# **Cisco XDR:** Security Operations Simplified


Why does the world
need a different
security approach?

# Our current landscape requires **simplicity**

We now work from anywhere and use more devices, apps and tools than ever before, and this complexity has created a persistent and growing security challenge. IoT and hybrid work have led to an expanded attack surface and security teams must protect an ever-growing ecosystem with inconsistent integration between technology.

Adversaries in the cyber world are like chameleons, constantly adapting to and blending in with their environment. Ransomware-as-a-Service has democratized methods formerly reserved for Advanced Persistent Threat (APT) groups, making it increasingly challenging to detect and prevent their attacks. With access to AI tools like ChatGPT, hackers can now create malicious software, automate spear phishing attacks, and enhance botnets to evade detection.

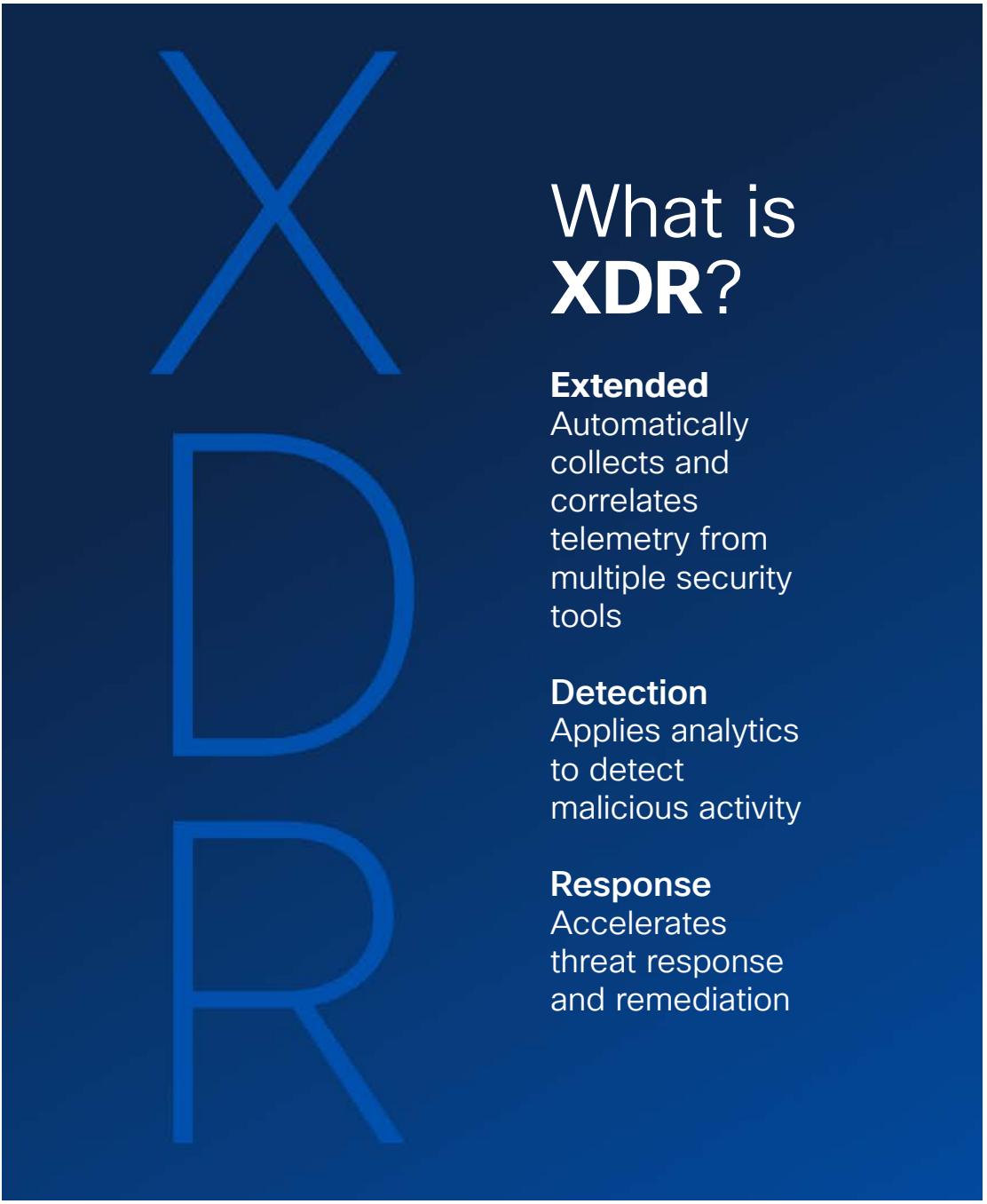
Networking equipment has become an attractive target for attackers due to its large attack surface and potential victim network access. Despite being a key component of an organization's IT infrastructure, these devices are often overlooked from a security perspective, poorly patched, and run on custom firmware, making them difficult to protect with standard security solutions.

This new normal calls for the ability to protect the integrity of every aspect of the organization to withstand unpredictable threats or changes and emerge stronger.

Want guidance and insights on how to purchase an XDR that fits your needs?

Adversaries are attacking networking devices at a staggering pace, particularly global threat actors looking to advance espionage objectives and facilitate stealth operations against secondary targets.

2023 Talos Year in Review




# What is **XDR**?

**Extended**
Automatically collects and correlates telemetry from multiple security tools

**Detection**
Applies analytics to detect malicious activity

**Response**
Accelerates threat response and remediation

# Cut through the noise, act on what matters

Extended Detection and Response (XDR) is a unified security solution that integrates and correlates data from multiple security products across an organization's networks, cloud, endpoints, email, and applications. It helps security operations teams to detect, prioritize, and respond to threats more efficiently and effectively. It reduces false positives and enhances threat detection and response through clear prioritization of alerts, providing the shortest path from detection to response. Single-vector point security products are not enough to protect against increasingly sophisticated multi-vector threat campaigns. This is where XDR comes in.

Effective XDR solutions are comprehensive, providing prioritized and actionable telemetry across all vectors – improving visibility and creating context across your environment. They should also enable unified detection from a single investigative viewpoint that supports fast, accurate threat response – with opportunities to elevate productivity even further through automation and orchestration. XDR solutions typically include features such as playbook-driven automation, guided incident response, threat hunting, alert prioritization and breach pattern analysis to empower security operations.

# What do security leaders want from XDR?

**Improved efficacy around advanced threat detection**
**51%** of professionals say their current tools struggle to detect and investigate advanced threats

**Improved alert correlation**
**36%** say their current tools aren't effective at correlating alerts

**Risk-based alert prioritization**
**26%** of security professionals want XDR to help prioritize alerts based on risk

**Bolster staff productivity**
**25%** want XDR to fill gaps within the security stack, while improving the efficacy and efficiency of threat detection and response

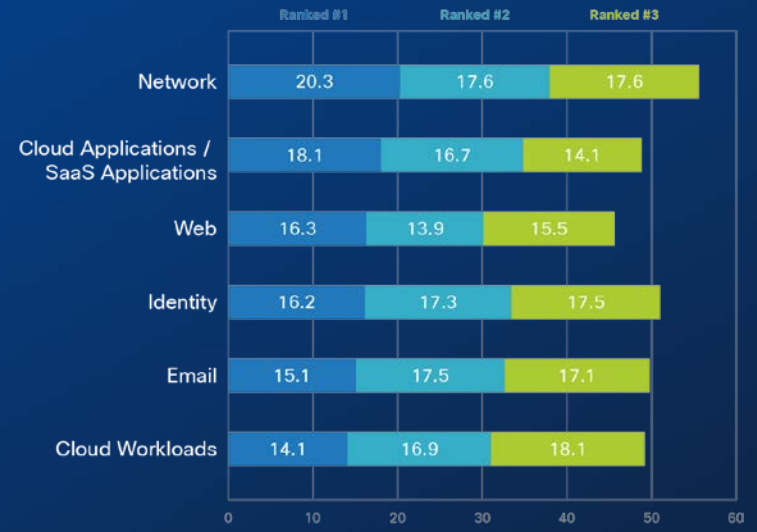
Source: ESD, The Impact of XDR in the Modern SOC.

**Streamline security operations**
**44%** say XDR will help consolidate security operations technologies into a common platform

Source: ESG, Why XDR Matters: (The Real Reasons) Why Security Leaders Care White Paper

# Network is the most important telemetry source, along with endpoint

**How would you rank the following telemetry sources?**




Source: IDC Most Important XDR Telemetry Sources


How does XDR work?

# The Burgled Apartment Analogy

You come home after a long day at work, when suddenly – oh no! – you realize your front door is wide open. You probably think back to when you closed it and wrack your mind to remember if indeed you did, or if this was a case of someone breaking into your home. Ultimately, you're looking for clues to help you determine what happened, and what to do next.

While a cyberthreat is a different type of threat, it can be just as damaging, and both require access to data, analysis, and decision-making tools for effective response. What if there was a tool that could help you do all these things more efficiently?

An XDR solution can do just that. We've outlined the threat detection and response steps below using the OODA decision-making framework, which stands for: **Observe, Orient, Decide,** and **Act.** Choosing an effective XDR solution can help you connect the dots between observation and action.

**Observe** an abnormality in your environment

Noticc my front door is opcn. Does this mean I have been robbed? Not necessarily, I could have accidentally left it open earlier, or someone else could have come in and left the door open. I need to know more.

**Orient** to the situation by gathering and analyzing detection data

Search my home and investigate further. I now notice that my TV and computer are missing.

**Decide** on the source of the threat

By corrclating picccs of information to provide a view of the situation, I can make decisions on what I think happened. My door was wide open, and valuables are missing - clearly my home has been burgled.

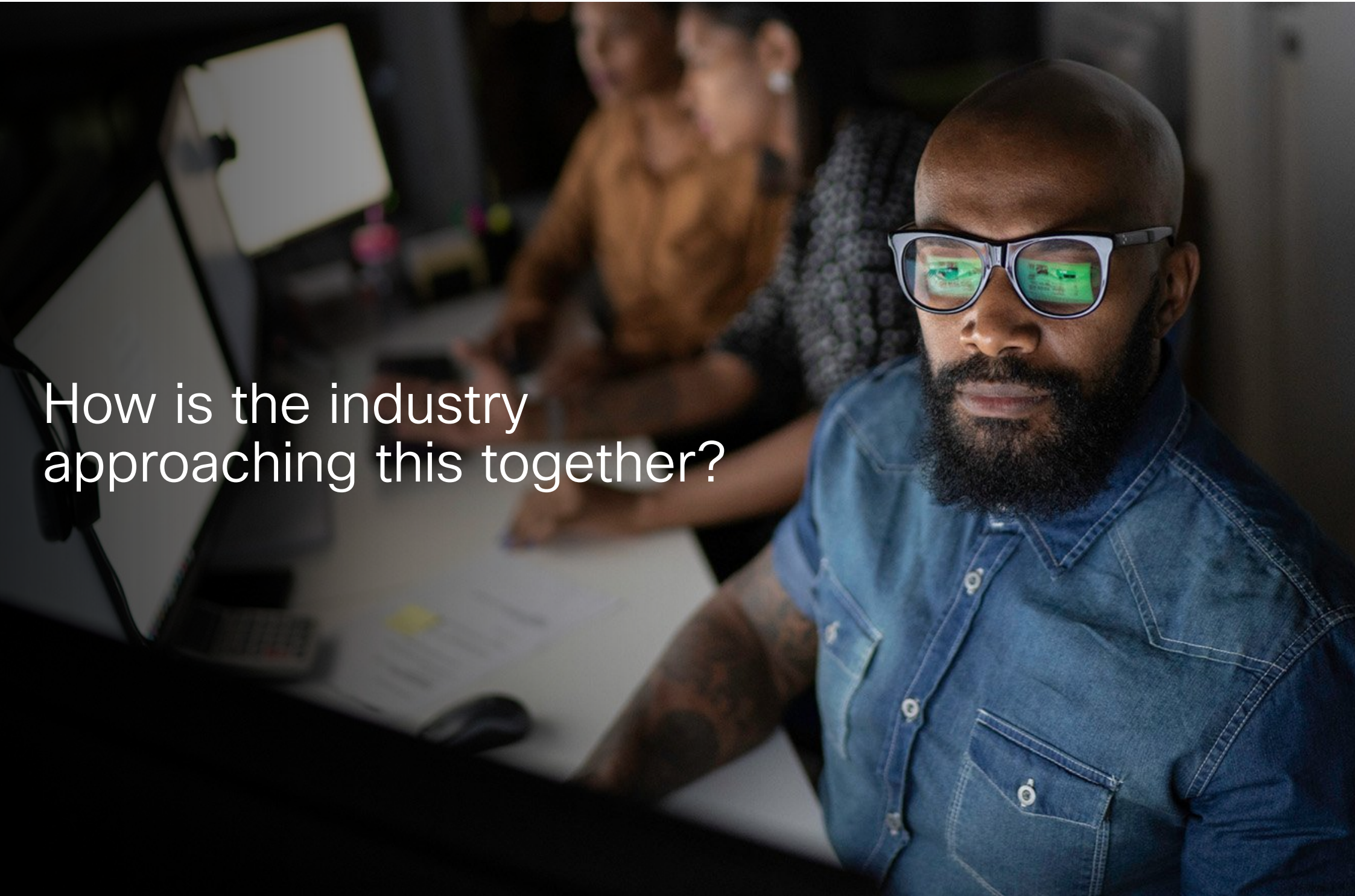
**Act** by responding to the threat

I call the police, report the theft. But based on my investigation, I also know the front door was the likeliest way the intruder got in, so I can take steps to protect my home better. Install better locks and get a security system!

Imagine that your home is like your security environment, and each door and window in your home is like a potential entry point for cybercriminals.

Just like you would install a security system in your home to protect against burglars, XDR can work like a security system for you.

If XDR detects something suspicious, it will alert your security team, just like a security system would sound an alarm. Then, you can take action to stop the cybercriminals from accessing your network, just like you would call the police to stop a burglar from entering your home.


How is the industry
approaching this together?

# Detect more, act faster, elevate productivity


To be truly effective, cybersecurity vendors must be open to sharing data and context so that advanced analytics across as many vectors as possible can rapidly detect and respond to the world's most sophisticated threat actor groups.

AJ Shipley, VP of Product Management for Threat Detection & Response, Cisco

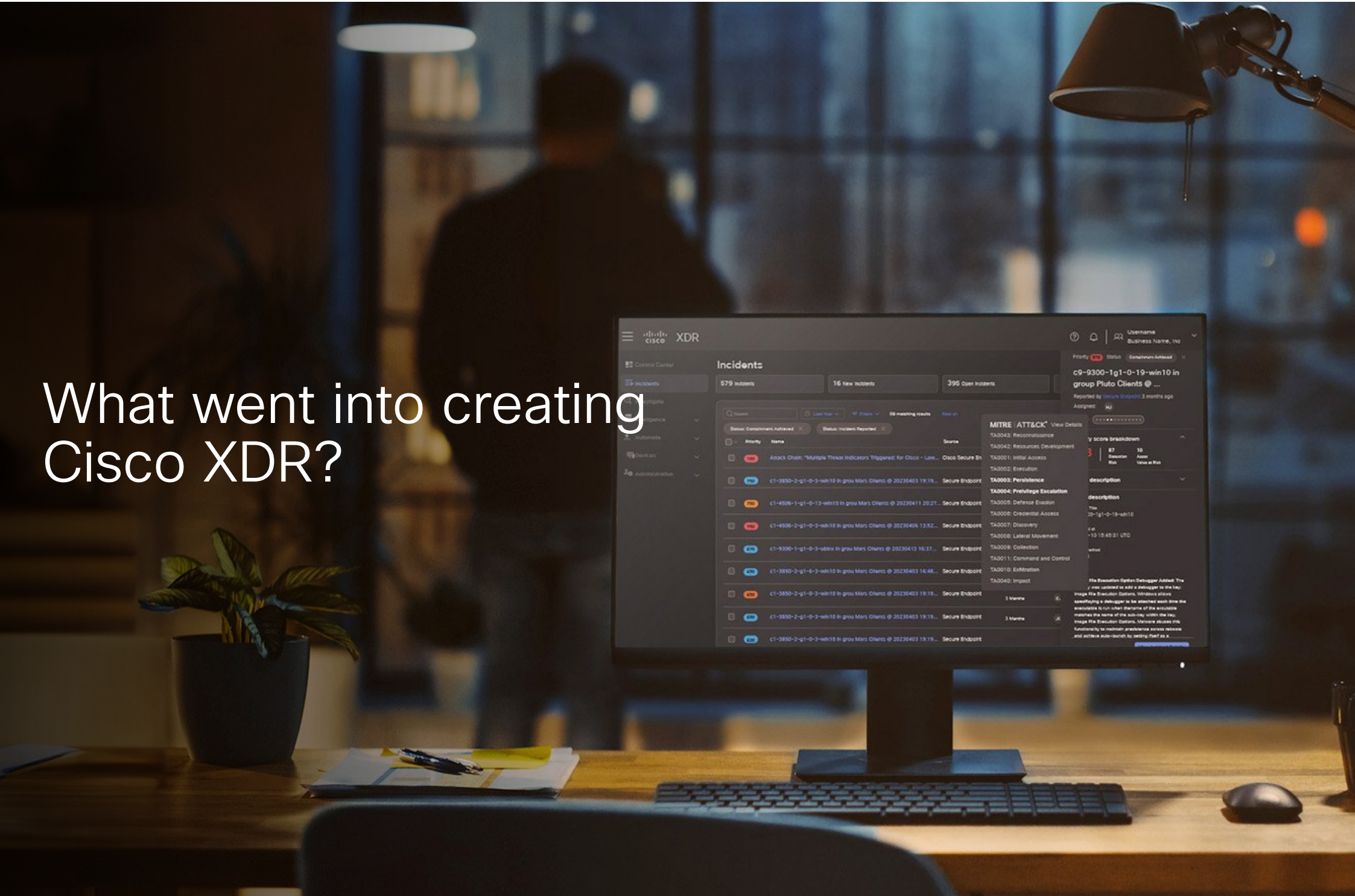
# In today's multi-vector, multi-vendor landscape, integration is essential.

Security vendors are collaborating to make it easier for customers to defend against threats and improve security resilience. Cisco protects 100% of the Fortune 100, and we're also customers of our customers. We depend on them for our family's healthcare needs and we bank with them for our mortgages and checking accounts. This is personal for us.

Since so many organizations use multi-vendor security approaches, no one can afford clunky vendor integrations that make it more difficult to protect your business. That's why we've built Cisco XDR as an open, extensible system with turnkey integrations with numerous third-party vendors – so you can adopt a unified and simplified approach across your security stack.

XDR is the unifying call for the industry to come together and position customers to protect their most critical assets.

# What went into creating Cisco XDR?



# Improving the security experience

When we asked CISOs to name pain points with their current XDR solutions, lack of integrations across other vendor tools was the most common response (45%). Security operations centers (SOCs) rely on multiple technologies to detect and respond to threats, but lack of integration often gets in the way, with SOC analysts forced to waste valuable time constantly switching back and forth between interfaces. 79% of security practitioners agreed that constant switching between interfaces diminished their ability to perform their jobs.

Cisco XDR was designed to help SOC analysts detect and respond to threats more quickly and effectively by providing a unified view of security data across multiple security tools and data sources. It empowers analysts of any skill level to perform advanced tasks within security operations; elevating productivity, and improving decision making times associated with key functions of detection, investigation and response:

1. **Simplifying data collection and analysis** by automating the collection and correlation of security data from across the organization's security environment
2. **Providing better context for alerts** with progressive disclosure of information to quickly determine the scope and severity of a potential threat.
3. **Improving incident response workflows** by providing a single interface for managing and tracking incidents across the entire organization's security infrastructure
4. **Leveraging workflow automation** to scale response actions and dramatically decrease remediation times

Cisco XDR provides a frictionless incident response experience that is streamlined and beginner-friendly, eliminating the need to visit multiple interfaces to accomplish a task. The XDR experience provides contextually-rich insights to analysts and displays differently based on experience level. Task-based access and assistive interface ramp up new users, while progressive disclosure avoids overwhelming beginners. It gives users the option and ability to dig deeper and get more detailed information as needed.

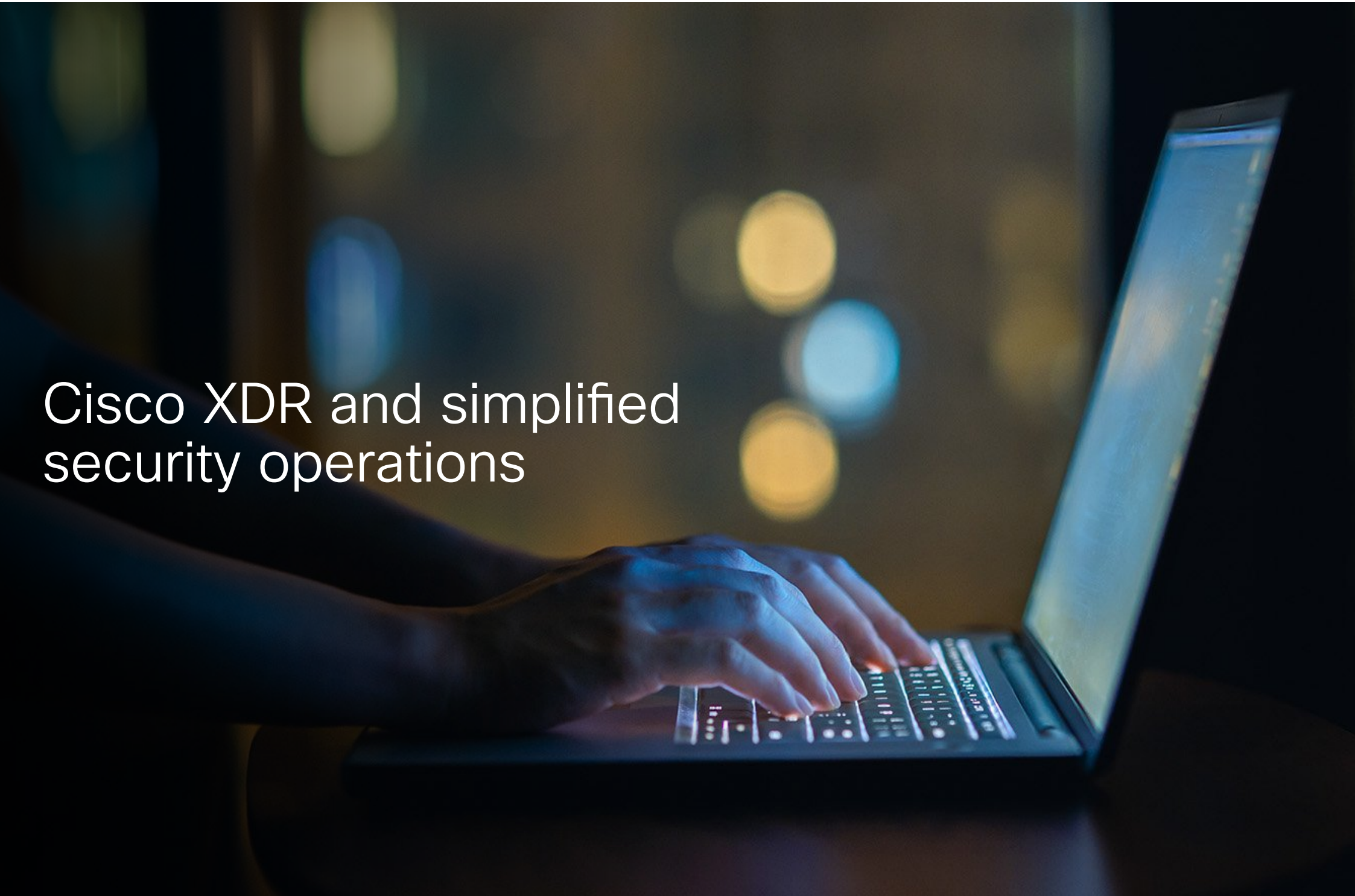
Security Operations Teams are constantly challenged to deliver on their mission statement, which is to identify security incidents and respond to confirmed threats swiftly to minimize impact. Most organizations do not have a DevSecOps Team to integrate and connect their security tools. When facing dangerous adversaries daily, the lack of integration across different point solutions makes the SecOps job even harder.

As we architected Cisco XDR, we crafted a solution that makes connecting disparate security tools a base principle – an expectation.

Practitioners know the value each telemetry source adds to an investigation. And because no one knows the Network better than Cisco, we've built in network detection as a critical telemetry source.

Cisco XDR is built by practitioners for practitioners, so we've incorporated analysis that correlates events across your environment, truly delivering a comprehensive view of what is going on. Analysts and Incident Responders are given risk - based focus on what to address first and guidance how to respond. With Cisco XDR, security analysts can shift from constantly making educated guesses on what has occurred in their environment to a focused mode of prioritized incident response, threat hunting, and confident resolution.

Briana Farro, Director of XDR Product Management, Cisco


Cisco XDR and simplified
security operations

# Act with greater speed, efficiency, and confidence

XDR shifts the focus from endless investigation to remediating the highest priority incidents with evidence-backed automation.

This means the threats that pose the greatest danger to your business get addressed first and security teams can make those decisions with confidence.

By doing XDR right, security teams can confidently respond to attacks, increase SOC efficiency, and automate tasks for a more proactive security strategy.

# Why Cisco XDR?

**We believe an effective XDR solution should do 5 things:**

1. Deliver a single detection and response solution for the SOC, that is risk-based, automated, and cloud-first
2. Stay open and extensible, integrating existing security investments to improve overall security posture
3. Leverage endpoint, network, email, cloud, and identity as foundational inputs for effective XDR detections
4. Prioritize threats based on greatest material risk to the organization
5. Leverage automation and orchestration capabilities to ensure rapid response

**Cisco XDR** can do all of this. We're optimized to keep your SOC running smoothly and to strengthen your overall security posture, improve security operations, and increase ROI.

# Take the fear, friction, frustration out of security

Cisco XDR is comprehensive - integrating with a broad portfolio of products including network, endpoint, email, identity, sandboxing, firewall, and more. In the name of simplicity, we've converged the data that security analysts need to do their job into a single console, so they can detect, investigate, and remediate threats in just a few clicks. What's more, actionable Talos threat intelligence and evidence-backed recommendations will empower your SOC analysts to confidently take action, no matter what comes next.

Cisco XDR is open, extensible, and cloud-first so you can leverage your existing security investments and gain unified security detection across your entire environment. With our 40-years-strong network heritage, we understand the network like no one else. With Cisco XDR, you'll benefit from deep network visibility, equipping SOC analysts with the network telemetry they need to pinpoint and confirm detections with ease.

And XDR is just the beginning. We want to partner with you in your security journey, so Cisco XDR is powered by Cisco Security Cloud — an open security platform aimed at helping you protect users, devices, and applications across your entire ecosystem, no matter what comes next.

## Learn more

5 Ways to Experience XDR eBook

Why XDR Matters: (The Real Reasons) Why Security Leaders Care White Paper

XDR Buyers Guide

## Ready to build the security operations of tomorrow, today?

Explore Cisco XDR

# Ready to build the security operations of tomorrow, today?

Explore Cisco XDR

Connection
we solve IT

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.connection.com/Cisco

C3347830-1125