Cisco XDR: Security Operations Simplified

Why does the world need another security approach?

Our current landscape requires **security resilience**

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.

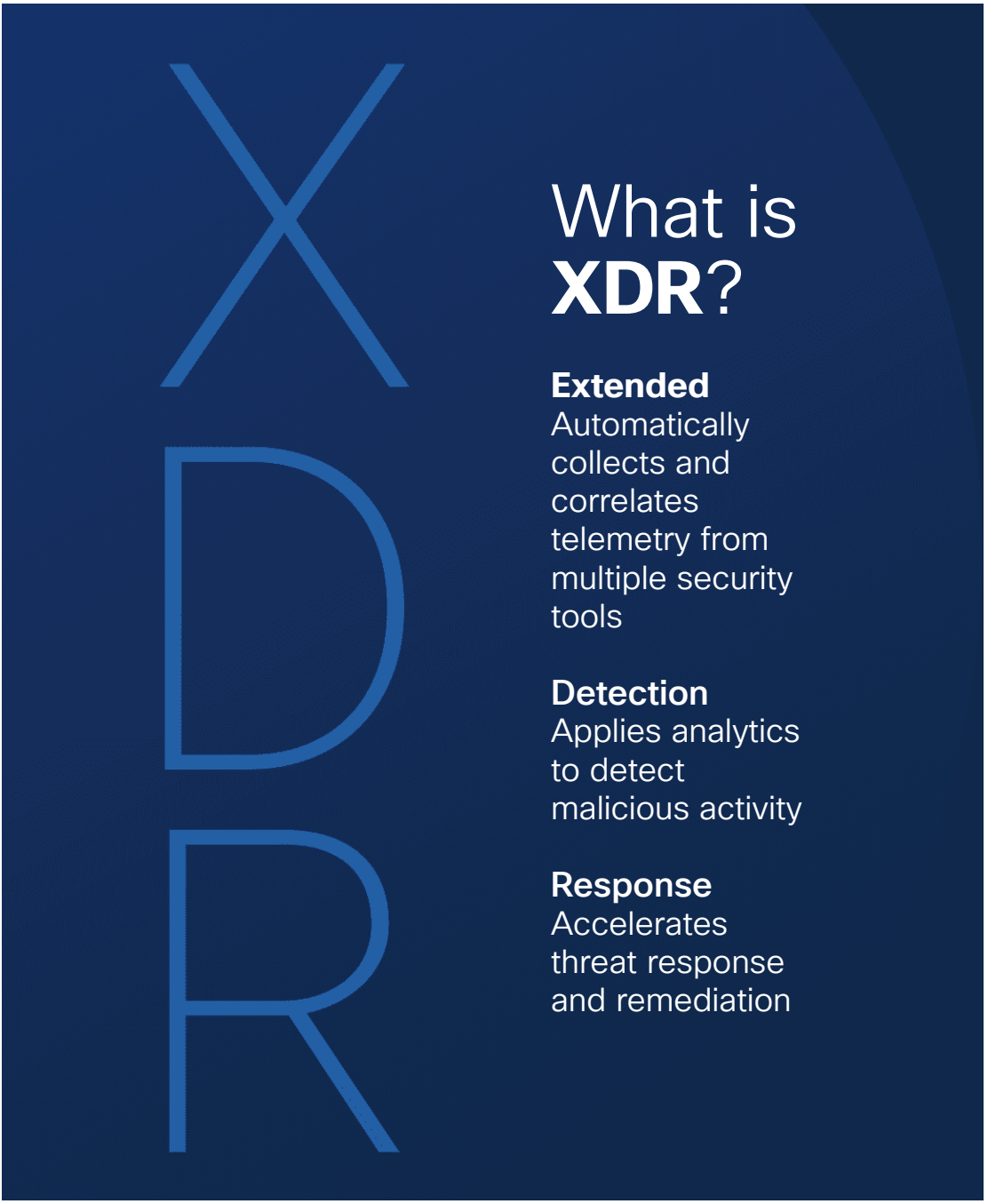
And the adversary is indistinguishable. They're like a chameleon, adapting to their environment, and blending in with their surroundings. They're always one step ahead, and it's becoming increasingly difficult to detect and prevent their attacks. They have the power to cause significant damage, and they're now using tactics and techniques that were once reserved for high-value targets. Remember the days of the Nigerian prince phishing emails riddled with typos? Well, those days are over. Hackers now have access to tools like ChatGTP, which allows them to launch targeted spear-phishing attacks that are personalized and difficult to detect.

It’s time for us to step up our game and find an approach that can keep us safe. Cyberattacks like phishing, malware, and ransomware are increasing rapidly each year. This new normal calls for security resilience – the ability to protect the integrity of every aspect of the business to withstand unpredictable threats or changes and emerge stronger. And security resilience calls for more than what the past has offered.

Want guidance and insights on how to purchase an XDR that fits your needs? Check out the XDR Buyer's Guide.

Toughen up cupcake, the Prince of Nigeria is sad too; no one falls for his emails anymore.

Anonymous



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 enhance threat detection and response through clear prioritization of alerts and providing the shortest path from detection to response. With threats becoming increasingly sophisticated, the old detection and response model, built upon self-contained point security solutions, which are then pieced together, doesn't go far enough. 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 SOC analysts want from XDR?

1. **Improved advanced threat detection and investigation**
   51% of professionals say their current tools struggle to detect and investigate advanced threats

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

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

4. **Improved security coverage, improved threat detection and response efficiency**
   25% want XDR to fill gaps within the security stack, while improving the efficacy and efficiency of threat detection and response

Top data telemetry sources that CISOs said XDR should cover:

EDR: 69%

Threat intelligence: 57%

NDR: 55%

Source: SOC Modernization eBook

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

Notice my front door is open. 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 correlating pieces 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 you or your security team, just like a security system would sound an alarm. Then, you or your security team 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?

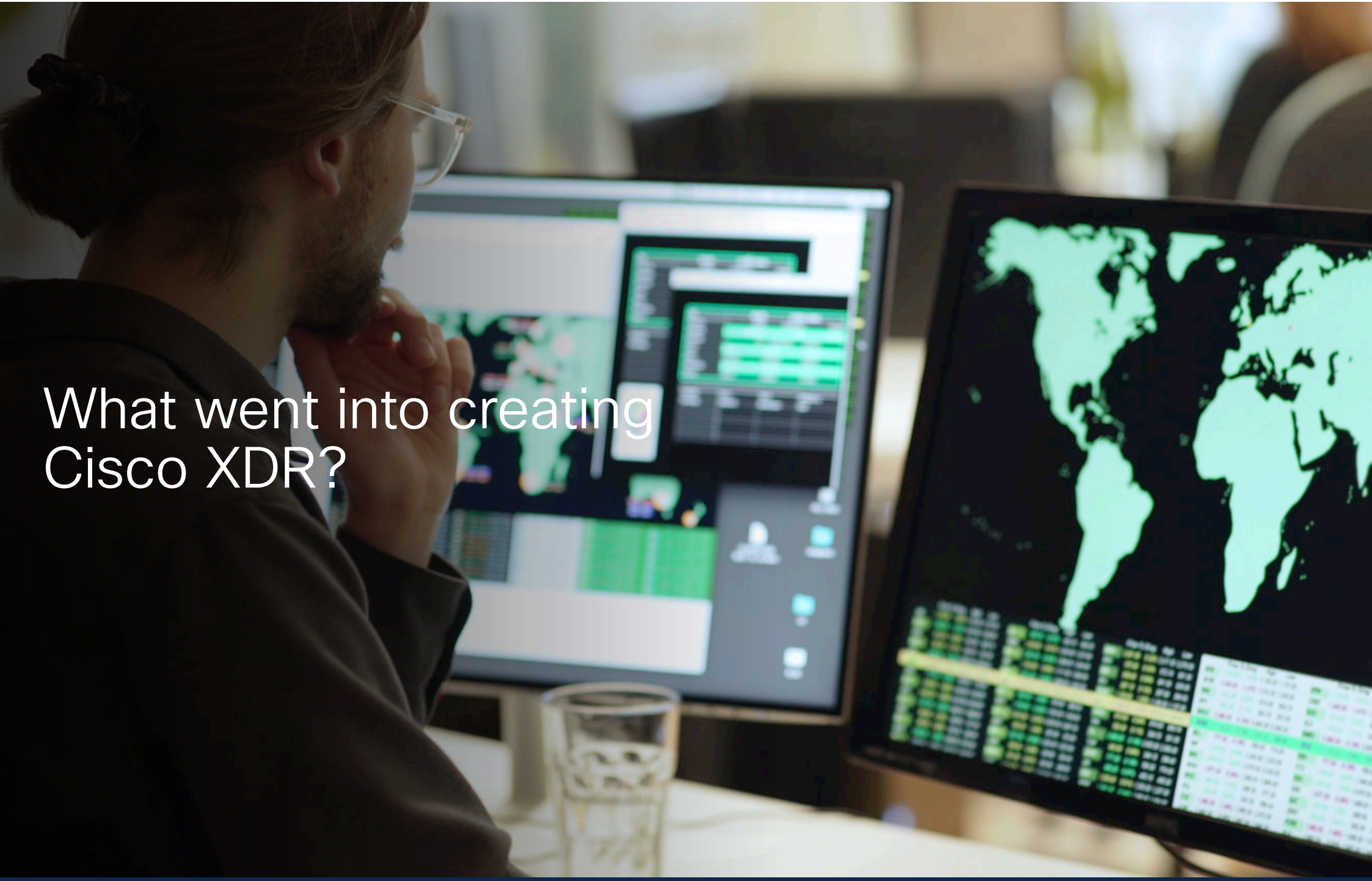
Detect more, act faster, elevate productivity to achieve security resilience

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 coming together to help customers more easily defend against threats and increase security resilience. At Cisco, we protect 100% of the Fortune 100, and in our everyday lives we're also customers of our customers. We bank with them for our mortgages and checking accounts, and we rely on them for our family's healthcare needs. This is deeply personal to us, and we take our responsibility to protect our customers' assets very seriously.

With many organizations employing multi-vendor security approaches, no one can afford clunky vendor integrations that make it harder or more time-consuming to protect your business. That is why we’ve built Cisco XDR as an open and extensible solution, with turnkey integrations with a variety of third-party vendors – so that you can adopt a unified and simplified approach to your security across your security stack. With the increasing sophistication of the adversary, 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 analyst 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 prevent security incidents and respond to confirmed threats swiftly to minimize impact. 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 took these complex challenges into account and crafted a solution that brings together disparate security tools. By understanding the telemetry in your environment and what it can tell you, we've incorporated analysis that correlates events across your environment, truly delivering extended detection, and presenting a comprehensive view of what is going on. Analysts and Incident Responders are then guided with intelligent recommendations on what to focus on first and 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 security resilience

XDR is a crucial component of security resilience

Today, uncertainty is a guarantee. Companies are investing in resilience across every aspect of their business, but these will all fall short without investment in security.

XDR is a crucial component of embracing security resilience for your business. Doing XDR right will strengthen your security posture by empowering security teams to prioritize threats by impact, detect threats sooner and accelerate response. This means the threats that pose the greatest danger to your business get addressed first and security teams can make those decisions with confidence.

Why Cisco XDR?

At Cisco, we believe every 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 and more, optimized to keep your SOC running smoothly. We know simplifying security operations is easier said than done. That's why we specifically designed Cisco XDR with the security analyst in mind.

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 resilience 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

An XDR Primer: The Promise of Simplifying Security Operations

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