

Cisco XDR for Manufacturing

Securing Industrial Operations with
Intelligent Threat Detection



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 – Forging resilience on the production line.....	9
Architectural drawing.....	10
Get started.....	11
Additional resources.....	11



Introduction

In today's evolving manufacturing landscape, the convergence of Operational Technology (OT) and Information Technology (IT) is driving unprecedented efficiency and innovation. However, this digital transformation also exposes industrial environments to complex cybersecurity risks.

As manufacturers integrate smart machines, IoT sensors, and interconnected systems, they face the challenge of protecting not only sensitive data but also critical physical infrastructure and production processes. The potential for cyberattacks to disrupt operations, compromise product quality, or even endanger worker safety has become a top concern.

Cisco® Extended Detection and Response (Cisco XDR) addresses these unique industrial challenges by providing a unified approach to threat detection and response across both IT and OT environments. This solution brief explores how Cisco XDR empowers manufacturers to strengthen their security posture, ensure operational continuity, and safeguard their intellectual property while embracing the benefits of smart manufacturing technologies.



Nearly half (47%) of OT/ICS environments faced ransomware in 2023.

Source: [The Crisis of Convergence: OT/ICS Cybersecurity 2023](#)



86% of IT decision makers reported having core OT functions running on outdated and unsupported operating systems

Source: [BlackBerry, Operational Technology Cyberattacks and the 2023 Threat Landscape](#)



Nearly 70% of OT organizations experienced a cybersecurity incident in 2023.

Source: [Foley & Lardner LLC, Cybersecurity in the Age of Industry 4.0](#)





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.

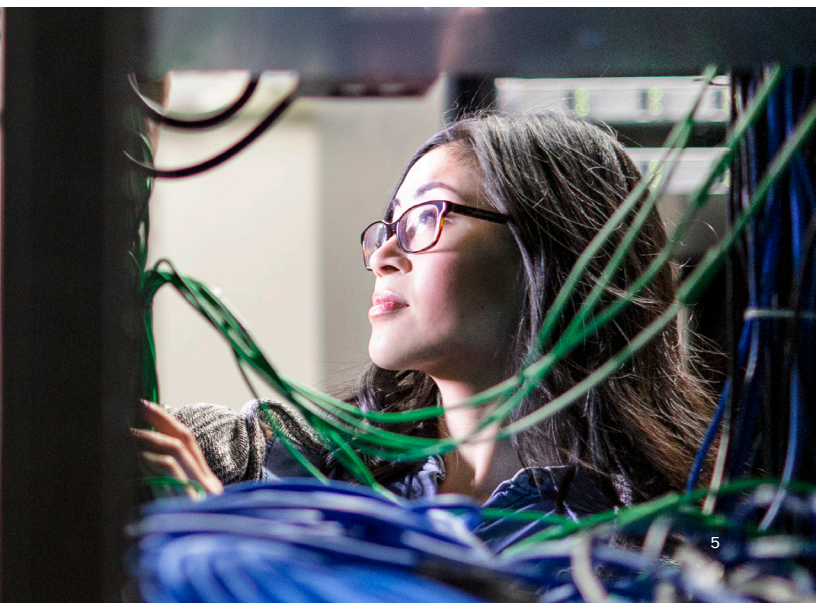
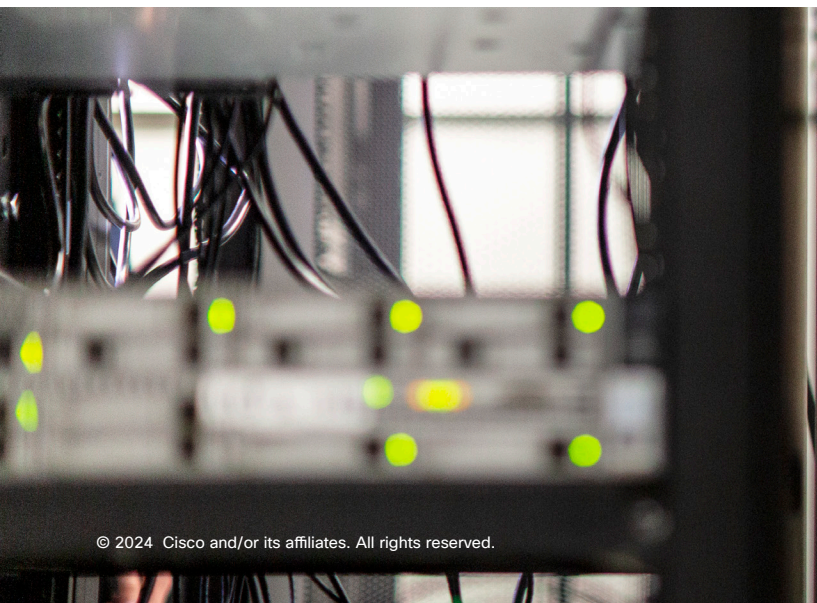
The solution's data ingestion and normalization engine processes vast amounts of telemetry data, standardizing it for analysis. Advanced algorithms correlate this data, identifying patterns and anomalies indicative of potential threats.


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 – Forging resilience on the production line

While understanding the benefits of Cisco® Extended Detection and Response (Cisco XDR) is valuable, nothing speaks louder than real-world results. Let's explore how this metal manufacturing company is using Cisco XDR to keep their product line running.

Ransomware strikes the production line

A leading manufacturer of precision metal components faced a series of ransomware attacks that threatened to halt production and compromise sensitive company data. Their legacy security systems struggled against increasingly sophisticated threats, resulting in costly downtime and damage to customer relationships.

“We are constantly putting out fires,” recalls Larry S., the company's chief information security officer (CISO). “Each attack felt like a blow to our operations, and we knew we needed a more robust defense.”

Casting a stronger shield

Recognizing the need for a comprehensive security overhaul, the company turned to Cisco XDR technology. This advanced solution promised to unify threat detection, investigation, and response across the entire IT ecosystem.

Larry S. explains, “XDR offered us the visibility and control we desperately needed. It was like upgrading from a magnifying glass to a high-powered microscope in terms of threat detection.”

Rapid recovery and enhanced protection

When integrated with the company's backup solution, the Cisco XDR system's automated features allowed for near real-time recovery of business operations after a ransomware attack. XDR could automatically detect, snapshot, and restore business-critical data at the first signs of an attack, often before it could spread laterally through the network.

“Our recovery time has been slashed dramatically,” Larry S. proudly states. “What used to take days now takes hours, and in some cases, mere minutes. XDR has truly revolutionized our security posture.”

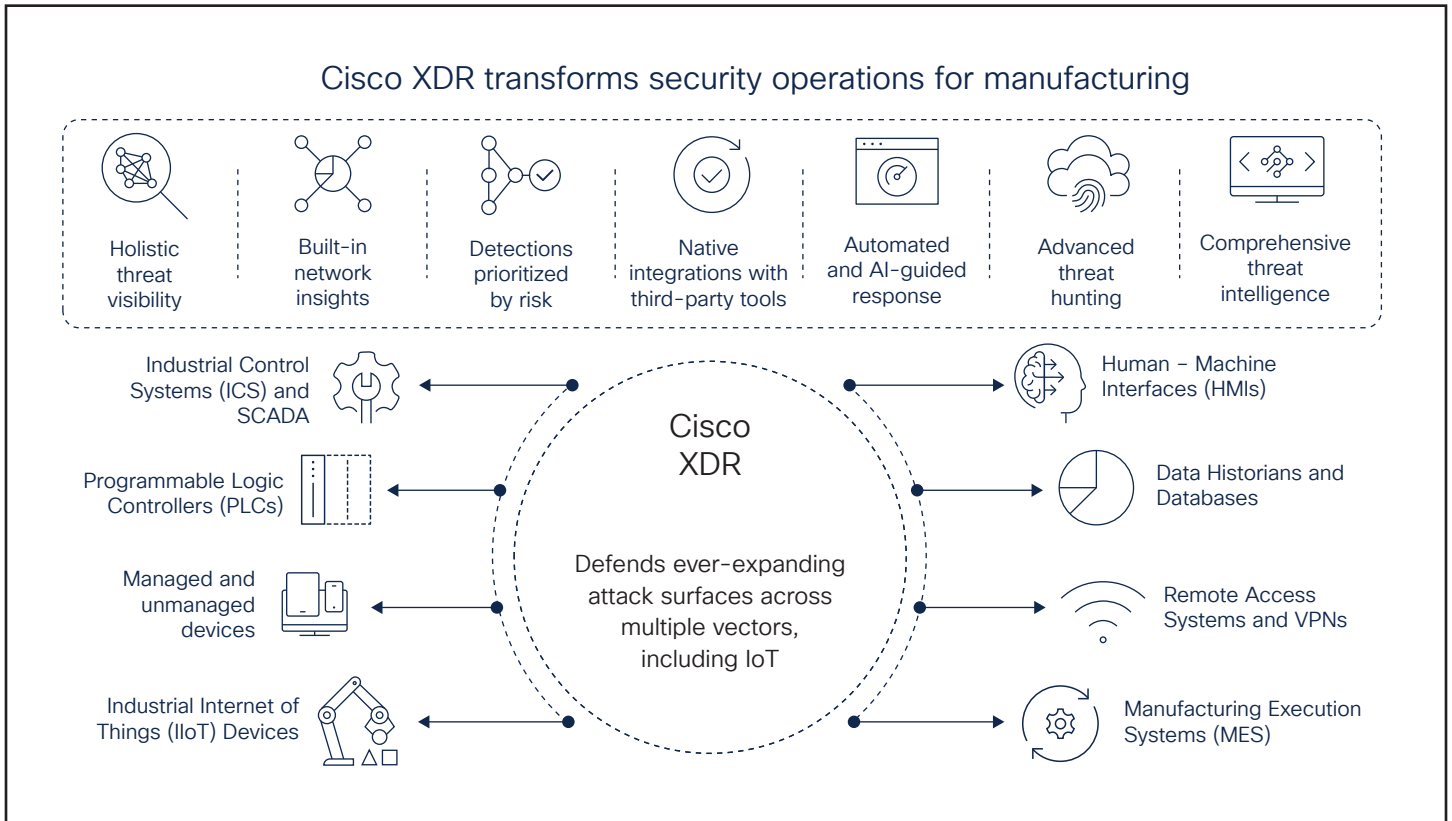
With XDR's advanced detection capabilities, the company has transformed its cybersecurity posture, ensuring production lines keep running smoothly and data remains secure.

“XDR offered us the visibility and control we desperately needed. It was like upgrading from a magnifying glass to a high-powered microscope in terms of threat detection.”

Larry S.
CISO



Architectural drawing



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



Get started

Cisco XDR offers a robust security solution for manufacturers navigating the complex cybersecurity landscape of modern industrial environments. By providing unified visibility across IT and OT systems, streamlined threat detection and response, and specialized security measures for industrial control systems, Cisco XDR enables manufacturers to protect their critical assets, maintain production continuity, and safeguard their competitive edge.

As cyber threats evolve alongside manufacturing technologies, organizations equipped with Cisco XDR can confidently pursue digital transformation initiatives, knowing they have a strong defense against sophisticated attacks that could impact both digital and physical assets.

Elevate your manufacturing cybersecurity strategy with Cisco XDR—where intelligent threat detection meets the unique demands of industrial operations, helping to ensure both innovation and security in the smart factory era.

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](#)

