

# Cisco XDR for Local Government

Strengthening Cybersecurity for  
Local Governments in the Digital Age





# 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: Building a secure and resilient community for all .....	9
Architectural drawing .....	10
Get Started .....	11
Additional resources .....	11



## Introduction

State and local governments face unique cybersecurity challenges as they balance the need to protect sensitive citizen data with the demand for transparent, accessible public services. These organizations manage a wide variety of critical infrastructure and essential services, from emergency response systems to utility networks, making them prime targets for cyberattacks. Limited budgets, legacy systems, and a shortage of cybersecurity talent further complicate their security landscape.

As government agencies increasingly adopt digital services and smart city initiatives, they must also contend with an expanding attack surface. Cisco® Extended Detection and Response (Cisco XDR) offers a comprehensive solution tailored to address these public sector challenges.

This solution brief explores how Cisco XDR empowers state and local governments to enhance their cybersecurity posture, help ensure continuity of vital public services, and maintain citizen trust in an era of evolving digital threats and increasing regulatory requirements.



Government facilities were the third-largest critical infrastructure sector targeted by ransomware attacks in 2023.

Source: [FBI Internet Crime Report 2023](#)



76% of cybersecurity incidents in the public sector resulted from system intrusion, lost or stolen assets, and social engineering.

Source: [Verizon 2023 Data Breach Investigation Report Public Sector Snapshot](#)



State and local governments experienced a 148% rise in malware and 51% in ransomware attacks in 2023.

Source: [Center for Internet Security, Nationwide Cybersecurity Review, 2022 Summary Report](#)





## 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.

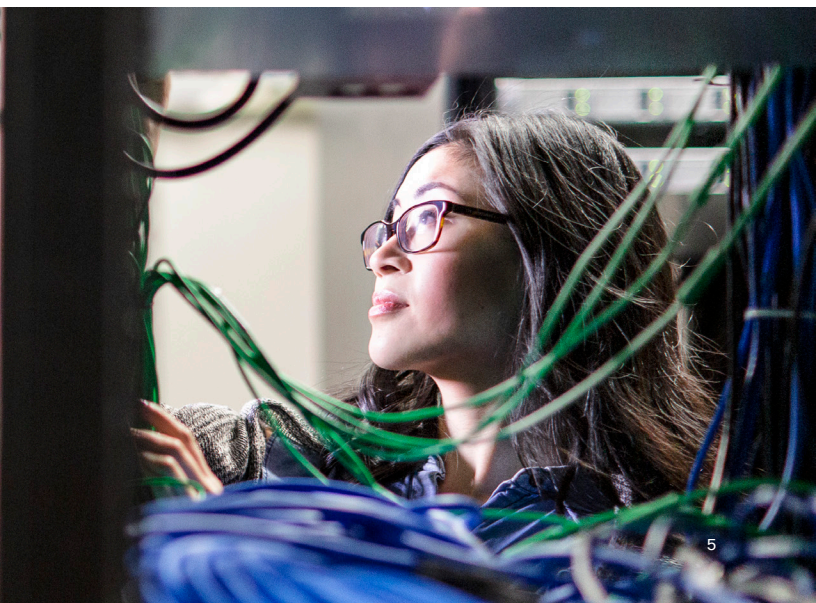
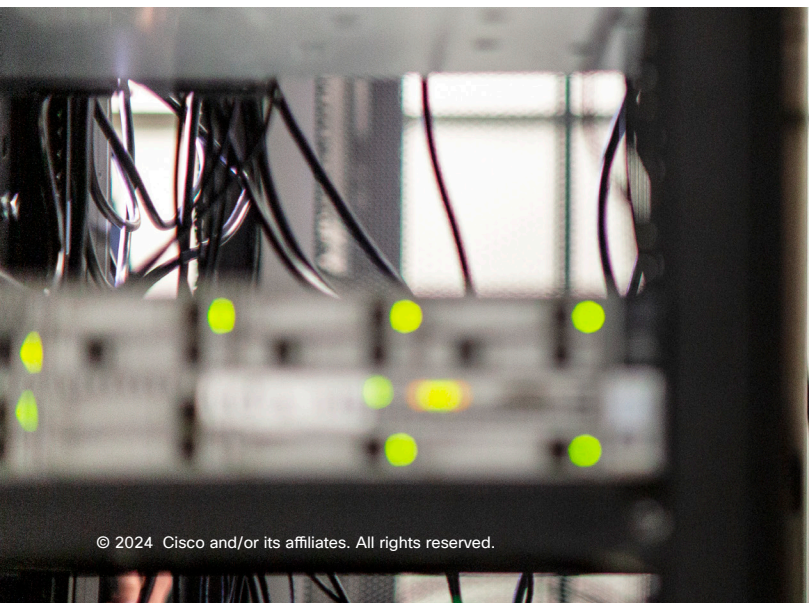
The solution's data ingestion and normalization engine processes vast amounts of telemetry data, standardizing it for analysis. Advanced algorithms correlate this data, identifying patterns and anomalies indicative of potential threats.


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: Building a secure and resilient community for all



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 a country council leveraged Cisco XDR to streamline operations and safeguard the data of their citizens.

### Securing Wexford's future

Wexford County Council, serving over 160,000 citizens in southeast Ireland, faces daily cybersecurity threats, including phishing attacks. Susie McCarthy, Technical Support Officer, notes, "One of our main challenges is the attempts to bypass our firewall to access sensitive data." With nearly 1,000 employees and diverse devices, the council requires a streamlined approach to protect this data. Following the National Cyber Security Centre's guidelines, Wexford must implement secure networks and strong access controls to enhance resilience against cyber threats.

### Streamlining security

Wexford's IT Infrastructure Team has significantly improved their network security and operations. McCarthy explains, "The idea of a centralized hub to pull in data from all the different tools made complete sense." The council transitioned to an Office 365 hybrid environment, implementing Microsoft best practices for domains and conditional access, complemented by additional security layers. This approach, combined with Cisco XDR, streamlined their security management. McCarthy adds, "It was brilliant how easy it was to integrate tools."

### Transformative results

The implementation of Cisco XDR significantly improved Wexford's security operations. The unified dashboard revolutionized data correlation and incident response.

"Incidents that used to take hours to investigate are now resolved in minutes," reports McCarthy.

Enhanced visibility allowed the team to view all security events in one place, distinguishing false positives from genuine

threats. Linda McDonagh, ICT Security Project Leader, adds, "Cisco XDR allowed us to quickly verify false alarms, saving us valuable time and resources."

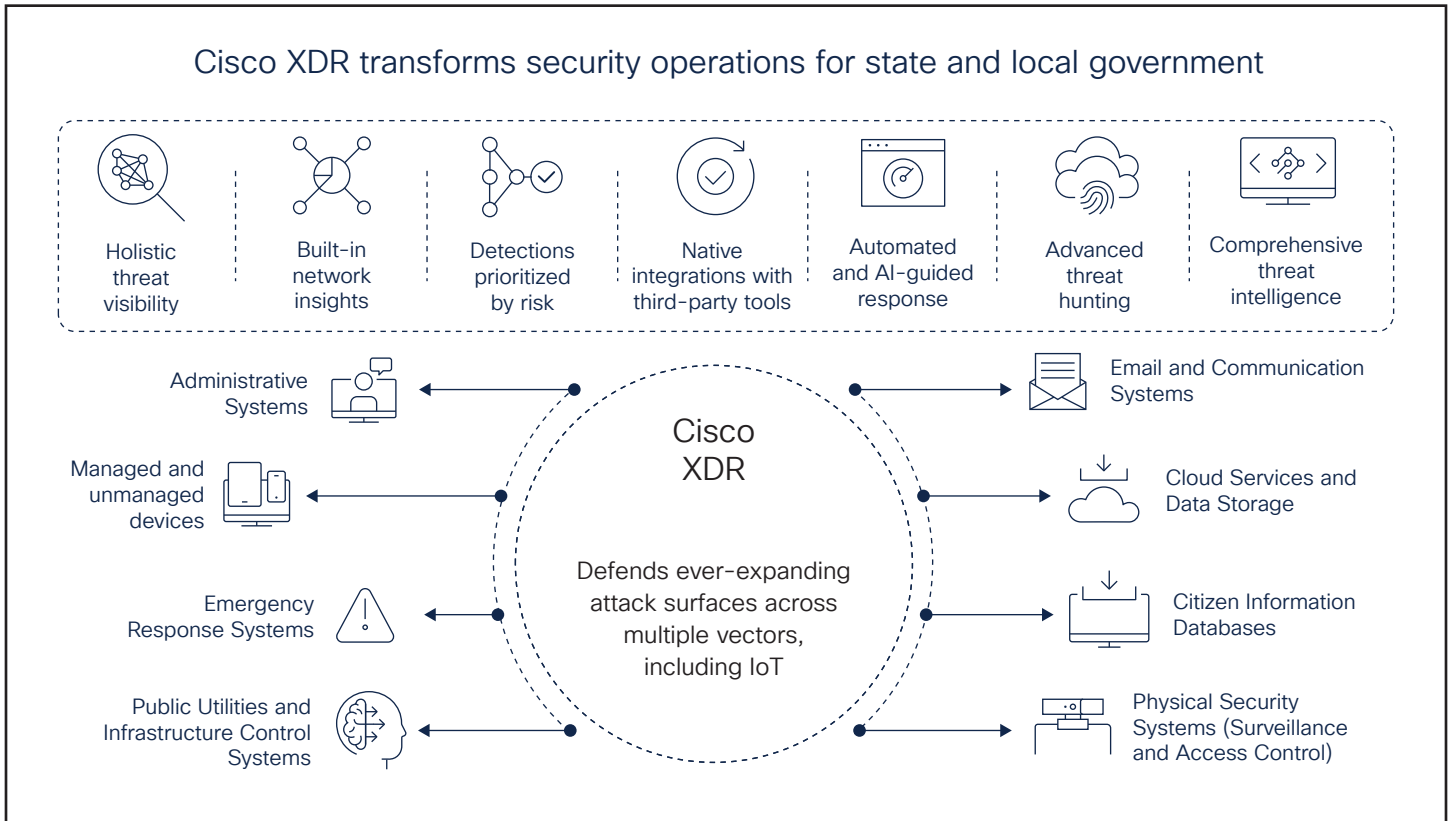
Automated reporting streamlined operations, ensuring comprehensive and accurate reports. Cisco XDR has enhanced efficiency, equipping the team to maintain a secure environment for residents.

"Incidents that used to take hours to investigate are now resolved in minutes. We have all the information we need right at our fingertips, significantly speeding up our response times."

Susie McCarthy  
Technical Support Officer  
ICT Security



## Architectural drawing



The architectural diagram illustrates how Cisco Extended Detection and Response (XDR) integrates seamlessly into a state and local government’s cybersecurity infrastructure. This comprehensive solution unifies data from various sources, including citizen services systems, government applications, network traffic, and cloud platforms. By correlating and analyzing this diverse data, XDR provides government security teams with unparalleled visibility across their entire digital ecosystem, enabling rapid threat detection and automated response to protect sensitive citizen information and critical government operations.

## Get Started

For state and local governments, cybersecurity is not just about protecting data; it's about ensuring the safety and well-being of the communities they serve. With critical public services at stake, these agencies must navigate a landscape filled with evolving cyber threats while managing limited resources and aging infrastructure.

Cisco XDR provides a vital security solution that empowers government organizations to proactively defend against attacks, streamline incident response, and enhance overall security posture. By integrating advanced threat detection and response capabilities, Cisco XDR enables state and local governments to focus on the mission of serving citizens, all while fortifying their defenses against the growing tide of cyber risks.

Elevate your government's cybersecurity strategy with Cisco XDR—where advanced threat detection meets the unique demands of public sector operations, helping safeguard both digital assets and public trust.

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](#)

