CARBONITE® + WEBROOT®

opentext™ BUSINESS SOLUTIONS

MDR IS HERE

Managed Detection and Response (MDR) Solutions Brief

It's a struggle for MSPs and their small and medium-sized business (SMB) clients to maintain an effective security posture 24/7/365. Both are targets for bad actors looking to steal valuable data, extort money from their victims and more.

According to research, **53% of breaches took SMB customers weeks or longer to discover.[1]**

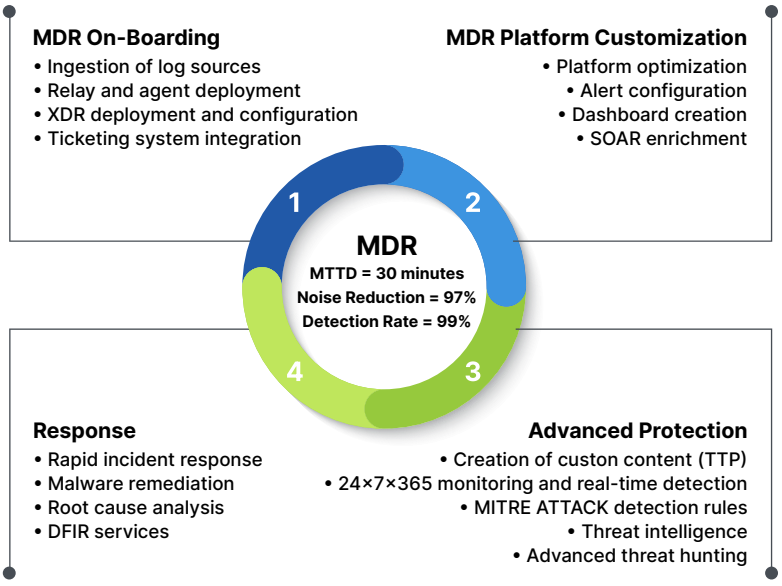
Our MDR solutions can help businesses minimize disruptions and reduce the time to discovery of adverse cyber events, including evolving threats like ransomware, with proactive threat hunting, detection and response capabilities.

[1] Verizon. "DBIR Small and Medium Business (SMB) Spotlight." (2021)

MDR solutions include:

OpenText MDR

It's a struggle for MSPs and their small and medium-sized business (SMB) clients to maintain an effective security posture 24/7/365. Both are targets for bad actors looking to steal valuable data, extort money from their victims and more. Also, according to research, 53% of breaches took SMB customers weeks or longer to discover.[1] But our MDR solutions can help businesses minimize disruptions and reduce the time to discovery of adverse cyber events, including evolving threats like ransomware, with proactive threat hunting, detection and response capabilities.



Webroot MDR powered by Blackpoint

Blackpoint's patented SNAP-Defense security operations incident response platform is a gamechanger. It excels at monitoring and catching modern hacking tradecraft, delivering real-time alerts and allowing for immediate threat response. As an MDR solution, Blackpoint SNAP-Defense is offered alongside Webroot® Business Endpoint Protection with Blackpoint's experienced team of cybersecurity professionals monitoring customer networks for threats and breaches.

WEBROOT™ opentext™ BUSINESS SOLUTIONS + blackpoint

CAPABILITIES

- Live Asset Visibility
- Multi-Point Threat Detection
- Lateral Spread Detection
- Privileged Account Monitoring
- Immediate Threat Response
- Remote Access Monitoring
- Insider Threat Visibility
- 3rd Party Integrations
- Risk & Compliance Reporting

Insurance and compliance support

Today's cybersecurity insurance providers frequently require an MDR solution as a prerequisite for coverage. Additionally, MDR can help achieve compliance with common data security standards issued by organizations like NIST, ISO, HIPPA, PCI and others. Both MDR by OpenText and Webroot MDR powered by Blackpoint can assist organizations in meeting these standards.

*with Webroot® Business Endpoint Protection **Add-on capabilities required.

Capability Mapping	OpenText MDR	Webroot MDR powered by Blackpoint
1. Endpoint Detection Capabilities		
Detects / Eradicates known malware	✓	✓*
Data Loss Prevention (DLP)	✓	✗
File Integrity Monitoring (FIM)	✓	✓**
Host-based Intrustion Detection / Intrusion Prevention System (IDS / IPS)	✓	✓
Network threat / anomoly detection (e.g. lateral movement)	✓	✓
User Behavior Analytics (UBA)	✓	✓**
2. Threat Types Detected		
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 (malicous employee, compromised credentials)	✓	✓**
Accidental release of data	✓	✓**
Suspicious user activity	✓	✓**
Suspicious application behavior	✓	✓
3. Threat Prevention		
Prevent potentially threatening applications from executing	✓	✓*
By whitelisting, blacklisting, sandboxing, etc.	✓	✓ Partial
Before they execute, or during execution	✓	✓ Partial
Prevention capabilities continue to function even when the endpoint no longer connected to the Internet or corporate network	✓	✓ for roaming devices ✗ for fully offline offenses
4. Response Capabilities		
May integrate with a Security Operations Center (SOC) to provide response, could be outsourced (e.g. via a Managed Detection & Response (MDR) Managed Service Provider (MSSP)	✓	✓
Isolate an endpoint from the network	✓	✓
Kill processes and/or banning specific applications	✓	✓
Delete files and/or registry keys	✓	✗ not automatically
Revert to last know good state	✗	✗ not automatically
Investigate endpoint activity to understand attack progression and root cause	✓	✓
5. Reporting		
Overview of why threat was detected	✓	✓
Ability to gather indicators of compromise (IOCs) from every detected threat	✓	✓
Timeline analysis of event	✓	✓
Endpoint and user information provided	✓	✓
Threats classified by severity	✓	✓

Visit Webroot.com/MDR to learn more and speak to a sales representative.