



# Cisco XDR for Education

Safeguarding Learning Environments  
with Simplified Security



# Contents

Introduction.....	3
The Power of Cisco XDR.....	4
Unified visibility across diverse IT ecosystems.....	5
Comprehensive threat detection and response.....	6
Ransomware recovery.....	7
Streamlined security operations.....	8
Customer story: Empowering the citizens of the future.....	9
Architectural drawing.....	10
Get started.....	11
Additional resources.....	11



## Introduction

Educational institutions are rapidly embracing digital transformation to enhance learning experiences and operational efficiency. Technologies like online learning platforms, connected classrooms, and digital administrative tools are revolutionizing education but are also increasing cybersecurity risks.

Protecting students, faculty, and research data is now more crucial than ever, as cybercriminals target educational data for its sensitivity and value. Additionally, securing vulnerable educational devices and complying with regulations such as FERPA adds another layer of complexity to the cybersecurity landscape.

The expansion of remote learning and digital collaboration tools further broadens the attack surface, making robust cybersecurity measures essential for educational institutions. Cisco® Extended Detection and Response (XDR) tackles these challenges by leveraging advanced technologies like Artificial Intelligence (AI) for real-time threat detection, prioritization, and response.

This solution brief explores how Cisco XDR can empower educational institutions to stay ahead of cyberthreats, helping ensure the safety and privacy of their digital ecosystems while enabling them to focus on their primary mission: delivering quality education.



2023 was the worst ransomware year on record for education, with a 92% rise in K-12 and 70% in higher education.

Source: [Malwarebytes ThreatDown](#)



LockBit and Rhysida were the primary attackers, responsible for about 50% of all attacks.

Source: [Malwarebytes ThreatDown](#)



Ransomware attacks on the education sector have cost the world economy over \$53 billion in downtime alone.

Source: [Comparitech](#)





## The Power of Cisco XDR

### Transforming security operations

Extended detection and response has become essential for organizations combating sophisticated cyberthreats. These solutions integrate data from multiple security layers, offering a unified view of an organization's security posture and addressing the limitations of traditional, siloed security approaches.

Cisco XDR distinguishes itself from other XDR solutions through:

- **Extensive integration.** Seamlessly integrates with a wide range of Cisco and third-party security tools, providing visibility across the entire IT infrastructure.
- **Deep network insight.** Leverages built-in network detections, providing agentless visibility and baseline activity monitoring to defend against data exfiltration and ransomware spread.

- **Robust threat intelligence.** Continuously updates with threat data from Cisco Talos®, helping ensure protection against emerging threats.
- **Cloud-native architecture.** Built on a cloud-native foundation, Cisco XDR offers scalability and flexibility for organizations of all sizes.
- **Broad security portfolio.** Integrates solutions across the network, endpoints, email, applications, identity, and cloud, helping ensure that threats are detected once and blocked everywhere.

By providing a comprehensive, correlated view of security data, Cisco XDR enables faster threat detection, more efficient incident response, and improved security outcomes, empowering organizations to stay ahead of evolving cyberthreats.

“Cisco XDR makes our security operations team faster and more effective at combating threats. The advanced workflows let us automate threat information enrichment and reactions, so our analysts can focus on resolving incidents instead of wasting time gathering information. Automation, like quarantine actions, enables us to proactively respond 24/7 to incidents and stop the spread of threats before any human interaction is necessary.”

– Gert-Jan de Boer  
Network and Security Specialist, aaZoo



## Unified visibility across diverse IT ecosystems

### See everything, secure everywhere

Cisco XDR offers unified visibility across diverse security ecosystems through extensive integrations and advanced visualization capabilities. This approach provides organizations with holistic insights into their security posture, regardless of the complexity of their IT infrastructure.

At the core of Cisco XDR's visibility is its wide range of integrations, including networks, endpoints, email systems, applications, identity, and the cloud. These integrations include both Cisco and select third-party tools, helping ensure comprehensive data correlation and analysis and eliminating potential blind spots.

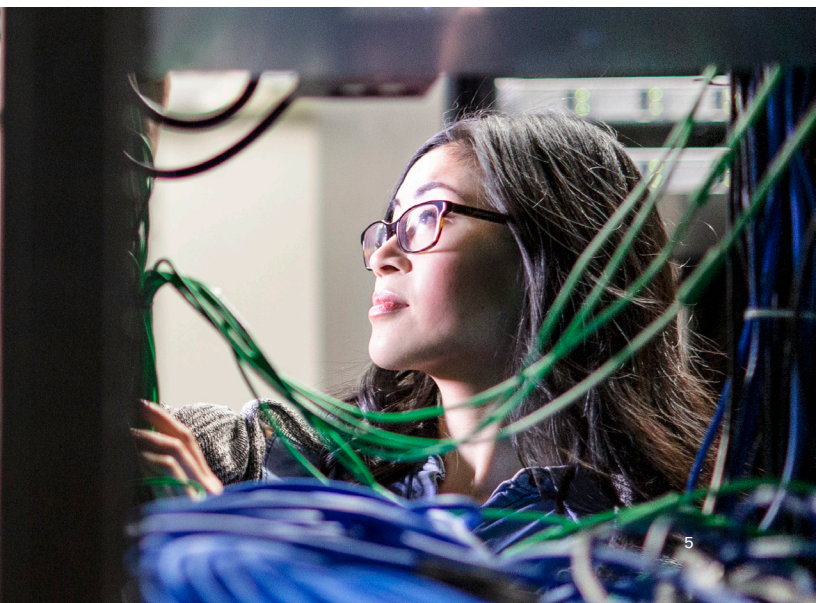
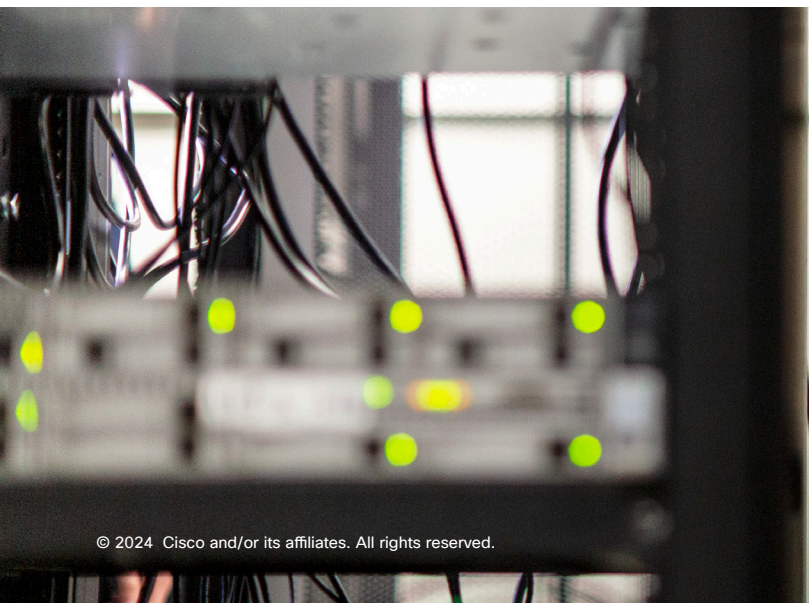
The solution's data ingestion and normalization engine processes vast amounts of telemetry data, standardizing it for analysis. Advanced algorithms correlate this data, identifying patterns and anomalies indicative of potential threats.


Cisco XDR's visualization capabilities further enhance visibility with dynamic, interactive graphical representations of the security landscape. These maps illustrate asset relationships, potential attack paths, and threat spread, allowing security analysts to quickly understand incident context, trace attack origins, and identify vulnerable assets.

## Impact to organizations

- **Comprehensive coverage:** Extensive native integrations across multiple security domains.
- **Holistic threat detection:** Correlates data from diverse sources to uncover sophisticated attacks.
- **Streamlined investigations:** Interactive visualizations and dashboards accelerate incident analysis.
- **Fewer blind spots:** Unified view minimizes gaps in security coverage.
- **Enhanced decision-making:** Real-time, contextualized data enables faster, more informed responses.

Customizable dashboards provide real-time views of the organization's security posture, focusing on high-risk assets, active threats, or compliance status. Progressive disclosure techniques enable analysts to drill down into specific incidents or assets for detailed information without being overwhelmed by data.



 Comprehensive threat detection and response**Detect sooner, respond faster**

Cisco XDR offers a sophisticated, multilayered approach to threat detection and response, leveraging advanced analytics and a broad integration ecosystem. The API-first approach aggregates and analyzes telemetry data to prioritize threats, providing a holistic view of the security landscape.

Using advanced algorithms and AI, Cisco XDR identifies complex attack patterns and subtle indicators of compromise, reducing false positives and enhancing detection accuracy. Integration with Cisco Talos intelligence provides real-time updates on emerging threats, defending against zero-day exploits and advanced attack techniques.

Cisco XDR offers a dual approach to threat response. Automated playbooks trigger rapid containment and mitigation of threats without human intervention, while the Cisco AI Assistant provides contextual guidance for complex scenarios. It recommends next steps and remediation tactics, empowering incident responders to make faster, more informed decisions.

Cisco XDR also maps detected threats to the MITRE ATT&CK framework, providing valuable context for investigations and identifying gaps in defensive capabilities.

This comprehensive approach significantly reduces the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), enhancing the organization's overall security resilience.

## Impact to organizations

- **Multivector threat visibility:** Unified view across network, endpoints, email, identity, applications, and cloud.
- **AI-powered analytics:** Advanced detection with reduced false positives and risk-based prioritization.
- **Automated and guided response:** Rapid mitigation with AI-assisted decision support and automated playbooks.
- **Comprehensive threat intelligence:** Real-time insights from Cisco Talos, aligned with MITRE ATT&CK for enhanced strategies.
- **Streamlined investigations:** Unified dashboard simplifies and accelerates incident management.



## Ransomware recovery

### Bounce back faster after an attack

Cisco XDR's ransomware recovery feature marks a significant advance in the fight against ransomware, leveraging sophisticated detection algorithms to identify early indicators of an attack. Upon detection, Cisco XDR automatically triggers a snapshot request to integrated enterprise backup and recovery solutions, reducing the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to near zero.

This rapid response contrasts with traditional Endpoint Detection and Response (EDR) tools, which may take hours to days to identify an attack and initiate a backup request. The integration with certified backup and recovery solutions, such as Cohesity, enables automated, near-instantaneous protection of critical assets. Cisco XDR's approach focuses on identifying attack patterns as they move across the network rather than waiting for direct attacks on critical systems.

By combining early detection, automated backup triggering, and rapid restoration capabilities, Cisco's ransomware recovery feature enhances organizational resilience. This minimizes potential data loss and operational downtime, crucial factors in maintaining business continuity in the face of increasingly sophisticated cyberthreats.

### Impact to organizations

- **Reduces data loss and downtime:** Helps achieve near-zero RPO and RTO
- **Proactive threat detection:** Identifies early indicators of ransomware attacks, allowing intervention before critical data is encrypted.
- **Automated backup initiation:** Triggers backup processes automatically in response to detected threats, eliminating manual delays.
- **Early attack chain detection:** Identifies subtle attack chains using telemetry and analytics, detecting ransomware before it reaches high-value assets.
- **Seamless integration:** Works with select backup and recovery solutions for comprehensive protection and rapid recovery capabilities.





## Streamlined security operations

### Minimize false positives and alert fatigue

Security teams often face an overwhelming volume of alerts from disparate security tools. Cisco XDR addresses this challenge through threat correlation and intelligent alert triage, significantly enhancing operational efficiency.

At the core of Cisco XDR's architecture is its sophisticated AI engine, which analyzes telemetry data from multiple security vectors. By leveraging behavioral analytics, anomaly detection, and pattern recognition, Cisco XDR can identify subtle Indicators of Compromise (IOCs) and potential threats that might go undetected in isolated alerts.

Cisco XDR also incorporates Security Orchestration, Automation, and Response (SOAR) capabilities through predefined playbooks and custom scripting. The automation engine can trigger actions across multiple security tools, such as isolating endpoints or updating firewall rules based on specific alert criteria or analyst-defined thresholds.

The solution uses Natural Language Processing (NLP) and machine learning algorithms to provide guided response recommendations. These recommendations are based on the specific attributes of each incident, historical data, and best practices, assisting analysts in making informed decisions quickly.

By implementing these advanced technologies, Cisco XDR reduces investigation and response times while minimizing false positives and alert fatigue, resulting in a more robust and resilient security posture.

## Impact to organizations

- **Improved efficiency:** Prioritizing alerts and automating routine workflows allows security teams to concentrate on critical issues, enhancing operational efficiency.
- **Enhanced threat detection:** Correlating data from multiple telemetry sources enables the detection of advanced threats that may otherwise be overlooked.
- **Faster response times:** With prioritized alerts and guided response actions, security teams can quickly address threats, minimizing the impact of incidents.
- **Reduced burnout:** By reducing false positives and alleviating alert fatigue, Cisco XDR helps prevent burnout, improving job satisfaction and retention.
- **Proactive threat mitigation:** Continuous monitoring and automated responses enable organizations to address potential threats before they escalate into serious incidents.







## Customer story: Empowering the citizens of the future



While understanding the benefits of Cisco XDR is valuable, nothing speaks louder than real-world results. Let's explore how one school district leveraged Cisco XDR to transform its cybersecurity posture and achieve tangible improvements across 49 campuses.

### Securing a digital classroom

Mansfield Independent School District (MISD), located in the Dallas-Fort Worth Metroplex, provides an environment where students learn to become productive citizens. MISD gives students the tools they need to learn, teachers the support they need to teach, and parents peace of mind regarding their kids' learning.

"We've got 110,000 computing devices and 134,000 endpoints that we must secure," says Jeremy Jameson, Director of Infrastructure and Cybersecurity at MISD.

"We empower students, staff, and parents with opportunities, training, and information; we don't just protect users. We must develop that around data availability and confidentiality."

### Managing a diverse ecosystem

Collecting data from hundreds of devices with different operating systems, makes, and models, and securing these devices, proved difficult. MISD recognized that efficient security management was essential for making

the devices resilient to threats. "Logs weren't giving us the granular visibility we needed to plug the security gaps," says Shawntee Cowan, Chief Technology Officer at MISD.

Cowan wanted to integrate MISD's security tools into one XDR platform to achieve greater visibility using a unified dashboard. After seeing a demo, MISD adopted Cisco XDR Premier.

### XDR insights and automation ease the burden

"The initial implementation was fairly easy," remarks Cowan. "The managed services team guided us to complete the initial deployment by explaining the steps. It wasn't too long before the XDR platform was populated with telemetry data. We were excited about how fast that happened."

Cisco XDR greatly reduced the number of logins across various tools and was easy for members of the security team to use. "We can open tickets and request additional information and that's a big advantage of having managed services," says Jameson.

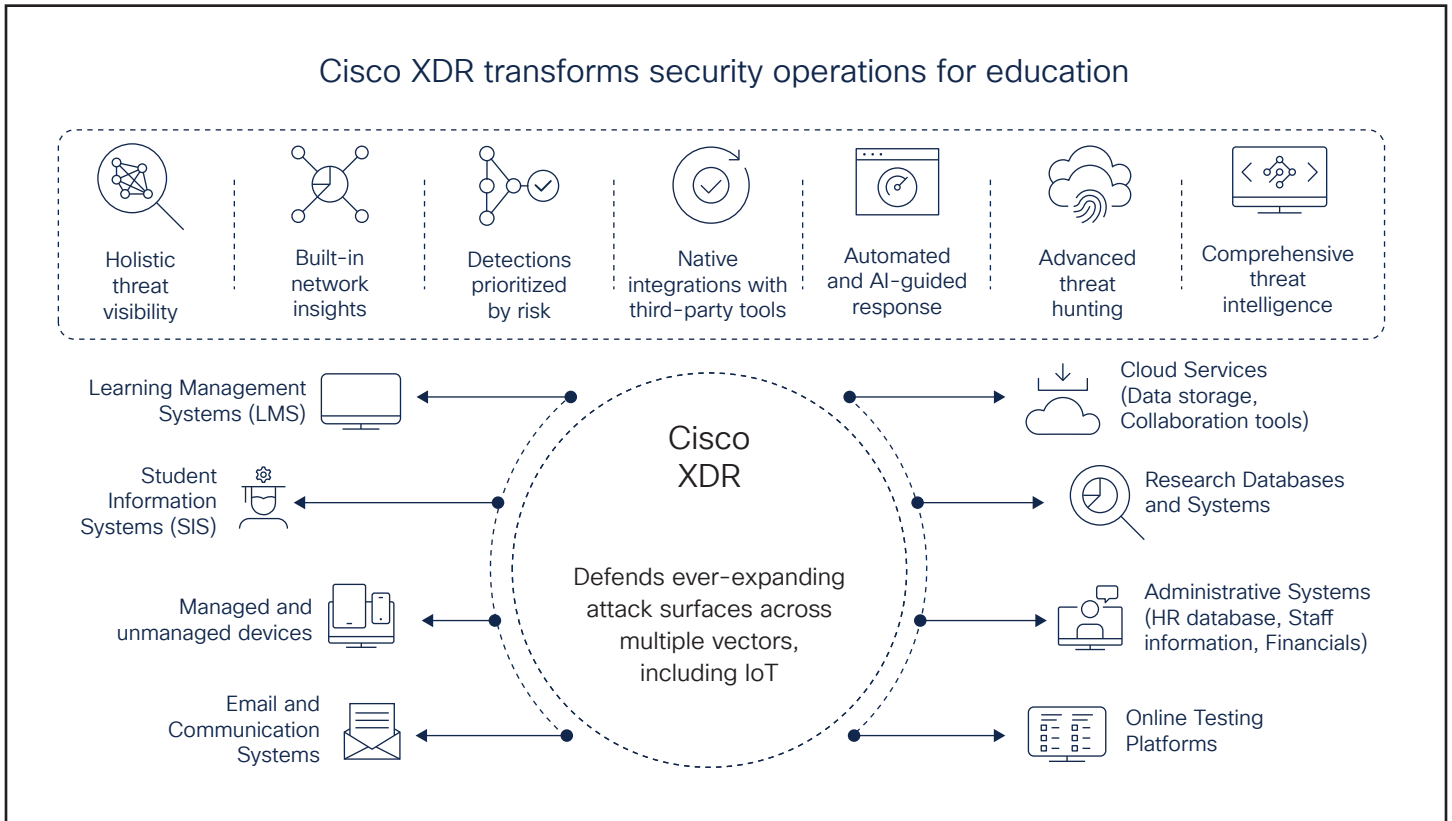
Cowan adds, "Cisco XDR managed services has streamlined our security operations. In addition to alerting us, XDR gives us additional insights and even fixes some of the issues. Having that extra level of support where we're not having to be up day and night worried about things is huge for our district."

"In a world of increasing cyberthreats, having that holistic visibility of our security environment in a single pane of glass and the capability of regular reporting has given me and everyone here that precious peace of mind. We feel more in control of keeping our environment safe."

– Shawntee Cowan  
Chief Technology Officer, Mansfield ISD



## Architectural drawing



The architectural diagram illustrates how Cisco Extended Detection and Response (XDR) integrates seamlessly into an educational institution's cybersecurity infrastructure. This comprehensive solution unifies data from various sources, including student information systems, educational applications, managed and unmanaged devices, and cloud platforms. By correlating and analyzing this diverse data, XDR provides education security teams with unparalleled visibility across their entire digital ecosystem, enabling rapid threat detection and automated response to protect sensitive student information and critical educational operations.



## Get started

Cisco XDR is a vital solution for educational institutions navigating the complexities of modern cybersecurity. By simplifying security operations and providing comprehensive threat detection and response, Cisco XDR enables schools and universities to create safer digital learning environments.

As cyberthreats continue to evolve, educational organizations equipped with Cisco XDR can confidently navigate the digital landscape, helping ensure the protection of sensitive data and continuity of critical educational services. Embrace the future of educational cybersecurity with Cisco XDR—where simplified security meets uncompromising protection.

Learn more about [Cisco XDR](#)

## Additional resources

[Cisco XDR At-a-Glance \(PDF\)](#)

[Cisco XDR Data Sheet \(PDF\)](#)

[Cisco XDR Demo](#)

[Cisco XDR Ransomware Recovery Demo](#)

