MXDR

Managed eXtended Detection & Response (MXDR): an outsourced Software-as-a-Service (SaaS) platform that provides comprehensive 24/7/365 protection from cyber threats, identifying and neutralizing never-before-seen attacks across a company's entire technology infrastructure.

SERVICE	MXDR	MDR	XDR	MEDR	SIEM	EDR
Monitor Your Entire Digital Infrastructure - Identify and detect risks across your network, cloud platforms, endpoints and applications.	✓	○	✗	✗	✗	✗
SIEM Access and Visibility - See all security log data in the SIEM, on demand access to retained logs.	✓	✗	✗	○	✓	○
Machine Learning & User Behavior Analytics - Real-Time Alerts driven by anomalous patterns in your data.	✓	○	○	✗	✗	✗
Instant Access to Security Experts - Communicate around the clock 24/7/365 with a US-based SOC Team.	✓	○	✗	✗	✗	✗
Issue Triage and Guided Remediation - Critical events and actionable insights are delivered in ~ 8 minutes.	✓	✓	✓	✓	✗	✗
Silencer Technology - Detect the indicators of attack faster and with a 95% confidence score.	✓	✗	✗	✗	✗	✗
Threat Hunting - Continuously hunting for suspicious activity across all of your environments.	✓	✓	✓	✓	✓	✗
Per Client Cyber-Risk Scoring - Based on 13 critical security factors and Indicators of Attack (IoA) from MITRE framework.	✓	✗	✗	✗	✗	✗
Pooled & Tiered Partner Pricing - Flexible and predictive pricing based off client profile.	✓	✗	✗	✗	✗	✗
Per Client On-Boarding Concierge - White-glove setup and integration to monitor and enhance existing security layers.	✓	✓	✓	✓	✗	✓

MEANING	SYMBOL
YES	✓
SOMETIMES Depending on the vendor.	○
NO	✗

Managed Detection & Response (MDR): an outsourced service that provides organizations with security monitoring and threat hunting services and responds to threats once they are discovered.

Extended Detection & Response (XDR): a consolidation of tools and data that provides extended visibility, analysis, and response across networks and clouds in addition to apps and endpoints.

Managed Endpoint Detection & Response (MEDR): EDR offered as a managed service. Involves a team of analysts reviewing EDR data detect and report threats.

Security Information & Event Management (SIEM): an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

Endpoint Detection & Response (EDR): the protection of internet-connected devices such as PCs, workstations, servers and smartphones against cyber threats.