Gradient CYBER

Choosing The Right MXDR to Safeguard your business

Managed Extended Detection and Response (MXDR) Solution Overview

Table of Contents

The Problem

The MXDR Solution

What Sets MXDR Apart?

What can an effective MXDR Solution Do?

How Gradient Cyber MXDR Works

What Differentiates One XDR Platform From Another?

What Differentiates One MXDR Service From Another?

The Gradient Cyber Advantage

How Much Does MXDR Cost?

How Can I Get Started With Gradient Cyber MXDR?

The Reality –

You’re already a target

Every mid-market organization, **no matter its size or industry**, faces significant risks of business, financial, regulatory, and reputational damage from various cyberattacks and security challenges, including:

- Ransomware
- Phishing
- Business email compromise (BEC)
- Supply chain attacks
- Cloud security vulnerabilities
- Insider threats
- Internet of Things (IoT) vulnerabilities
- Distributed Denial of Service (DDoS)
- Advanced Persistent Threats (APT)
- Third-party risks
- Zero-Day Vulnerabilities
- Data Leakage and Loss
- Weak or Stolen Credentials
- Nation-state attacks

Those that are less mature and have not invested in threat detection and response capabilities across people, processes and technology **run the highest risk.**

Why Does This Continue to Be a Problem Despite **Decades of Cybersecurity Advancements?**

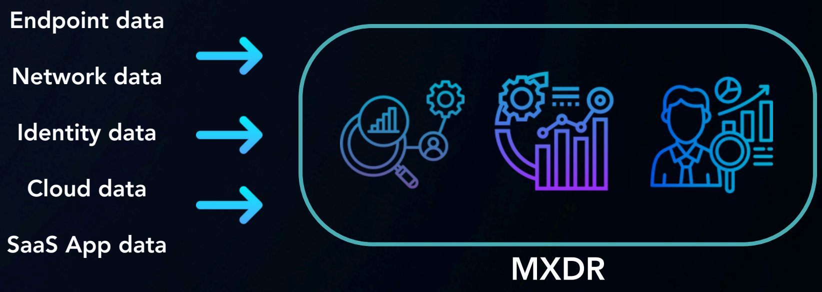
- **Complex, Evolving IT Environments**: Modern IT landscapes are increasingly complex and dynamic, presenting a large attack surface. The shift from on-premises infrastructure to cloud-based networks, reliance on third-party SaaS applications, the rise of IoT devices, and a growing remote workforce have all made securing the network perimeter far more difficult.
- **Sophisticated, Well-Resourced Attackers**: Cybercriminals are more savvy, well-equipped, and motivated than ever before. They have easy access to an underground marketplace of advanced tools, techniques, and procedures, making cyberattacks more accessible and less risky for perpetrators. The sophistication and scale of both independent hackers and organized crime groups continue to grow.
- **Industry-Wide Cybersecurity Talent Shortage**: The industry has long faced a severe shortage of cybersecurity professionals. Overwhelmed by alert fatigue, fragmented security tools, and underfunded security budgets, many organizations struggle to keep up with evolving threats, leading to burnout and high turnover among security staff.

When a Service Model **is the Best Solution**

There comes a point where certain business needs are so essential—yet so complex—that they are best handled through a service model. This is true for utilities like power, water, and communications, and now it applies to cyber threat detection and response. For many organizations, especially in the mid-market, managing this escalating challenge independently is no longer feasible.

The MXDR Solution

Managed Extended Detection and Response (MXDR) is a comprehensive cybersecurity service that unifies several critical detection capabilities: Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Cloud Detection and Response (CDR), and SaaS Detection and Response (SaaSDR). This integrated approach provides a powerful, all-in-one solution to effectively combat modern cyber threats.



Endpoint data

Network data

Identity data

Cloud data

SaaS App data

MXDR

Key Features of Top MXDR Providers

Leading MXDR providers not only offer advanced security services but also bring their own XDR platforms, staffed with 24x7x365 SOCs and teams of cyber analysts. These experts monitor network activity, user behavior, and various telemetry data to detect indicators of compromise (IOCs), threats, and anomalies. They also perform rapid investigation, response, and remediation to protect your organization.

What Sets MXDR Apart

Unlike many traditional cybersecurity products, MXDR offers a holistic view of your organization's security and risk posture. Since attackers operate with increasing sophistication, focusing solely on endpoint, network, or identity-based signals in isolation is insufficient. MXDR integrates and correlates data across multiple layers—endpoint, network, cloud, and identity—allowing for a comprehensive understanding of attackers' movements and intent, enabling more effective defense.

Comprehensive Threat Detection and Response

A threat detection and response solution must analyze telemetry data across all domains in real-time, providing a full situational analysis without overwhelming teams with false positives. This involves more than reacting to threats after an exploit—it requires proactive detection before an exploit occurs. To achieve this, the solution must offer 360-degree visibility into both structured and unstructured data using AI and big data technologies. It's not just about collecting large amounts of data but about gaining actionable insights from it, enabling organizations to take proactive steps in defense.

A robust MXDR solution dramatically reduces two critical metrics:

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)

both of which are essential for identifying and stopping attackers before they can achieve their objectives.

What can an effective **MXDR Solution Do?**

By integrating AI, machine learning, and human-in-the-loop threat-hunting techniques, MXDR solutions can quickly detect early signs of attack activity. This proactive approach helps intercept attackers before they steal financial assets, intellectual property, or sensitive records like customer, patient, or employee data.

Key Signals an attacker has already breached your defenses

Network Signals

1. Unusual Traffic Patterns & Anomalies: North-South & East-West
1. Recon Activity
2. Lateral Movement
3. Malware Comms
4. Protocol / App Misuse

Endpoint Signals

1. Malware and Ransomware
2. Suspicious Behavior
3. Fileless Attacks
4. Credential Misuse
5. Zero-Day Exploits

User Behavior Signals

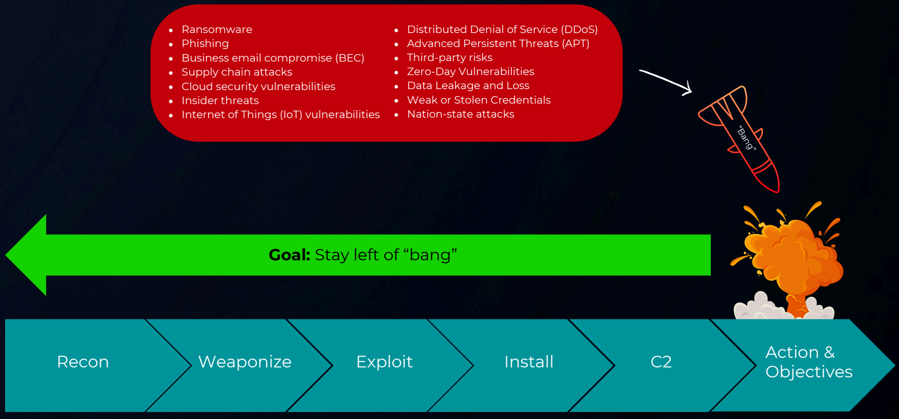
1. Anomalous Access Patterns
2. Excessive or Unusual Data Access/Transfer
3. Multiple Failed Login Attempts
4. Simultaneous Logins from Diverse Locations
5. Role and Permission Changes

SaaS Signals

1. Unauthorized Access or Logins
2. Data Leakage or Exfiltration
3. Suspicious or Malicious Activities
4. Misconfigurations & Compliance Violations
5. Compromised or Shared Accounts

Cloud Service Signals

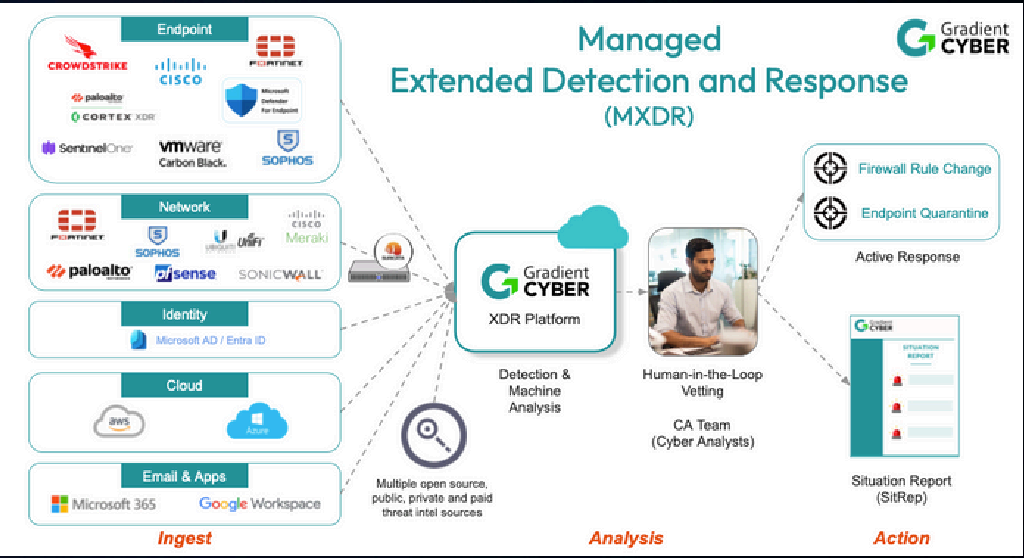
1. Misconfigurations
2. Unauthorized or Anomalous Access
3. Resource & Service Anomalies
4. Data Leakage or Exfiltration
5. Non-compliance with Security Policies



- Ransomware
- Phishing
- Business email compromise (BEC)
- Supply chain attacks
- Cloud security vulnerabilities
- Insider threats
- Internet of Things (IoT) vulnerabilities
- Distributed Denial of Service (DDoS)
- Advanced Persistent Threats (APT)
- Third-party risks
- Zero-Day Vulnerabilities
- Data Leakage and Loss
- Weak or Stolen Credentials
- Nation-state attacks

How Gradient Cyber MXDR Works

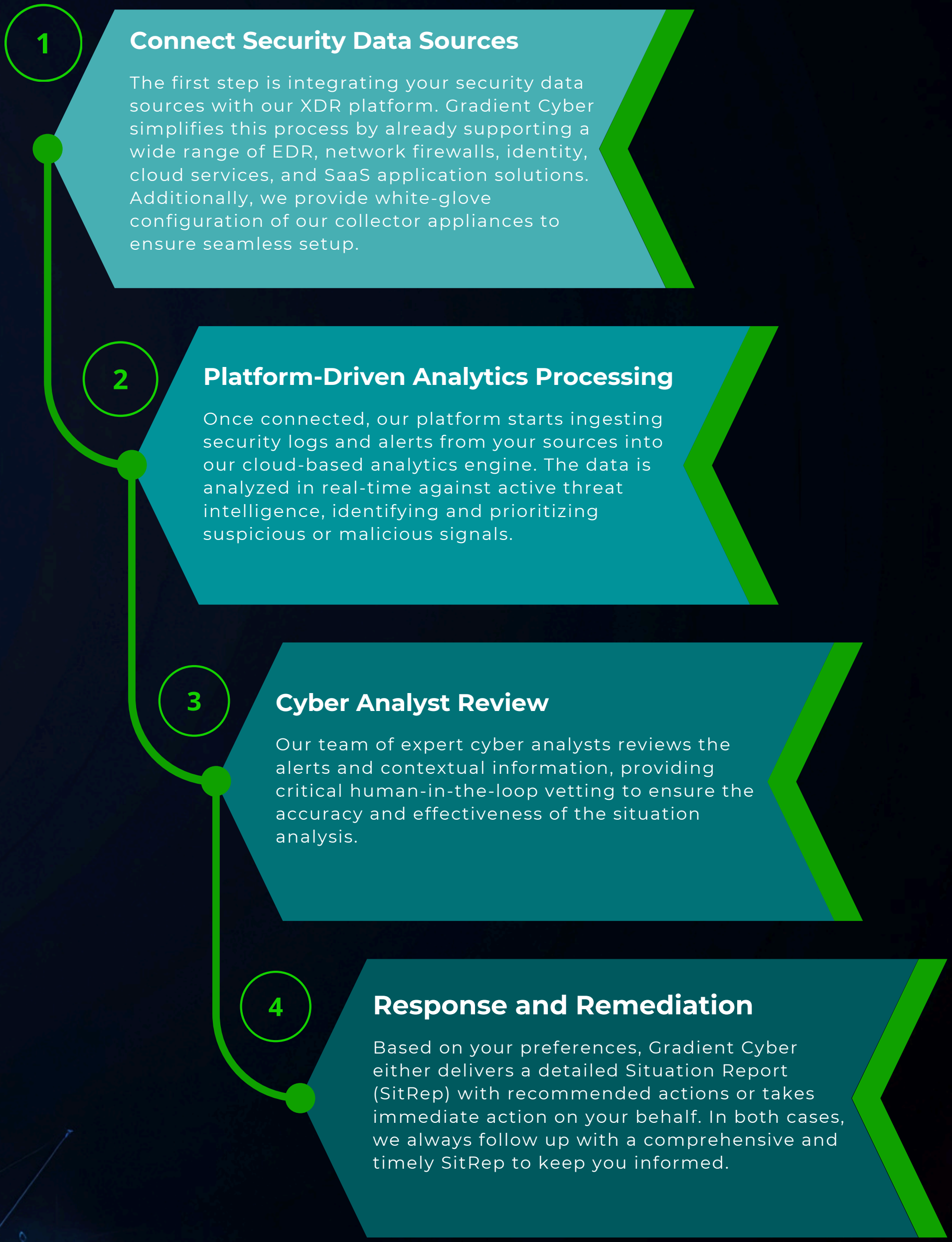
Our MXDR solution integrates data from multiple security telemetry sources, analyzing network signals—like botnets, DNS anomalies, and unauthorized TOR activity—and endpoint signals, such as privilege escalation attempts and unauthorized software installations.



By combining this data with real-time threat intelligence on current and historical attacker tactics and tools, our solution pinpoints specific kill chain activities that form the basis of advanced cyberattacks.

This comprehensive approach enables proactive defense against a wide range of threats, from phishing and malware to identity-based attacks like lateral movement and account anomalies.

From Data Source to Situational Report
The Gradient Cyber Difference



1

Connect Security Data Sources

The first step is integrating your security data sources with our XDR platform. Gradient Cyber simplifies this process by already supporting a wide range of EDR, network firewalls, identity, cloud services, and SaaS application solutions. Additionally, we provide white-glove configuration of our collector appliances to ensure seamless setup.

2

Platform-Driven Analytics Processing

Once connected, our platform starts ingesting security logs and alerts from your sources into our cloud-based analytics engine. The data is analyzed in real-time against active threat intelligence, identifying and prioritizing suspicious or malicious signals.

3

Cyber Analyst Review

Our team of expert cyber analysts reviews the alerts and contextual information, providing critical human-in-the-loop vetting to ensure the accuracy and effectiveness of the situation analysis.

4

Response and Remediation

Based on your preferences, Gradient Cyber either delivers a detailed Situation Report (SitRep) with recommended actions or takes immediate action on your behalf. In both cases, we always follow up with a comprehensive and timely SitRep to keep you informed.

What Differentiates One XDR Platform from Another?

Not all MXDR platforms approach cybersecurity the same way. XDR solutions generally evolve from three distinct heritages: EDR-based, SIEM-based, and network-centric (specifically network threat analytics) XDR platforms.

EDR-Centric XDR

Many XDR solutions originate from Endpoint Detection and Response (EDR) platforms. While endpoint telemetry is valuable, these platforms often face several limitations:

- **Endpoint-Centric Focus**: Strong on endpoint data but often weak in other areas, particularly network traffic.
- **Limited Network Insight**s: They tend to lack robust capabilities for analyzing network traffic.
- **Vendor Lock-In**: Many are tied to specific endpoint agents, limiting visibility to only where those agents are installed.

SIEM-Centric XDR

XDR solutions evolved from Security Information and Event Management (SIEM) platforms are proficient in log collection, correlation, and alerting, which are essential for log management and compliance. However, they also have notable challenges:

- **Compliance Over Security**: SIEM-centric platforms are often focused on compliance needs rather than proactive threat detection.
- **Big Data Motivation**: These platforms are data-heavy, leading to storage-centric designs rather than analytics-driven ones.
- **Scalability Issues**: SIEMs were not built to handle the massive data volumes seen in modern SOCs, nor are they optimized for advanced AI/ML analytics or complex threat analysis queries.

What Differentiates One XDR Platform from Another?

Most XDR platforms have entered the XDR market from either an EDR or SIEM heritage.

Network-centric XDR

The third pathway into XDR is network-centric. This is the approach Gradient Cyber has taken. Fewer vendors have entered in this manner as network threat analytics are harder to develop, require the processing of large volumes of network telemetry, and are prone to a high false positive rate if not well-tuned to the uniqueness of each particular IT/network environment. Yet, these are the exact problems Gradient Cyber has been solving for years. The advantages of a (properly designed) network-centric XDR include:

- Open, vendor agnostic - zero lock-in
  - Data source / API integrations through managed service install, config and operation
- Network visibility is ground truth
  - The toughest analytics to build and interpret
  - Tracks every network device, including IoT devices not supported by endpoint tools
  - Comprehensive East-West monitoring. Edge FW logs only see North-South traffic
  - Full packet (Bi-flow and PCAP) sees more than FW logs (the scope of many XDR vendor ‘network analytics’)
  - Span port above and below the firewall facilitates auditing/cross reference of logs
- EDR and User and Entity Behavior Analytics (UEBA) further enrich XDR’s ability to piece together a complete attack progression / kill chain sequence

Each platform type has strengths but also distinct weaknesses, making it critical for organizations to choose a solution that aligns with their needs, particularly when it comes to balancing endpoint, network, and cloud security.

What Differentiates One MXDR Platform from Another?

When choosing an MXDR service for mid-market organizations, several key differentiators should be considered:

Mid-Market Focus

Does the vendor specialize in serving mid-market organizations? The cybersecurity needs of SMBs, mid-market firms, and large enterprises differ significantly. A solution built specifically for the mid-market is critical to addressing their unique challenges. Beware of vendors claiming that one-size-fits-all solutions work across the board.

Technology Agnostic

Is the MXDR solution flexible enough to integrate with your existing security infrastructure? Many vendors push "land and expand" strategies, locking customers into using specific EDR or firewall solutions. A truly agnostic MXDR service should work seamlessly with your current tools, avoiding vendor lock-in.

Platform Ownership

Does the MXDR provider own and operate their own XDR platform? This is crucial for long-term flexibility. As data sources and analytics technologies evolve, the platform must adapt. A provider that controls its platform can offer more responsive updates, integrate the latest AI advancements, and tailor dashboards and reporting to your specific needs. If the vendor can't manage their platform down to its core, they may struggle to keep up with the dynamic nature of modern cybersecurity.

Is Your MXDR Provider Secure?

When evaluating an MXDR provider, it's critical to ensure that they themselves are secure. One of the key indicators of this is SOC 2 Type 2 compliance.

This certification shows that the provider's security operations center (SOC) has undergone a thorough and rigorous vetting process, ensuring their internal controls are designed and operating effectively to protect sensitive data.

Make sure your MXDR provider is not just SOC 2 compliant, but specifically Type 2, which involves ongoing audits over time and proves that security controls are maintained continuously, year after year. This level of compliance is more demanding but offers a greater level of trust and assurance.

The Gradient Cyber Advantage

Purpose-built for the mid-market, Gradient Cyber's MXDR solution offers a powerful combination of EDR, identity, and deep network traffic analytics, enhanced by real-time data analysis for accurate threat detection and response.

Our cloud-based, AI-driven platform, integrated with NIDS, is fully operated in-house by our SOC 2 Type 2 compliant, 24/7 Security Operations Center. Backed by a team of experienced analysts, we prioritize personal relationships, ensuring ongoing support from installation to optimization.

Key differentiators include:

- **Comprehensive data sources**: Integrating EDR, identity, and rich network analytics, with live data analysis of both PCAP and bidirectional flow (Biflow).
- **Resilient and scalable cloud-based platform**: Embedded with machine learning and NIDS, and supported by deep in-house knowledge across all analytics and operations.
- **Optimized data collectors**: Local processing minimizes network bottlenecks and reduces unnecessary storage costs.
- **Human-in-the-loop analysis**: Automated processes are supported by skilled analysts who vet final actions for accuracy.
- **Dedicated, hands-on support**: We emphasize personal touchpoints, from tailored installations to regular risk and compliance reviews, making us easy to work with and responsive to evolving needs.

With Gradient Cyber, businesses benefit from a comprehensive, scalable solution that combines cutting-edge technology with a personal, hands-on service experience.

How Much Does MXDR Cost?

When considering the cost of MXDR, it’s useful to first evaluate what it would take to build effective threat detection and response capabilities on your own. This includes:

1. **Security Telemetry Collection**: You'll need systems that can gather the right data from key locations and forward only necessary information to a cloud-based engine, avoiding network congestion and costly cloud data fees.
2. **A Robust XDR Platform**: This platform must ingest data, integrate active threat intelligence, use continuously evolving analytics (both human and AI-driven), provide a user-friendly interface, and integrate with other security products (firewalls, EDR, SOAR systems).
3. **SOC 2 Type 2 Compliance:** Maintaining a SOC 2 Type 2 compliant Security Operations Center ensures that security controls are functioning effectively, safeguarding sensitive data and ensuring operational resilience.
4. **Ongoing Management**: You'll need developers and administrators to manage software updates, data storage, resilience monitoring, and keep the system running smoothly.
5. **Skilled Security Analysts**: A trained security team is necessary to handle the constant stream of alerts and security telemetry from your IT environment.

For a typical mid-market organization, building and maintaining these capabilities can easily cost in the high six to seven figures annually. However, with Gradient Cyber, a mid-market business can typically expect to spend about one-third the cost of hiring a single experienced cybersecurity analyst per year.

Return on Investment (ROI)

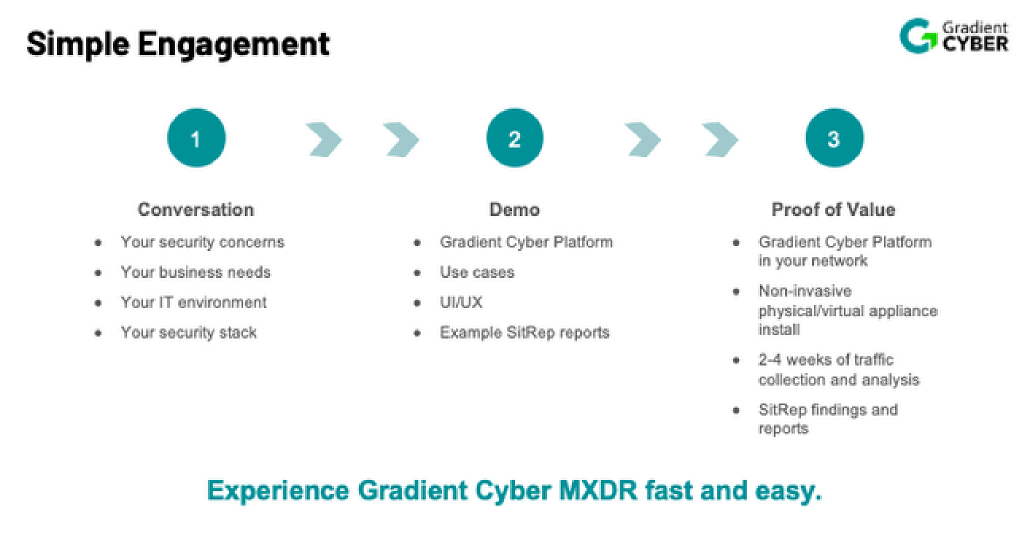
Beyond cost savings, the real ROI comes from having a top-tier threat detection and response capability that identifies attackers before they can complete their mission.

While preventative measures are important, they won’t stop every attack. The ability to detect and respond to threats before significant damage or data loss occurs—potentially saving millions—is where the value of MXDR truly shines. Moreover, partnering with a service provider that focuses exclusively on the mid-market ensures that the solution is tailored to your needs, offering the best protection possible.

Get Started with **Gradient Cyber MXDR:**

At Gradient Cyber, we understand that every organization has its own unique set of challenges, risks, and IT environments—each forming its own “gradient.”'

That’s why we offer a straightforward 3-step process to get MXDR up and running:



Simple Engagement

Gradient CYBER

1 Conversation

- Your security concerns
- Your business needs
- Your IT environment
- Your security stack

2 Demo

- Gradient Cyber Platform
- Use cases
- UI/UX
- Example SitRep reports

3 Proof of Value

- Gradient Cyber Platform in your network
- Non-invasive physical/virtual appliance install
- 2-4 weeks of traffic collection and analysis
- SitRep findings and reports

Experience Gradient Cyber MXDR fast and easy.

Once you’ve gone through this process, we’re confident you’ll see the tangible value of partnering with Gradient Cyber for MXDR—giving your business the advanced threat detection and response it needs, along with the peace of mind you deserve

Gradient
CYBER

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