



According to research, **53% of breachers took SMB customers weeks or longer to discover.**<sup>1</sup>

The MxDR services can help businesses minimize disruptions and reduce the time to discovery of adverse cyber events, including evolving threats like ransomware, with proactive threat hunting, endpoint detection and response capabilities and even XDR.

# Managed Extended Detection and Response (MxDR)

## Enterprise Grade Cyber Security Services for the MSP

Cyber criminals operate 365 days a year, carrying out endless attacks on organizations of all sizes and industries. MSPs are choosing OpenText MxDR services to stop bad actors and malware that target their customers to steal valuable data, extort money and more.



- Detect unknown threats
- Leverages behavior-based detections
- Rapidly detect threats
- Investigations and remediations included
- Extendible visibility beyond the endpoint

### OpenText MxDR Managed Services Leader

**0% NOISE | 100% DETECTION**

MITRE Engenuity ATT&CK® Evaluations for Managed Services assessed OpenText MxDR as **managed security services provider leader.**



<sup>1</sup> Verizon, "DBIR Small and Medium Business (SMB) Spotlight." (2021)

## Cyber Resilience for Business Impact

### Reduces Alert Fatigue

Security analysts manually verify thousands of alerts a day, many registering false positives. The resulting noise distracts teams and increases the risk of missing a legitimate threat. Prioritize actionable threats to reduce alert fatigue.

### Detects Email Threats

Phishing attacks have evolved in volume and sophistication. Without advanced tools, security managers are blind to threats lurking in employee email communications. Correlate email threats to quickly identify malicious activity.

### Uncovers Hidden Attacks

SOC managers need to mitigate unknown threats before attackers can cause damage. But, outdated solutions lack visibility into endpoint, network and other log sources, allowing threats to stay hidden. Eliminate blind spots with OpenText MxDR services.

### Solves Cyber Skills Gap

Security teams must defend against and investigate high volumes of cyber threats each day. Staff, skill and experience shortages limit teams' ability to counter threats. Scale and strengthen the organizations' security posture with OpenText Security Services.

## Cyber Readiness for Compliance and Insurability

OpenText MxDR provides EDR and MDR capabilities

- Whether you need to simply mitigate financial, legal or reputational risk
- Whether you need help achieve common data security standards prescribe through legislation or industry standards, like compliance with NIST, ISO, HIPPA, PCI
- Whether you need achieve prerequisite for insurance coverage

Capabilities	OpenText™ MxDR
<b>1. Endpoint Detection Capabilities</b>	
Detects & Eradicates known malware	Add <b>Webroot®</b>
Detects & Eradicates unknown threats	✓
Data Loss Prevention (DLP)	✓
File Integrity Monitoring (FIM)	✓
Host-based Intrusion Detection / Intrusion Prevention System (IDS / IPS)	✓
Network threat / anomaly detection (e.g. lateral movement)	✓
<b>2. Threat Types Detected</b>	
Malware (crimeware, ransomware, trojans, exploit kits, etc.)	✓
Misuse of legitimate applications (PowerShell, WMI, MSHTA)	✓
File-based attacks (Microsoft Office, Adobe, PDF, etc.)	✓
Unwanted software (browser toolbars, PUPs)	✓

Insider threats (malicious employee, compromised credentials)	✓
Accidental release of data	✓
Suspicious user activity	✓
Suspicious application behavior	✓
<b>3. Threat Prevention</b>	
Prevent potentially threatening applications from executing	Add <b>Webroot®</b>
By whitelisting, blacklisting, sandboxing, etc.	✓
Before they execute, or during execution	✓
Prevention capabilities continue to function even when the endpoint no longer connected to the Internet or corporate network	✓
<b>4. Response Capabilities</b>	
May integrate with a Security Operations Center (SOC) to provide response, could be outsourced	✓
Isolate an endpoint from the network	✓
Kill processes and/or banning specific applications	✓
Delete files and/or registry keys	✓
Revert to last known good state	Add <b>Carbonite®</b>
Investigate endpoint activity to understand attack progression and root cause	✓
<b>5. Reporting</b>	
Ability to gather indicators of compromise (IOCs) from every detected threat	✓
Timeline analysis of event	✓
Endpoint and user information provided	✓
Threats classified by severity	✓

## Affix MxDR services to your MSP Solutions

Ready for the MSP's business model and need for financial flexibility, OpenText provides MxDR services for any size partnership and end-user. Contact a Sales Rep for a quote.

## About us

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

## Connect with us

- [OpenText Security blog](#)
- [OpenText Security Services Email](#)