Securing endpoints in the Google Workspace for Education ecosystem

Overcoming the limitations in Google Workspace for Education to protect staff, student and network devices.

The proliferation of Google Workspace for Education

Google Workspace for Education, which was originally known as G Suite for Education, builds upon the Google Workspace suite of cloud-based productivity and collaboration tools and adds solutions for K-12 schools and higher education institutions. It enables educators and students to work in real-time, view files from anywhere and communicate easily through email and video conferencing.

Google Workspace for Education has become very popular in the education market over the past few years. A recent survey of college students in 52 colleges across America1 found that students highly preferred Google's productivity and collaboration applications over those from Microsoft. It's no wonder that Google's latest statistics2 show that more than 170 million students and educators around the world use Google Workspace for Education.

Limitations in protecting endpoints

Despite all the benefits that Google Workspace for Education provides, there are a few gaps in functionality. One of the key functionality gaps is in managing all the diverse devices used by educators and students. While Google Endpoint Management is included in Google Workspace for Education, it doesn't have what your IT Systems Administrators need to ensure that every endpoint is managed efficiently and, most importantly, secured.

Missing capabilities to manage updates and patches

Google Endpoint Management does not have the capability you need to update and patch endpoints. Patching operating systems and third-party applications is important because they may have vulnerabilities that can be exploited by hackers, potentially exposing private student and faculty data, allowing ransomware attacks or causing other security breaches. In fact, according to one study, 56% of K-12 schools and 64% of colleges and universities were hit by a ransomware attack in the past year and 74% of those attacks resulted in the institution being locked out of their data via encryption.[3]

Updates and patches limited by device type

Regarding endpoint management in Google Workspace, Computerworld4 stated that its mobile management capabilities were “extremely primitive” and that its support for macOS and Windows computers is limited making it an “inferior choice.”

Updates and patches limited or non-existent for third-party applications

> “According to ComputerWorld, the support in Google Endpoint Management for managing macOS and Windows is “limited” and its mobile management tool is “extremely primitive.”

Schools often use third-party applications to supplement their educational programs, such as learning management systems, educational games, and student information systems. While these applications can be beneficial, they can also pose security risks if they are not properly patched and updated. Again here, Google Endpoint Management is missing the capability of performing essential updates and patches for operating systems and third-party software applications like Adobe, Cisco, Slack, VMware and Zoom.

Unprotected endpoints elevate the risks of ransomware and other cyberattacks

Educational institutions are prime targets for cybercriminals as they store large amounts of sensitive student and faculty data, including personally identifiable information (PII), financial data, and academic records. And given that most have limited budgets and resources to dedicate to cybersecurity, they are a particularly attractive target for cybercriminals.

The damaging effects of ransomware and cyberattacks

According to Gartner,5 75% of organizations will face one or more ransomware attacks by 2025. And the impact of an attack can be devastating. The US Government Accountability Office6 states that a single cyberattack on an educational institution can halt classes for up to three weeks and cost anywhere from $50,000 to $1 million to remediate the incident.

> 75% of organizations will face one or more ransomware attacks by 2025.
>
> *Gartner*

Unpatched vulnerabilities are the primary cause of cybersecurity attacks

Unpatched systems are the number one cause of cybersecurity incidents according to a study produced for BitSight by the Marsh McLennan Cyber Risk Analytics Center.[7] According to Marsh McLennan, there is a strong link between having unpatched systems and experiencing a cyberattack. The highly destructive WannaCry, NotPetya, Bluekeep, and other exploitations of recent years specifically targeted systems that had not been updated with security patches.

Most of the top causes of cybersecurity attacks are related to endpoint security

In addition to unpatched systems, the study found that most of the top eight causes of cyberattacks were related directly or indirectly to security flaws in endpoints. In addition to unpatched systems, the security flaws included outdated software versions on desktop and mobile devices, systems already compromised by malware, and systems that are insecure because they are not configured properly. And when you factor in the bring your own device (BYOD) programs implemented in many schools, it collectively and compellingly emphasizes the need for enhanced measures in managing and securing endpoints.

How enhanced patch management reduces risks and disruptions

Schools can reduce the risk of cyberattacks and disruptions by going beyond the native abilities of Google Endpoint Management and Google Workspace for Education. Adding a more robust Unified Endpoint Management (UEM) solution that can automate patch management for all devices, as well as for third-party applications, can provide the following benefits.

Improve security

Patching vulnerabilities in third-party applications can help prevent data breaches and other security incidents, protecting both students and staff.

Ensure compliance

Schools are required to comply with various data privacy regulations, such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA). Patching third-party applications can help schools meet these requirements.

Maintain functionality

Patching can also ensure that third-party applications function properly, preventing disruptions to teaching and learning.

> Unpatched systems are the number one cause of cybersecurity incidents.
>
> *A Marsh McLennan Cyber Risk Analytics Center Study for BitSight*

KACE Cloud provides the endpoint management educational institutions need

The KACE Cloud platform, part of the KACE® by Quest® family of unified endpoint management solutions, eliminates infrastructure challenges, saves time and maximizes your resources with automated cloud patching on every device.

The most comprehensive patching capabilities available

KACE Cloud can perform the conventional patching from the cloud of operating systems (OS) and the standard Microsoft applications but where it stands alone is in the patching of over 350 third-party software applications. These 350 third-party apps include products from Adobe, Cisco, Slack, VMware and Zoom, and represent over 10,000 patches and growing that can be deployed throughout your IT environments using cloud-based patch management. And KACE Cloud tests and verifies OS and application patches before adding them to your catalog to prevent the deployment of defective patches and updates. IT Managers can now secure institution-owned and bring-your-own devices (BYOD) with a wide range of features while easily automating endpoints tasks with KACE Cloud endpoint patch management.

> KACE Cloud can test and deploy updates and patches for operating systems, all the standard Microsoft applications plus patches for over 350 third-party software applications – that's over 10,000 third-party patches and growing!

Maintain configuration standards across your endpoints

Take a proactive approach to policy management with the automation of KACE Cloud. Use the power of perpetual policy enforcement when administering apps, location rules, Windows custom profiles, or security standards. With this policy-based endpoint management solution, you can proactively maintain your configuration standards across every endpoint in your environment.

Protect the remote devices that access your network

KACE Cloud ensures you can protect your remote devices with a wide range of features that allow you to lock, erase, change passwords, or reset to factory settings. With location tracking, you can collect real-time location data, set and display compliance information and track location history.

Simplify the deployment and management of endpoints

KACE Cloud zero-touch deployment for onboarding and deployment of new devices eliminates manual configuration and gets your workforce up and running quickly. Configure devices more efficiently by pushing applications and implementing preconfigured user settings for newly deployed devices. The bring your own devices (BYOD) of your students and staff can be enrolled seamlessly, ensuring institution resources are protected and external devices are not making your network defenseless from cyberattacks.

Enhanced endpoint security and management with a budget friendly price

There are several cloud-based endpoint management products that claim to help, but they usually come with a high price tag and limited features. The pricing for the KACE Cloud endpoint management solutions compares very favorably with cloud-based patch management solutions that do not have 3rd party application patching and is substantially less expensive than solutions like Microsoft Intune.

Why you can trust KACE portfolio of products in your education institution

Educators have consistently comprised the largest percentage of KACE customers for decades. That is why KACE was first in the industry to integrate Google Chromebook endpoint management in 2015. Known for innovative endpoint management in the education space, it is no surprise that, with the advent of cloud based modern device management, KACE provided a way to help schools perform complete device management without having to invest and maintain the infrastructure that was associated with endpoint management systems. So, no servers, VPNs, upgrades, long term contracts, agent deployment and so on. KACE Cloud is the answer for enhancing the management and security of endpoints for institutions using Google Workspace for Education.

Learn more about KACE Cloud

We invite you to learn more about KACE Cloud, and our pricing, which is listed right on our website at www.quest.com/products/KACE-Cloud.

Learn more about our other KACE solutions

KACE's integrated portfolio of solutions further expands beyond cloud-based endpoint management. If there are requirements for functionality such as license compliance, asset management, scripting and management of servers, non-computers like printers, power backup, video conferencing devices, alarms or IoT that cloud-based solutions can't provide, KACE Cloud is fully integrated with the KACE Systems Management Appliance (SMA) that schools like Florida State University have depended on for decades. This way they have the flexibility to manage any device exactly the way they want to – now and in the future.

And with the KACE portfolio of solutions, the annual "big summer refresh" is made simple. In addition to the KACE Cloud option, the KACE Systems Deployment Appliance (SDA) has been streamlining imaging and reimaging projects for schools and school systems like Seminole County Public Schools for decades. Again, you have another alternative to ensure that you have the flexible options you need now and in the future.

1. College Pulse and SADA Systems, "Google Workspace vs. Microsoft 365: Tomorrow's Workforce Weighs In," June 2022.
2. Google, "Elevate education with simple, flexible, and secure tools with Google Workspace for Education," March 2023.
3. Sophos, "The State of Ransomware in Education 2022," July 2022.
4. Computerworld, "Google Workspace vs. Microsoft 365: Which has better management tools?," June 2022.
5. Gartner, "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware," January 2021.
6. U.S. Government Accountability Office, "As Cyberattacks Increase on K-12 Schools, Here Is What's Being Done," December 2022.
7. BitSight, "The Top 8 Security Flaws That Will Get You Hacked," November 2022.

KACE by Quest