opentext™

SERVICE OVERVIEW

Managed Extended Detection & Response (MxDR)

Uncover hidden risks and unknown threats in minutes, not days

30 years of security experience

365/24/7 realtime defense

7 minutes mean time to respond

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 MxDR security 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% detection rate with zero false positives.

The 2022 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 virtual Security Operation Center (VSOC), OpenText MxDR provides comprehensive 24×7×365 security monitoring supported by machine learning and 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, firewall, 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 in its SIEM, based on its threat research, with a seven-minute mean time to respond (MTTR). 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.

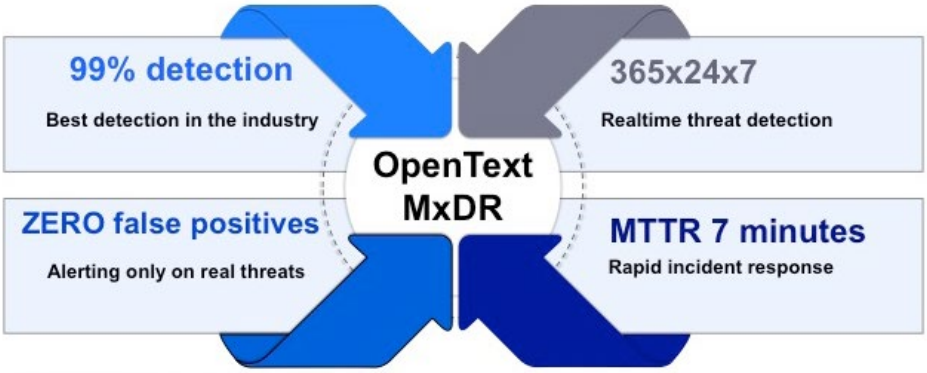
Integrated threat intelligence

OpenText MxDR leverages multiple technologies that differentiate it from other providers. One of these technologies, threat intelligence is integrated with OpenText's SIEM, helping the business understand the scope and impact of any security event. BrightCloud 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 0-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 analysts and security personnel 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 analysts' time, provides confidence in findings and increases accuracy of threat identification.

Managed Extended Detection & Response - MxDR



MITRE ATT&CK Evaluations 2023 : OpenText emerged as the only vendor with zero false positives

Benefits of OpenText MxDR:

OpenText MxDR 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% detection rate with mean-time-to-respond (MTTR) within 7 minutes.
- Security workflows that eliminate event noise with zero false positives.
- Threat correlation and root-cause analysis.
- Daily automated reporting.
- Advanced workflows and 500+ TTPs detections.
- Powered with SIEM and integrated with BrightCloud Threat Intelligence.
- Behavior-based threat detection across endpoints, networks, cloud environments and beyond. Bring your own security stack or use at-no-extra-cost EDR (Endpoint Detection & Response) provided by OpenText.
- Custom development of behavioral detections.
- Meets your insurance requirements for EDR and MDR.
- 24×7 monitoring with Virtual Security Operations Center (VSOC) staffed with OpenText security professionals with more than 30 years of experience: SOC analyst, threat hunters, incident responders, malware experts, and the dedicated Program Manager.

opentext™

Complementary services

Incident and Breach Response
Threat Hunting
Security Assessment 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 Enterprise	MxDR SMB
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	✓	✓
AI/Machine learning/Behavioral detection	✓	✓
SIEM	✓	✓
Remote Monitoring and Management integration	✓	✓
Endpoint detection and response(EDR) agent	✓	✓
Custom integration(with existing EDR)	✓	
Realtime detection and alerting	✓	✓
Threat intelligence service	✓	✓
Threat hunting	✓	✓
Incident response retainer	✓	+
Custom development of behavioral detections	✓	✓

+ requires add-on

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact