13 Email Security Threats Targeting K–12 and How to Protect Your Schools

Why Your District Needs to Take Email Threats Seriously

K–12 school districts are increasingly targeted by sophisticated cybercriminals. With limited IT resources, valuable student and staff data, and widespread use of cloud platforms like Google Workspace and Microsoft 365, your schools are prime targets for email-based attacks.

Understanding the different types of email threats—and how to defend against them—is essential to protecting your district.

ManagedMethods provides advanced, AI-powered threat protection tailored to K–12 environments, helping districts detect and block email threats that traditional filters often miss.

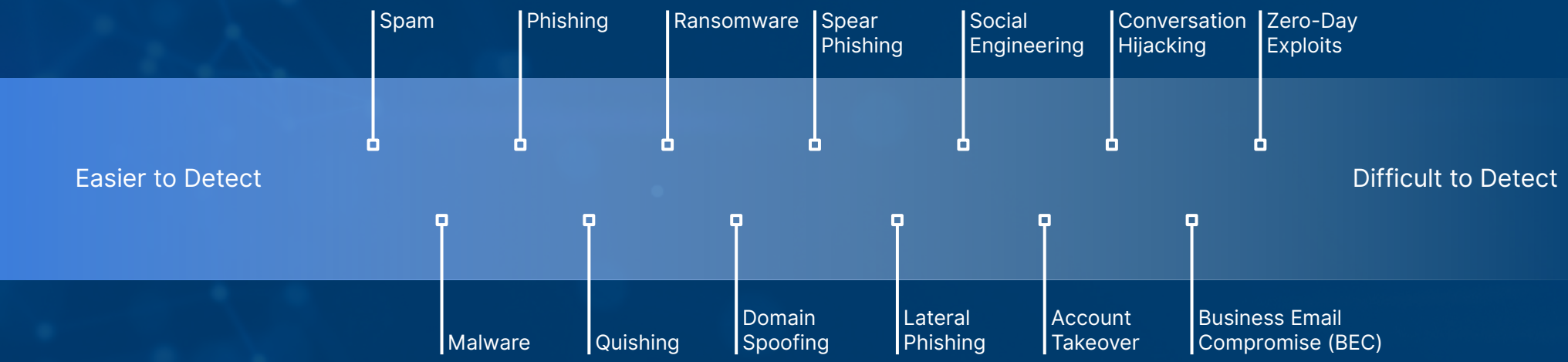
Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Detecting Email Threat Types

This Guide Ranks the 13 email threat types from easiest to hardest to detect. This ranking is based on how likely these threats are to bypass traditional filters and the level of human or AI intervention typically needed to detect them effectively.

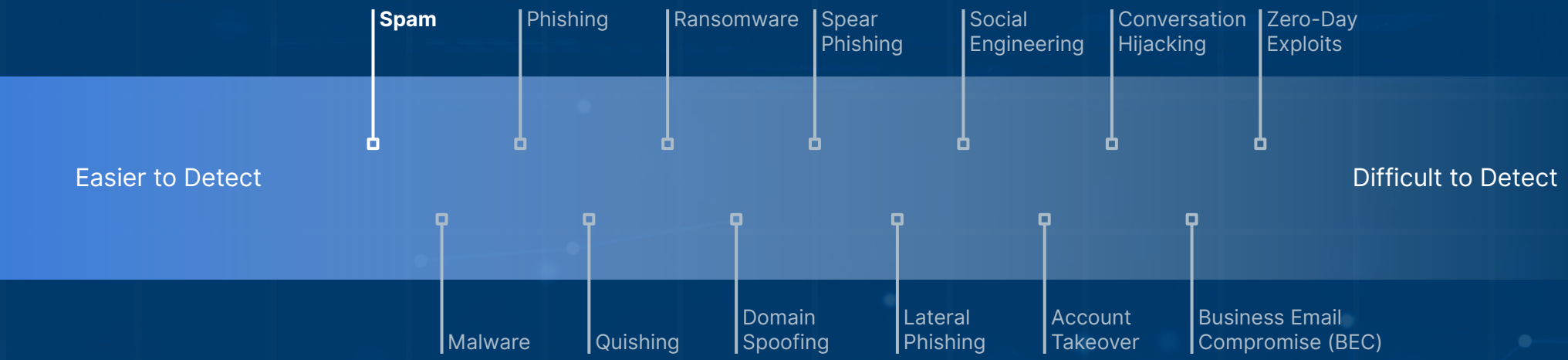


Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Spam



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Spam

Basic bulk email. Low sophistication, easily filtered.

What it is: Unsolicited bulk email that can clutter inboxes or carry hidden threats

K–12 impact: Increases the risk of phishing and reduces productivity

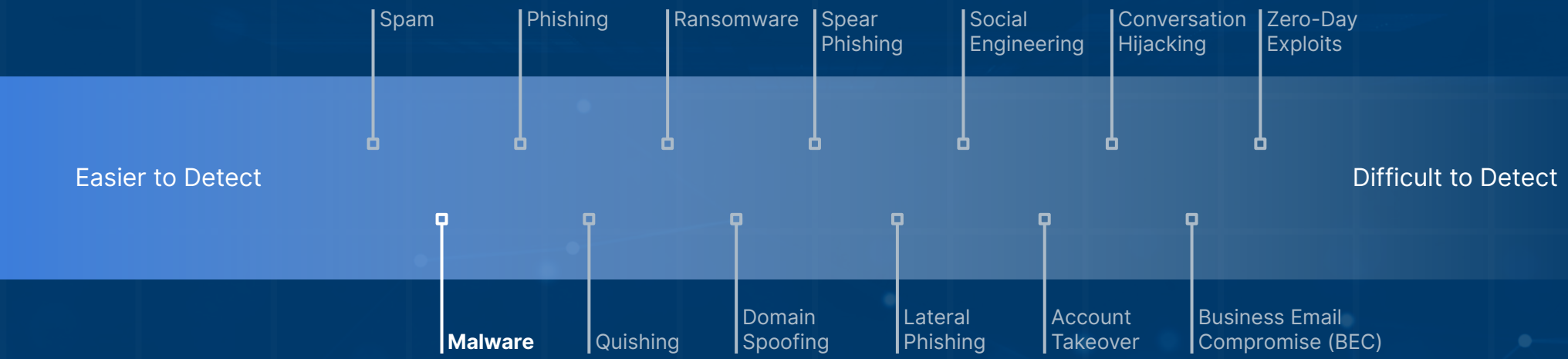
Protect your schools: Advanced filtering ensures clean inboxes and reduces risky clutter—without blocking legitimate content

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Malware



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

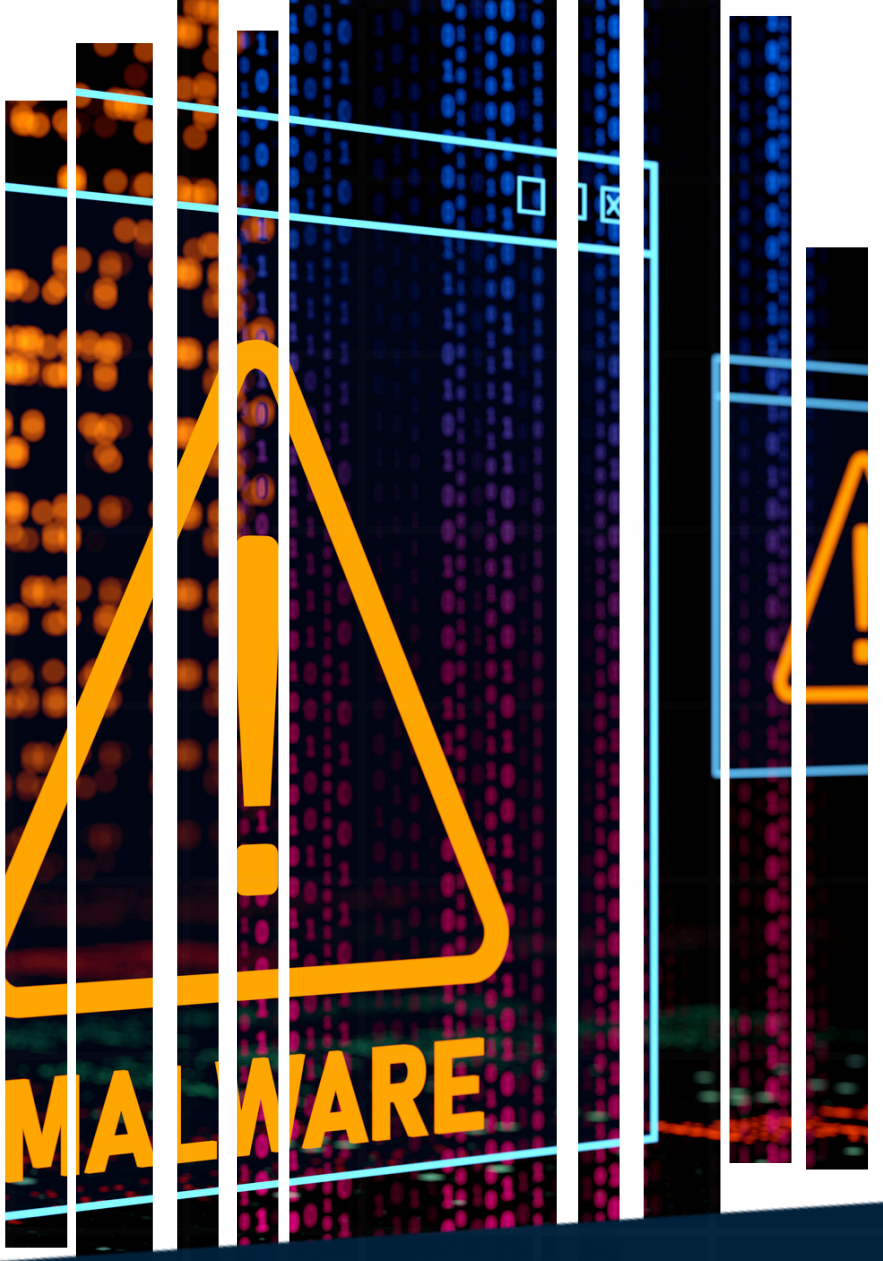
Malware

Traditional attachment-based threats.
Still dangerous but widely known.

What it is: Emails with infected attachments designed to install malicious software

K–12 impact: Malware and spyware can shut down learning systems, leak data, and more

Protect your schools: Use tools that scan attachments and linked files for known and emerging malware signatures

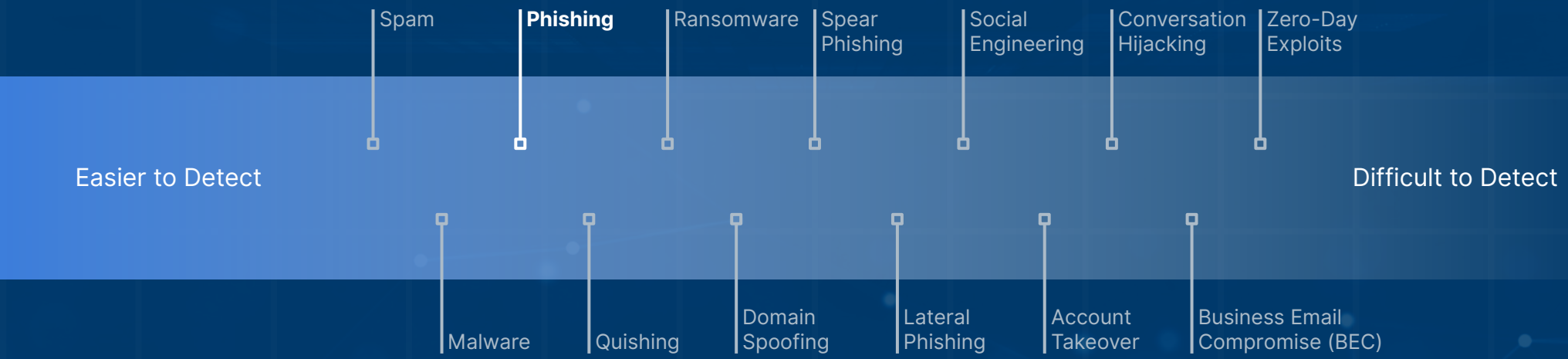


Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Phishing



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Phishing

Mass emails with malicious links or fake login pages. Often detected by basic filters.

What it is: Fake emails designed to trick recipients into clicking malicious links or entering credentials into spoofed websites

K–12 impact: Can compromise accounts, lead to data breaches, re-direct vendor payments to criminals, disrupt learning and school operations, and more

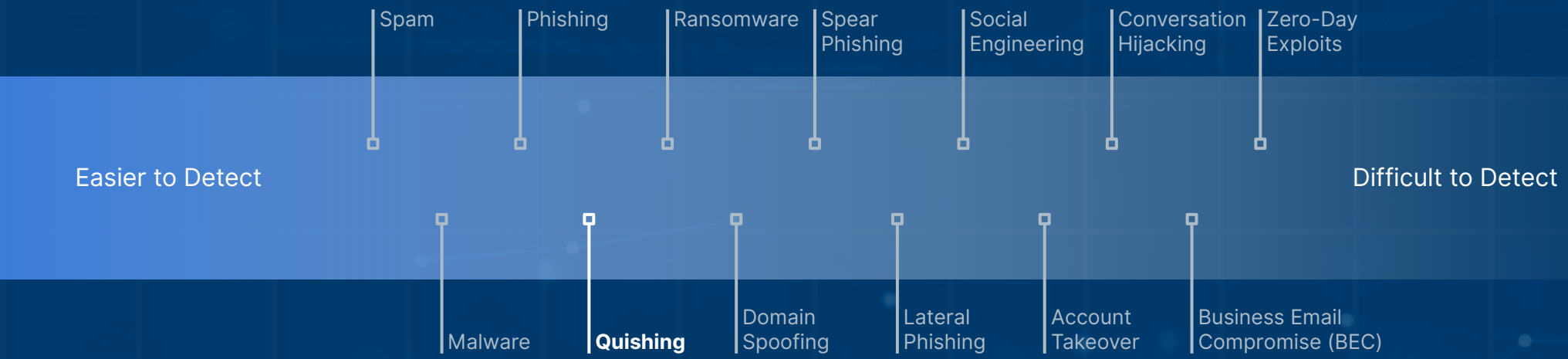
Protect your schools: AI-powered phishing detection catches suspicious patterns and URLs—beyond native email filters.

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Quishing



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Quishing

A newer twist on phishing using QR codes. Slightly more evasive but still relatively simple.

What it is: Attackers embed malicious QR codes in emails, bypassing link scanners

K–12 impact: Staff or students scan a QR code with their phone, unknowingly giving up credentials or installing malware

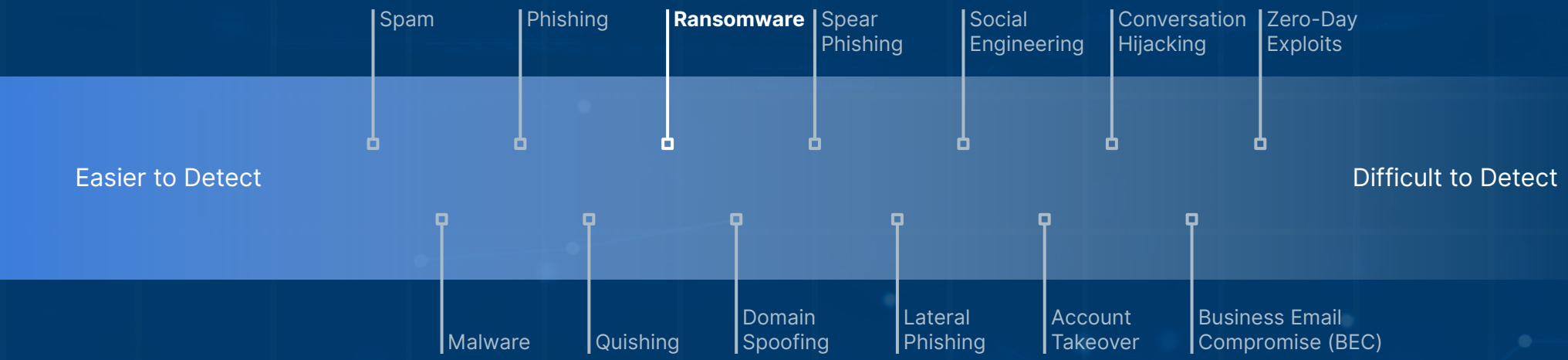
Protect your schools: Use an email security tool that can scan image files and alert you to suspicious QR activity embedded in the email and attachments

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Ransomware



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Ransomware

Can be caught by scanning and sandboxing, but harder if obfuscated or delivered via links.

What it is: Malware that locks down systems or files until a ransom is paid

K–12 impact: Encrypts district data and halts operations until a ransom is paid. Can cause significant learning disruption and financial losses, whether or not the ransom is paid

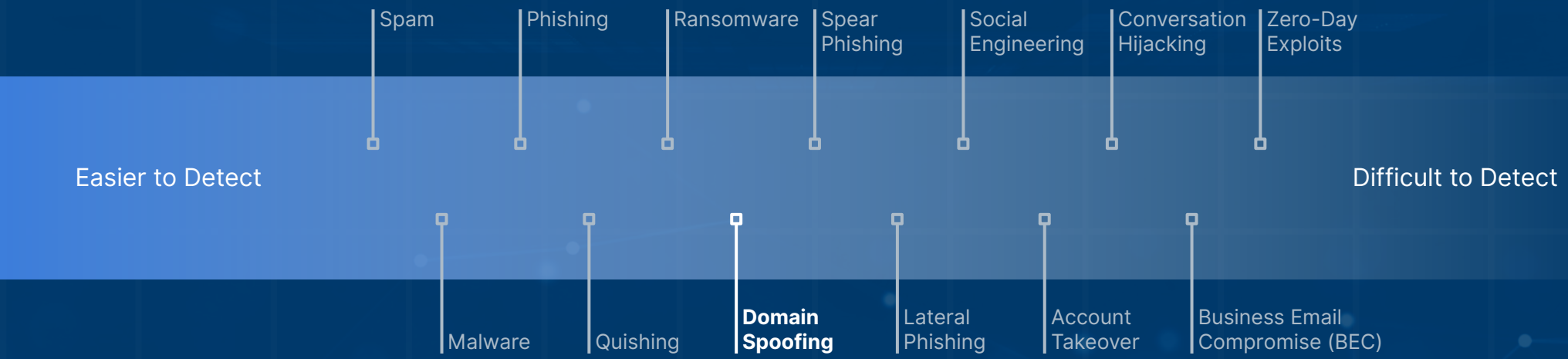
Protect your schools: Use tools that can proactively detect ransomware payloads in email attachments, links, and shared files and alert your IT team for fast response

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Domain Spoofing



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Domain Spoofing

Can bypass detection without proper DMARC, SPF, and DKIM enforcement.

What it is: Emails appear to come from a trusted domain but are sent from look-alike or fraudulent domains

K–12 impact: Fools staff, parents/guardians, and other stakeholders into trusting senders to get them to click on malicious links or download malicious files

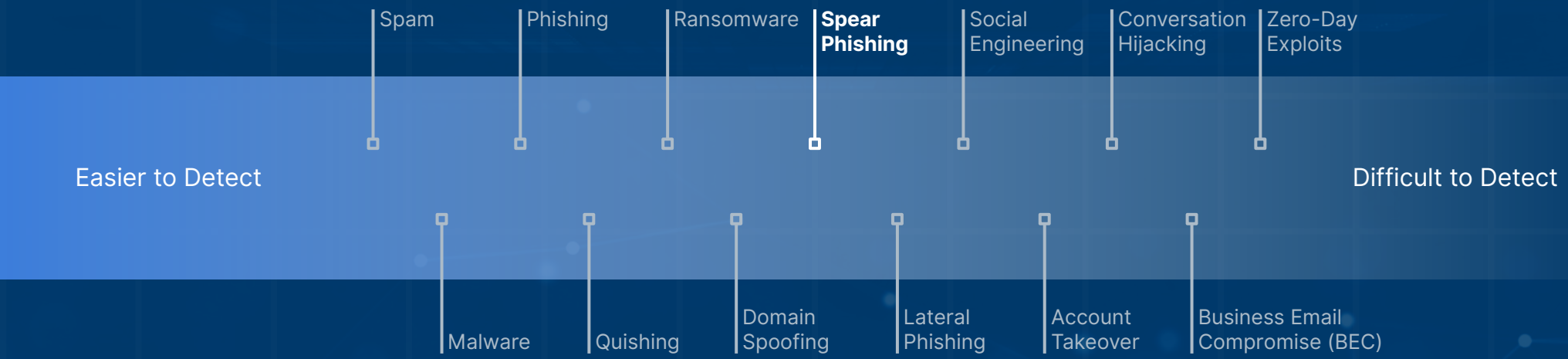
Protect your schools: Use tools that can analyze domains and monitor DMARC to identify and flag spoofed domains

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Spear Phishing



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Spear Phishing

Highly personalized—often evades standard filters due to lack of malicious links or payloads.

What it is: Highly targeted emails impersonating trusted individuals

K–12 impact: Attackers pose as superintendent, principal, etc. requesting urgent action to get someone to remit payment, provide sensitive information, click malicious links, etc

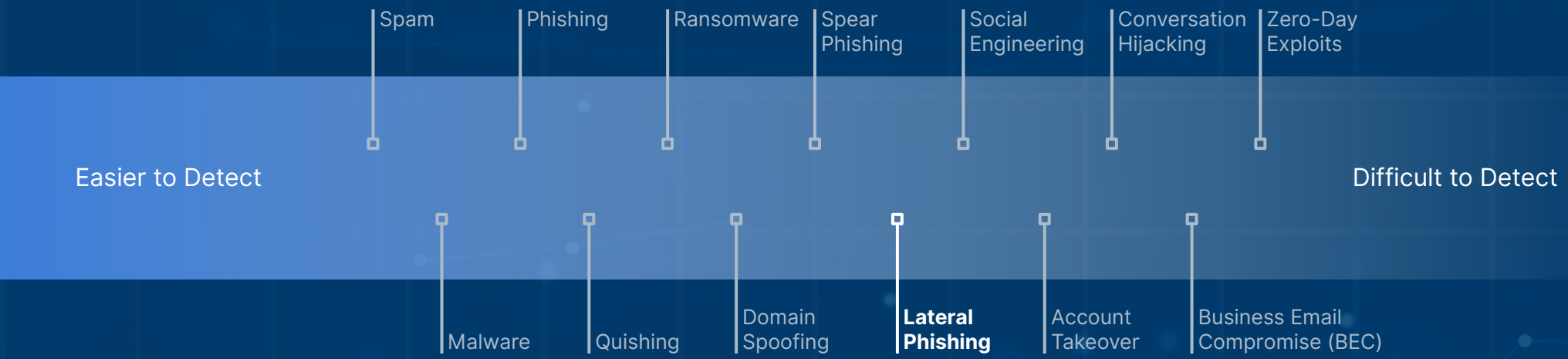
Protect your schools: Identity-aware AI tools detect impersonation attempts using header anomalies, domain analysis, and tone recognition

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Lateral Phishing



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Lateral Phishing

Difficult to detect without behavioral analytics since the email sends from a legitimate account.

What it is: A compromised internal account is used to send phishing emails to others within the district or to trusted partners

K–12 impact: Lateral phishing emails will not be detected by traditional filters, making them highly effective at getting recipients to act

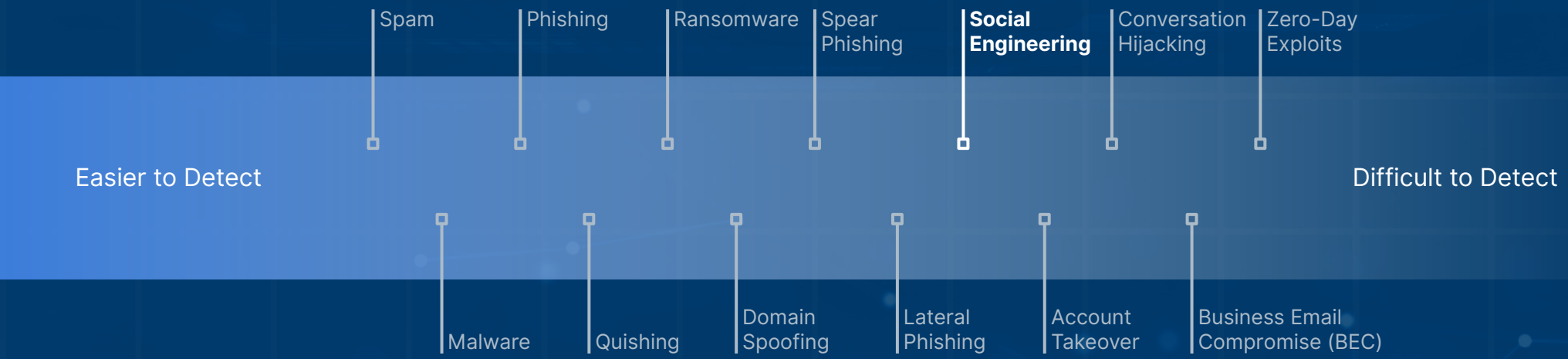
Protect your schools: Use tools that can detect suspicious internal message patterns, flags unusual sharing or email behavior, and alerts admins in real time to stop the spread

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Social Engineering



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

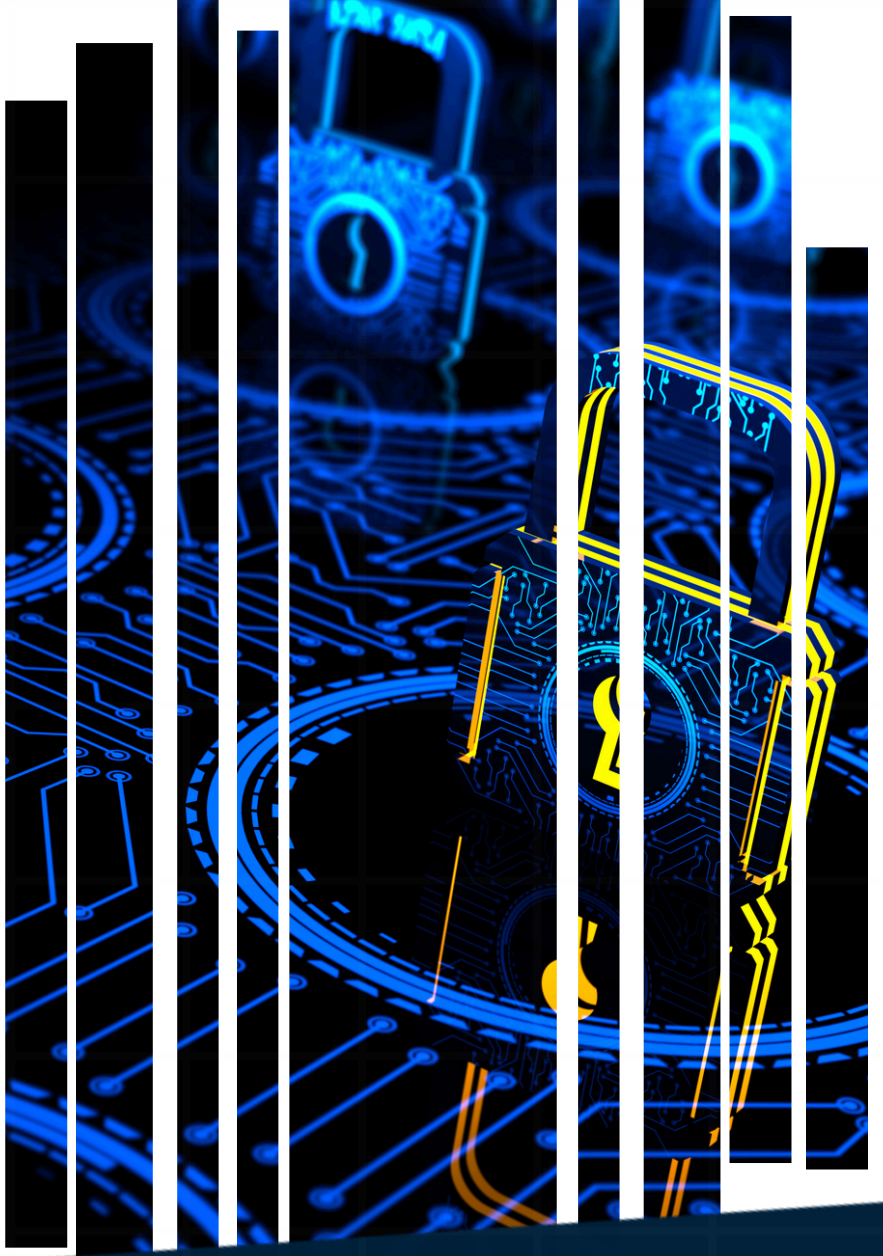
Social Engineering

No malware, no bad links—relies on manipulating people through credible-looking messages.

What it is: Attackers manipulate users into sharing sensitive information, often without using malicious attachments or links

K–12 impact: Staff members can be tricked into revealing login credentials or student data, or remitting payments to criminals

Protect your schools: Behavioral AI tools flag unusual access and sharing patterns and alerts IT teams to potential risks

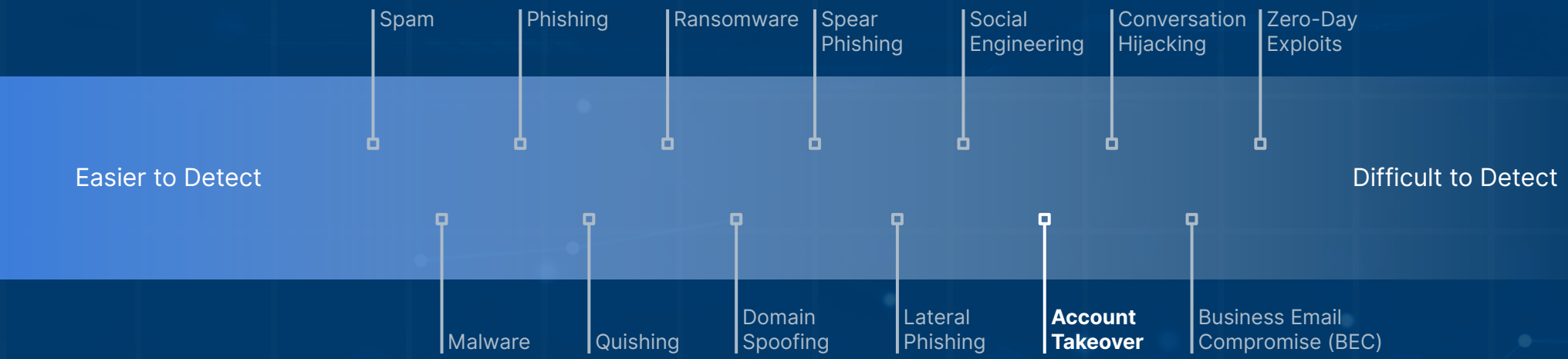


Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Account Takeover



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Account Takeover

Appears as legitimate account activity unless monitored for unusual patterns and login activity.

What it is: A legitimate account is compromised and used to spread attacks internally

K–12 impact: A student's or teacher's account is hijacked and used to phish others or access sensitive files

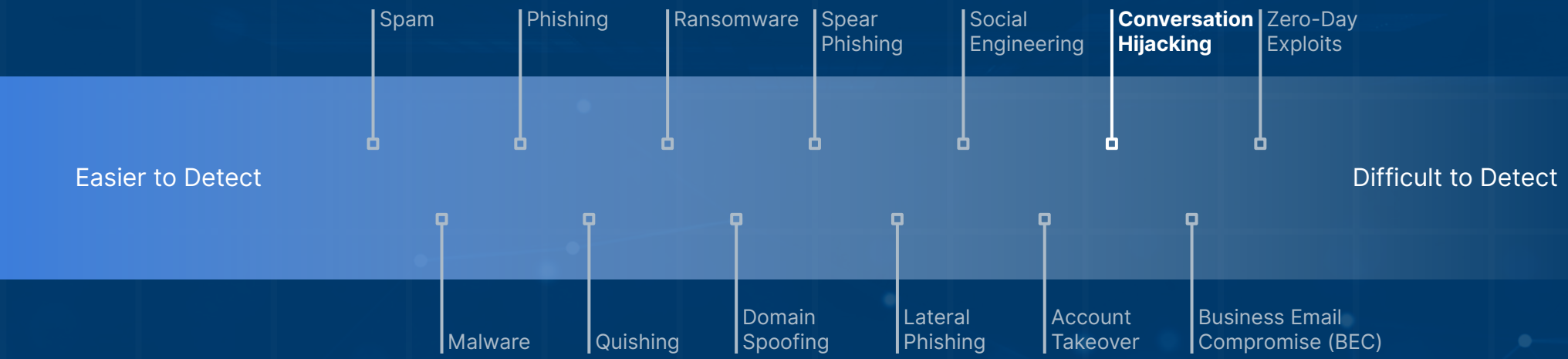
Protect your schools: Invest in a security tool that will monitor geographical access to your users' accounts and account behavior 24/7/365, and alert your IT team to suspicious behavior

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Conversation Hijacking



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Conversation Hijacking

Exploits trust in ongoing threads—extremely subtle and context-driven.

What it is: Attackers insert themselves into existing email threads, often after compromising an account

K–12 impact: An attacker can reply to an existing thread between district admins and vendors to redirect funds or links

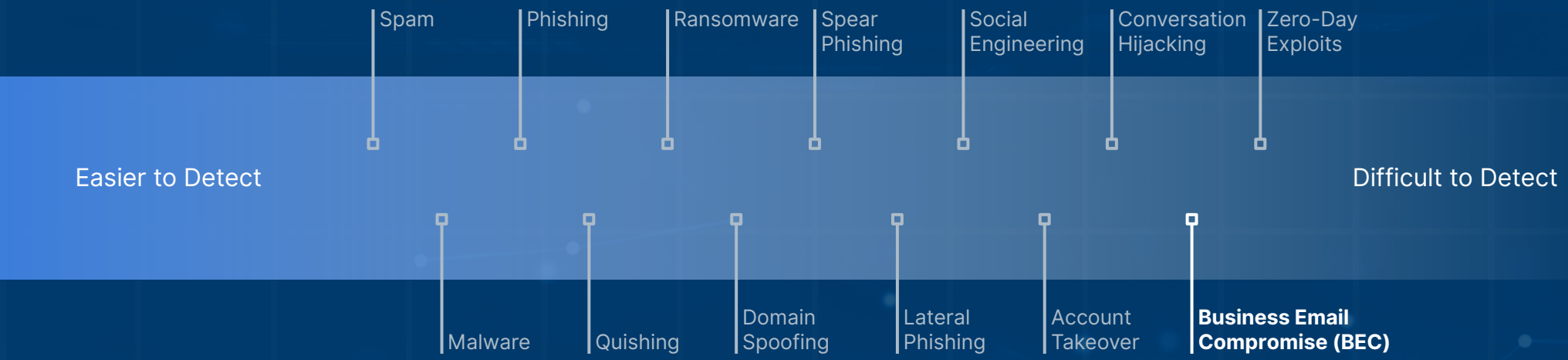
Protect your schools: AI-powered email security tools use anomaly detection to flag changes in conversation participants, tone, and/or context and alert tech teams immediately

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Business Email Compromise (BEC)



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Business Email Compromise (BEC)

No links, no attachments—relies on social engineering, tone, and urgency to manipulate.

What it is: Attackers compromise or spoof district email accounts to redirect payments, steal sensitive data, or gain access to higher-permissions level accounts

K–12 impact: Can manipulate staff into rerouting payments to a fraudulent account, stealing W2s, and other sensitive data

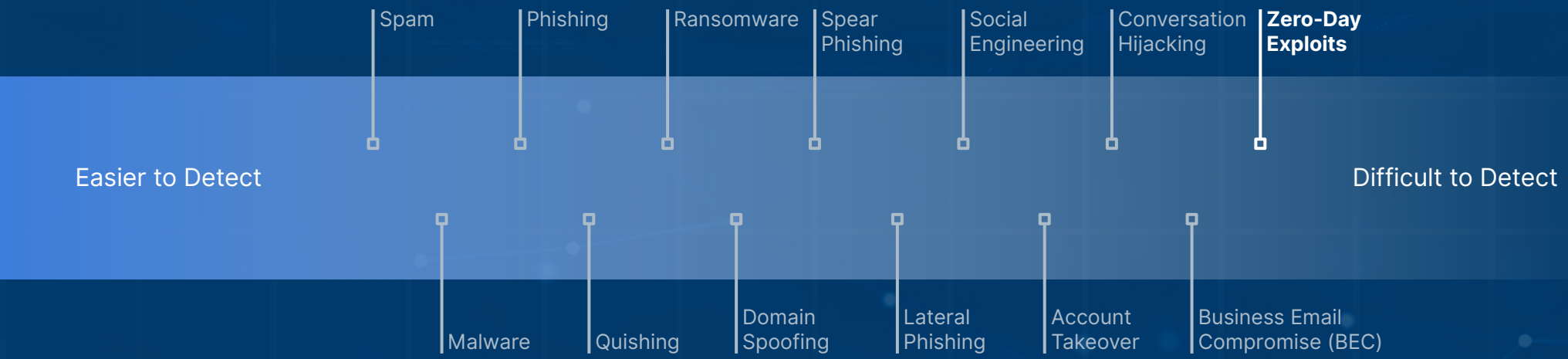
Protect your schools: Use security tools that monitor your district's internal accounts for unusual behavior, internal threats, and suspicious domain spoofing

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Zero-Day Exploits



Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Zero-Day Exploits

Targets vulnerabilities no one knows about.
Requires advanced AI-based behavior detection.

What it is: Attacks that exploit vulnerabilities before vendors issue patches

K–12 impact: Can more easily bypass security by exploiting unknown vulnerabilities in email systems

Protect your schools: AI threat detection is required to identify suspicious email activity, unusual account behaviors, and scans files

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Native Email Filters Aren’t Enough

Google Workspace and Microsoft 365 both offer baseline spam and phishing filters. These tools work well for catching generic threats—emails with known malicious links, blacklisted domains, or clearly inappropriate content.

However, they fall short when it comes to detecting more advanced strategies such as social engineering, account takeovers, lateral phishing, and zero-day attacks. **These filters also don’t understand intent. They can’t assess whether an email is socially engineered or if it’s out of character for the sender.**

Another limitation is visibility. Native tools often lack detailed insights and alerting for IT teams. **If a phishing message is delivered to 10 or 100 inboxes, it’s not always obvious until someone reports it—or worse, clicks.**

Managed Methods

K-12 Cybersecurity & Safety Made Easy

www.managedmethods.com | (303) 415-3640

Protect Your District from the Next Phishing Attack

Request My Demo
Click Here

Phishing emails are evolving. Are your defenses keeping up?

- **Near real-time** phishing detection powered by CoT AI
- **Full integration** with Gmail and Outlook
- **Actionable alerts** and insights sent to your IT team
- **Automated remediation** before the threat spreads
- **Tailored to K–12** threat patterns and language
- **Zero extra dashboards**—fully integrated into Cloud Monitor

Advanced Phishing Protection by ManagedMethods

Email threats are evolving fast. ManagedMethods gives your team the visibility, automation, and protection needed to stay ahead—built specifically for K-12 schools.

Advanced Phishing uses chain-of-thought (CoT) artificial intelligence to analyze 6 key determining factors to decide if an email is phishing or not. Each use complex analysis, using a specific set of heuristics, rather than simple rules or filters.

Mismatched Senders
The display name doesn't match the email address or the sending domain doesn't match the signing domain

Urgency & Threats
Subjects or messages demanding immediate action, threatening account closure, or asking for passwords/money

Impersonation
Pretending to be a known person, company, or authority figure; also, slightly misspelled domains

Suspicious Links/Requests
Asking to click links to log in, verify accounts, or provide sensitive information; also, requests to call phone numbers to fix fake problems or scan QR codes

Unusual Financial Requests
Unexpected invoices, changes to payment details, or requests for wire transfers and gift cards

Odd Attachments/Instructions
Emails with strange file types or instructions to install software

Managed Methods

Monitor | Alert | Respond

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Your Problems, Our Solutions

Data Security
Data loss prevention for sensitive student, staff, & district data stored in Google Workspace & Microsoft 365

Threat Protection
Stop phishing & malware attacks in email & drives using advanced, chain-of-thought reasoning AI

Web Filtering
Browser-level student safety and CIPA compliance with minimal impact on end users

Monitor & Audit
Automated security & behavior monitoring & remediation 24/7/365 with actionable notifications

Safety Signals
Detect self-harm, cyberbullying, suicide, threats of violence & explicit content signals

Classroom Management
Easy, affordable classroom management integrated with Content Filter for optimal control

"**Purchasing Cloud Monitor is one of the best decisions we've made and I would recommend it to other IT teams in K-12.** For us, Cloud Monitor is hands-off 99% of the time and doesn't take many people to run it. It's definitely worth the investment and, when it comes to protecting our data and users in Gmail and Google Workspace, Cloud Monitor is the best cloud security solution that we've found."

Stephen Gauss, Network Administrator

- Automate Google/Microsoft Security
- Data Loss Prevention
- Control FERPA Violations
- Manage 3rd Party Apps
- Control Compromised Accounts
- Quarantine/Delete Phishing Emails
- Manage Lost/Stolen Chromebooks
- Identify Access By Internal/External IP
- Find & Delete Specific Emails
- Find Specific Files
- Manage Google Classrooms
- Block Embedded YouTube Videos
- Online Safety Alerts & Reporting
- Monitor Student Safety

Managed Methods

Monitor | Alert | Respond

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Cloud Monitor

Google Workspace & Microsoft 365 Security, Safety, and Compliance

Data Security
Data loss prevention for sensitive student, staff, & district data stored in Google Workspace & Microsoft 365

Threat Protection
Stop phishing & malware attacks in email & drives using advanced, chain-of-thought reasoning AI

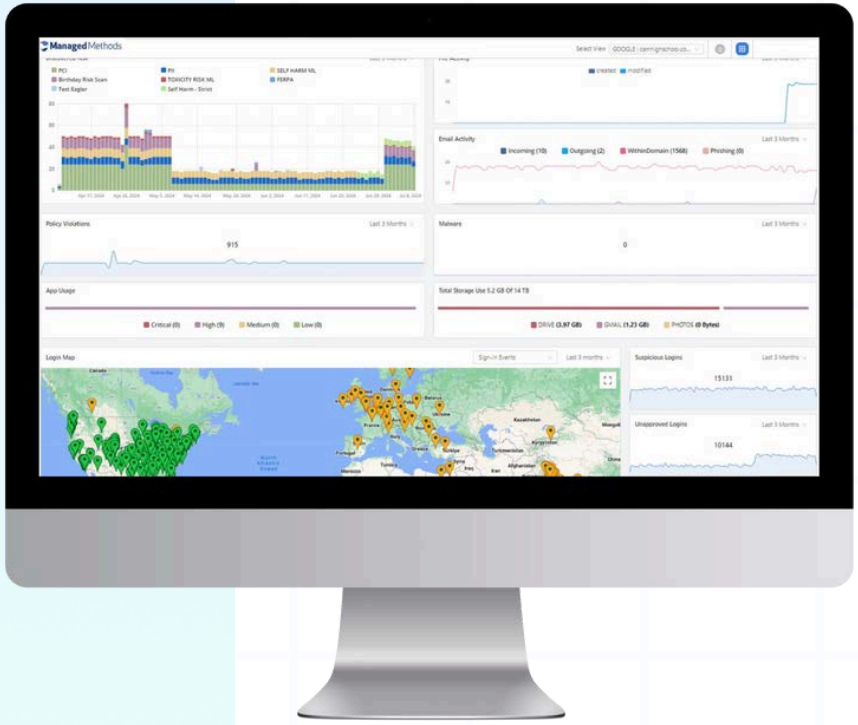
Monitor & Audit
Automated security & behavior monitoring & remediation 24/7/365 with actionable notifications

Safety Signals
Detect self-harm, cyberbullying, suicide, threats of violence & explicit content signals

3rd Party Apps Control
Easily detect and revoke 3rd party apps connected to your district's environment with risky access levels

Easy To Deploy, Easy To Use
Cloud Monitor can be deployed in minutes without extensions, proxies, or agents and does not require extensive training

Cloud Monitor provides a centralized command center for managing Google Workspace and Microsoft 365 cybersecurity and student safety risks that saves K-12 IT admins a significant amount of time and effort.



"**Purchasing Cloud Monitor is one of the best decisions we've made and I would recommend it to other IT teams in K-12.** For us, Cloud Monitor is hands-off 99% of the time and doesn't take many people to run it. It's definitely worth the investment and, when it comes to protecting our data and users in Gmail and Google Workspace, Cloud Monitor is the best cloud security solution that we've found."

Stephen Gauss, Network Administrator

Learn More About **Cloud Monitor**

EDTECH BREAKTHROUGH AWARD 2024 — BEST OVERALL IT SOLUTION PROVIDER - EDUCATION MARKET -

THE EDTECH AWARDS — COOL TOOL WINNER 2024

TECH & LEARNING AWARDS OF EXCELLENCE — BEST OF 2023

www.managedmethods.com | (303) 415-3640

Managed Methods

Monitor | Alert | Respond

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Content Filter

E-rate CIPA Compliance and Online Safety Anywhere, Anytime

Content Filter is a modern, minimalist take on the web content filter. It uses browser-level URL blocking and artificial intelligence to provide student safety, security, and CIPA compliance for K-12 schools.

Web Filtering
Out-of-the-box and highly customizable block & allowlisting made easy

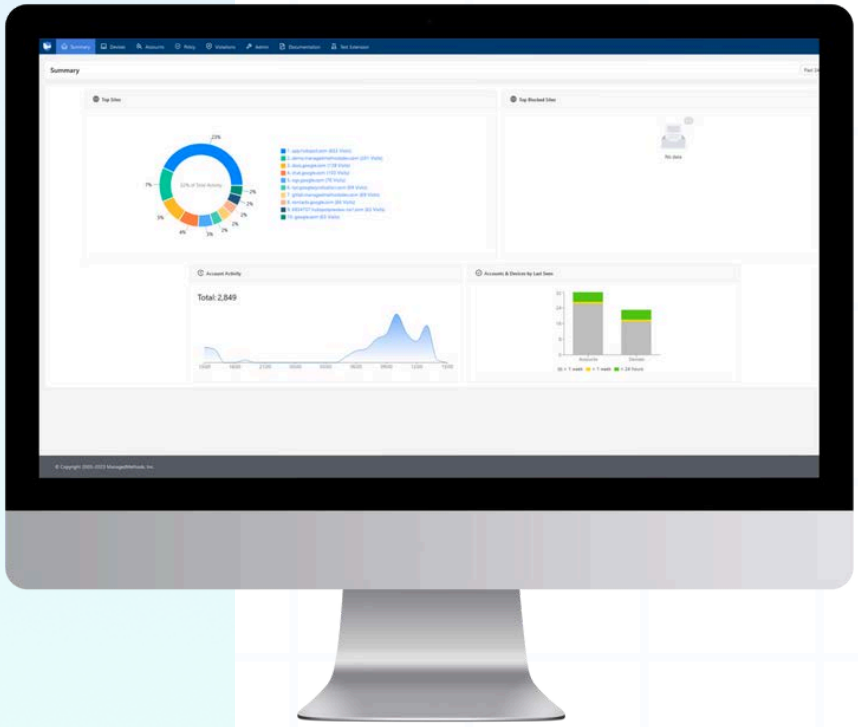
Student Safety
AI-enabled self-harm, suicide, cyberbullying, violence and explicit content detection

YouTube & Games
Highly customizable YouTube and gaming access management

Classroom Management
Empower teachers to keep students focused and engaged with classwork

Device Management
See your devices last known location and account logins. Flag the device as lost/stolen to block Chrome access

Easy To Deploy, Easy To Use
Content Filter can be deployed in minutes and is so lightweight that it won't impact end user experience, even while using other filters



"**Content Filter is so lightweight that we were able to run it at the same time as our existing solution without impacting our end users' experience. We were set up in about 15 minutes and we started seeing results almost immediately**. We were able to report on activity and see what students were attempting to access. It was also impressive that it had no impact on our end users when running both web filters at the same time. It's a no-brainer for us."

Manuel Sanchez, Director of Technology

Learn More About **Content Filter**

2023 WINNER Campus Technology NEW PRODUCT OF THE YEAR

2023 WINNER THE Journal NEW PRODUCT OF THE YEAR

www.managedmethods.com | (303) 415-3640

Managed Methods

Monitor | Alert | Respond

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Classroom Manager

Safe and Engaged Classroom Learning Made Easy

NEW! Classroom Manager integrates with our Content Filter platform, allowing teachers to manage access to certain websites and online content for increased student engagement and safety in the classroom.

Browser Management
Easily block, close, and set certain tabs active for individual students, groups of students, or the whole class

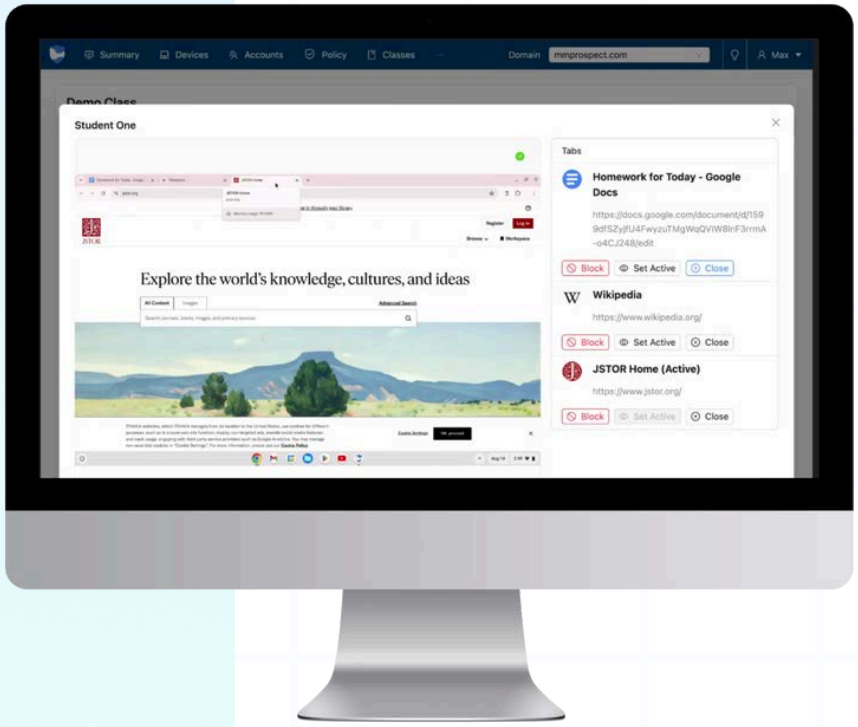
Announcements
Write announcements and send it to the entire class at once using the Chat feature

Pin Student Views
Pin students to the top of the interface to keep a closer eye on students who need more help

Scenes
Group students to allow or block access to online content. Scenes can be pre-set and shared with other teachers

Follow Me
Manage students accessing additional resources during class time, so they don't have to check out

Admin Panel
Set up and manage classes, see how many classes are currently active, and more through the admin panel



"Our teachers love using Classroom Manager! It's easy to navigate, keeps students focused, and eliminates distractions. **The simple, intuitive interface allows teachers to seamlessly manage their classrooms, personalize learning when needed, and customize Classes** to fit their unique teaching style and student needs—making lessons more engaging and effective."

Karen Brunker, Technology Director

Learn More About Classroom Manager

1EDTECH TrustEd Apps CERTIFIED OneRoster®

www.managedmethods.com | (303) 415-3640

Managed Methods

Monitor | Alert | Respond

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Where Are Your Security, Safety, and Compliance Gaps?

Google Workspace/Microsoft 365 Security & Safety	Managed Methods	GoGuardian	Lightspeed	Securly	Linewize	Blocksi
API-Driven Cloud Security, Cloud Native	●	●	●	●		●
Uses Proxies, Agents, and/or Gateways			●	●	●	●
Google Security and Data Loss Prevention	●					
Shared Drive Security and DLP	●					
Gmail AI-Powered Phishing & Malware Threat Protection	●					
Gmail Content Monitoring	●	●	●	●	●	●
Microsoft 365 Security and Data Loss Prevention	●					
Outlook AI-Powered Phishing & Malware Threat Protection	●					
Outlook Content Monitoring	●	●	●	●	●	●
OneDrive/SharePoint Security and DLP	●					
3rd Party Apps Detection and Management	●					
Account Takeover Detection and Response	●					
Student Safety Monitoring in Gmail, Docs, Slides, etc	●	●	●	●	●	●
Student Safety Monitoring in Outlook, Word, PowerPoint, etc	●					
AI & Machine Learning Powered Content Monitoring	●	●		●		
Customizable Filters and Policies, Self-Service	●	●	●	●	●	●
Audits & Reporting for Google/Microsoft Security & Safety	●					

Where Are Your Security, Safety, and Compliance Gaps?

Web Filtering & Classroom Management	Managed Methods	GoGuardian	Lightspeed	Securly	Linewize	Blocksi
Integrated with Google Admin console	●	●	●	●	●	●
Policies by OUs & Groups	●	●	●	●	●	●
Customizable Block/Allow Lists	●	●	●	●	●	●
Filtering by Site Categorization	●	●	●	●	●	●
Online Student Safety Monitoring & Alerts	●	●	●	●	●	●
AI-Powered Student Safety Policies	●	●	●	●		●
Device Management	●	●	●	●	●	●
Available on Chrome	●	●	●	●	●	●
Available on Edge	●	●	●	●	●	●
Available on iOS & macOS		●	●	●	●	●
Integrated Classroom Management/Teacher Tool	●	●	●	●	●	●
Teachers can Block/Allow Specific Websites	●	●	●	●	●	●
View Students' Screens	●	●	●	●	●	●
Open/Close Tabs for Individuals & Entire Class	●	●	●	●	●	●
Group Students into Customizable Scenes	●	●	●	●	●	●
Built-In Video Conferencing		●		●		●
Teacher Training Provided	●	●	●	●	●	●
OneRoster SIS Integration	●	●	●	●	●	●

K-12's Trusted Brand in Cybersecurity & Safety

"**During our free audit, we found out some of our student accounts were getting hacked from other countries.** I would have had no idea without that early warning system. I was able to show the district this is important for us to have for two reasons. One, to detect it, and two, to deal with it in real time."

James Hatz, Technology Coordinator

"The return on investment is huge. Most districts, ourselves included, don't have an enormous budget. **What I love about Cloud Monitor is that not only is it affordable, but you get so much with it. You can really do a lot**."

Michael Tapia, Director of Enterprise Information Services

60+

5-star Google reviews

FREE! GOOGLE/MICROSOFT 365 AUDIT
Request My Free Audit

Your Time Is Limited. Your Risks Are Not.

They say that time is the only thing that money can't buy. And when you're being pulled in a hundred directions and a cyber incident occurs, time is at an all-time premium.

K-12 technology departments are notoriously understaffed and underfunded.

ManagedMethods is familiar with the many unique needs and challenges impacting your district's cybersecurity and safety, and is committed to making a difference.

You need tools that are affordable and easy to use.

Learn why district leaders across the country trust ManagedMethods' suite of products to keep their data secure and their students safe.