SOLUTION BRIEF

Multi-Signal Managed Detection and Response for U.S. Education Institutions

Prevent learning disruptions and protect student data with 24/7 threat detection, investigation, and rapid containment.

Schools, libraries, and consortia in the United States are facing a surge in cyber threats that have put the privacy of students and staff, and the continuity of education, at risk. In the past five years, cyberattacks have accelerated rapidly, exposing millions of sensitive student records, disrupting classes, and forcing districts to divert precious resources to emergency IT recovery. Ransomware, phishing, vendor breaches, and DDoS attacks have become regular occurrences, hitting districts large and small across the country.

In fact, threat research from eSentire's Threat Response Unit (TRU) shows that the **Education industry saw the greatest proportion of browser-sourced malware and 'unknown' initial access vectors**. This increase in cyberattacks can be attributed to several factors.

First, employees in this sector are made up of educators, administrative staff, and students often sharing segmented but linked networks. The 'unknown' vector often points to out-of-scope endpoints or network segments as the origin for intrusions; in this case, student WiFi networks provide one such possibility. Second, educators often use search engines to find documents such as lesson templates, exposing them to malware distributed via search advertisements or SEO poisoning.

In some cases, cybercriminals demanded ransoms, threatened to leak data, and left schools scrambling to restore learning systems. The cost of these incidents is measured not only in dollars, often **exceeding $700,000 per day in lost productivity and recovery**, but also in lost instructional time and community trust.

Moreover, TRU also found that identity-driven threats have skyrocketed since 2023, now accounting for 59% of all confirmed cases in early 2025, highlighting a **156% surge in identity-based attacks between 2023 - 2025**. Our threat research shows that the education industry was disproportionately represented on name-and-shame leak sites from 2020-2023, likely due to an abundance of student logins found in stealer logs.

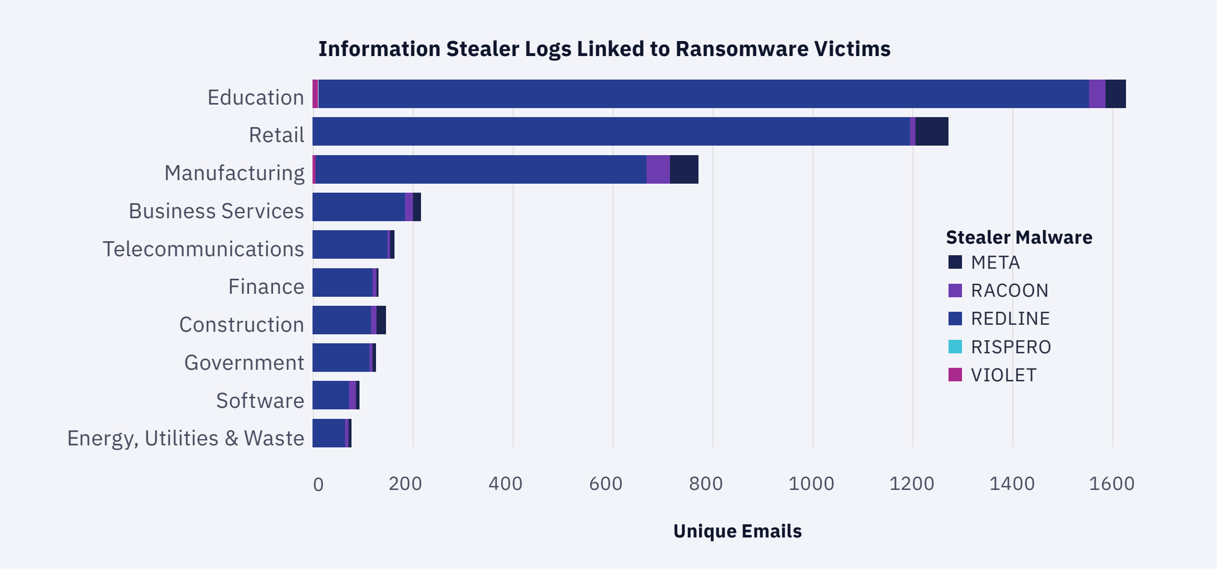


Figure 1: Breakdown of information stealer logs containing identifiable account names tied to ransomware victims identified on name-and-shame leak sites between 2020 and 2023.

Educational institutions, including schools, libraries, and consortia, are uniquely vulnerable. They must serve a large, diverse, and often underage population while balancing limited cybersecurity budgets, aging infrastructure, and a growing digital attack surface. Most districts lack dedicated security teams and cannot monitor networks around the clock. At the same time, attackers are growing more sophisticated, leveraging supply chain vulnerabilities and social engineering to bypass defenses.

The result: education institutions have become soft targets in the eyes of cybercriminals.

What's more, securing the Education sector is complex. IT/Security teams are often stretched thin, managing dozens of campuses and thousands of endpoints with limited staff. Many rely on outdated systems, flat networks, and third-party applications that introduce risk but are critical to day-to-day operations. When attacks do occur, the impact is immediate: online learning platforms, communication systems, and payroll can all be taken offline in a single incident, leaving administrators, teachers, and families in the dark.

Moreover, the regulatory landscape is also evolving. Yet many boards still lack comprehensive incident response plans or the resources to conduct regular security assessments and staff training. The growing frequency of attacks has also triggered steep increases in cyber

How the FCC Cybersecurity Pilot Program Helps Eligible Education Institutions Strengthen their Cyber Defenses

The FCC Schools and Libraries Cybersecurity Pilot Program is a three-year initiative that will provide up to $200 million in funding to help eligible public and private K-12 schools and libraries address the growing cybersecurity risks facing educational institutions by supporting the deployment of advanced cybersecurity services and equipment.

Eligible funding categories include advanced firewalls, endpoint protection, identity protection and authentication, and monitoring, detection, and response solutions:

Advanced and Next-Generation Firewalls

Capabilities may include deep packet inspection, intrusion prevention, application-layer controls, threat intelligence integration, and support for segmentation/micro-segmentation.

Endpoint Protection

Solutions such as Endpoint Detection and Response (EDR), anti-malware, and managed endpoint security that provide proactive threat detection and automated response for workstations, laptops, tablets, and mobile devices.

Identity Protection and Authentication

Multi-factor authentication (MFA), single sign-on (SSO), privileged access management (PAM), and identity threat detection and response (ITDR) to secure user access across networks and cloud environments.

Monitoring, Detection, and Response

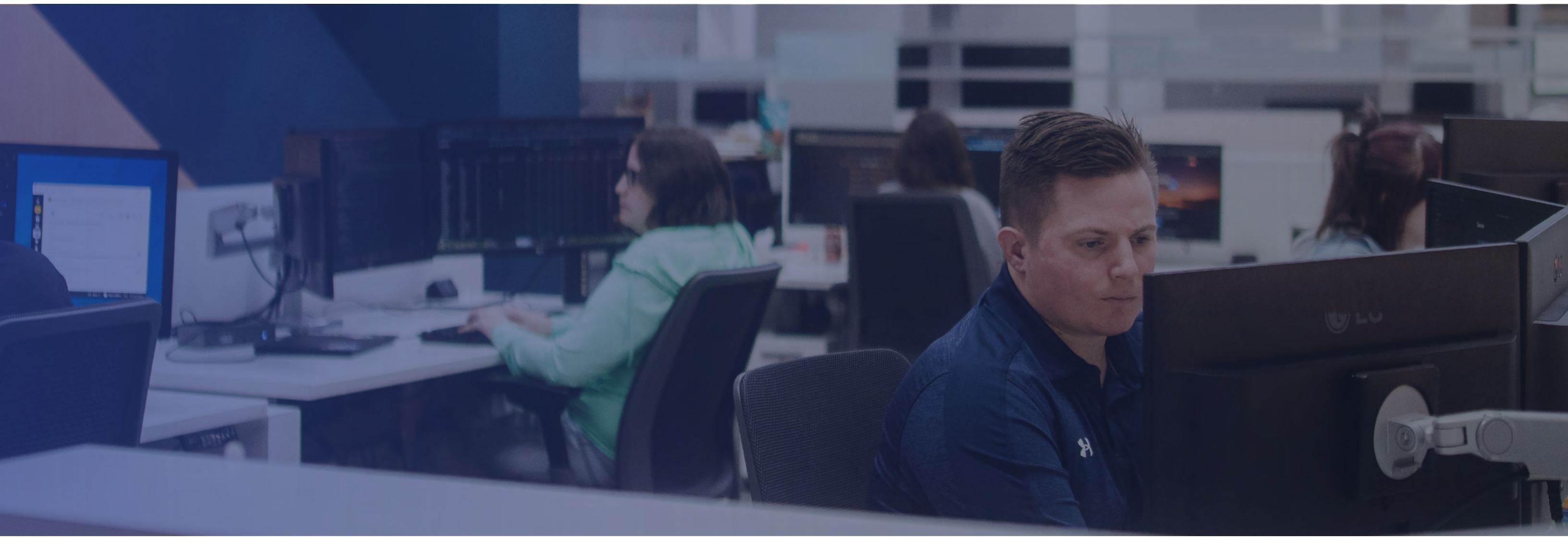
Security operations center (SOC)-as-a-service, SIEM (Security Information and Event Management), log monitoring, managed detection and response (MDR), and threat intelligence platforms. These solutions provide continuous visibility and incident response across hybrid and cloud-connected environments.

Introducing eSentire MDR to Take Your Security Program to the Next Level

We are recognized globally as The Authority in Managed Detection and Response (MDR) because we hunt, investigate, and stop sophisticated cyberattacks before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry—financial services. Over the last two decades, we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers (SOCs) and 2,000+ customers across 80+ countries, we have scaled to deliver cybersecurity services across highly regulated industries with a proven track record of success in securing the education sector.

At eSentire, we go beyond the market's capability in threat response and specifically address cybersecurity risks. Our Next Level MDR solution ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. We combine AI-driven precision with elite human expertise to deliver the most resilient, outcomes-driven security protection in the industry.

The Atlas XDR platform provides automated blocking capabilities to prevent attackers from gaining an initial foothold while our expert Elite Threat Hunters initiate human-led threat investigation and containment at multiple levels of the attack surface. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level.



Security Operations Built on Expert AI

eSentire Atlas AI isn't another automation script or task eliminator. It's a multi-agent Generative AI system purpose-built and embedded across eSentire's Atlas AI Security Operations Platform to scale human expertise – trained on real-world workflows validated by investigations across 2,000+ customers globally.

Atlas AI is fully embedded into our platform and included as part of your MDR service. Designed to scale human expertise, not replace it, Atlas AI gives your security operation a competitive edge by providing transparency, context and validation previously unattainable in minutes. We show up and prove results:

35%
Faster threat intelligence vs commercial feeds

99%
Noise reduction across customer environments

95%
SOC expert alignment with Atlas AI investigations

99.3%
Of threats isolated at the first host

200
New threat protections added per day to harden customer defences

43x
Investigation acceleration with 5 hours of investigation work achieved in less than 7 minutes

96%
SOC analyst retention, with an average tenure of 6 years

Maximize Your FCC Cybersecurity Pilot Program Funding with eSentire

eSentire is uniquely positioned to help K-12 schools, districts, and libraries make the most of the FCC Cybersecurity Pilot Program. Our services are fully aligned with all four categories of eligible funding, including advanced firewalls, endpoint protection, identity protection and authentication, and 24/7 threat monitoring, detection, and complete response capabilities.

How We Help You Capture Every Eligible Dollar:

1. **Comprehensive, Eligible Coverage:** eSentire's 24/7 multi-signal MDR portfolio aligns directly with all four FCC-eligible funding categories: advanced firewalls, endpoint protection, identity protection/authentication, and monitoring, detection & response. We help you cover the full spectrum of eligible services so you can apply for the maximum allowable funding, instead of leaving dollars unclaimed on the table.
2. **Strategic Solution Design & Documentation:** Our expert team partners with you to design a cybersecurity project plan that addresses your true risk profile and operational needs, ensuring all proposed services are eligible and well-justified in your FCC applications. We provide clear scope, cost breakdowns, and compliance language to support your submission and improve the likelihood of a higher funding commitment.
3. **Bundled, Integrated Solutions:** We deliver multi-signal MDR as a bundled service, covering firewalls, endpoints, identity, and 24/7 monitoring, allowing you to consolidate technology spend into a single, comprehensive project that can be submitted for reimbursement. This reduces complexity and increases your claimable spend within your funding cap.
4. **Rapid Implementation & Ongoing Compliance:** With fast onboarding and full documentation support, we help you activate funded services quickly so you can invoice the FCC for reimbursement as soon as possible. We also support the required annual and final reporting, keeping you in compliance for the duration of the Pilot and beyond.
5. **Demonstrable Value & ROI:** Our reporting and analytics through the Insight Portal help you track security improvements and outcomes, supporting the case for future funding and demonstrating the effectiveness of your investments to the FCC and your stakeholders.

Our Services

Our cybersecurity services portfolio is designed to stop breaches, simplify security, and minimize business risk. We provide around-the-clock threat protection that is proactive, personalized, and cost effective.

Continuous Threat Exposure Management (CTEM)

CTEM and advisory programs that identify security gaps and build proactive strategies to address them.

Managed Detection and Response (MDR)

Combine AI-driven security operations, multi-signal attack surface coverage and 24/7 Elite Threat Hunters to help you take your security program to the next level.

Digital Forensics and Incident Response

eSentire Digital Forensics and Incident Response services are available as IR Readiness, Incident Response Retainer or Emergency Incident Response Services.

Why K-12 Education Institutions Choose eSentire

Build Resilience. Prevent Disruption.

- **AI-Driven Security Operations Platform** - Our multiagent Generative AI system is embedded across the Atlas Security Operations Platform to empower human experts that protect your complete attack surface.
- **24/7 SOC-as-a-Service** - Get unmatched, complete threat response capabilities with a 15-min Mean Time to Contain, driven by our open XDR Platform.
- **Talent Expertise** - Outmaneuver even the most sophisticated attackers with the eSentire Cyber Resilience Team, who are personally dedicated to protecting your organization.
- **Threat Intelligence** - Stay ahead of advanced cyberattacks with proactive threat intelligence, original threat research, and the eSentire Threat Response Unit (TRU), a world-class team of seasoned industry veterans.
- **Measurable MDR Value** - Get full transparency into the health of your environment and how we protect your critical assets from threats with our Executive Dashboard, Insight Portal, and Cyber Resilience Score.
- **Culture & Experience** - Our team is your team, and we are motivated to demonstrate each and every day that an Attack On You Is An Attack On Us.

Mapped

MITRE ATT&CK

Certified

AICPA SOC 2

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Awards

IDC LEADER

MSSP Alert THE TOP 250 MSSPs 2024 EDITION

NAMED #8 & TOP MDR PROVIDER

FORRESTER WAVE LEADER 2025 Managed Detection And Response Services In Europe

FORRESTER WAVE CUSTOMER FAVORITE 2025 Managed Detection And Response Services In Europe

$6.5T+ Total AUM	**300+** Technology Integrations	**6000** Daily Human-led Investigations	**700** Daily Escalations
20M Daily Signals Ingested	**3M** Daily XDR Automated Disruptions	**400** Daily Threat Containments	**15min** Mean Time to Contain

Gartner Peer Insights™

★★★★★

4.7 out of 5

★★★★★

"eSentire Provides A Bullet-Proof Suite Of Products!"

IT Manager

In the Banking Industry

Read full review here >

★★★★★

"eSentire provides SOC services at an affordable price."

Senior Cyber Security Admin

In the Consumer Goods Industry

Read full review here >

★★★★★

"Excellent partner that is proactive with alerts, new detection intelligence, and overall very responsive to customer incidents."

Director of IT Infrastructure & Cybersec

In the Healthcare and Biotech Industry

Read full review here >

G2

★★★★★

4.7 out of 5

★★★★⯪

"eSentire's got your back at anytime 24/7"

Brice A.

Enterprise Company

Read full review here >

★★★★★

"Top notch MDR partner."

Verified User in Manufacturing

Enterprise Company

Read full review here >

★★★★★

"eSentire is an extension of my team."

Phil M.

Mid-Market Company

Read full review here >

Ready to Get Started?

We're here to help! Reach out to connect with an eSentire security specialist and build a more resilient security operation today.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US ☎ 1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.