users with a high quality help desk that's tightly integrated with the KACE SMA's IT asset management (ITAM), configuration management, reporting, and alert capabilities. The KACE SMA's service desk capabilities provide advanced functionality to automate repetitive tasks, along with robust incident management (e.g. ticketing) capabilities. The integration of the service desk with other KACE SMA processes enables IT to deploy a single solution for IT asset management, endpoint security and end user support, reducing both the human and financial resources required for complete lifecycle management of all connected systems and devices.

SPONSORED BY:

QuestTM

For more information, visit:
www.quest.com/kace/