Navigating Security in an Ever-Changing Digital World

Managed Extended Detection and Response

The State of Cybersecurity Threats and Cisco XDR

Evolving Threat Landscapes and Traditional Approaches to Detection and Response

In the ever-evolving landscape of cybersecurity, change is the only constant. As technological advancements make organizations more efficient, they also provide opportunities for bad actors to exploit vulnerabilities. This has led to a surge in cyberattacks, including an 84% increase in ransomware incidents from 2022 to 2023.[1] During this time businesses paid over $1 billion in ransomware payments[2]. On average, the cost of recovering from a data breach is currently $4.5 million[3]. Unfortunately, the true scope and impact of these attacks is difficult to gauge, as many organizations choose not to report incidents for fear of damaging investor or client relations.

To defend against these sophisticated attacks, a patchwork of security tools is often deployed, which can become overwhelming for the teams managing them. While well-intentioned, this approach can strain even the most skilled specialists, who are already overworked and spread too thin. Running multiple security tools that do not communicate with each other results in fragmented visibility and limited context. This leads to ineffective threat detection, prioritization, and investigation since security teams may miss complex, connected attacks and cannot focus on the most important threats to their organization.

Moreover, the lack of a unified view means cybersecurity analysts must manually correlate security telemetry to understand the full scope of an attack, which can result in wasted time. Traditional detection and response solutions can overload security teams by generating a high volume of alerts that overload security teams by generating a high volume of alerts – many of which are false positives. This alert overload makes it challenging to effectively identify complex attacks and prioritize threats. This results in blind spots and prolonged response times, especially for organizations without large security or IT teams.

Ultimately, the effectiveness of your security infrastructure depends on the personnel operating it. Not all organizations have fully staffed Security Operations Centers (SOCs) and relying on individual heroics is unsustainable. Additionally, a shortage of budget and skilled resources makes it difficult to attract and retain qualified IT security professionals, which means security teams must do more with less resources.

What this means for organizations

To create and deploy an adaptable security system, SecOps teams need to have clearly defined roles and protocols. As such, organizations should look to solutions that can integrate existing security solutions and are intuitive to the teams operating them. To that end, the connective nature of Extended Detection and Response (XDR) solutions helps organizations mitigate threat detection and response through increased visibility of networks, cloud, endpoints, email, identity and applications, and much faster time to detection.

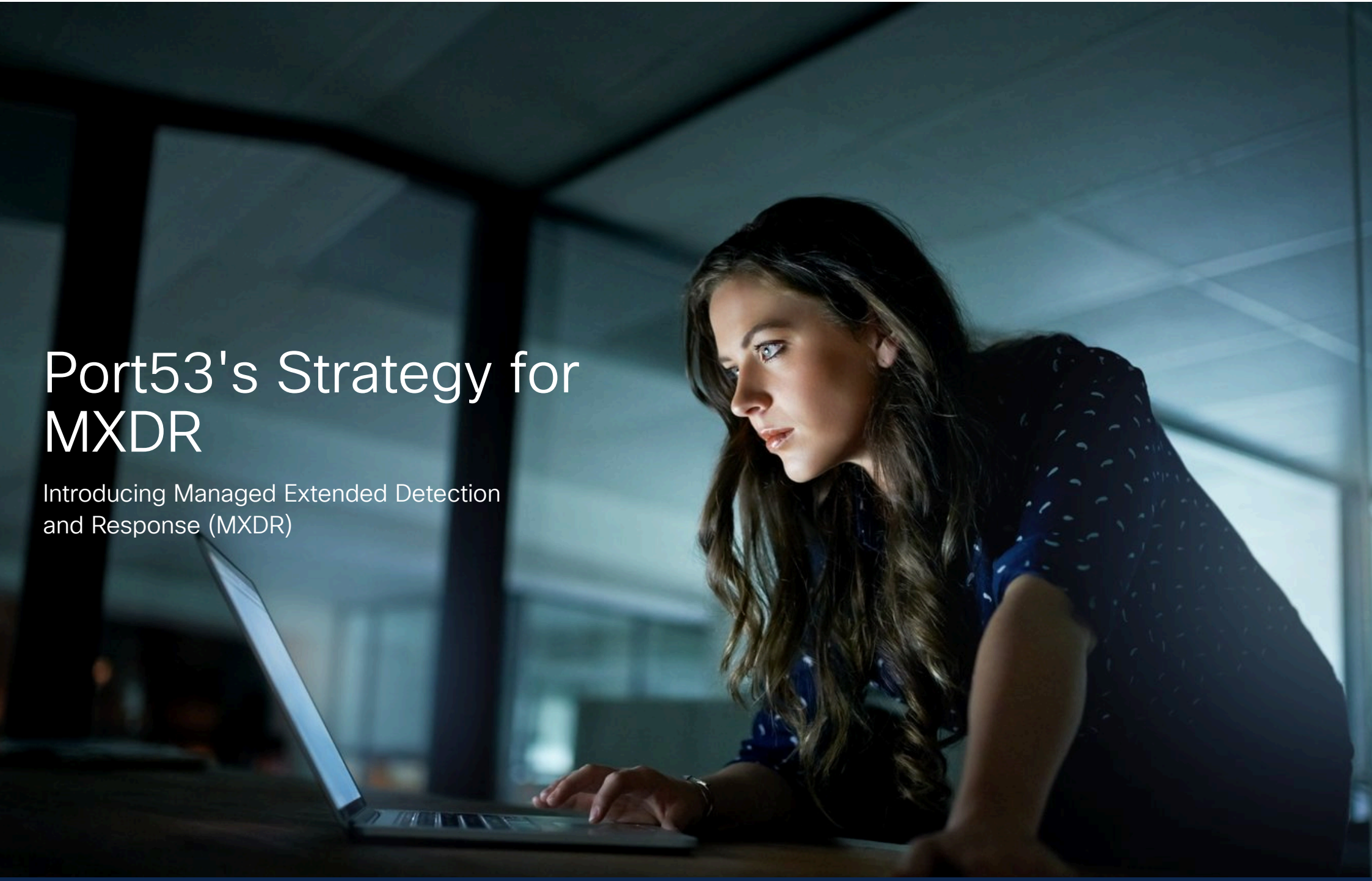
Cisco XDR offers significant benefits for organizations struggling with limited security personnel and increasingly sophisticated cyberattacks. By consolidating and correlating data from both Cisco and select third-party telemetry sources, it provides a unified view of the threat landscape, enabling even resource-constrained teams to effectively detect and respond to sophisticated threats. This improves threat detection and response times, enhancing the overall security posture of the customer. Cisco XDR also includes AI-driven guidance and automation capabilities to provide data-driven assistance, actionable next steps, and remediation recommendations. This not only reduces human error but also accelerates response times by automating incident response and repetitive workflows.

Cisco XDR offers flexible licensing options to meet the needs of every organization.

- **Cisco XDR Essentials** – the foundational security platform. Ideal for organizations that use only Cisco products, Cisco XDR Essentials includes full-featured native integration of the Cisco security portfolio, and additional threat intelligence from the Cisco Talos security research team.

- **Cisco XDR Advantage** – includes all the features in Essentials plus curated integrations with select third-party tools to rapidly respond to threats, regardless of vector or vendor.

- **Port53 MDR powered by Cisco XDR** – offers the full feature set of XDR Advantage along with managed extended detection and response (MXDR) services provided by Por53 Technologies security experts. Ideal for organizations that do not have the capacity or expertise to deploy and manage an XDR solution.



Port53's Strategy for MXDR

Introducing Managed Extended Detection and Response (MXDR)

Introducing Port53's Managed Extended Detection and Response (MXDR)

Establishing an enterprise-class approach to detection and response requires both a robust platform and the right people to manage it. Port53's Managed Detection and Response Program powered by Cisco XDR assists organizations that need a SOC, need to fill gaps in their security operations, or require 24x7x365 support from a team of world-class experts. Port53's MXDR powered service includes the following:

- 24x7 response across the lifestyle of each security event with white glove support by Port53 SOC Analysts
- Integration support for Cisco security solutions and Cisco-curated integrations with select third-party tools
- Platform co-management to facilitate ongoing optimization of the security stack
- Port53 Attack Surface Management
  - Penetesting-as-a Service
  - Vulnerability Management
  - Dark Web Scanning
- Port53 Risk Management, adopt a risk managed approach to cyber strategy by aligning to an industry standard cyber framework.

By leveraging the varying ranges of Port53’s managed detection and response offerings, organizations can ensure they are equipped to handle current security threats and are prepared to address future challenges with confidence and efficiency, no matter their scope or needs.

What Are the Benefits of Adopting a Managed Extended Detection and Response Framework?

The business outcomes provided by Port53's MXDR service include these six foundational benefits:

1. **Realize faster time to value** through turnkey SOC operations that allow you to focus on your core competencies while shrinking the total cost of security ownership

2. **Operate with confidence** by shifting the burden of recruiting, training, and managing security staff to Port53 – our experts detect, prioritize, and investigate incidents 24x7x365

3. **Future-proof your security** by taking a proactive approach to protecting and defending your environment by evolving and optimizing your defenses

4. **Detect and prioritize alerts in minutes** across your security environment using advanced investigation processes and response playbooks

5. **Accelerate incident response** through AI-driven processes and 24/7 threat monitoring

6. **Gain greater visibility** across an integrated security architecture driven by a combination of behavioral modeling, machine learning and global threat intelligence

Real-World XDR Case Studies

Customer Success Story:

County of Hardin

Background and Challenges

With a two-person IT team, the Iowa-based County of Hardin struggled to stay ahead of evolving cybersecurity threats. Their IT environment had become increasingly complex due to each department having its own software needs. Gaps in their cybersecurity became clear, particularly as they tried to meet strict insurance requirements for immutable backups and comprehensive security measures. They needed a partner who could provide the necessary expertise and solutions.

Solution and Implementation

The County of Hardin added penetration testing to identify and address vulnerabilities, deployed Cisco Secure Endpoint and transitioned to a Managed Detection and Response solution, and most recently, upgraded from Cisco SecureX to XDR, marking a significant step forward in their cybersecurity journey. The IT team at the County of Hardin appreciates that Port53 not only provides top-tier cybersecurity solutions but also acts as an extension of their own team. Alerts that occur off-hours are promptly handled by Port53's SOC-as-a-Service, allowing the county's IT team to rest easy knowing their systems are in capable hands.

"Port53 has been a game-changer for us. We were always winging it on our own, but as security requirements became stricter, we knew we needed help. With Port53, we not only get the right solutions but also the right people to help us when we need it. They bring something new to every meeting, and we've never had a bad experience with them."

– IT Team, County of Hardin

Partner perspective

Factors to Consider When Choosing an MXDR Partner

Choosing an MXDR provider can be a daunting, complex, and highly consequential decision for your organization's security. When seeking a provider, you'll want one with a strong industry reputation, positive customer testimonials, a comprehensive range of services, and evergreen support. Ensure their solutions are flexible, scalable, and can seamlessly integrate with your existing security infrastructure.

Assessing the Provider's Capabilities and Expertise

When analyzing which MXDR providers are best for your organization, it is important to ensure they possess in-depth knowledge of the latest threats and advanced detection technologies. This should be accomplished by assessing their incident response procedures, threat hunting capabilities, and the experience levels of their security analysts. It is also essential that they offer round-the-clock monitoring and support that guarantees a rapid response to security incidents.

Evaluating Service Level Agreements (SLAs) and Pricing Models

The terms you agree to with the vendor are crucial. Reviewing the provider's Service Level Agreements (SLAs) regarding performance and reliability is important, and it is also important to ensure there are no hidden fees, service paywalls, or scale triggers that result in heavy, unexpected costs. Consider the response and resolution times where provided. If this information is not available, that speaks volumes about the service you're evaluating.

Ensuring Regulatory Compliance and Data Privacy

Building and maintaining security systems in compliance with industry or regional regulatory requirements, as well as privacy statutes, is paramount. Ensure they have solid methods of data protection, appropriate encryption standards, and an incident response plan to protect your sensitive data and meet compliance requirements. This will help verify that the provider complies with applicable industry standards and relevant regulations.

Cisco and Port53 MXDR Offering Overview

Key Benefits

- Experienced security analysts led by experienced service leadership
- Cutting edge detection and response capability powered by Cisco XDR
- White-glove handling by SOC analysts throughout the security event lifecycle

Service Features

- Continuous threat monitoring and rapid incident response
- Full integration of Critical Threat Intelligence (CTI) with security controls and Proactive Threat Hunting
- Leverage current security investments with robust third-party product integration
- Service co-management - keeps your team involved in SOC operations as you desire

Support and Service Excellence

- Designated Technical Account Manager to drive customer satisfaction
- Monthly technical consultation with the Port53 SOC Team
- Quarterly business reviews with executive leadership

Power of Partnership

Invest in a security partnership, not just a security platform.

Port53 MDR powered by Cisco XDR combines the best of two worlds: Cisco's industry leading XDR technology with a white gloved co-managed service approach delivered by Port53.

Client testimonial:

"Port53's services are a game-changer for any organization looking to bolster its cybersecurity defenses. With their proactive approach and skilled analysts, Port53 delivers. Period. Their 24/7 real-time monitoring ensures threats are identified and neutralized before they can impact our organization. The SOC team leverages advanced threat intelligence to stay ahead of evolving cyber threats. Port53's tailored approach means our solution is aligned with the specific needs of our business, ensuring maximum protection without unnecessary complexity.

What truly sets Port53 apart is their commitment to customer success. Their team provides clear, actionable insights, regular updates, and unparalleled support, making even complex cybersecurity processes easy to understand and implement. Knowing our cyber assets are safeguarded by experts who truly care about our success, out internal IT Team is able to focus more on maintaining daily operations and direct user support to our employees; this increases our productivity as a department and as a company.

Bottom line, Port53's SOC services offer peace of mind and a strong line of defense in today's ever-changing cybersecurity landscape. Highly recommended for any organization prioritizing security and reliability, and wanting to increase IT Staff and End User productivity and quality of life in their respective roles!"

– IT Director at a manufacturing organization

Laying the Foundations of Your MXDR Strategy

At Cisco, we take pride in our long history and reputation for delivering robust, intuitive, and scalable security solutions. With that history comes the infrastructure and ability to provide a high level of quality, the flexibility to adapt with changing times, and a legacy of helping customers stay protected and successful.

How Does Cisco Stand Above the Competition?

When it comes to other similar solutions in the market, we excel in three key areas. First, our superior built-in network telemetry detects complex threats like lateral movement and data exfiltration, which most XDR solutions cannot match since many of them evolved from endpoint detection and response (EDR) products. Furthermore, with the recent acquisition and integration of Splunk, Cisco delivers a comprehensive SOC platform that grows with you, as your needs change, by meeting you wherever you are in your security operations journey.

Secondly, unlike competitors that lack robust integrations with third-party solutions, Cisco XDR offers native integrations with other Cisco tools and supports a diverse range of third-party security products. This allows you to integrate best-in-class tools within a centralized dashboard, improving data telemetry, investigation, and response capabilities, while optimizing ROI for existing solutions and minimizing overall costs.

Lastly, leverage Port53 MDR powered by Cisco XDR for comprehensive detection and response with superior support. Port53 security experts do the heavy lifting of defending your environment for you by detecting, investigating, and responding to incidents 24/7. This end-to-end service includes taking remediation steps on your behalf through automated response actions.

Conclusion

In today's ever-evolving threat landscape, staying ahead of cyberattacks is essential. With elite security experts by your side, you can operate with confidence, simplify your security operations, and ensure robust defense against sophisticated threats across multiple vectors.

We reduce risks across your threat landscape by leveraging a network-led approach to security, enriched with Cisco Talos intelligence and a dedicated global security team. This comprehensive defense, with our turnkey 24/7 SOC, helps you stay ahead of evolving threats. These services increase time-to-value by mitigating threats while providing your organization with insights approved by human security specialists and augmented by world-class AI. Ultimately, by providing your team with tools and automation that will help them focus on their highest priorities, Cisco XDR helps you lower the total cost of owning a robust security system.

At Cisco, we empower you to bring your security visions to life. Imagine accelerating your incident response through AI-driven processes and expert-led actions, with 24/7 threat monitoring and swiftly automated remediation, all powered by Port53's Managed XDR. In partnering with Cisco, you can achieve these goals and more. Our advanced threat detection technologies and comprehensive security services, provide cost effective solutions that are scalable, secure, flexible, and seamlessly integrate with your existing infrastructure. With us, you gain more than just a technology partner; you also gain the assurance that your organization is well-defended and ready for any security challenge.

Learn More

For additional information about Cisco XDR please visit the following webpages.

Cisco XDR
Port53 Managed XDR