ManagedMethods

Cloud Security Solutions for the K-12 Education Environment:

WHAT THEY DO, WHAT THEY DON'T DO, AND USE CASE SCENARIOS

Cloud Security Made Easy

managedmethods.com

Introduction

K-12 administration and staff are taking on an increasingly broad role in student safety--both on and off campus. And while threats to student safety and data security make this role critical in today's education environment, there are a lot of questions about just how administrations can effectively take on this role.

As we at ManagedMethods meet with technology leaders and the technical staff at school districts and K-12 educational institutions across the country, we're hearing confusion about cloud security and the products and services that schools need for this purpose. We field a lot of good questions about what solutions will help schools keep their students and staff members safe and their sensitive data secure.

Unfortunately, there's no single solution that can do everything that schools typically want to do. As is common with all types of security, there are layers of solutions that do distinctly different things—and not every layer is needed by every school. What's more, budgets sometimes play an important role in what solutions a school can afford to use.

At the same time, claims by security vendors are sometimes confusing. It can be a real challenge to understand what a solution does, as well as what it doesn't do. Just where does a solution fit within the layers of security, and how can it help? What gaps in cloud security might be left unaddressed?

Cloud security products for education tend to fall into three categories in terms of their capabilities and the use cases they address. The purpose of this eBook is to help you and your technology team understand those categories and the products that fit into them, so you can make a more informed decision about whether to evaluate or deploy a solution from that layer of security.

This isn't meant to be a comprehensive buyer's guide. Rather, it's intended to help you determine which types of solutions best meet your school's needs at a time when administrations are being tasked to increase safety and meet stringent compliance requirements for data privacy and security. And while ManagedMethods does provide solutions for many of the use cases discussed, this isn't meant to sell you our solution—it's meant to be educational.

Keep in mind that many of us at ManagedMethods are parents with school-age children, and all of us are concerned members of the communities where we live and work. We are passionate about helping schools get the maximum benefit from their tech budgets to protect people and sensitive information while also allowing students and educators to fully embrace and use technology to get great learning results. We follow the education technology market closely and are happy to discuss the various security layers, use cases and product categories with school technologists who want help to sort through their options.

Why Schools Need Cloud Security Solutions

K-12 educational institutions have embraced cloud computing in the past few years. Many schools now have a 1:1 model, meaning each student is issued a notebook or tablet device in order to access online learning materials and resources, both in the classroom and at home. Teachers, administrators and staff members use cloud-based productivity applications like email, spreadsheets and word processing. Everything from classroom lessons, student projects and grade books to individualized instruction plans and school budgets are now hosted in the cloud. Google G Suite for Education and Microsoft Office 365 Education have become as essential as books, pencils and whiteboards were a generation ago—schools can't function without these education-oriented technologies and applications.

Regulations Mandate Data Security Oversight

While these new cloud-based solutions offer a lot of benefits, they also introduce the risk of exposure of information or data that must be protected from loss, theft or abuse. There are numerous data security and privacy requirements that are mandated by laws and regulations such as the Family Educational Rights and Privacy Act (FERPA); the Children's Internet Protection Act (CIPA); the Children's Online Privacy Protection Act (COPPA); the Health Insurance Portability and Accountability Act (HIPAA); and many other state laws and local policies.

As an example of local or regional legislation, ManagedMethods' own home state of Colorado enacted the Student Data Transparency and Security Act in June of 2016. This act supplements existing laws pertaining to the collection, management, storage, and sharing of Student Personally Identifiable Information (PII). The purpose of this law is to increase transparency and security of all Student PII that the Colorado Department of Education (CDE) and Local Education Providers (LEPs) collect and maintain.

There can be significant penalties for failure to adequately protect personal and financial data such as payroll information, school financial information, and student personal information.

According to the K-12 Cybersecurity Resource Center, there have been more than 350 cybersecurity-related incidents since 2016, many of which exposed personal data. Many of the reported incidents were unintentional mistakes as opposed to outright cyberattacks, meaning well-intentioned people just got careless.

Technology Supports the Well-Being of People

Schools are now being held accountable for what is happening in students' personal lives, even off-campus and outside of school hours. The types of questions administrators are expected to ask and answer are: Is a student or group of students bullying others via social media? Does a student show signs of anger to the point where he or she can pose a danger to others? Are there signs that a student is being physically or emotionally abused at home? Are students circulating sexually explicit and other offensive content among their peer groups?

Given that the clues to answer these types of questions often appear in email messages, on social media or in cloud file sharing apps like Drive or OneDrive, it's possible to use technology to uncover threats, signs of mental illness or stress, bullying, abuse, and offensive content. Then alerts can be sent and action can be taken to help ensure the well-being of students, faculty and staff.

For example, during the extensive reviews of past school shootings, it was learned that in some of those events, content hinting at the nature of the events was posted prior to the actual occurrence of the violence. Had technology been implemented to analyze such content, early warning signs could have been flagged, prompting potential intervention.

ManagedMethods can attest to an incident at a high school where three students' intent to commit suicide was discussed via a shared Google doc. Technology used to routinely scan G Suite flagged the word "suicide," alerting school administrators to the plan. An intervention led to getting the kids into counseling sessions. Without technology in place to spot these clues, the unthinkable could have happened.

The Three Most Common Categories of Cloud Security in K-12

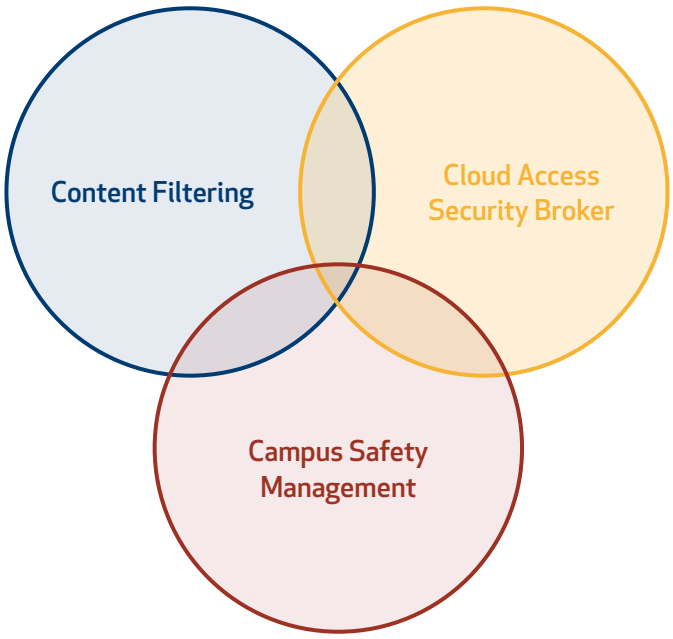
There are three distinct layers of cloud security that are fundamentally important to K-12 educational institutions. It's important to note, however, that not every layer is needed by every organization. Rather, the need is determined by local interests and priorities. What's more, budget constraints may impact what schools can afford to put in place.

We'll look at the following three layers of cloud security solutions:

- **Cloud Application Security (aka CASB)**
- **Internet Filtering / Content Filtering**
- **Campus Safety Management**

For public schools in particular, budgets are tight and schools need to maximize their capabilities with their investments. Some cloud security products do more than others, but no product meets every need or every use case. These products do overlap with some functions, but mostly they are complementary to each other. Some work together to provide extra assurance or visibility of the situations that are uncovered.

We can't list every vendor that sells into the K-12 education market; there are simply too many. Where we do list products, the list is meant to be representative of a class of solutions that perform certain functions or serve certain use cases, brought to market by vendors who have a focus on the education marketplace.



Cloud Application Security

Many schools have already adopted cloud-based application software for use in the classroom and the administrative offices. A Cloud Application Security solution – sometimes referred to in the industry as a Cloud Access Security Broker, or CASB – is designed specifically to provide a strong level of visibility, control and protection of these types of applications and the data associated with them.

What a Cloud Application Security Solution Does

Cloud application security is a fundamental control layer of cloud security. It's primarily concerned with analyzing and controlling what is happening with the school's web applications like Google G Suite, Google Drive, Office 365 Mail, OneDrive, SharePoint, Slack, Box, Dropbox and ShareFile. The native security capabilities inherent in these applications are limited or require expensive license upgrades, which dictates the need for enhanced security.

The new generation of cloud application security solutions connect directly into the applications through an application programming interface (API), which makes security an integral part of the application. (Previous generations of cloud application security solutions used cloud gateways, which provided far less control of cloud applications.)

Cloud Application Security provides three key functions:

- **Visibility** into what's going on within the cloud application. This gives IT administrators the ability to know who is doing what within the applications, as well as what information and images are being sent, received, stored, shared or viewed.
- **Control** over activities and behavior, driven by policies. This includes the ability to detect, alert on, and block activities that violate relevant regulations and school policies.
- **Protection** against malware, phishing and other threats. Schools must be able to protect against threats that can lead to data loss, theft or corruption or the disruption of school operations such as through ransomware. Protection features often include threat detection, data loss prevention, and active monitoring of user behaviors.

Example Vendors with Products in This Category

With a special focus on the K-12 education market, ManagedMethods is in this product category. The leading cloud application security vendors that cater to the education market are:

- ManagedMethods
- Cisco (CloudLock)
- SysCloud
- Palo Alto (Aperture)

Examples of Problems Cloud Application Security Addresses

- All uploaded files and incoming email messages and attachments are screened for phishing, malware and other threats. Messages and files are quarantined if a threat is found.
- All emails and attachments are scanned for keywords that indicate some sort of risk; for example, "suicide," "bomb" or "gun." Administrators can be alerted if a potential risk is uncovered.
- Content that is being sent outside the school network is screened for specific words, phrases or patterns to prevent sensitive data from leaving the school environment.
- Offensive content or images posted into the school's cloud apps can be uncovered and alerted on. For example, if there is a document containing hate speech or there are sexually explicit images stored on Google Drive.
- Account logins are checked to see where someone is connecting from. For example, a login from Russia is most likely indicating an account takeover that could lead to a data breach. The account can be frozen until the credentials are changed.
- The system monitors for large quantities of files being downloaded or deleted, possibly indicating insider abuse.
- Schools have the ability to implement policy scanning to ensure that the data security and student privacy aspects of regulations such as CIPA, COPPA, HIPAA, and FERPA, among others, are maintained in order to prevent compliance violations.

Example Use Cases in an Education Environment

- A staff member in the administrative office mistakenly attempts to email a spreadsheet containing employee salary information to a mass distribution list. The cloud application security system recognizes the sensitive nature of the data and alerts the user and the IT admin of the potential violation.
- A student attempts to upload pornographic images to his Google Drive account with the intention of sharing them with his classmates for the shock value. The cloud application security system can detect the illicit images, revoke the file share upload and alert an IT administrator.
- A school nurse attempts to share a student's medical record to a local clinic. This violates a HIPAA regulation and the file share is revoked and a warning message sent.
- An email message containing a phishing link has been sent to faculty members of a school. The cloud application security system identifies the threat inside the original message and quarantines the message before it can be distributed to the intended recipients.
- A student saves a profanity-laced document in his Google Drive. The cloud application security system scans the document and finds the offensive words, which are a violation of school policy, and alerts an IT administrator.
- Three students form a suicide pact and share their plans using their school email accounts. The cloud application security system detects the keywords such as "take my own life" and "suicide" and alerts school authorities.
- A school's payroll clerk receives a spoofed email message that appears to come from the school superintendent. The message directs the clerk to click on an embedded link to update the W4 tax forms for all faculty and staff members. The cloud application security system detects the suspicious embedded web URL link and scans it for phishing and social engineering and alerts the admin and warns the user about the sensitive data policy violation and potential phishing.

Limitations of a Cloud Application Security Solution

Cloud application security technologies don't inspect content posted to social media or sent via direct messaging apps, which is where students are likely to conduct bullying campaigns, exchange "sext" messages, express threats against other people or the school, or reveal suicidal thoughts. Moreover, cloud application security doesn't do anything at the device level, just at the cloud application level.

Internet Filtering / Content Filtering

School districts often choose to deploy a content filtering solution to comply with the Children's Internet Protection Act (CIPA). Content filtering products quickly scan through text, data, and possibly images to search for content that meets specified criteria, such as offensive language or regulated data.

Some filtering solutions only screen a website's URL and not the actual content. These solutions have limited capabilities because even websites with "clean" or "whitelisted" URLs can contain explicit content. According to edtech vendor GoGuardian's research, nearly 20% of explicit content occurs on educational sites that teachers rely on, making content filtering a desirable layer of security for schools.

What Content Filtering Does

Content filtering typically works at the web browser level by looking for specific character strings or general content that, if matched against a policy, indicate undesirable content that is to be blocked in real time. Text on a page is typically screened for explicit content and sometimes also for violence- or hate-oriented content. Sophisticated solutions might process images as well as text-based strings. Some products use machine learning or artificial intelligence to continuously learn from the context of content to reduce false positives and false negatives.

Solutions might use web proxies or gateways, directing traffic through them in order to do the screening and filtering. In addition, these solutions might work off school premises, such as at students' homes, because the filtering is done at the browser level via an installed agent or browser extension on a Chromebook, tablet or other laptop. Some solutions can integrate with a school's Active Directory system to enable policies by user or group, and some can inspect encrypted traffic over SSL connections. It's important to ask these vendors about the full range of their capabilities and feature sets.

Example Vendors with Products in This Category

Representative vendors with products in this category include, but are not limited to:

- iBoss
- GoGuardian
- Lightspeed Systems
- Securly
- ContentKeeper

Examples of Problems a Content Filtering Product Addresses

- Compliance with CIPA and COPPA
- Students purposely or accidentally viewing explicit content
- Students surfing time-wasting websites when they should be doing classwork

Example Use Cases in an Education Environment

- Students can take a Chromebook home to continue online learning in the evening and parents can be assured that their children won't be able to access offensive or explicit content.
- A teacher can blacklist a particular website, even if the content is safe, to keep students from wasting class time by browsing that site.
- On days when standardized testing is being administered across a school district, policies can be used to block students from going to any websites other than the ones hosting the tests.

Limitations of Internet / Content Filtering Solutions

These products tend to focus on browser sessions in search of offensive or explicit content. They are not looking for malware, phishing, ransomware and these types of security threats, even though they are often passed through web-based email messages and documents.

Campus Safety Management

The environment that students live in today is so open that it can be difficult for any school district to keep students safe. Nevertheless, schools now take on a far greater responsibility than just educating students. They also attempt to assure the well-being of students, faculty and staff members by gaining awareness of threats and potentially harmful actions within the greater school community. For example, many schools utilize technology to support their suicide prevention program.

Laws vary state by state, but in some cases, schools are required to intervene when a child is a target of bullying. For instance, David's Law in Texas requires schools to notify parents by the next day if their child has been a target of bullying, and to notify the parents of the perpetrator within a reasonable amount of time. The law provides immunity to educators who report bullying, while schools have the authority to investigate cyberbullying and to work with law enforcement on such investigations.

Campus safety management solutions also can help students maintain a positive digital footprint. At a time when prospective employers and college admissions offices scrutinize individuals for their behaviors and beliefs, it's important that youngsters learn how to maintain a clean profile.

What Campus Safety Management Products Do

The capabilities vary greatly by product or service, but in general this category of solutions can identify risky behaviors or intentions in various ways.

- Data science, machine learning and pattern matching technologies reveal content in email, documents, shared files, images, photos and more which indicates potentially harmful activities or intentions; for example, a student who is planning violet actions at school, or a student contemplating suicide.
- A trained staff of operations personal is on call continuously monitoring alerts to interpret the meaning or intent of postings and messages sent to/from students. These operators can look for content indicating potentially harmful activities or intentions.
- Students can use the solution or service to confidentially ask for help with personal struggles or social issues that he or she might find difficult to talk about.
- School officials, counselors and/or law enforcement officials are alerted when risky or suspicious content is discovered or submitted.

Example Vendors with Products in This Category

Representative vendors with products in this category include, but are not limited to:

- Gaggle
- GoGuardian (Beacon)
- Bark
- Social Sentinel
- Securly

Examples of Problems a Campus Safety Management Product Addresses

- Students sharing sexually explicit content with each other
- A student making threats against the school or another person
- A student expressing suicidal thoughts
- A student involved in an abusive relationship
- A group of students cyberbullying another youngster

Example Use Cases in an Education Environment

- A student sends an email message to a friend, mentioning intentions of suicide. The safety management solution/team analyzes and reviews the content that clearly indicates the student is in imminent danger of self-harm. A safety representative forwards the email to a school district administrator and calls the emergency contact. The student is located in a school bathroom moments before harm is done.
- A student submits a homework assignment that requires writing an essay. The story seems to be about the student being in an abusive dating relationship. Before the teacher has a chance to read the essay, a relationship manager reads the essay and

flags it for review by a school counselor, who then reaches out to the student and her parents to provide help. The school also contacts the parents of the suspected abuser, who attends the same high school.

- A small group of students was involved some off-campus criminal activity and they bragged about it to friends. People shared the stories of the criminal behavior over email. Keywords in the messages led the safety management solution to alert a resource officer, who read the email messages and then notified law enforcement.

Limitations of a Campus Safety Management Solution

The limitations vary greatly by product. Some of these solutions only work with school-sanctioned products such as Office 365, Google G Suite or Canvas LMS, or they only review posts to public social media sites. Students can still use private or direct messaging applications, apps with tight security settings, or non-school-provided social media and mobile applications to share their objectionable content, discuss their malicious or harmful intentions, or conduct their cyberbullying.

Tech buyers should thoroughly investigate a solution's capabilities as well as which platforms and applications it works with. It's just as important to understand what a solution doesn't do, and what platforms and applications it doesn't work with, as the excluded platforms and apps might be the ones that children are most likely to use to communicate with each other.

Combining Layers to Get Deeper Insight to Resolve Issues Quickly

As mentioned earlier, these cloud security products provide layers of protection. When solutions from two or more layers are used together, they tend to complement each other. There might be some overlap in capabilities, but this serves to provide "backup" such that if one product misses an incident, the other might pick it up. When both products detect an incident, this pretty much confirms it's not a false-positive alert.

In other cases, one product might detect an incident worthy of an alert, and another product provides much more detail to help IT administrators go deeper into what has occurred and resolve the issue more quickly.

For example, there is a ManagedMethods customer that has all three layers of the cloud security solutions described: Cloud Application Security, Content Filtering, and Campus Safety Management. One of its schools had an incident where its campus safety management solution detected a keyword in a student's Google email account. The IT administrator got a notification email with the student's name, the file name and the keyword that triggered the alert.

Now, the system administrator could have spent time logging into the Google console and maneuvering through directories and files to find the specific file in question. Instead, this school district used the ManagedMethods Cloud Application Security console to see the same incident alert on the screen, but with additional details the other product didn't provide.

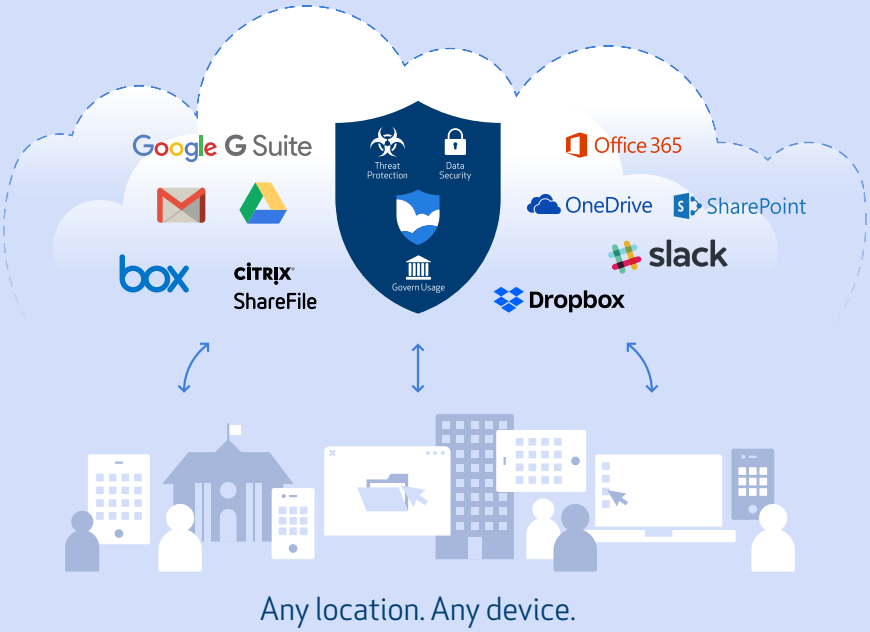
ManagedMethods revealed who sent the email message, who the internal and external recipients were, what the message subject line said, and what domain the file attachment is in. It also provided a full historical analysis—who edited the file in the last three days, who downloaded it, who printed it, who moved it, etc. This kind of detail goes far beyond what a campus safety management solution, or a content filtering solution, can do, but it's all complementary. It all helps the school do what it wants to do, which is identify a risky situation and all the people involved in order to resolve the issue quickly.

In this particular case, ManagedMethods helped the other products complete the full picture acting in complement to each other.

Conclusion

School districts and educational institutions face a range of challenges pertaining to school community and personal safety and data security. There is no single software product or service that will solve all issues. Given limited human and financial resources, school technology leaders and administrators need to prioritize the types of problems they can address and look at the best types of solutions that can help them achieve their goals within their budget.

Need more information? Talk to us—we're happy to answer whatever questions you might have.



About ManagedMethods

ManagedMethods offers the most efficient way to gain visibility into how data is stored, accessed, and shared in popular cloud applications, including Google G Suite, Microsoft Office 365, OneDrive, and Sharepoint, as well as to secure cloud-based email. ManagedMethods is the industry's only cloud application security solution that can be deployed in minutes with no special training, and with no impact on users or networks. Learn more at managedmethods.com.

Phone: +1 (303) 415-3640

General Questions: info@managedmethods.com