SOLUTION BRIEF:

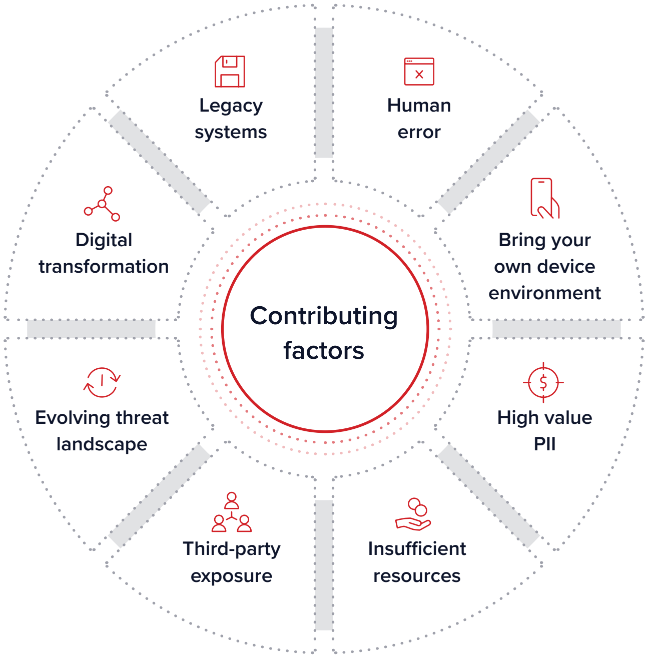
Focus on Cybersecurity: Education

The education sector has a unique set of cybersecurity risks it must factor in relative to a broad array of personal devices used to access information and learning platforms, as well as the adhering to governmental requirements that protect students' sensitive data. In February 2020, the U.S. Department of Education issued a statement regarding its enforcement of cybersecurity requirements and provided notice of increased scrutiny around cybersecurity programs.[1] Under it, K – 12 schools and districts, as well as higher education institutions, are subject to requirements set by three regulatory bodies: Health Insurance Portability and Accountability Act - HIPAA, Family Educational Rights and Privacy Act - FERPA and Children's Online Privacy Protection Rule - COPPA.

With constrained and under resourced security/IT teams, the workload significantly increases to properly manage these requirements and ensure compliance to avoid severe penalties. Since 2005, the Privacy Right Clearinghouse reported that over 780 data breaches have occurred in K-12 schools and institutions of higher education that led to 14,871,122 compromised records.[2] Unfortunately, the risk associated with students' data is increasing and compounding the problem is the unexpected shift to virtual learning environments that only increase the pressure on constrained cybersecurity resources. As the education industry looks to bridge the gap, a holistic approach that matures prevention, detection, response and recovery capabilities will be critical in mitigating risk to the education sector.

Top Education Security Challenges

1. A clear understanding of risk-based best practices
2. Lack of visibility into personal devices (BYOD)
3. Technical capabilities to identify and contain threats across multiple technologies and devices
4. Zero-day risks, often associated with global mega attacks
5. Lack of internal resources and expertise
6. Lack of response plan and slow response to past incidents
7. Compliance with regulatory requirements



[1] Federal Student Aid, an office of the Department of Education, 2020

[2] Department of Education, REMS, 2019

eSentire: Observing Risks in the Education Sector

We understand the unique challenges your cybersecurity team faces. We've seen the dynamic nature of threats that seek valuable personally identifiable information (PII) data specifically target the education sector. Over the past three years, educational institutions around the globe have seen an increase in incidents bypassing traditional prevention technologies, causing expensive remediation efforts.

Large-scale data breaches in the education sector

In 2017, the U.S. Department of Education warned school districts regarding the increase in cyberattacks which extort money to avoid PII data from being released on students, teachers and employees.[3]

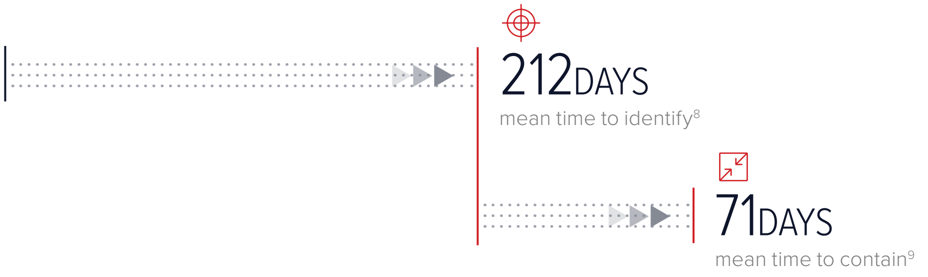
In 2018, over 300 universities worldwide and 144 U.S. universities were part of a cyberattack by Iranian hackers that stole over 30 terabytes of data costing universities over $3.4 billion dollars.[4]

In 2019, Georgia Institute of Technology reported that they were breached, exposing the PII data of 1.3 million students, teachers, staff and student applicants.[5]

80% of attacks on the educational sector were ransomware attacks distributed via malware on websites.[6]

Industry reports indicate 28% of security incidents convert to data disclosure for Educational Services.[7]

Due to the complicated and unique nature of the education sector, cybersecurity teams continue to see rising timeframes to identify and contain security incidents.



212DAYS
mean time to identify[8]

71DAYS
mean time to contain[9]

Unfortunately, the financial consequences of data disclosure have proven devastating. Detection and escalation, notification and post breach costs are significantly higher than in other sectors.

$142 per record lost[10]

$4.77M average cost of a data breach[11]

Costs associated with a breach	Detection and escalation costs[12]	Post breach costs[13]	Notification costs[14]
Average total cost in 2019 (USD)	$1,270,000	$1,070,000	$210,000

[3] Government Department of Student Privacy, A new type of cyber extortion, 2017

[4] Department of Justice, 2018

[5] SC Magazine, Georgia Tech stung with 1.3 million-person data breach, 2019

[6] DBIR Report, 2020

[7] Verizon DBIR Report, 2020

[8] Ponemon: Cost of a Data Breach Report, 2019

[9] Ponemon: Cost of a Data Breach Report, 2019

[10] Ponemon: Cost of a Data Breach Report, 2019

[11] Ponemon: Cost of a Data Breach Report, 2019

[12] Ponemon: Cost of a Data Breach Report, 2019

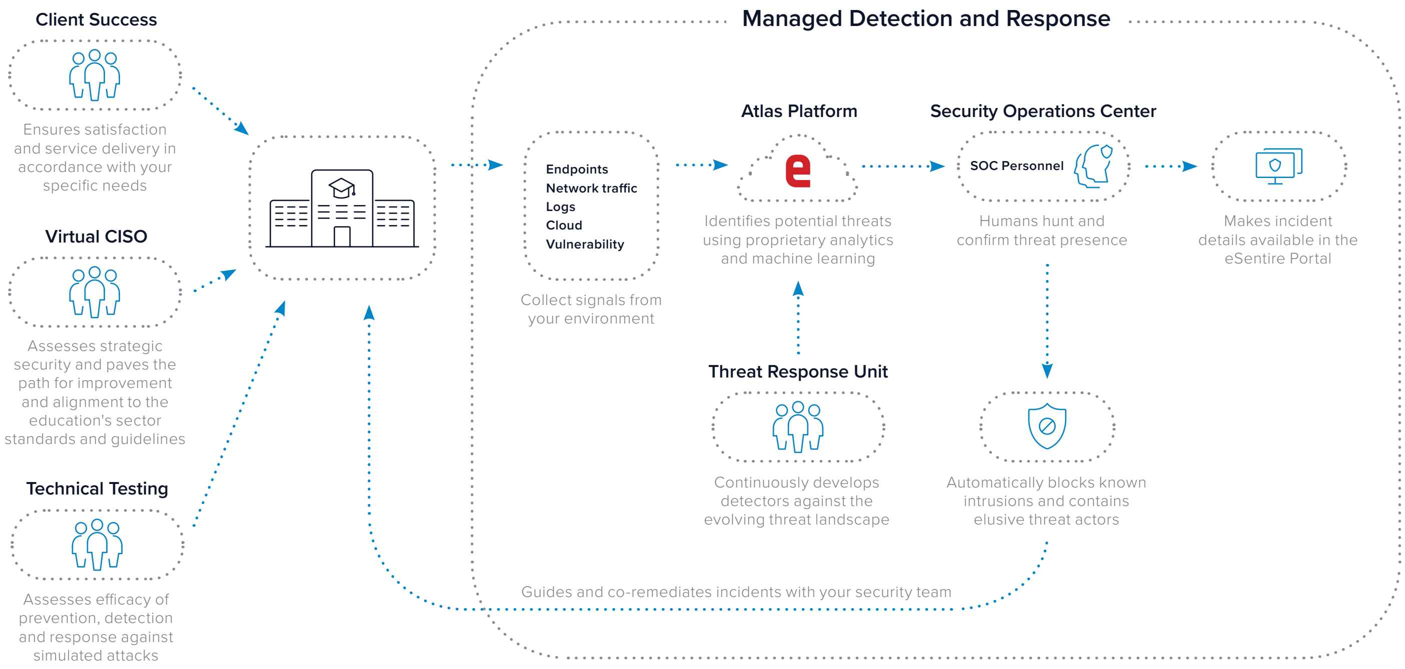
[13] Ponemon: Cost of a Data Breach Report, 2019

[14] Ponemon: Cost of a Data Breach Report, 2019

A Comprehensive Approach to Protect the Education Industry

Whether your organization is a K-12 school district or a higher education institution, threat actors are going to capitalize on vulnerable systems and your highly valuable PII data. Ultimately, the difference between organizational protection and potential disruption will come down to the speed at which you can identify and contain an attack.

At eSentire, our comprehensive approach helps organizations test, mature, measure and protect their environments from a multitude of risk factors. Our Managed Detection and Response (MDR) services rapidly identify and contain threats that bypass traditional security controls. Ingesting signals across the litany of devices that access your systems every day, we combine endpoint, network, log, vulnerability and cloud data to identify known and elusive threats. Averaging 20 minutes from identification to containment, we ensure attackers don't have time to achieve their objectives. Our risk management services test your existing defenses against simulated attacks, assess and measure your security posture and help to build a path for resiliency that ensures alignment with regulatory requirements and a better security posture And these services are supported by a dedicated team focused on your organization's unique requirements and compliance objectives.



Client Success

Ensures satisfaction and service delivery in accordance with your specific needs

Virtual CISO

Assesses strategic security and paves the path for improvement and alignment to the education's sector standards and guidelines

Technical Testing

Assesses efficacy of prevention, detection and response against simulated attacks

Managed Detection and Response

Endpoints
Network traffic
Logs
Cloud
Vulnerability

Collect signals from your environment

Atlas Platform

Identifies potential threats using proprietary analytics and machine learning

Security Operations Center

SOC Personnel

Humans hunt and confirm threat presence

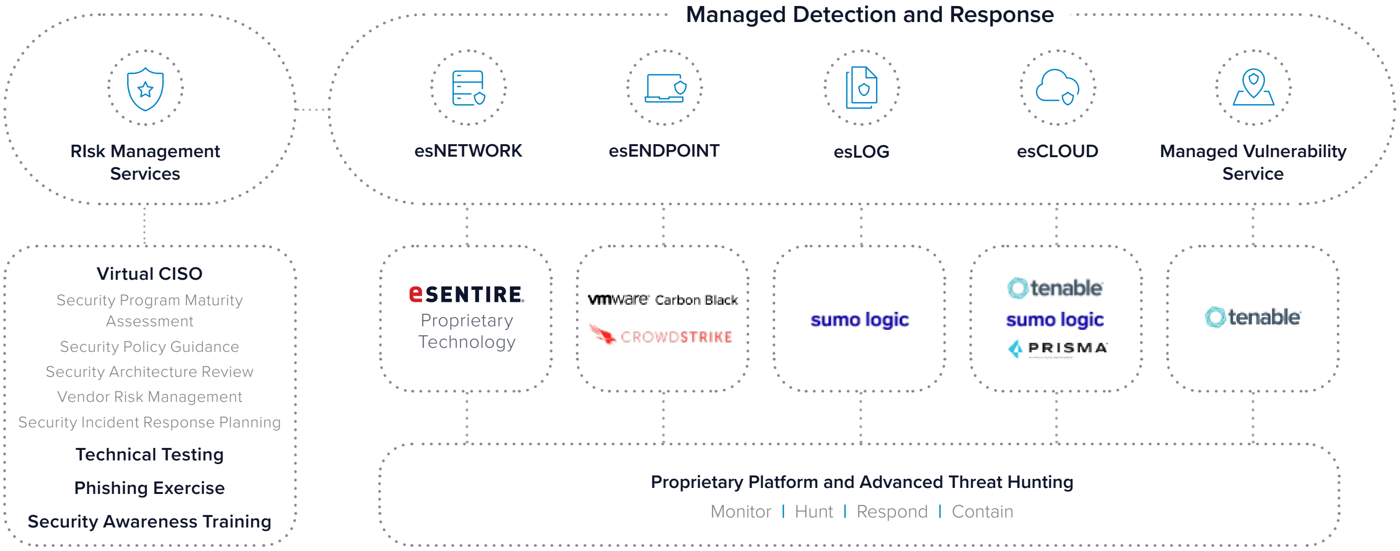
Makes incident details available in the eSentire Portal

Threat Response Unit

Continuously develops detectors against the evolving threat landscape

Automatically blocks known intrusions and contains elusive threat actors

Guides and co-remediates incidents with your security team



RIsk Management Services

Managed Detection and Response

esNETWORK

esENDPOINT

esLOG

esCLOUD

Managed Vulnerability Service

Virtual CISO

Security Program Maturity Assessment

Security Policy Guidance

Security Architecture Review

Vendor Risk Management

Security Incident Response Planning

Technical Testing

Phishing Exercise

Security Awareness Training

eSENTIRE Proprietary Technology

vmware Carbon Black

CROWDSTRIKE

sumo logic

tenable

sumo logic

PRISMA

tenable

Proprietary Platform and Advanced Threat Hunting

Monitor | Hunt | Respond | Contain

eSentire Service Alignment to Education's Top Challenges

	eSentire Managed Detection and Response	eSentire Managed Risk Programs
A clear understanding of risk-based best practices	N/A	• Virtual CISO • Security Program Maturity Assessment • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Vendor Risk Management
Lack of visibility into personal devices (BYOD)	• esLOG • Managed Vulnerability Service (MVS)	• Virtual CISO • Vulnerability Management Program
Technical capabilities to identify and contain threats across multiple technologies and devices	• esNETWORK • esENDPOINT • esLOG • esCLOUD *Limitations across public access devices (BYOD)	N/A
Zero-day risks, often associated with global mega attacks	• esNETWORK • esENDPOINT • esLOG • esCLOUD • Managed Vulnerability Service (MVS)	• Virtual CISO • Vulnerability Management Program
Lack of internal resources and expertise	• esNETWORK • esENDPOINT • esLOG • esCLOUD • Managed Vulnerability Service (MVS)	• Virtual CISO • Security Program Maturity Assessment • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Vendor Risk Management
Lack of response plan and a slow response to past incidents	N/A	• Virtual CISO • Vulnerability Management Program
Compliance with regulatory regimes	• esNETWORK • esENDPOINT • esLOG • esCLOUD • Managed Vulnerability Service (MVS)	• Virtual CISO • Security Program Maturity Assessment • Security Policy Guidance • Security Architecture Review • Security Incident Response Planning • Vendor Risk Management

Understanding Regulatory Compliance Requirements

The education sector in the U.S. must operate under three core regulatory requirements: FERPA, COPPA and HIPAA. FERPA is specifically aligned with the rights granted to parents of students under the age of 18 and students over the age of 18 enabling control over the data that they provide to their educational institution. Additionally, under COPPA, educational institutions are required to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's personal information. And HIPAA is relevant to any institution that provides medical care and/or medical procedures to their students. Finally, the education sector is responsible for meeting U.S. Department of Education requirements made up of rules and requirements for organizational, operational, and procedural assessments to identify gaps and mitigate risk against growing cyberattacks.

Guidance from the Department of Education

Standards and Guidelines	Applicable eSentire Services
Employee training and management	Managed Risk Programs - vCISO
Information systems, including network and software design, as well as information processing, storage, transmission and disposal	Managed Risk Programs - vCISO
Detecting, preventing and responding to attacks, intrusions, or other systems failures	Managed Detection and Response (MDR)

FERPA Compliance

Standards and Guidelines[15]	Requirements	Applicable eSentire Services
Cybersecurity training	Ongoing training should be issued to employees who work with student data.	Managed Risk Programs - vCISO
Encryption	Encryption on devices is required to help secure student data on a physical level if property is stolen.	N/A
Vulnerability management programs	Perform vulnerability scans on your IT infrastructure and databases for potential vulnerabilities. If vulnerabilities are found, immediately correct the issues.	Managed Detection and Response (MDR)
Cybersecurity assessments and information security plans	Perform regular assessments of your information security plan and update accordingly.	Managed Risk Programs - vCISO
24x7 network monitoring	Maintain a monitoring solution to actively identify, block and respond to threats and monitor for compliance changes and enforcement.	Managed Detection and Response (MDR)

[15] *How to comply with FERPA, https://resources.infosecinstitute.com/how-to-comply-with-ferpa/#gref*

Many educational institutions do not realize that they do fall under COPPA compliance. Put simply, COPPA applies to operators of websites and online services that collect personal information from children under the age of 13.[16]

Under COPPA, each of the following PII (personally identifiable information) data must be protected:[17]

1. full name
2. home or other physical address, including street name and city or town
3. online contact information like an email address or other identifier that permits someone to contact a person directly — for example, an IM identifier, VoIP identifier, or video chat identifier
4. screen name or user name where it functions as online contact information
5. telephone number
6. Social Security number
7. a persistent identifier that can be used to recognize a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier
8. a photo, video, or audio file containing a child's image or voice
9. geolocation information sufficient to identify a street name and city or town
10. other information about the child or parent that is collected from the child and is combined with one of these identifiers

COPPA Compliance

Standards and Guidelines[18]	Requirements	Applicable eSentire Services
Post COPPA-compliant privacy policy	Post a clear, comprehensive privacy policy that details how personal information collected regarding users under 13 is used	Managed Risk Programs - vCISO
Notify parents of information collection practices	Give parents direct notice of information collection practices before you collect PII data	Customer responsibility
Achieve parental consent	Receive consent from parents to collect PII data on students/children under the age of 13	Customer responsibility
Honoring parents ongoing rights over their children's PII data	Methods must be in place to honor ongoing rights of the parents regarding reviewing their child's PII, revoking consent for collecting PII and enable them to delete data whenever they please.	Customer responsibility
Implement security policies and procedures	Implement and maintain reasonable information security procedures to protect the security, confidentiality and integrity of personal information collected from users under 13	Managed Risk Programs - vCISO

[16] *FTC.gov, Six Step Compliance Plan*

[17] *FTC.gov, Six Step Compliance Plan*

[18] *How to comply with COPPA, https://resources.infosecinstitute.com/how-to-comply-with-coppa-7-steps/#gref*

Experience the eSentire Difference

Organizations all over the world rely on eSentire as their first line of defense and trusted partner in the fight against an ever-evolving threat landscape. Our 97 percent client retention rate is testament to delivering on our core mission: a client's network can never be compromised. Our expert teams that deliver and support our services are consistently developing the latest methods that ensure your organization is protected against the latest threat actors and aligned to standard guideline requirements that keep your stakeholders, employees, students and systems safe from disruption.

97%
CUSTOMER RETENTION RATE

750+
GLOBAL CUSTOMERS

ACROSS
6
CONTINENTS

IN
60
COUNTRIES

6+
INVESTIGATIONS EVERY MINUTE

640+
CONFIRMED SECURITY INCIDENTS A DAY

	eSentire MDR	PSEUDO MDR
24x7 always on monitoring	✓	Limited
Full spectrum visibility (PCAP, Endpoint, Log, Vulnerability, Cloud)	✓	Limited
Detection utilizing signatures and IOCs	✓	✓
Detection of unknown attacks leveraging patterns and behavioural analytics	✓	Limited
Continuous elite threat hunting	✓	✗
Alerting of suspicious behaviour	✓	Limited
Alerts	✓	✓
Confirmation of true positive	✓	Limited
Remediation recommendations	✓	✓
Tactical threat containment on client's behalf	✓	Limited
24x7 investigation and SOC support	✓	✗ Need IR Retainer
Incident response plan	✓	✗ Need IR Retainer
Remediation verification	✓	✗ Need IR Retainer

> "More confidence that our network is managed and better monitored."
> -- **Tim Canady,** ***IT Specialist,*** *Rockingham County Schools*

> "We have improved security monitoring with a reduction in workload on in-house staff."
> -- ***Network Engineering,*** *Educational Institution*

Ready to get started? We're here to help.

Reach out schedule a meeting to learn more about MDR

eSENTIRE

DOWLEY SECURITY SYSTEMS