



Cisco XDR for Financial Services

Fortifying Financial Institutions
Against Cyber Threats



Contents

Introduction.....	3
The Power of Cisco XDR	4
Unified visibility across diverse IT ecosystems.....	5
Impact to organizations	5
Comprehensive threat detection and response	6
Impact to organizations	6
Ransomware recovery	7
Impact to organizations	7
Streamlined security operations.....	8
Impact to organizations	8
Customer Story – Banking on Security.....	9
Architectural drawing.....	10
Get Started	11
Additional resources	11



Introduction

In the fast-paced world of financial services, cybersecurity is more than just a checkbox—it's a fundamental necessity. Financial institutions are increasingly targeted by sophisticated cyber threats that aim to compromise sensitive customer data, financial transactions, and critical infrastructure.

With the rise of digital banking, mobile payments, and emerging technologies like blockchain, the attack surface has expanded significantly, rendering traditional security measures inadequate. On top of this, stringent regulatory requirements such as General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes-Oxley (SOX) add complexity to the cybersecurity landscape.

Cisco® Extended Detection and Response (Cisco XDR) is a robust solution to help overcome unique challenges faced by the financial sector. This solution brief delves into how Cisco XDR empowers banks, investment firms, and other financial services companies to effectively detect, investigate, and respond to threats across their entire digital ecosystem, ensuring the integrity of financial operations and maintaining customer trust in a rapidly evolving environment.



Extreme losses from cyber incidents have more than quadrupled since 2017 to \$2.5B.

Source: [Global Financial Stability Report](#)



Cybersecurity risk (45%) poses the greatest threat to growth in the banking sector.

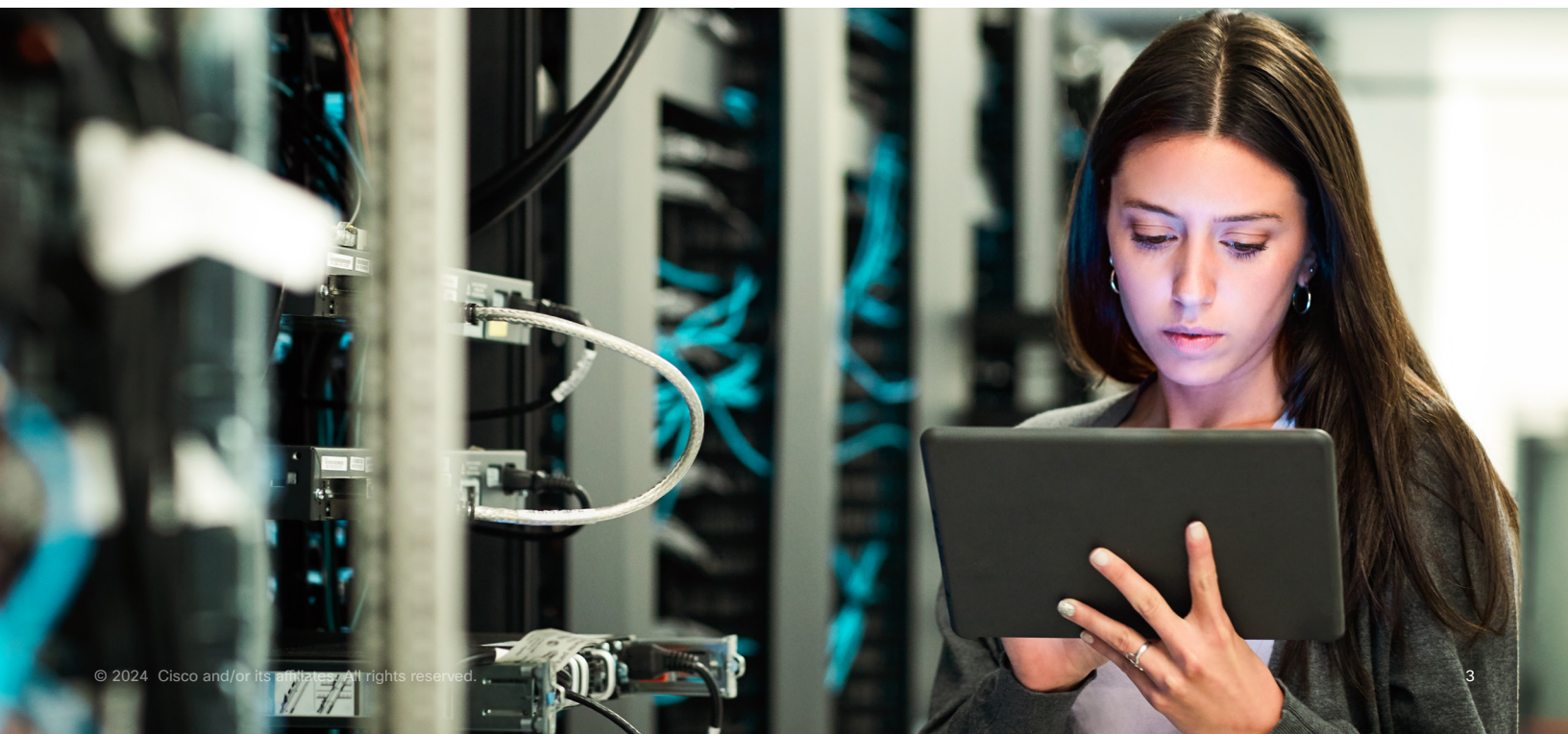
Source: [Future-Proofing Banking:](#)

[The Enterprise Transformation Imperative](#)



Financial firms increasingly rely on third-party IT providers, as shown by a 2023 ransomware attack that impacted 60 credit unions.

Source: [IMF Blog: Rising Cyber Threats Pose Serious Concerns for Financial Stability](#)





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.

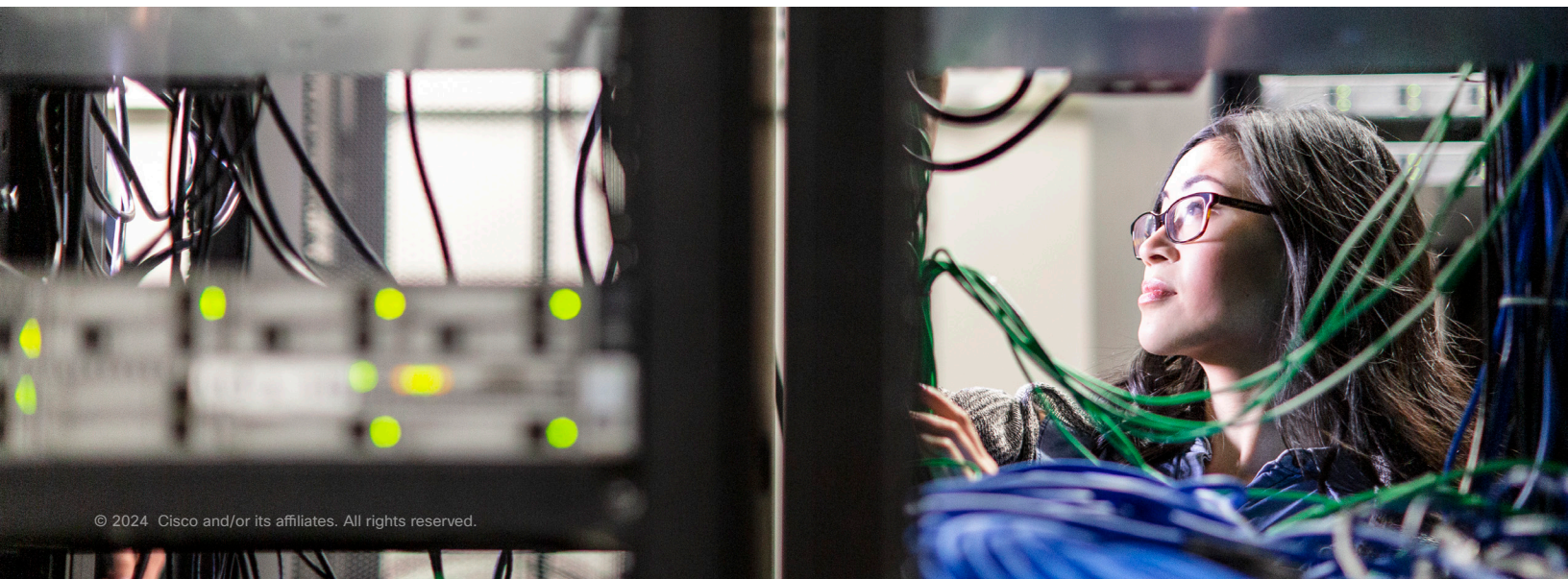
The solution's data ingestion and normalization engine processes vast amounts of telemetry data, standardizing it for analysis. Advanced algorithms correlate this data, identifying patterns and anomalies indicative of potential threats.


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.

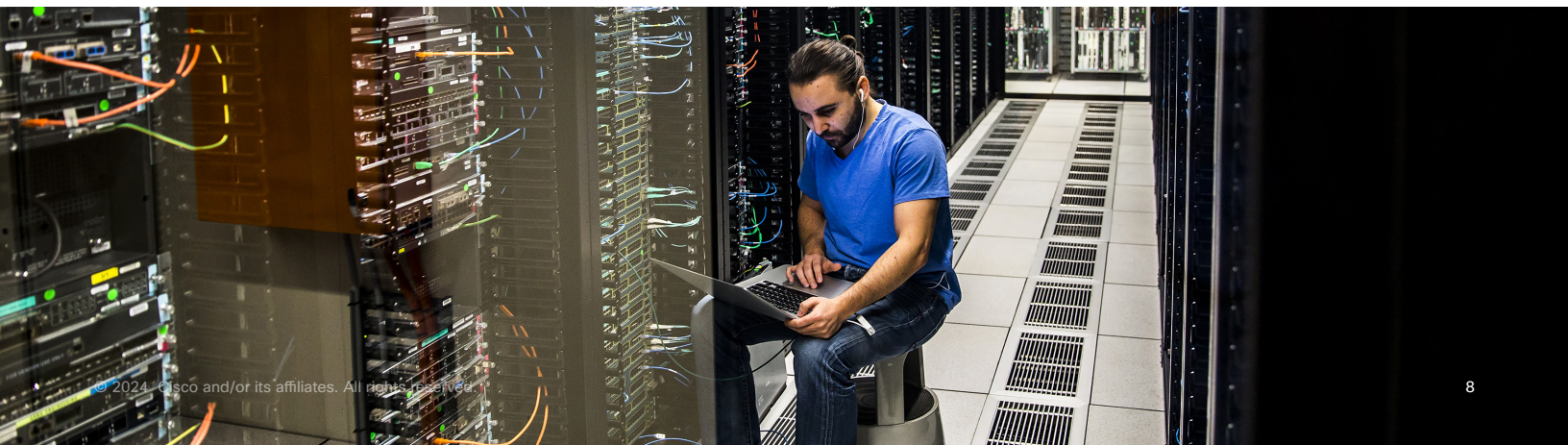
Cisco XDR also incorporates Security Orchestration, Automation, and Response (SOAR) capabilities through predefined playbooks and custom scripting. The automation engine can trigger actions across multiple security tools, such as isolating endpoints or updating firewall rules based on specific alert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

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 regional financial institution leveraged this security solution to enhance threat detection and streamline security operations.

Evolving email threats

A large regional financial institution faced increasing challenges from sophisticated phishing attempts targeting its employees. These attacks were becoming more difficult to detect with traditional email filters, potentially exposing sensitive customer data and financial systems to risk.

“We observed a concerning risk in advanced phishing tactics,” notes Sarah J., Director of Cybersecurity for the bank. “It became clear that our existing security measures needed reinforcement to protect against these evolving threats.”

Implementing Cisco XDR

To address these challenges, the financial institution chose Cisco XDR after seeing a demo. This solution integrated security across the network, endpoints, email, and cloud environments, providing comprehensive visibility and automated response capabilities.

Sarah explains, “XDR gave us the ability to connect the dots across our entire IT infrastructure. It's like having a team of expert analysts monitoring our systems 24/7.”

Cashing in on security

The Cisco XDR implementation enhanced the ability to detect and respond to potential threats. In one instance, the system identified suspicious activity following a clicked email link, correlating it with unusual network traffic patterns. The solution automatically contained the potential threat and alerted the security team for further investigation.

“With XDR, we've dramatically reduced our response times,” Sarah continues. “What might have taken hours or days to detect and resolve can now be addressed in minutes. It's a game changer for protecting our customers' trust and our bank's integrity.”

Cisco XDR has not only improved the security posture against phishing and other cyber threats, but also streamlined compliance processes, positioning the bank at the forefront of financial cybersecurity.

“XDR gave us the ability to connect the dots across our entire IT infrastructure. It's like having a team of expert analysts monitoring our systems 24/7.”

Sarah J.
Director of Cybersecurity



Architectural drawing



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

Get Started

In an industry where every moment matters and customer trust is essential, Cisco XDR serves as a vital ally in the defense against cyber threats. With its ability to deliver real-time threat intelligence, automated response capabilities, and comprehensive visibility across complex financial networks, Cisco XDR equips financial institutions to stay one step ahead of cybercriminals while helping meet rigorous regulatory standards.

As the financial services sector continues to innovate with technologies like blockchain-based payment systems and AI-driven mobile apps, organizations armed with Cisco XDR can confidently navigate the shifting threat landscape.

Embrace the future of cybersecurity with Cisco XDR—where advanced threat detection aligns with the unique demands of the financial systems.

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](#)

