Gradient CYBER

CHOOSING THE RIGHT MXDR TO SAFEGUARD YOUR BUSINESS

Managed Detection and Response (MXDR) Solution Overview

gradientcyber.com

contact@gradientcyber.com

Table of Contents

The Problem

Every mid-market organization - regardless of size, vertical, or security investment - is at risk of business, financial, regulatory, and reputation damage from a myriad of attack types and overarching security concerns 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.

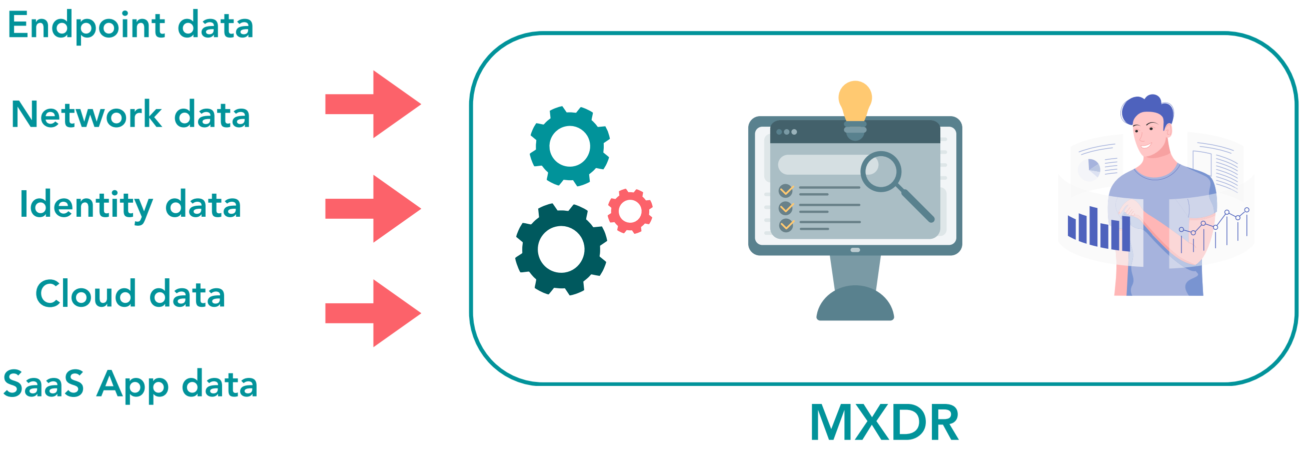
But, why, after decades of cybersecurity advancements, does this continue to be a raging problem? There are three primary reasons:

1. **IT environments are highly complex and dynamic**, presenting a large attack surface for attackers to enter and wreak havoc. The ‘disappearing perimeter’ due to network migration from on-premises to cloud, heavy dependency on 3rd party SaaS applications, IoT, and a high percentage of remote workers only make it more challenging.
2. **Attackers are savvy, well-tooled and financially-motivated.** With easy access to a rich dark-web ecosystem of tools, techniques and procedures - and at relatively low risk of being caught, let alone tried and convicted - the number and sophistication of independent and organized crime rings will only grow.
3. **The industry at large faces an enormous cybersecurity staffing and expertise gap** (and has for years). Alert overload, disparate technologies (that often aren’t integrated or properly configured) and oversubscribed budgets from which to purchase comprehensive security solutions only make it worse - to the point of high security personnel burnout and turnover.

There comes a point, where a business need is so fundamental - and yet so challenging to accomplish alone - that it is simply best addressed by a service model. This is true for power, water, communications, and has become true for cyber threat detection and response. There is simply no other way for most organizations - certainly in the mid-market - to fight the ever-escalating fight.

The MXDR Solution

Managed Extended Detection and Response (MXDR) is an advanced cybersecurity service that **combines the capabilities of Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Cloud Detection and Response (CDR), and Software as a Service Detection and Response (SaaSDR) into a unified solution.**



Endpoint data

Network data

Identity data

Cloud data

SaaS App data

MXDR

Top MXDR providers also have their own XDR platforms, 24x7x365 SOCs and cyber analyst staff to monitor your network, and user telemetry, detect IOCs, threats and anomalies, and perform rapid investigation, response and remediation on your behalf.

What distinguishes MXDR from most cyber security products capabilities is its holistic approach to viewing and managing the security and risk posture of the entire organization. If it’s true that attackers are sophisticated (and it is), then we have to accept that **simply looking at endpoint or network or identity based signals alone - or independently - will not effectively piece together their movement and intent.**

A threat detection and response solution must look deeply within and across these telemetry domains to form a situation analysis at speed and without generating a load of false positives. Not just after an exploit, but also before an exploit occurs. Not just a partial view of network activity, but complete 360-degree visibility of structured and unstructured data using AI and big data technologies. And not just a recording of massive amounts of data, but a means to gain sharp insight and take proactive measures based upon it.

What Can a Robust MXDR Solution Do?

First and foremost, an MXDR solution works on your behalf to identify suspicious and malicious activities that are the hallmarks of a breach or attack in progress. Using a spider web of AI, machine learning and human-in-the-loop threat hunting techniques, early evidence of kill-chain activity can be identified and responded to - either manually or automatically.

Network Attack Signals

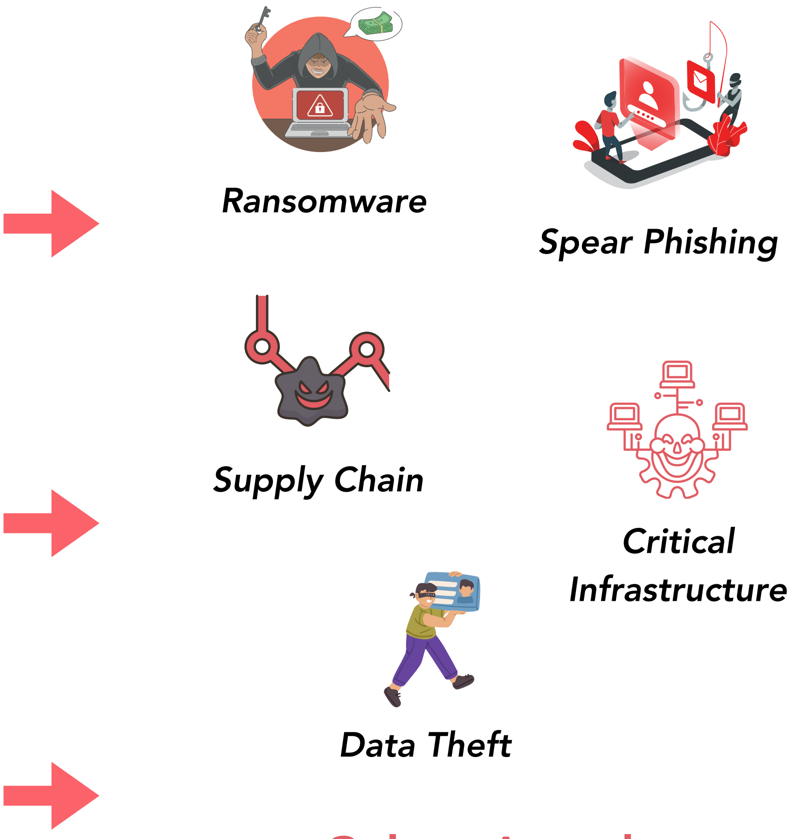
- Botnets
- DNS Anomalies
- Malware Signatures
- Unauthorized Port Scans
- Unusual Traffic Patterns
- Zero Day Exploits
- Unauthorized Peer-to-Peer Networks
- Phishing Attacks
- Unchecked TOR Communications

Endpoint Attack Signals

- Installed Malware
- Zero Day Exploits
- Unauthorized Software Installation
- Privilege Escalation Attempts
- Unauthorized Group Modifications

Identity Attack Signals

- Lateral Movement
- Password Change Thresholds
- Zero Day Exploits
- Account Anomalies



Ransomware

Spear Phishing

Supply Chain

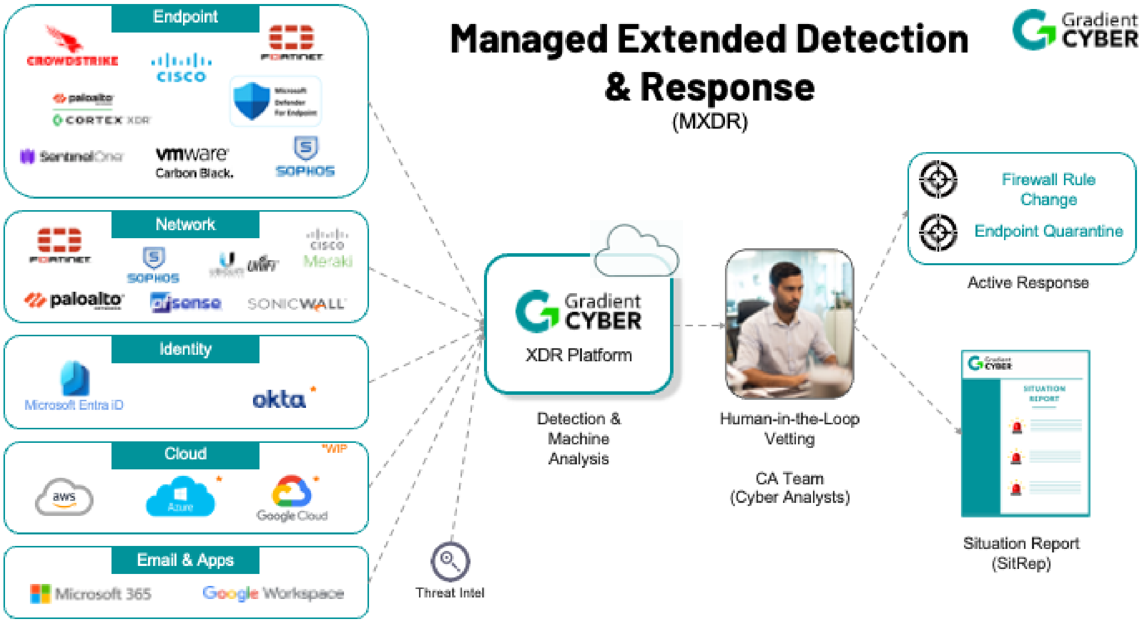
Critical Infrastructure

Data Theft

Cyber Attacks

How Gradient Cyber MXDR Works

Our advanced MXDR solution seamlessly integrates data from a myriad of security telemetry sources, drawing insights from network signals - such as botnets, DNS anomalies, and unchecked TOR communications - endpoint signals like unauthorized software installation and privilege escalation attempts, and more. By merging this data with real-time threat intelligence feeds detailing present and historical attacker tools, tactics, and procedures, our solution can identify specific kill chain activities that form the foundation of advanced cyber attacks. This holistic approach enables proactive defense against threats ranging from phishing attacks and malware signatures to identity attack signals like lateral movement and account anomalies.



From Data Source to SitRep...

Step One: Connect Security Data Sources

The first step is to connect your security data sources to our XDR platform

- Gradient Cyber makes this fast and easy by already having integrated with a wide variety of popular EDR, network firewall, identity, cloud service provider, and SaaS application solutions
- We also ‘white-glove’ configure our collector appliances with/for you

Step Two: Platform-Driven Analytics Processing
Gradient Cyber immediately begins ingesting native security logs and alerts from your security data sources into its cloud-based analytics engine

- Data is streamlined and pitted against active threat intelligence
- Suspicious and malicious signals are identified, contextualized, and prioritized

Step Three: Cyber Analyst Review and Analysis
Gradient Cyber cyber analysts review alerts and contextual information - adding the critical human-in-the-loop vetting that ensures situation analysis accuracy and efficacy.

Step Four: Active or Passive Response / Remediation
Depending on your response preferences, Gradient Cyber provides a situation report (SitRep) complete with advice on response / remediation actions, or we take action on your behalf. Either way we always follow up with a detailed and timely SitRep.

What Differentiates One XDR Platform From Another?

Not all MXDR processes and platforms come at this problem from the same perspective. There are three predominant platform evolutions into XDR: EDR heritage, SIEM heritage and network (more specifically, network threat analytics) heritage.

EDR-centric XDR

Many XDR vendor platforms have evolved from endpoint protection platforms. While endpoint telemetry is important, these platforms have several weaknesses:

- **Endpoint-centric analytics**
- **Weak at networking**
- **EDR lock-in**
- **Typically only has XDR visibility where endpoint agents are present**

SIEM-centric XDR

Security information and event management (SIEM) platforms are very good at log and event collection, correlation and alerting - all key to log management and compliance requirements. But SIEMs were never designed to keep up with the overwhelming volume of data in present-day security operations centers (SOCs), let alone integrate highly-advanced AI/ML analytics or sophisticated analyst queries required for threat analysis. SIEM-centric XDR has the following broad weaknesses:

- **Compliance-centric, not security-centric**
- **Big data-storage motivated**
- **Price scales with data storage**

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**

What Differentiates One MXDR Service From Another?

Mid-market MXDR differentiators can be netted down to a few key factors:

Does the vendor cater to the mid-market?
The needs of SMB, mid-market organizations, and large enterprises vary substantially. Any vendor who says otherwise is disingenuous.

Is the solution agnostic to data sources or does it demand particular EDR or firewall instances?
Many MXDR solutions are "land and expand" add-ons to existing security products, designed more around vendor lock-in

Does the MXDR provider own and operate their own XDR platform?
Data sources will change. Analytics will evolve, especially with the rapid advancement of AI. Dashboard and reporting needs must adapt to user needs. If your MXDR provider is unable to get down to the 'bare metal' of its underlying platform how will it be able to adapt its service to a highly-dynamic cybersecurity environment?

Is your MXDR provider safe and secure, in and of themselves?
Your MXDR provider should have a security operations center that is SOC 2 Type 2 compliant - year in and year out. Make sure your provider is at least Type 2. This is a far more rigorous, time-consuming and expensive vetting process.

The Gradient Cyber Advantage

Purpose-built for the mid-market, our MXDR solution boasts an unparalleled blend of EDR, identity, and deep network traffic analytics, enhanced by real-time data analysis for precise detection and responses. We offer a resilient cloud-based, AI-driven platform with an integrated NIDS, run and understood completely in-house. Complemented by our SOC 2 Type 2 compliant 24/7 Security Operations Center and a dedicated, seasoned analyst team, we emphasize personal relationships, ensuring consistent touch points, and a hands-on approach from installation to solution optimization. Key aspects of the Gradient Cyber value proposition include:

- **Comprehensive MXDR data sources.** Rich EDR and identity data integrations. Strong network analytics heritage. One of the few vendors who does live data analysis of both PCAP and bidirectional flow records (Biflow). The combination of EDR, identity, deep network traffic analytics, and current threat intelligence gives our MXDR platform the best possible data from which to make accurate and timely detection and response decisions.

- **Cloud-based, AI-infused platform that is both highly resilient and predictably scalable.** We run our own platform. This means we have intimate knowledge of all aspects of data collection, data normalization, machine-learning and analyst-driven analytics, SitRep development, user interface / user experience, and response / remediation operations. As well, our platform has an embedded network intrusion detection system (NIDS) that actively checks for known threats and protocol anomalies.

- **Optimized data collectors rich with local processing.** Our on-premises and cloud collectors operate at unparalleled speed. Further, knowing what to process locally ensures we do not create network bandwidth bottlenecks or unnecessary data transfer and storage costs.

- **Human-in-the-loop, seasoned, highly-skilled cyber analysts.** While SitReps are increasingly automated, we never leave the final judgment on an analysis or recommended action to a machine. You wouldn't trust a robot to do 100% of your medical analysis, nor should you - anytime soon - trust a completely automated detection and response process without experience cyber analyst vetting.

- **24x7x365 Managed Security Operations Center that is SOC 2 Type 2 compliant.** SOC2 Type 2 is a rigorous certification that ensures robust security, confidentiality, and service availability, instilling trust and confidence in our clients and stakeholders.

- **Personal relationships.** Trusted guidance. Easy to work with. Our customers laud the fact that we have frequent touchpoints that go a long way in making them feel comfortable. Touchpoints include monthly risk and compliance status, cyber risk briefings and action reports (SitReps), product training, and ongoing solution optimization as your IT environment evolves. We do not just 'throw the solution over the wall'. This starts from the very beginning of an engagement where we hand-hold installs to completion - where some competitors use an impersonal "here's a manual, you're on your own" approach. The latter might be fine up market, but it doesn't work in mid-market. For us, this extends all the way to the manner in which SitReps are shared, and response actions are invoked - either passively or actively. Our team prides itself on the personal relationships we have with our customers.

How Much Does MXDR Cost?

The best way to think about MXDR cost is to first consider what it would take to accomplish effective threat detection and response on your own. To do so, you would need the following:

- An ability to **collect the right security telemetry**, at the right locations, and only forward to a cloud processing engine what it needs (which also avoids network bandwidth congestion and expensive cloud ingest/egress charges)
- A **platform** that ingests data feeds, integrates active threat intelligence feeds, runs evergreen analytics that are constantly adapting to human and AI insights, provides a comprehensive UI/UX capability and is able to integrate with security enforcement products (firewalls, EDR, etc.) and other back-end security orchestration, automation, and response (SOAR) systems.

- **Ongoing SOC 2 Type 2 security operations center compliance**, which ensures that a service provider's security controls are both designed effectively and operating as intended over a period of time, providing assurance to clients and stakeholders about the safeguarding of sensitive data and operational resilience.
- **Developers and administrators** to keep all of the above operating smoothly with software updates, data storage management, resilience monitoring etc.
- Finally, you will need an **appropriately sized and skilled security analyst team** who has the bandwidth and acumen to deal with the daily flood of alerts and other security telemetry produced by your IT environment

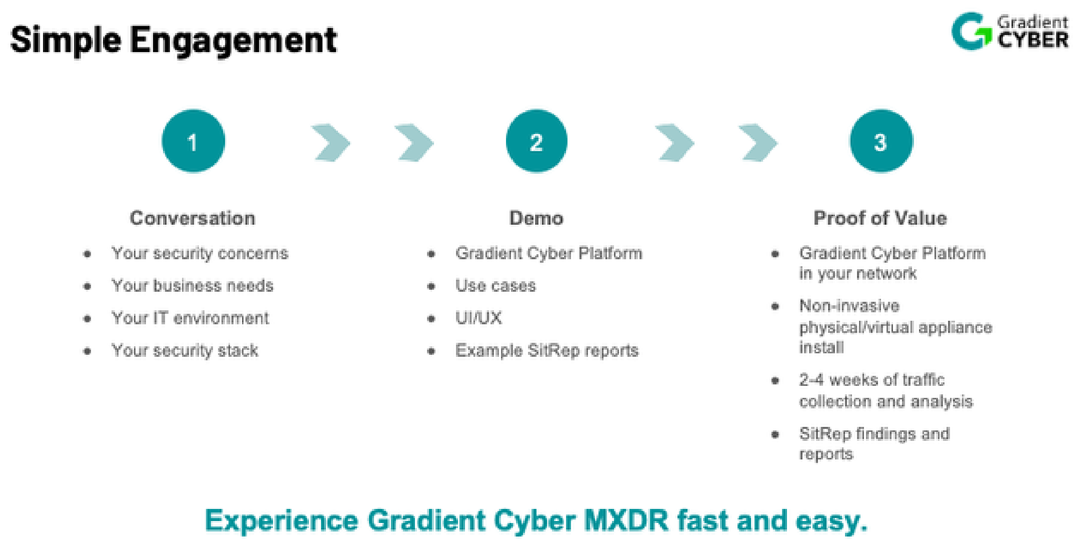
The cost of the above can easily get into high six to seven figures per year for a typical mid-market organization.

Actual cost, of course, depends on the number of endpoints in your network, as well as your network spread (number of premises and cloud locations). But with Gradient Cyber, **a typical mid-market organization will expend around ⅓ the cost of a single experienced cyber security analyst per year.** The return on full 'do-it-yourself' cost is outstanding under any scenario.

The more important ROI, however, is in recognizing that your investment in 'prevention' will simply not get the job done. Attackers will get in. That is unavoidable. Having a top-shelf threat detection and response capability that can root them out before their damage or exfil mission is complete - which can cost millions of dollars - is the real ROI. And having an MXDR service performed by a company who focuses on the mid-market - with 100% of its energy - is your best approach.

How Can I Get Started With Gradient Cyber MXDR?

Built directly into our name, every business, every IT environment, and every organization's risk tolerance is unique - effectively its own 'gradient'. Given this reality, we advocate a simple, but effective 3-step process for determining how best to get MXDR up and running for you:



Simple Engagement

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 an engagement is complete, we are confident you'll see the value of MXDR, and more specifically Gradient Cyber MXDR - all designed to give you the threat detection and response capability you need, and the peace of mind you deserve.