Your IT environment is constantly evolving

Is your endpoint management strategy evolving with it?

THE CHALLENGE

As your organization evolves, the pressure on your IT team to manage and secure your environment grows with it. IT departments today are challenged to manage a growing number of endpoints, endpoint types, applications and user access rights, all while balancing business and user needs and adhering to budget requirements.

Moreover, the ever-expanding reach of cybercrime requires your IT team to proactively prepare for a potential attack and to act quickly to mitigate issues when an actual breach occurs. Preparation includes adhering to strict privacy regulations.

The systems management landscape has also changed over the years. Basic client management tools (CMTs) for desktops and laptops gave way to mobile device management (MDM) solutions for tablets and smartphones. Enterprise mobility management (EMM) solutions came along and filled mobile security gaps and added mobile application management capabilities. But none of these on their own are enough in today’s complicated endpoint environment, which now includes internet-of-things (IoT) technologies, wearables and other devices.

Modern-day endpoint management requires attention to traditional and mobile devices as well as emerging technologies. Cobbling together disparate legacy tools, manual processes and added-on emerging technologies, however, is not ideal.

HOW THIS AFFECTS YOU

• Visibility into endpoint activity is disjointed or incomplete.
• System downtime creates user frustrations and lowers productivity.
• Devices and applications slip through the cracks, creating system vulnerabilities.
• Users do not have the appropriate access rights — or necessary limitations.
• Noncompliance with industry regulations can result in steep fines.
• Budgets and other resources are stretched thin.
• Your IT team has no time to focus on innovation.

Quest named a Major Player in IDC MarketScape1

“UEM is an inevitability in most enterprises.”

— IDC MarketScape

You need a hybrid UEM solution.

Combining traditional and mobile endpoint management expands visibility, increases security and ensures compliance.

**WHAT YOU CAN ONLY DO WITH QUEST**

Quest® KACE® brings together traditional and mobile endpoint management along with the application, security and user access rights management capabilities required for modern unified endpoint management (UEM). KACE provides total endpoint management, from onboarding and asset configuration to setting up user privileges, keeping assets up to date and compliant, scanning for risks, and reporting on the current state of the environment. KACE also includes a robust, built-in help desk.

Gain visibility into every endpoint in your environment using a comprehensive inventory tool that gathers finite data on different device types and how they are being used — including data centers, printers and other systems.

With KACE, you can perform manual or autonomous vulnerability scanning to discover risks associated with out-of-date hardware, operating systems and applications or over-privileged users. Use this information to run automated patching or manually troubleshoot issues before they become an inlet for cyberthreats.

Integrated mobile device management enables you to configure, manage and redeploy mobile devices as needed. This comprehensive yet flexible solution helps you effectively manage company-owned and personally owned devices or a combination of both from a single location. Maintain mobile device compliance with privacy regulation requirements. Enroll and track new devices as they are added to your network, and protect them using security commands, such as password reset and lock and wipe.

Maintain a least-privileged user environment to empower users with the tools they need to do their jobs effectively while reducing overall organizational risk. With KACE, you can assess user access from a single location, configure user groups and requirements, and push those requirements to users with minimal disruption to workflow.

**A BETTER WAY**

For most organizations today, having a UEM strategy that allows them to manage mobile devices, traditional desktop and laptop computers, as well as user rights from a single software solution is not just a nice-to-have — it’s crucial. According to IDC, “by 2024, 72% of enterprises expect to be either 100% on UEM or have the majority of endpoints managed by the technology.”

Unified endpoint management with KACE solutions gives organizations access to both traditional and modern systems management — in one robust solution. For your team that means:

**Broad visibility**

See activity on traditional computers, mobile devices and other endpoints from a single console and track granular details on each asset and its users.

**Robust security**

Configure automatic endpoint environment assessments and address cyberthreats as soon as they emerge.

**Privacy compliance**

Provide informative compliance data to stakeholders throughout your organization and run detailed reports for audits.

To learn more about the IDC MarketScape report on UEM and the organization’s assessment of the Quest solution, visit the IDC website.

“While KACE itself has a broad set of features beyond UEM, Quest’s software portfolio is even broader, with adjacent products in identity and IAM tools, security, user environment management, virtualization and performance monitoring and storage/data protection.”

— IDC MarketScape

---