Deloitte.

Modernize Cybersecurity Operations with Managed Extended Detection and Response (MXDR) by Deloitte

Learn how our streamlined platform can help you reduce total cost of ownership, improve efficacy, and support long term resilience.

Robust cybersecurity measures are more critical than ever in today's evolving digital landscape, as focus and investments in security increase.

Deloitte research found that 88% of surveyed governing boards addressed cyber-related issues quarterly or more frequently in 2024[1], up from 70% in 2023[2]. Similarly, security spending is expected to increase more than 15% from 2024 to 2025, according to Gartner®[3].

To help clients navigate these challenges, MXDR by Deloitte provides a fully managed cybersecurity platform—bringing together thousands of experienced cybersecurity specialists, demonstrated processes, and support for leading third-party technologies — to help organizations hunt, detect, respond to, and remediate cybersecurity threats.

With this expanded reach—including support from many leading cybersecurity solutions vendors — from CrowdStrike, Microsoft, Palo Alto Networks, and others—Deloitte's MXDR services provide broad protection capabilities for enterprises utilizing a wide range of cybersecurity platforms, such as Microsoft Defender and Microsoft Sentinel.

1. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/risk/deloitte-cn-ra-future-of-cyber-survey-en-241213.pdf

2. https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf

3. Gartner Press Release, Gartner Forecasts Global Information Security Spending to Grow 15% in 2025, August 28, 2024. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

What's driving the urgency for increased cybersecurity vigilance?

The cybersecurity market has grown exponentially as organizations face growing threats from cyber criminals and nation states.

Increasing frequency and sophistication of cyberattacks

Cyberattacks are becoming more frequent and sophisticated, targeting organizations of all sizes. A Deloitte survey found a significant jump in reported threats related to data loss—up from 14% in 2023 to 28% in 2024[4]. Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every two seconds by 2031[5]. These attacks can cripple operations and result in significant financial losses.

AI cyber optimization

Artificial intelligence (AI) is used by cybersecurity practitioners and adversaries alike. It helps bad actors launch more sophisticated attacks and powers advanced cybersecurity solutions. According to Gartner®, "By 2028, 25% of enterprise breaches will be traced back to AI agent abuse, from both external and malicious internal actors.[6]" In addition, nearly 40% of surveyed organizations leverage AI capabilities in their cybersecurity programs focusing on digital infrastructure monitoring, threat hunting, and automated security.[7]

Regulatory compliance

Stringent regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Cybersecurity Maturity Model Certification (CMMC) require robust cybersecurity measures to protect sensitive data and critical infrastructure, with non-compliance leading to significant fines and reputational damage.

Emphasis on Total Cost of Ownership (TCO)

In 2025, CISOs prioritize cost optimization and vendor consolidation to manage TCO. With scrutinized IT budgets, data and AI security, identity, and SecOps are prioritized. Managed services offer a resilient option for reducing expenses through outsourcing.[8]

Expanded attack surfaces and sophisticated threats

The adoption of cloud services, internet of things (IoT) devices, and remote work has significantly increased the attack surface, providing more entry points for cyber adversaries. Cybercriminals are using advanced tactics like social engineering, zero day exploits, and supply chain attacks. Nation-state actors and organized crime groups are also increasingly active, necessitating broad cybersecurity measures.

"25% of enterprise breaches will be traced back to AI agent abuse, from both external and malicious internal actors"

- Gartner Press Release

4. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/risk/deloitte-cn-ra-future-of-cyber-survey-en-241213.pdf

5. https://cybersecurityventures.com/ransomware-report-2021/

6. Garter Press Release, Gartner Unveils Top Predictions for IT Organizations and Users in 2025 and Beyond, October 22, 2024, https://www.gartner.com/en/newsroom/press-releases/2024-10-22-gartner-unveils-top-predictions-for-it-organizations-and-users-in-2025-and-beyond. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

7. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/risk/deloitte-cn-ra-future-of-cyber-survey-en-241213.pdf

8. April 2025 Security Update. Cleveland Research Company. April 14, 2025.

How rising complexity of cybersecurity threats increases the need for MXDR services

Endpoint Prevention, Detection, and Response (EPDR):

Enhanced visibility and protection for laptops, desktops, servers, and private clouds. EPDR solutions provide near real-time monitoring and response to endpoint threats, leveraging advanced analytics and ML to detect anomalies and potential threats.

Extended Detection and Response(XDR):

XDR solutions consolidate multiple data sources to deliver broad threat detection capabilities using security information and event management (SIEM), logging, and AI-driven analytics. By integrating data from various security tools, XDR provides a unified view of the threat landscape, enabling faster and more accurate threat detection and response.

Identity Prevention, Detection, and Response (IPDR):

Early detection and automatic response to identity-based attacks. IPDR solutions focus on protecting user identities and credentials, which are often targeted by attackers to gain unauthorized access to systems and data.

Cloud Security:

MXDR offers a variety of capabilities designed to detect, prevent, and respond to threats targeting cloud infrastructure and workloads, in addition to mitigating risks related to utilizing SaaS platforms.

Incident Response (IR):

IR services help manage emergencies through sensor deployment and rapid response to cyber incidents, assisting organizations contain and remediate threats to reduce damage and recovery time.

Adversary Threat Hunting:

Continuous threat hunting uses AI/ML and data-driven insights to proactively search for malicious activity within an organization's network, leveraging advanced analytics and threat intelligence to help identify and mitigate threats before they cause harm.

Operational Technology Prevention, Detection, and Response (OTPDR):

Protection for systems managing industrial equipment and processes. OTPDR solutions are designed to secure operational technology environments, which are increasingly targeted by cyber adversaries due to their critical role in industrial operations.

Deloitte's MXDR services now support a broader range of technology platforms.

Deloitte's MXDR services can help organizations to build a modular, software-as-a-service (SaaS)-based cybersecurity solution that aligns with existing tools and operational models. In response to client needs, MXDR's capabilities – already available for platforms such as CrowdStrike, Palo Alto Networks, are now available to clients who happen to select Microsoft cyber security products.

Deloitte's MXDR services helps security teams detect threats earlier, respond more effectively and improve TCO through enhanced automation and coordination. Key advantages of the Deloitte MXDR solution include:

- **Seamless integration:** MXDR integrates smoothly with existing security tools, enhancing their capabilities. This seamless integration helps organizations leverage their existing investments in their chosen technologies and also benefit from the advanced capabilities of MXDR.
- **Broad coverage:** Deloitte's MXDR services offers extensive coverage across endpoints, identities, operational technologies, and incidents, helping clients reduce the risk of cyberattack success.
- **Demonstrated experience:** Deloitte's cybersecurity specialists apply deep experience and proven practices to help organizations manage cyber threats. Our teams work with clients to address complex and evolving security challenges.
- **Automation and efficiency:** Deloitte's MXDR uses automation to enhance threat detection and response efficiency, helping to reduce the burden on internal teams. Automation helps streamline security operations, so organizations can respond to threats more quickly and effectively.

Demonstrated capabilities and experience

Recognized as the number one cyber consulting firm for 12 consecutive years by Gartner®[9], Deloitte provides broad cybersecurity solutions built on a foundation of demonstrated capabilities and extensive experience, including:

- **Global access:** With access to cyber talent in more than 150 countries throughout the Deloitte Touche Tohmatsu Limited network of member firms, our cybersecurity professionals bring a wealth of knowledge and experience to every engagement. This global access offers clients service and support regardless of their location.
- **Innovative solutions:** Deloitte continuously invests in research and development to stay at the forefront of cybersecurity innovation. By leveraging cutting-edge technologies and methodologies, Deloitte delivers effective, forward-thinking solutions.
- **Client-centric approach:** Deloitte's client-centric approach meets the specific needs and objectives of each organization with tailored solutions. This personalization helps clients achieve their cybersecurity goals while enhancing the value of their investments.
- **End-to-end service offerings:** Deloitte's cybersecurity services span the spectrum of security needs, from strategy and advisory to implementation and managed services. This broad approach helps clients focus on improving their cybersecurity posture through a single, trusted advisor.

9. https://www.deloitte.com/global/en/about/recognition/analyst-relations/consulting-managed-security-services-revenue-gartner-market-share-reports.html. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Advantages for Enterprises Using Integrated MXDR Solutions

- Enhance threat detection and response: Leverage advanced analytics and ML to identify and mitigate threats more quickly and accurately.
- Improve security posture: MXDR's advanced threat detection capabilities help organizations build a more resilient security posture.
- Operate more cost-effectively: Consolidate security tools and services into a single platform to help improve TCO and simplify operations.
- Simplify regulatory compliance: Understand alignment to regulatory requirements through MXDR's broad security management controls and processes.

MXDR in action

Though every organization's cybersecurity journey is unique, Deloitte designed MXDR to deliver efficacy, efficiency, and ease for clients. Here are two examples of what that looks like for two MXDR clients.

1. AI powers detection and mitigation with MXDR

When a client faced an attempted breach by a nation-state threat actor, Deloitte's AI Center of Excellence and cybersecurity teams collaborated to deploy a Zero Day Threat (ZDT) Detection model as part of our MXDR solution. This deep learning-based model, designed to detect anomalies and novel threats beyond traditional methods, identified nearly 80,000 suspicious connections. The MXDR Adversary Pursuit team then investigated and blocked malicious IP addresses associated with the threat.

This proactive, integrated approach helped the client avoid a significant security incident and demonstrates how Deloitte's combination of advanced AI and human expertise enables rapid, effective responses to sophisticated cyber threats. As part of Deloitte's ongoing commitment to evolving our MXDR capabilities, these advanced protections and continuous improvements are made available to all clients, supporting organizations in strengthening their security posture against emerging risks.

2. Enhancing visibility and threat response

A large company with limited cybersecurity operations struggled with insufficient threat detection, high alert fatigue due to untuned data sources, and a lack of antivirus and incident ticketing tools. This resulted in limited network visibility and inadequate response capabilities.

Deloitte helped strengthen these critical operations with MXDR's experienced team, demonstrated processes, and solution configurations and integrations. Together, this enhanced the company's security posture with 24/7 monitoring and increased visibility for in-scope systems deployed across 10,000 agents.

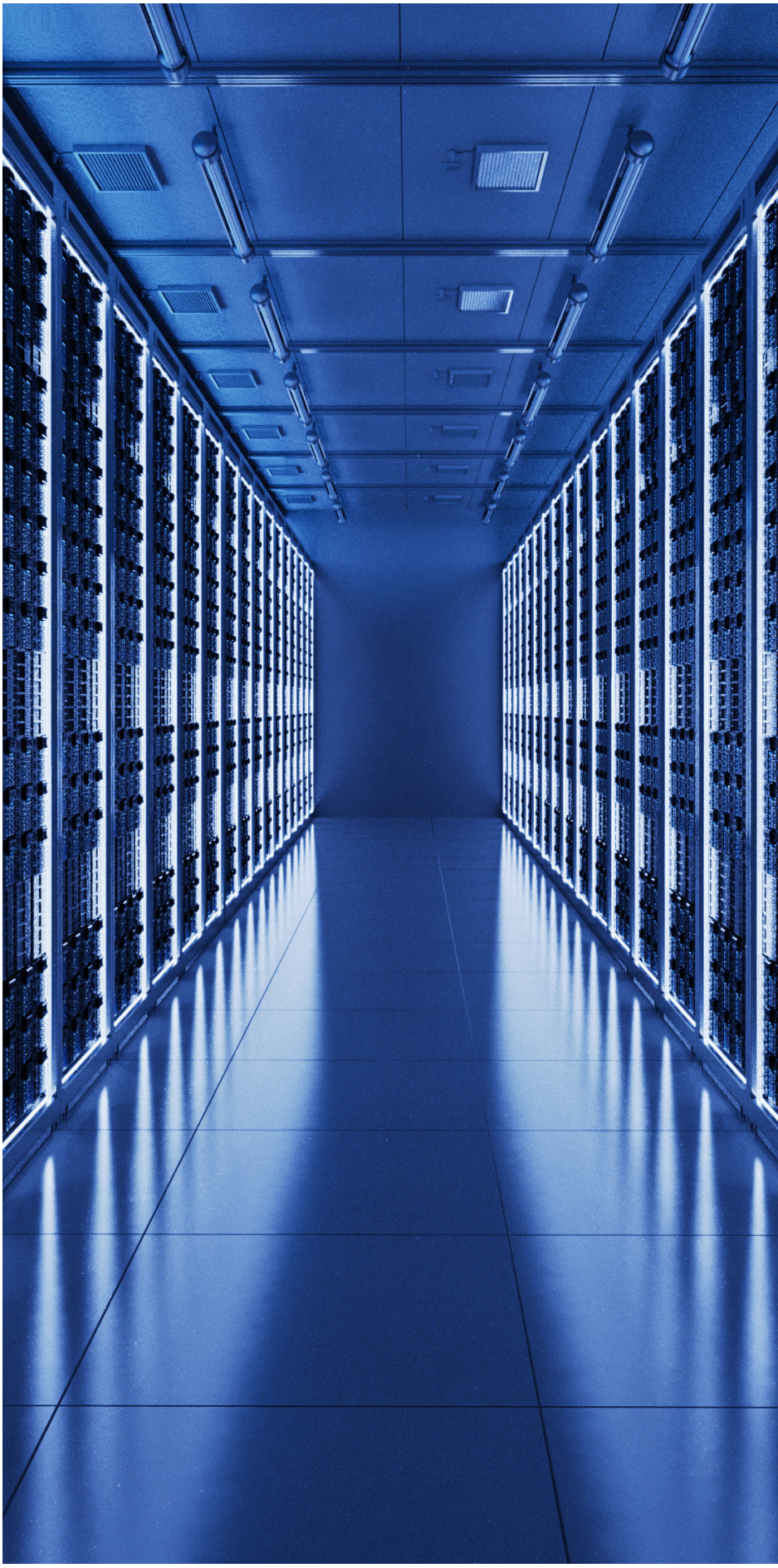
The client now uses MXDR to prevent advanced threats reducing false positives, ultimately delivering cost-effective, rapid, and potent security outcomes.

Next Steps

As cyber threats continue to evolve, enterprises should adopt broad, integrated cybersecurity solutions.

Deloitte's MXDR services assist clients across a variety of technologies. With advanced technologies and experienced management capabilities, Deloitte helps organizations achieve their goals, understand compliance guidelines, and protect their business.

For more information on how Deloitte's MXDR services can help you enhance your cybersecurity strategies and solutions, connect with us.



Contact us:

Chris Richter
Senior Managing Director
Deloitte Touche Tohmatsu Services, Inc.
chrichter@deloitte.com