

CARBONITE® + WEBROOT®

OpenText Security Solutions

Managed Detection & Response (MDR)

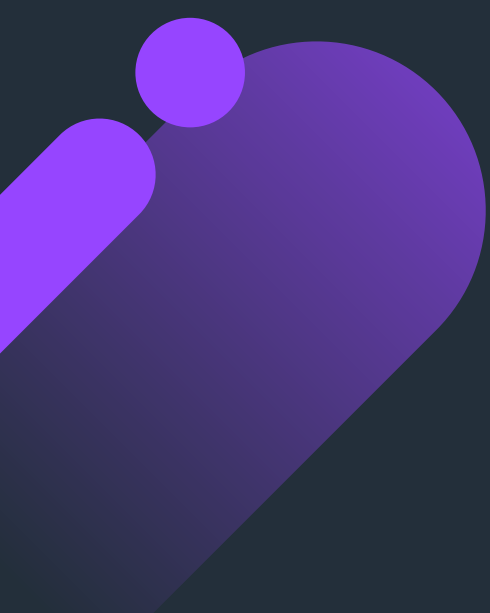
Uncover hidden risks and threats before they make an impact financially, legally or reputationally





OpenText Managed Detection and Response (MDR)

pairs best-in-breed technologies with security personnel who have 15+ years of experience working breach response investigations and malware analysis engagements. This extensive experience and understanding of threat actors' tactics, techniques and procedures (TTPs) leads to faster time to value, identification and remediation of risks. OpenText continuously leverages this experience to improve its detection and response capabilities and build advanced algorithms for threat modeling.



Advanced threat detection & analytics

Through the OpenText cloud-based Security Operation Center, OpenText MDR provides comprehensive 24x7x365 security monitoring supported by machine learning and MITRE ATT&CK analytics. OpenText's next-gen Security Information and Event Management (SIEM) solution can ingest any log source and develop correlations between desktops/laptops, servers, firewall logs, IoT devices, Intrusion Detection System (IDS) logs, proxy logs, etc. using artificial intelligence and advanced workflows. OpenText continuously develops custom content in its SIEM based on



AI-powered threat detection



99% detection rate—highest in the industry



Award-winning threat intelligence



97% alert noise reduction

TTPs to deliver a 99% detection rate and a 30-minute mean time to detection (MTTD). Response can be automated based on alert criticality to ensure the fastest path to threat remediation, and remediation can be controlled in a hands-on fashion. — and most importantly the validation of threats. In addition, advanced threat detection and analytics provide deep insights into the origin of threats and their overall impact to the business.

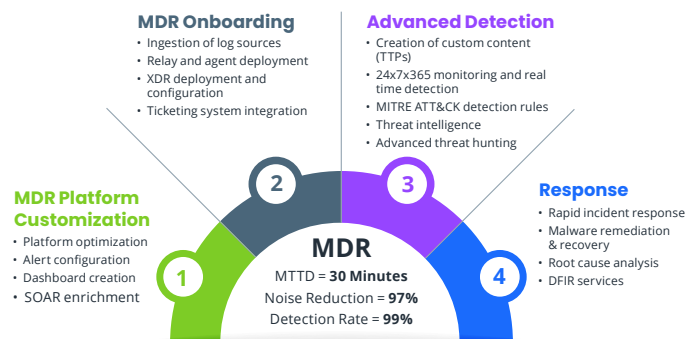
Integrated threat intelligence

OpenText MDR leverages multiple technologies that differentiate OpenText from other providers. One of these technologies, threat intelligence, is integrated with OpenText's next-gen SIEM, helping the business understand the scope and impact of any security event. Threat intelligence also allows users to correlate data sets of known malicious files and data points identified from ingested log sources. Directly integrated threat intelligence 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 & noise reduction

OpenText Security Services' workflows are unmatched in the industry and can reduce alert and event noise by up to 97%, leaving analysts and security personnel more time to focus on patching, upgrades, configurations and so on. OpenText processes and the ability to correlate data effectively are strengths that organizations can greatly benefit from. Reduction of event noise and alerts saves analysts time, provides confidence in findings and increases accuracy of threat identification.

Managed Detection & Response (MDR) by OpenText



OpenText MDR services are designed to provide confidence in uncovering hidden risks and threats before they can damage a business:

- Faster time to detect and respond to threats
- Threat correlation & analytics
- Real-time detection & automated alerting
- Integrated threat intelligence
- Real time alerting & response
- Daily automated reporting
- Advanced workflows
- Custom IOC creation



Learn more about our complementary security services

[Security Assessment Service](#)

[Security Health Check](#)

[Threat Hunting Service](#)

[Security Services Catalog](#)

OpenText offers three tiers so organizations can select the MDR Service that best meets their needs.

	MDR Essentials	MDR Professional	MDR Enterprise
Next-Gen SIEM			
Log ingestion	✓	✓	✓
24x7x365 monitoring	✓	✓	✓
MITRE ATT&CK detection rules	✓	✓	✓
AI/machine learning	✓	✓	✓
Platform access and dashboard	✓	✓	✓
Real-time detection	✓	✓	✓
Real-time alerting	✓	✓	✓
Integrated threat intelligence	✓	✓	✓
Security Services			
Dedicated Security Advisor		✓	✓
Program Manager		✓	✓
Threat hunting		✓	✓
SIEM content development		✓	✓
IOC content sharing			✓
Digital Forensics & Incident Response (DFIR)			
Threat triage support		✓	✓

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.

© 2022 OpenText. All rights reserved. OpenText, Carbonite, and Webroot are each trademarks of OpenText or its subsidiaries. All other trademarks are the properties of their respective owners.