Quest

KACE™

2 Steps to Achieve Endpoint Compliance with KACE®

INCREASING REGULATIONS

Next to ongoing security issues, meeting compliance mandates is one of the biggest challenges IT professionals face today. The proliferation of endpoints in your IT landscape, thanks to bring-your-own-device (BYOD) policies and internet-of-things (IoT) technologies, adds to the headache. The ever-present possibility of a Microsoft license compliance audit means you need assurance that you are adhering to software compliance rules at all times. There are also data protection and security regulations that IT admins need to comply with.

Keeping track of all those endpoints is difficult enough, but ensuring that each one meets all compliance requirements is a monumental task. Compliance is about protection, and all organizations are subject to some type of security regulation or policy, whether it's an internal requirement or externally mandated.

The specific external requirements change on a frequent basis, thanks to the heightened security risks of our increasingly complex IT environments. In addition to security regulations, companies must comply with software use requirements and internal policies that keep users from introducing vulnerabilities into the network.

With so many moving pieces, achieving endpoint compliance is complicated.

HOW THIS AFFECTS YOU

- An increase in BYOD and IoT devices makes asset management more time consuming. It also adds increased risk to the business.
- Your native tools are underpowered and can only deliver a limited view of your endpoints.
- You're stressed about a possible Microsoft audit, where the auditor might discover that you are not complying with your licensing agreements, which could result in large fines.
- You're unaware of your specific software license usage and concerned that some licenses may be under used and wasting your precious IT budget.

- Your limited IT staff struggles to stay on top of evolving internal and external endpoint data protection and security compliance requirements.
- Your limited IT budget cannot address the potential security concerns that you face — including patch management, user rights administration and port accessibility.
- The consequences of noncompliance with data protection and security regulations include hefty fines, legal action, security breaches and damage to your brand's reputation.

You need an endpoint compliance strategy that gives you clear visibility into all the devices connecting to your network.

You need a complete view of your software utilization and implementation in real-time for all endpoints.

You need peace of mind that data protection and security compliance regulations are being met across the board.

> "We now manage software license compliance through the KACE SMA — as well as our entire asset inventory. KACE allowed us to focus on those projects and gave us tons of time back into our schedules."
>
> *Jessica Asti, Foundation Radiology Group*

2 STEPS TO BUILDING A UNIFIED ENDPOINT COMPLIANCE STRATEGY

Maintain systemwide endpoint compliance using the Quest® unified endpoint management (UEM) solution to replace manual efforts. Keep track of desktops, mobile devices, servers, routers, printers and IoT devices from a centralized dashboard. Automatically ensure that every endpoint meets necessary endpoint compliance requirements.

Build a unified endpoint compliance strategy and gain peace of mind in two steps:

- **Step 1**: Maintain software license compliance.
- **Step 2**: Adhere to data protection and security compliance regulations.

Step 1: Maintain software license compliance.

Make software license optimization and compliance an easy-to-obtain reality across all types of endpoints with the inventory, license metering and reporting capabilities of the KACE® Systems Management Appliance (SMA) and the KACE Asset Management Appliance (AMA).

The KACE AMA is a subset solution of the KACE SMA. The KACE SMA is a comprehensive solution for all endpoint management requirements including asset management, patching, software management and distribution, and helpdesk capabilities. The KACE AMA focuses on comprehensive and flexible software and hardware asset management.

The KACE AMA offers strategic support around cost controls, helping you align your software contracts and purchases with your users' actual consumption. The KACE AMA also helps you implement mature software asset management (SAM) processes and deliver trustworthy compliance data, so that agencies can meet policy deadlines.

Inventory. Before you can begin to adhere to your software license agreements, you need to know exactly what devices are connecting to your network and what applications are running on each device. The KACE SMA and the KACE AMA give you a clear overview of your entire endpoint landscape. KACE provides a full view of your organization's software utilization and implementation in real time, making it possible to streamline asset management, service end-user devices more efficiently, and avoid audit-related fines or license overpayments.

Software metering and harvesting. The software license metering feature in the KACE SMA and the KACE AMA helps you save money by monitoring your software utilization on every endpoint. Overutilized software can result in hefty fines when an audit takes place. Underutilized software means you're wasting your precious IT budget. This capability automatically flags software on any endpoint that is over- or underutilized, ensuring optimal use of your purchased licenses and harvesting of the licenses that are not needed.

Reporting. The comprehensive, automated reporting feature in the KACE SMA and the KACE AMA outlines your software and hardware inventory and provides proof of audit compliance. You no longer need to worry about over- or underspending IT budget on software licensing. With more than 180 out-of-the-box reports, you can confidently demonstrate that your organization is both secure and compliant.

FITARA compliance. The Federal Information Technology Acquisition Reform Act (FITARA) regulates the way the U.S. federal government manages IT budgets — including budget designated for software purchases. The KACE SMA and the KACE AMA help federal agencies gain control of their IT expenditures and improve visibility into their endpoint environment. Agencies can reduce spend on over-licensing and cut back on the risk of under-licensing systems. Through software license tracking, software usage metering, and help with planning and budgeting, the KACE SMA enables federal agencies to easily meet FITARA requirements.

Hardware asset management. In addition to software license compliance, organizations need to keep track of hardware disposal compliance. The asset management functionality in the KACE SMA and the KACE AMA makes it easy for IT administrators to automate reporting for hardware that is out of date and ready for recycling. KACE can also easily archive all your asset records. In addition, you can reduce costs by automatically pulling warranty information for all your systems and devices directly into the asset inventory to avoid post-warranty maintenance.

Step 2: Adhere to data protection and security compliance regulations.

Organizations across all industries must comply with a range of data protection and security compliance regulations. These standards and rules are increasing in number and complexity as our society becomes more and more data-driven. The General Data Protection Regulation (GDPR) protects citizens of the EU from misuse of their personal information. Any organization that does business in Europe must comply. The state of California is following suit with the California's Consumer Privacy Act (CCPA), which protects the personal data belonging to residents of California.

The healthcare industry must adhere to Health Insurance Portability and Accountability Act (HIPAA) regulations that protect individuals' personal health information (PHI), including electronic data, or ePHI. The Payment Card Information (PCI) Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The standard was created to increase controls around cardholder data to reduce credit card fraud.

To help meet these data security regulations, the KACE SMA provides proactive and reactive measures to ensure that unknown applications are never installed, patch management is automated and system vulnerabilities are identified and fixed.

Device discovery. Identify and inventory all connected devices using automated network discovery with the KACE SMA. Gain complete visibility and control over your endpoints, enabling you to avoid threats from unprotected devices.

Policy enforcement. The KACE SMA supports security policies such as firewall and anti-virus configuration settings. Organizations can specify prohibited applications, and KACE will block them from being downloaded or uninstall them if necessary. You can also input information handling parameters, enabling KACE to perform spot checks of workstation local drives for files containing sensitive data such as ePHI, credit card information or information belonging to residents of the EU or State of California.

Automated patch management. Automate your software security patch updates with the KACE SMA and keep a complete log history of updates and patches. Demonstrate to government regulators that your endpoint security strategy includes processes for mitigating risk and avoiding a data breach. Ransomware attacks such as WannaCry have been successful with targeting organizations that are not up to date with their patches. Automate your patching and avoid being the next ransomware victim.

> "Security is a big deal in health care, and KACE helps keep us compliant."
>
> *Rudy Bracey, Assistant IT Administrator, St. Dominic Hospital*

> “Microsoft conducted an audit of our software licenses. We sent them reports from the KACE SMA, showing multiple agreements that covered all our licenses. The KACE SMA really helped us pass the audit.”
>
> *Michael Grimshaw, IT Operations Manager, AGC Inc.*

Security vulnerability scanning. The KACE SMA helps you stay aware of the real-time state of your endpoint environment. If a vulnerability is discovered, KACE can help you quarantine an individual computer, device or group of endpoints.

Mobile device management. Be prepared as new mobile and IoT devices are added to your network. Proactively inventory, manage and secure corporate-owned or employee-owned mobile devices. Our KACE Cloud Mobile Device Management (MDM) solution makes it easy to enroll devices and collect comprehensive inventory information. Using a broad set of commands, from resetting a password to wiping a stolen device, KACE Cloud MDM minimizes risk and protects your network from data loss and cyberattacks.

Operating system updates. Ensure that your organization is up to date with the latest patches, features and functions of Windows 10. The KACE Systems Deployment Appliance (SDA) enables you to address your migration needs by automating your migration to Windows 10. Also react quickly to re-image systems when you suspect an endpoint infection. Protect yourself from the next ransomware attack.

Access rights management. Many government and industry security regulations and internal security policies require that some form of rights management is in place to prohibit the wrong people from accessing sensitive information. KACE Privilege Manager (PM) supports you in ensuring that every employee has the appropriate access or administration rights. It also gives you comprehensive least-privileged administration and application control and enables you to easily and securely delegate administrative controls.

KACE PM performs security audits for administrative accounts and access and removes the need for local admin access on desktops. Users still have the access they need to do their jobs in a controlled environment. KACE PM also helps enforce your local system passwords and accounts.

In addition, organizations can enhance USB port security by restricting USB access with the functionality in KACE Desktop Authority (DA). When it comes to protecting information within your document management system, KACE RemoteScan ensures that sensitive data from scanned documents is immediately transmitted to your secure server rather than stored on your local endpoints. RemoteScan uses the encryption you already have in place with your virtual channels, without opening any new ports.

Audits and reporting. The KACE SMA supports logging and alerts for “audit-worthy” scenarios in relation to the PCI Standard and other regulations. KACE keeps administrators up to date on their current security posture in line with requirements for maintaining security systems and applications, enabling more timely response and preemptive actions when needed.

THE RESULT

Gain clear visibility into your endpoint landscape, including the applications that are deployed on each device. Understand where software licenses are being over- or underutilized and allocate resources accordingly to mitigate risks. Adhere to FITARA compliance regulations, data protection requirements imposed by the GDPR and CCPA, as well as security regulations under HIPAA and PCI standards. Take the necessary steps to meet your endpoint compliance goals.

Thanks to KACE, you’ll always be prepared for a software license compliance audit with automated reports ready to share. You’ll have peace of mind knowing that your organization is fully compliant and that you’re two steps ahead of the ever-evolving data protection and security regulations for your industry. Be ready for the next audit with KACE.

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product.   For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

Quest, KACE and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.

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 website (www.quest.com) for regional and international office information.