CRASH COURSE

MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

Gradient CYBER

MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

What's In This E-Book?

Gradient CYBER

Why Read this E-Book?

Cybercrime is the world's third-largest economy after the US and China, according to the World Economic Forum (WEF).

Based on data from Cybersecurity Ventures, it is projected to cost the world $8 trillion in 2023 and **$10.5 trillion by 2025.**

If your organization has a bank account, intellectual property, or any information about customers or employees, **you are a target.**

No number of pure security prevention products will save you. Attackers will get into your IT environment. They may already be in. Careless or malicious insiders - by definition - are already in. **You must have a detection and response solution.**

This e-book will give you a crash course on why you ought to consider adding **Managed Extended Detection and response (MXDR)** to your security armament.

First, let's start with **15 top of mind cyber attacks and risks** that make the news every day. If any of these get your attention, then knowing a little more about MXDR will be worth your time.

Here are the first five...

1 **Ransomware:** Malicious software that encrypts files, demanding payment for their release.

2 **Phishing:** Deceptive communications designed to trick individuals into revealing sensitive information.

3 **Business Email Compromise (BEC):** Fraudulent emails impersonating business contacts to deceive victims into transferring funds.

4 **Supply Chain Attacks:** Compromising software or hardware suppliers to gain access to target systems.

5 **Cloud Security Vulnerabilities:** Weaknesses in cloud services that can lead to unauthorized data access or loss.

Gradient CYBER

Here are the next five...

6 **Insider Threats:** Risks posed by individuals within an organization, intentionally or unintentionally causing harm.

7 **Internet of Things (IoT) Vulnerabilities:** Security weaknesses in IoT devices, making them susceptible to hacking.

8 **Distributed Denial of Service (DDoS):** Overwhelming a network or service with traffic to render it inoperable.

9 **Advanced Persistent Threats (APT):** Prolonged and targeted cyberattacks to steal data or surveil targets.

10 **Third-Party Risks:** Security threats originating from external partners or service providers.

And here are the last five...

11 **Zero-Day Vulnerabilities:** Previously unknown software flaws exploited before developers can fix them.

12 **Data Leakage and Loss:** Unintentional or unauthorized transmission and loss of sensitive data.

13 **Weak or Stolen Credentials:** The use of compromised login information to gain unauthorized access.

14 **Nation-State Attacks:** Cyberattacks initiated by governments to spy, disrupt, or steal from other nations.

15 **Social Engineering Attacks:** Techniques that deceive individuals into divulging confidential data or performing compromising actions.

Gradient CYBER

What if your organization gets hit?

It could cost you dearly. And the risk is not low. Cyber attacks are as prevalent as radiation from the sun.

Three factoids for context...

1

$4.45M

It's lucrative.

Average total cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million. That's an increase of 15.3% from USD 3.86 million in the 2020 report.

Ponemon Institute

2

$1.02M

The longer they hide, the more pain they inflict.

Average cost difference between breaches that took more than 200 days to find and resolve, and those that took less than 200 days. Breaches with identification and containment times under 200 days cost organizations USD 3.93 million. Those over 200 days cost USD 4.95 million—a difference of 23%.

Ponemon Institute

3

39 Seconds

They're very busy.

There is a hacker attacks of computers with Internet access - every 39 seconds

University of Maryland

Gradient CYBER

Surely there are signals that they're in my network?

Without question. It's like a fugitive tracker in the woods. There are **always** clues as to where they are, where they've been, what they are doing, and what they are likely to do next.

Here is a sample set of 25 signal types that MXDR solutions use to find the bad guys in action.

Endpoint Signals

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

Network Signals

1. **Unusual Traffic Patterns and Anomalies - north-south and east-west**
2. **Recon Activity**
3. **Lateral Movement**
4. **Malware Comms**
5. **Protocol / App Misuse**

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 and 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**

Gradient CYBER

Here's the problem.

It's really hard find and process signals.

Find the signal

Overwhelming Data Volume
Millions, if not billions, of daily logs and alerts

False Positives
Time required to chase down issues that aren't real is costly, painful and leads to burnout

Understand the signal

Lack of Contextual Information
Difficult to assess a raw alert with no context (user behavior, network activity, asset criticality, etc.)

Diverse Data Sources
Harmonizing and correlating data from different sources requires time and expertise

Prioritize the signal

Dynamic Threat Landscape
The nature of threats changes constantly. A high priority today might not be tomorrow.

Incomplete Risk Profiling
Without a complete risk profile of an org's assets, prioritizing even contextual signals is tough

Report the signal

Communication Barriers
Conveying tech findings to non-tech stakeholders is laborious

Fragmented Reporting Tools
Multiple SOC reporting tools can lead to inconsistent or incomplete reporting

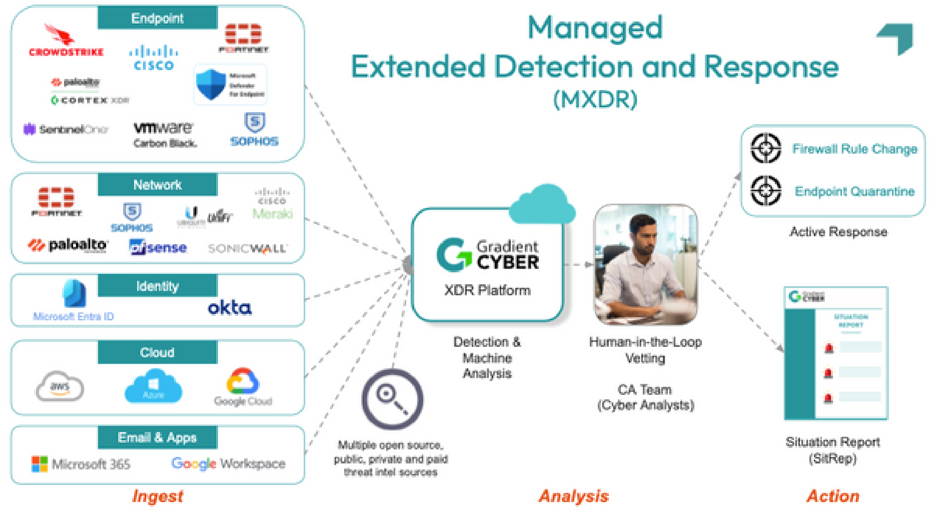
Take action on the signal

Ownership
Who has the time and expertise?

Automation
What system integrations are required?
Who will test, verify and maintain?

The Solution.

Managed Extended Detection and Response (MXDR)



The five key things an MXDR solution does for you:

1. It plugs in to your existing security stack
2. Alerts, logs, traffic flow data, threat intel, etc. are ingested into an XDR platform
3. AI and human analytics correlate, contextualize and prioritize events
4. Security analyst staff produce SitReps
5. Active or passive corrective action is taken, depending on your stack and service options

The Benefits of MXDR

In a nutshell, MXDR does three things:

1. MXDR reduces your Mean Time to Detect (MTTD) the adversary in your IT environment.
2. MXDR reduces the Mean Time to Respond (MTTR) to signals.
3. MXDR Does both of these at a much lower cost than you can do on your own.

But there’s more to it than that...

- MXDR gives you 24/7 threat monitoring and response
- MXDR gives you your own SOC without the headaches
- MXDR keeps you on the cutting edge of security intel and technology
- MXDR prevents IT staff burnout and turnover
- MXDR helps ensure compliance across industry standards and frameworks

Want to learn more?

Check out our educational blog:
What is MXDR? An in-depth look.

Check out our solution page:
Gradient Cyber MXDR

Talk to us.
We love to share and educate.

Gradient
CYBER