Deloitte.

# Managed Extended Detection and Response (MXDR) by Deloitte

MXDR by Deloitte combines an integrated and modular detection and response Software as a Service (SaaS) platform with managed security services to provide military-grade threat hunting, prevention, detection, response, and remediation capabilities…simply put, to provide outcomes for resiliency.

## WHY SHOULD YOU CONSIDER MXDR?

- Adversaries have become faster and more sophisticated, increasing an ever-expanding threat landscape
- System compromises are commonplace, resulting in involuntary information disclosures and loss of revenue
- Increasing regulatory and operational pressures require businesses to solve ever-increasing complex threats at lower costs combining both compliance *and* detection requirements
- Ransomware accounts for the majority of interactive attacks, widening the potential targets and damage across businesses and compounding the impact of insider threats
- Information Technology and Operational Technology environments (i.e., on-premises, cloud-based,) continue to expand, complicating efforts to identify potential threats and vulnerabilities
- Lack of resources and technology to adequately and proactively provide detection and response coverage

### Strategy & Implementation

- Strategy, Capability, and Maturity Assessment
- Incident Response & Readiness
- Threat Hunting and Compromise Assessment
- Next Generation Security Operations Center
- Security Information & Event Management
- Insider Threat Programs
- Cyber Analytics (*User & Entity Behavior Analytics*)
- Security Orchestration, Automation, & Response
- Threat Intelligence Programs
- Master Operator & Hunting Training

### Cyber Intelligence & Products

- Intelligence Platforms (Athena / Matchlight / Deloitte Intelligence Service Portal)
- Operational Threat Intelligence (TIA)
- Over the Horizon Pursuit (*SPECTRE*)
- Digital Risk Protection (*Matchlight*)
- Threat Intelligence Program Development
- Next-Generation Hunt Platform
- Data Reconnaissance
- Platforms (MXDR, Managed Security Services, Intelligence)

**Deloitte Detect & Respond (D&R) portfolio**


### Managed Extended Detection & Response (MXDR)

- ***Unified Detection and Response***
- ***Digital Risk Protection***
- ***Cyber Threat Intelligence***
- ***Insider Threat Detection***
- ***Adversary Pursuit: Proactive Hunting***
- ***Cloud SaaS: Prevention, Detection and Response***
- ***Cloud Security: Prevention, Detection and Response***
- ***Zero Trust: Identity Prevention, Detection and Response***
- ***Enterprise Prevention, Detection and Response***
- ***Attack Surface Management (ASM) & Vulnerability Management (VM)***
- ***Incident Response (IR) – Contain & Recover***

## THE MXDR DIFFERENCE

MXDR by Deloitte combines industry-leading technology with experienced Deloitte teams to provide a modular set of threat hunting, detection, response and remediation capabilities to clients in delivery models designed to meet both their cybersecurity and business requirements.

This offering is designed to give clients access to the advanced threat detection and response capabilities their organizations require, while unburdening them of the complexity of having to build and maintain this infrastructure on their own. For organizations looking to expand coverage while optimizing spend, MXDR reduces the strain of recruiting and retaining large, specialized teams in a labor-constrained market.

**BENEFITS**

**Outcome -** focused | **Near real-time breadth & depth** of visibility into threats | **Advanced & industry-leading** technology capabilities | **Modular** architecture | **Advanced** analytics | **24x7x365 delivery**


# MXDR by Deloitte

**Unified Composable & Modular Cloud Delivered SaaS**

## Full visibility and collaboration with 24x7x365 service delivery

Alliances* with targeted providers allow Deloitte to integrate capabilities to provide true "hands on" coverage against threats.

**Amazon Web Services (AWS)| CrowdStrike| Exabeam | Google Cloud Chronicle| ServiceNow| Splunk| Zscaler**

**Current Alliance footprint as of January 2022*

## Value Provided

- Increase cyber resiliency and cyber operations maturity
- Focused on security outcomes
- Provide collaborative and scalable prevention, detection, response, and remediation
- Predict and prevent future attacks by leveraging internal and external intelligence
- Conduct lessons learned to identify future countermeasures
- Identify what is being defended using agent and agentless capabilities, collecting telemetry into assets & identities clients are responsible for. Includes rogue system detection
- Significant reduction in mean time to identify, detect, and respond
- Improve MITRE ATT&CK® coverage and overall visibility

## MXDR Client Stories

### Consumer Client

The client fell victim to a ransomware attack and recognized that without proper protection that they could continue to be impacted and / or targeted. Deloitte provided a proactive defense capability coupled with a response component allowing the client to not only detect and identify threats with greater fidelity, but also promptly respond and eradicate those attacks.

### Life Sciences & Healthcare Client

The client sought a security provider as they realized their current capabilities could not support their growth. Deloitte was selected because the MXDR platform represented a solution encompassing the traits that they valued, including leading practices, scalability, and efficiency of tools and actions. The quick deployment time of the solution was an added benefit for the client.

## CONTACTS


**Deborah Golden**
Principal
US Cyber & Strategic Risk Leader
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
debgolden@deloitte.com

**Curt Aubley**
Managing Director
US Detect & Respond Leader
Deloitte & Touche LLP
caubley@deloitte.com

**Steve Mahar**
Managing Director
Sales Leader Detect & Respond
Deloitte Services LP
smahar@deloitte.com


| Services | Capability Descriptions | Outcomes |
|---|---|---|
| **Unified Extended Detection and Response (XDR)** | Central XDR security information and event management (SIEM)/logging/analytics management combines agent, agentless, Endpoint Detection & Response (EDR), Network Detection & Response (NDR) data fusion and 24x7x365 SLA driven support to improve the mean time to prevent, detect, and respond to cyber attacks | • Improved time to prevent, detect, and respond to cyber attacks<br>• Consolidation of tools and lower complexity<br>• Identify exposed data, brand misuse, and dark web fraud<br>• Reduce business costs, limit reputational damage, and reduce enterprise attack surface<br>• Bolster enterprise PDR in cloud native FedRAMP delivery model<br>• Improve mean time to detect and respond to cyberattacks<br>• Increase visibility of enterprise assets<br>• Provide containment and remediation actions to remove the adversary from the client environment<br>• Retain required talent by investing in the personnel |
| **Digital Risk Protection** | Continuous digital asset monitoring that is operationalized with analytics & actionable intelligence to promptly identify and decrease the impact of exposed data | |
| **Cyber Threat Intelligence** | Predictive cyber threat intelligence informed by adversary tactics, techniques and procedures (TTPs), tailored analysis, and malware analysis | |
| **Insider Threat Detection** | Evaluate the environment to identify users and roles with relevant access and implement controls | |
| **Adversary Pursuit: Proactive Hunting** | Continuous hunting leveraging intelligence, artificial intelligence/machine learning, and a hypothesis driven approach with the Deloitte Threat Hunting Platform and Master Hunter Operator trained teams | |
| **Cloud SaaS: Prevention, Detection and Response (PDR) Hunting** | Leverage cloud access security broker (CASB) and data loss prevention (DLP) technology to detect and respond to SAAS targeted attacks | |
| **Cloud Security: PDR** | Initiate service discovery to learn what is and is not secured, along with supporting instances, containers, cloud services, serverless, various cloud platforms and operating systems | |
| **Zero Trust: Identity PDR** | Provide visibility into identity, anomalous behavior, detection of lateral movement, and advanced threats to detect compromised identities | |
| **Enterprise PDR** | Support assets both on and off network to prevent both malware and ransomware attacks using next generation antivirus and end point detection & response | |
| **Attack Surface & Vulnerability Management** | Bolster host and network endpoint and virtual and private clouds across multiple technology environments providing real time visibility into vulnerabilities, asset tracking, and rogue system detection. | |
| **Incident Response (IR)** | Identify incident management gaps in current processes and procedures, and streamline response to adversary techniques to provide containment, eradication, and remediation actions to remove the adversary from the client environment | |
| **Master Operator & Hunt Training** | Provide advanced training to equip security analysts and operators with hands-on technical skills to defeat various adversaries | |