Managed Extended Detection and Response (MxDR)

Uncover hidden risks and unknown threats in minutes, not days

Benefits

- 30 years of security experience
- 24×7×365 real-time defense
- Rapid response
- Zero false positives

OpenText Managed Extended Detection and Response (MxDR) integrates with leading technologies and is built on 30 years of digital forensic and incident response expertise.

OpenText personnel each have years of experience working on threat hunting, breach response investigations, and malware analysis engagements. This extensive experience and understanding of threat actors' behavior combined with more than 500 tactics, techniques, and procedures (TTPs) leads to faster time to value and identification and remediation of risks. OpenText continuously builds on this experience and provides an unparalleled 99-percent detection rate with zero false positives.

The MITRE Engenuity ATT&CK® Evaluations for Managed Services recognized OpenText next-level Managed Detection and Response offerings for quick detection of real incidents and a 99-percent detection rate for all attack tactics.

Read the press release for details.

Advanced threat detection and analytics

From the OpenText Security Operations Centers, OpenText MxDR provides comprehensive 24×7×365 security monitoring supported by MITRE ATT&CK® behavioral analytics and detection. OpenText's cloud-based security information and event management (SIEM) can ingest any log source and develop correlations from telemetry collected on desktops, laptops, servers, firewalls, email servers, Active Directory, IoT devices, intrusion detection systems, proxy, and other telemetry sources using artificial intelligence and advanced workflows.

OpenText continuously develops behavioral detections, based on its threat research, with a rapid response. The response can be automated based on alert criticality to ensure the fastest path to threat remediation, and the remediation can be controlled in a hands-on fashion—and most importantly, the validation of threats. Advanced threat detection and analytics will provide deep insights into where threats originate and the overall impact to the business.

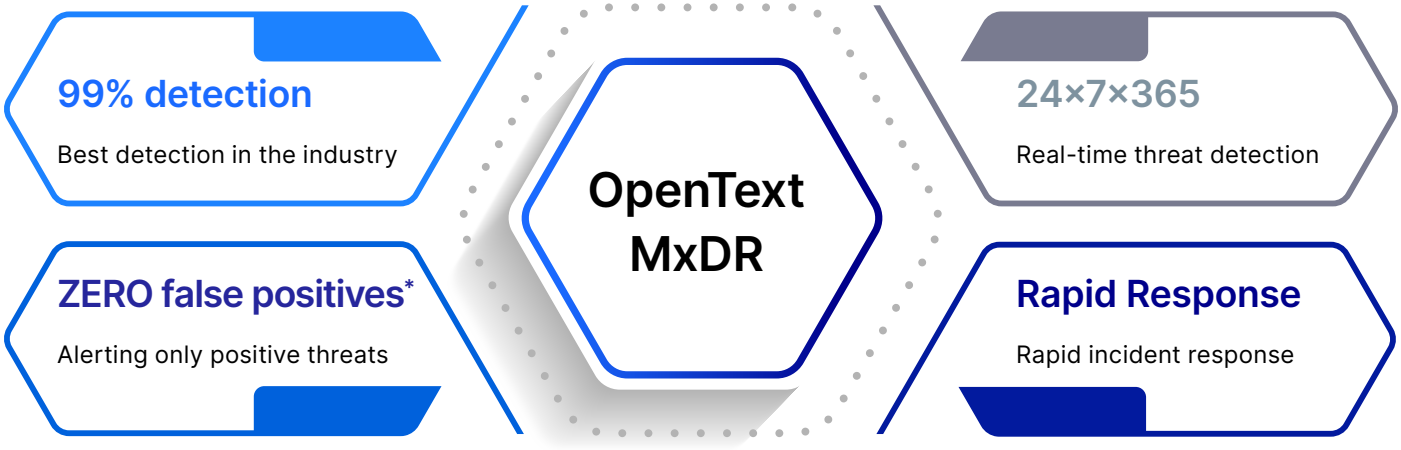
Integrated threat intelligence

OpenText MxDR leverages multiple technologies that differentiate it from other providers. One of these technologies, threat intelligence is integrated with OpenText MxDR, helping the business understand the scope and impact of any security event. OpenText™ Threat Intelligence also allows the correlation to be drawn between data sets of known malicious files and data points identified from ingested log sources. Having threat intelligence directly integrated allows for immediate threat validation to known malware. In addition, endpoint and network technologies are integrated into the solution with people, processes, and procedures in the event of a zero-day or targeted event.

Alert validation and noise reduction

OpenText workflows are unmatched in the industry and can eliminate alert and event noise with zero false positives, leaving organizations with more time to focus on actual threats and business priorities. Organizations benefit from OpenText's ability to correlate data effectively, while eliminating event noise and false positive alerts saves time, provides confidence in findings and increases accuracy of threat identification.

Managed Extended Detection and Response - MxDR



* MITRE ATT&CK Evaluations: OpenText emerged as the only vendor with zero false positives

Benefits of OpenText MxDR:

OpenText MxDR TTP Services are designed to provide confidence in detecting unknown risks and threats, before they can do damage to a business. It provides:

- Behavioral analytics based on MITRE ATT&CK® framework and artificial intelligence delivering a 99-percent detection rate with Integrated-time-to-respond (MTTR) within minutes.
- Security workflows that eliminate event noise with zero false positives.
- Threat correlation and root-cause analysis.
- Automated reporting.
- Advanced workflows and 500+ detections.
- Integration with OpenText Threat Intelligence and is powered by SIEM.
- Behavior-based threat detection across endpoints, networks, cloud environments, and beyond. Bring your own security stack or use an OpenText provided stack.
- Custom development of behavioral detections.
- Compliance with insurance requirements for EDR and MDR.
- 24×7 monitoring with a Security Operations Center staffed with OpenText security professionals with more than 30 years of experience: SOC analyst, threat hunters, incident responders, malware experts, and the dedicated Cybersecurity concierges.

Complementary services

Incident and Breach Response
Threat Hunting ›

Security and Privacy Assessment ›

For more information, contact us at securityservices@opentext.com

MxDR service tiers

OpenText MxDR services are designed for SMB, enterprise, public sector, and MSPs alike.

	MxDR
Data sources	
Endpoints, servers, web servers, and cloud-based systems	✓
Enterprise Egress (N/S) firewall	✓
Office 365® audit logs	✓
Cloud audit logs	✓
Proxy	✓
Other XDR sources	+
Features	
500+ TTPs	✓
24×7×365 threat detection monitoring	✓
MITRE ATT&CK detection condition sets	✓
SIEM	✓
Remote Monitoring and Management integration	✓
Endpoint detection and response (EDR) agent	✓
Custom integration (with existing EDR)	✓
Real-time detection and alerting	✓
Threat intelligence service	✓
Threat hunting	✓
Incident response retainer	✓
Custom development of behavioral detections	✓

Contact us for your customized quote

opentext™