

Securing Magnaflux's Intellectual Property with Gradient Cyber's MXDR

The Client

Magnaflux is a leading global provider of non-destructive testing (NDT) solutions, ensuring the safety and integrity of critical components in industries like aerospace, automotive, and oil & gas.

Headquarters

Glenview, IL

Industry

Non-destructive testing (NDT)

Company Size

220 employees, 8 IT staff

Parent Company

Illinois Tool Works (ITW)
Fortune 200 company
(\$16B revenue)

Why Magnaflux came to us

Magnaflux's IT team was burdened with security monitoring for its global network of endpoints, VPNs, VLANs, and firewalls. With a small team responsible for such a large infrastructure, the risk of intellectual property (IP) loss and the intense workload of managing security logs, alerts, and indicators of compromise (IoC) became overwhelming. Brad Bilotta expressed concern about having the bandwidth to effectively detect and respond to threats without increasing headcount or investing heavily in security tools.

Key Challenges

Small IT team handling a global network

Concerns over intellectual property loss

Overloaded with alert fatigue, making proactive security efforts nearly impossible

Securing Magnaflux's Intellectual Property with Gradient Cyber's MXDR

The Challenge

With a small IT team responsible for a global network, Magnaflux struggled to balance their daily IT workload with the need to protect sensitive intellectual property from increasingly sophisticated cyber threats. The manual effort to analyze logs and alerts was overwhelming and left them vulnerable to potential data breaches, particularly involving their proprietary chemical formulations used in NDT.



Without MXDR, we'd have to add two IT headcount, and \$100K budget for hardware and software and other things like AI that I'd have to start dabbling with. And that's a distraction.



Brad Bilotta

Division IT Manager, Magnaflux

The Solution

Magnaflux chose Gradient Cyber's MXDR platform to solve their security challenges. Our AI-driven, human-augmented solution provided round-the-clock threat detection and response across their entire network, including endpoints, cloud environments, and user activity. Our team of seasoned security analysts helped take immediate action on alerts, ensuring critical vulnerabilities were addressed before they became breaches.

Key Features of Our Managed XDR Solution




Comprehensive telemetry coverage from endpoints, networks, and cloud systems

Proactive threat detection using AI-powered analytics and human oversight

24/7 monitoring and SOC 2
Type 2 compliance

The Results

With Gradient Cyber's MXDR, Magnaflux was able to:

-  Avoid the need for two additional IT staff, **saving them \$100,000 in yearly costs.**
-  Significantly reduce alert fatigue and manual log analysis, **freeing the IT team to focus on strategic business initiatives.**
-  **Gain peace of mind** knowing that their sensitive IP was continuously monitored and protected from potential breaches.

The Value

By implementing Gradient Cyber's MXDR platform, Magnaflux not only improved its cybersecurity posture but also empowered its IT team to focus on core business operations, ultimately driving greater efficiency and protecting critical intellectual property from potential threats.

About Gradient Cyber

[Gradient Cyber](#) provides **Managed Extended Detection and Response (MXDR) solutions tailored for mid-market organizations.** Combining AI-powered analytics with human expertise, we deliver **24/7 threat detection** and response across networks, endpoints, cloud environments, and applications.

Our **technology-agnostic platform integrates seamlessly with existing IT and security stacks** to craft customized security solutions, ensuring early detection and prevention of cyberattacks. With Gradient Cyber, businesses gain proactive protection against evolving cyber threats, reducing risk and allowing IT teams to focus on growth.

For more more information: [Contact Us](#)