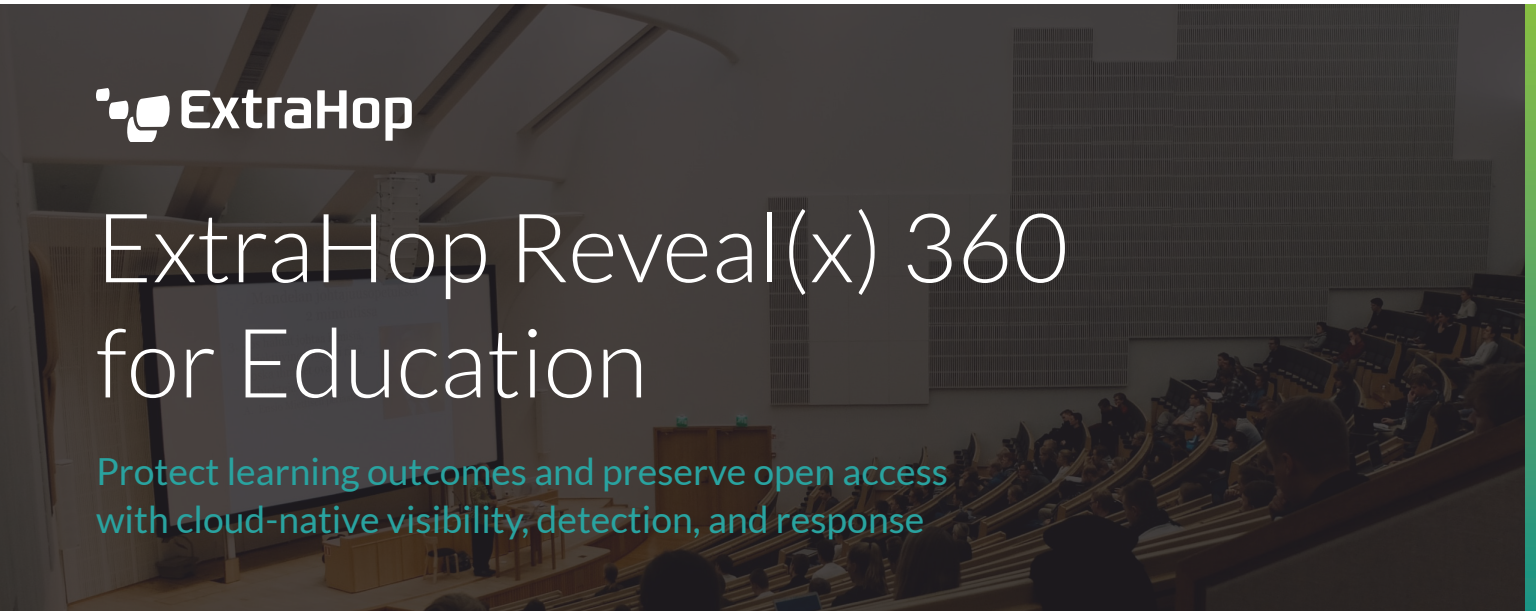

ExtraHop Reveal(x) 360 for Education

Protect learning outcomes and preserve open access with cloud-native visibility, detection, and response

Educational institutions make good targets for cyberattacks because they face a unique dual challenge. As schools, colleges, and universities strive to deliver open access to learning they also must protect sensitive student data and valuable intellectual property.

One missed phishing email, one successful ransomware attack, or one broken learning experience significantly impacts the communities the sector serves. The ramifications go beyond the potential loss of school time. The risk to affected schools includes stolen research, costly recovery, and reputational harm.

> “Ransomware attacks on colleges increased 100% between 2019 and 2020.[2]

Despite what’s at stake, IT and security teams face numerous challenges:

Accelerated digitalization of learning in response to the global COVID-19 pandemic added unprecedented numbers of new unmanaged devices, cloud services, and remote access, expanding the attack surface.

Large populations of untrained users requiring access to digital resources—students of all ages, faculty, staff, community members, and volunteers—strain security awareness and proactive prevention efforts.

Advanced persistent threats put every network-connected asset at risk for compromise. A 700% increase in ransomware attacks and a record-breaking number of cyber incidents targeting education in 2020[1] are constant reminders of the razor-thin margin for error.

Compliance with regulatory requirements, including the Family Education Rights and Privacy Act (FERPA), Higher Education Opportunity Act (HEOA), HIPAA, CCPA, GDPR, and others add time-consuming overhead and reporting obligations.

The Challenge: Educational Institutions Cannot Afford to Fail

Cyber attacks on colleges, universities, and K-12 institutions reached record-breaking levels in recent years. While much of this is attributable to the abrupt shift to remote instruction over the last year, digital learning tools and online experiences are here to stay.

As institutions incorporate blended learning into post-pandemic curriculum strategies, the nation’s education system continues to face an average of two attacks per school day[3]. This new reality and the increasing sophistication of threats place considerable responsibility on stretched-thin IT resources.

It is evident that the reliance on prevention alone is no longer sufficient to stave off targeted attacks or determined adversaries. The risk goes far beyond Zoombombing. Once breached, intruders move laterally to acquire student and financial records, hold institutions hostage with ransomware, exfiltrate valuable personal data, and worse.

[1] Source: K12 Security Information Exchange
[2] Source: BlueVoyant: State of Education 2021 Report
[3] Source: Source: The Hill

The Opportunity: Gain Visibility, Reduce Risk, and Respond Quickly

Improving an overall security posture starts with stopping advanced threats before they result in a breach. To beat back intruders already inside a network, educational institutions need complete visibility, real-time situational awareness, and high-fidelity contextual data. You can boost the ability of your IT and security teams to protect sensitive student data and deliver an open, accessible learning environment.

UNIFY VISIBILITY AND IMPROVED CYBER HYGIENE

Network visibility is the cornerstone of cyber-risk management frameworks, like the NIST CSF, and regulations, such as CCPA and HIPAA. Comprehensive real-time visibility is critical to stop cyber threats, demonstrate compliance, and maintain service levels.

- Without east-west traffic visibility, 70% of your hybrid network is in the dark and risks missing intruders who find ways past even the most world-class defenses
- Encrypted traffic leads to dark spaces, which attackers can exploit to mask malicious activities, or application performance issues go undetected
- Up-to-date and complete asset inventory and classification (including IoT devices, VoIP phones, and printers) are essential to improve network security and health

TAKEAWAY

Educational institution IT and security functions that closely collaborate to identify gaps, blind spots, troubleshoot degraded performance, and uncover threats increase the speed and scale of digital learning delivery and overall student experience.

MITIGATE RANSOMWARE ATTACKS

The prevalence of advanced persistent threats, phishing attacks, and zero-day exploits have created ideal conditions for ransomware to flourish. These circumstances have rendered traditional signature-based methods ineffective, requiring schools, colleges, and universities to embrace a real-time behavioral analysis approach. Machine-learning-backed detections and guided investigation are table stakes to respond and contain incidents before they inflict learning disruption.

- Passively monitoring all network traffic and decoding common application protocols—without the need for agents or log files—surfaces real-time awareness of unusual activity
- ML-driven behavioral analytics are crucial to automatically correlate attack behaviors and track movement across the network
- Incident response teams need to know which events and alerts require immediate attention based on the local context and observed behaviors

TAKEAWAY

Educational institution IT and security teams that combine real-time insights into the network with advanced machine learning to detect unusual behavior can more rapidly detect, quarantine, and recover from ransomware attacks.

ENABLE FRICTION-LESS COLLABORATION ACROSS IT AND SECURITY OPS

The pervasiveness, velocity, and scope of today's sophisticated threats demand an integrated approach.

- War rooms and the IT blame game slow response times and distract from resolving incidents and delivering major initiatives
- Streamlining threat response workloads and troubleshooting across NetOps, SecOps, and CloudOps is possible if each team has access to the same deep visibility data across the entire hybrid environment
- Operational and cost efficiency gains are possible by minimizing tool sprawl and technologies with overlapping functionality

TAKEAWAY

Educational institution IT and security teams that break down silos by standardizing on a single source of truth eliminate operational friction and boost productivity.

The Solution: Reveal(x) 360 SaaS-Delivered NDR for Education

ExtraHop Reveal(x) 360 is the first and only SaaS-based network detection and response (NDR) that provides on-demand, unified visibility across edge, core, and cloud environments to detect and respond to threats before they cause damage.

ExtraHop sensors passively monitor your network and analyze all network interactions to improve your organization's ability to stop advanced threats like ransomware and troubleshoot downtime and slow applications.

Reveal(x) 360 is backed by the ExtraHop Threat Research team. As soon as new threats and attack tactics are discovered, new detectors can be quickly deployed to immediately improve the expertise and effectiveness of SecOps teams.

Achieve 360-degree visibility to quickly detect, investigate, and respond to threats with an integrated workflow for unparalleled insight across the hybrid network, cloud workflows, and IoT devices. Even network traffic is encrypted with TLS 1.3.

Detect suspicious activity with cloud-based machine learning and advanced behavioral analysis to uncover indicators of compromise, such as command and control, brute force, lateral movement, privilege escalation, unusual protocol communication, and data staging and exfiltration. Decrypt traffic to identify threats and anomalies within SSL/TLS encrypted traffic.

Stop advanced threats that other solutions won't see, streamline your operations, and accelerate investigations into any incident with a click. No war rooms. No waiting on other teams.

COMPLETE VISIBILITY

Discover and classify all assets communicating on the hybrid network

Identify and profile every managed, unmanaged, or rogue device—including enterprise IoT.

Eliminate frictions between NetOps, SecOps, and CloudOps teams

REAL-TIME DETECTION

Monitor and safeguard network traffic in real-time a line rate up to 100 Gbps

Improve analyst efficiency with a single integrated workflow with real-time threat detection

Enable faster answers through cloud-based machine learning

INTELLIGENT INVESTIGATION & RESPONSE

Troubleshoot incidents and investigate root cause in less time

Use historical data to hunt threats and discover if you have been previously impacted

Automate and orchestrate responses through integrations with like CrowdStrike, Phantom, Demisto, and Palo Alto Networks

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats––before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

© 2021 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.

520 Pike Street, Suite 1600
Seattle, WA 98101

877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com