

OpenText MDR: Co-managed detection and response for MSPs

24×7×365 co-managed detection and response that helps MSPs expand security monitoring, investigation, and initial response without staffing a full, in-house SOC.



Benefits

- 24×7×365 SOC monitoring, triage, and threat hunting
- Hands-on Tier-1 response
- API-first integrations, plus flexible syslog ingestion
- Co-managed, multi-tenant operations built for MSPs

MSPs are expected to protect every customer around the clock, but few can hire, train, and retain the analysts needed to staff an around-the-clock security operations center. Alerts pile up across endpoint, email, identity, network, and cloud tools, while compliance and cyber insurance demands keep rising. Meanwhile, attackers don't keep business hours, and in its 2026 DBIR report, Verizon found that about 96 percent of ransomware victims were SMBs.¹

OpenText™ MDR closes that gap with co-managed detection and response purpose-built for MSPs. A global SOC team monitors, investigates, and hunts threats 24×7×365, taking initial Tier-1 response actions on validated incidents while the MSP retains full visibility and control.

¹ Verizon, [2026 Data Breach Investigations Report](#), 2026.

OpenText Core MDR and MDR Complete deployment options

Deliver a multi-tenant service across your customer base through OpenText Secure Cloud

- OpenText Core MDR and OpenText MDR Complete run in Secure Cloud (multi-tenant SaaS), consumed as a service with a per-device monthly subscription

Two tiers, one platform: Choose your level of SOC involvement

OpenText MDR is built around a simple idea: you choose the level of SOC support that fits your resources and security expertise. With OpenText EDR, you manage security operations in house. With Core MDR, the OpenText SOC handles validated high-confidence threats, allowing your analysts to focus on incidents that require deeper investigation. With MDR Complete, the SOC also manages more complex alert categories, making it a strong fit for MSPs without dedicated security staff. Whichever level you choose, your customers benefit from around-the-clock protection across Microsoft 365®, endpoints, and identities.

Core MDR focuses hands-on response on the most common, highest-impact “Big 3” attacks: malware, ransomware, and phishing-related domains.

MDR Complete extends SOC coverage to the alert categories that require deeper analysis and judgment, including identity and access attacks, script-based attacks, network and IOC threats, data exfiltration risks, and risky browser extensions.

Both tiers run on the OpenText Detection & Response platform with built-in SIEM and SOAR and connect to the security stack your customers already own through API-first integrations and flexible syslog ingestion. They are billed per device, per month, so whichever tier you choose, the economics stay predictable as you scale.

Always-on SOC coverage without the staffing burden

Around-the-clock monitoring is the foundation of both tiers. SOC Tier-1 analysts act as your front line of defense. They investigate every alert in the covered categories, validate which are true threats and which are false positives, and add context analysis so that anything handed over to you arrives prioritized and ready to act on. That reduces dwell time, dashboard fatigue, and the hours your team spends chasing noise.

Hands-on response where it matters most

Instead of stopping at alerting, the SOC executes defined, repeatable response actions. The SOC executes non-disruptive containment actions when supported by integrated tools. For example, depending on the tools integrated in each environment, the SOC can quarantine a malicious file or run a full scan through endpoint tools and revoke an active session through identity or Microsoft 365 integrations.

Disruptive actions, such as endpoint isolation or account disablement, are escalated to the MSP with full context and a recommendation, following agreed escalation paths. The SOC automates non-disruptive response actions while keeping disruptive remediation decisions in your hands.

With Core MDR, out-of-the-box global workflows are enabled by entitlement, so alerts in covered categories are automatically escalated to the SOC without configuration.

MDR Complete includes out-of-the-box global workflows that cover every threat category covered by MDR Complete, so any alert in the covered category is escalated to the SOC. Moving between tiers is a simple entitlement change: same agent, no reinstall, and no changes to your deployment scripts.

“... we found that about 96% of ransomware victims were SMBs.”²

Extend your MDR service with an optional Incident Response Retainer for pre-contracted digital forensics and incident response (DFIR) hours or subscribe to the OpenText Cyber Resilience Program for advice, guidance, and assistance from a full catalog of cybersecurity services, including tabletop exercises that help your customers rehearse and mature their incident response, and security health checks that benchmark how far that maturity has come.

Note: In both tiers, the MSP has visibility into all alerts. The difference is which alert categories are automatically escalated to the Tier-1 SOC through out-of-the-box workflows. Where a remediation step sits outside the platform, such as uninstalling a risky browser extension, the SOC notifies you with a clear recommendation and your team completes the action.

Works with the tools your customers already have

Core MDR and MDR Complete work alongside a broad range of existing security tools, helping MSPs retain supported products instead of requiring a complete replacement of their security stack. More than 35 included API integrations deliver rich telemetry and enable automated response actions across endpoint, email, identity, cloud, network, and MSP service management tools.

The Compliance Storage add-on extends visibility with syslog ingestion from hundreds of syslog-capable sources, including firewalls, switches, routers, and servers, supporting log retention and compliance reporting. Built-in SIEM and SOAR capabilities are included in the base subscription alongside OpenText™ Threat Intelligence (BrightCloud) enrichment, with 60 days of telemetry retention by default.

By correlating endpoint, identity, and cloud telemetry, the platform helps detect attacks that endpoint-only MDR solutions can miss, including credential-based attacks, compromised Microsoft 365 accounts, and impossible-travel sign-ins.

A single lightweight agent works alongside existing endpoint protection, and OpenText endpoint security is not required. A unified installer manages entitlements and activates only licensed capabilities, making it easy to add 24x7 SOC coverage, SIEM, and SOAR to the tools your customers already use.

Co-managed operations built for MSP economics

Multi-tenant architecture and shared workflows let you provision and manage MDR across your entire customer base from a single console within OpenText™ Secure Cloud. Transparent per-device pricing with month-to-month billing and no contract minimums gives you predictable economics, and you can move between Core MDR and MDR Complete at any time as your practice evolves.

Co-managed is a deliberate design choice, not a limitation. Unlike black-box MDR services, you retain visibility into every alert, case, and SOC action while maintaining control of disruptive remediation decisions. The SOC handles triage, validation, and initial response, while you provide customer context, complete remediation, and manage customer communications. The SOC communicates with you, never around you. And if your team has its own security expertise, the built-in SOAR lets you create your own automated workflows alongside the SOC's escalations.

MDR is also a growth engine, not just a service line. From the same console and the same billing relationship, you can switch on DNS protection, security awareness training, email security, and cloud backup, growing recurring revenue per customer while avoiding the overhead of juggling multiple vendors, consoles, and invoices. That is the difference between reselling commodity MDR and selling managed outcomes.

Real-world use cases at a glance

Contain ransomware before it spreads. When a covered ransomware alert is automatically escalated, the SOC investigates the activity and initiates applicable response actions to help contain the threat and limit further impact.

² Verizon, [2026 Data Breach Investigations Report](#), 2026.

ARS Technology drives 20% YoY growth through its OpenText Cybersecurity partnership

ARS Technology starts customers on endpoint protection, then expands to MDR as trust and results build, managing every customer environment from the unified OpenText Secure Cloud console. Assessment-based onboarding generates a unique deployment for each customer, which ARS says makes clients feel the solution was built specifically for them.

“Endpoint protection builds the trust. MDR builds the resilience. With OpenText Cybersecurity, it’s a natural evolution from protection to active threat response.”

Alex Serrano

President & Lead Technology Consultant, ARS Technology

[Read the success story ›](#)

Also available: OpenText Core EDR

Prefer to retain in-house control? OpenText Core EDR provides endpoint protection, detection, response, SIEM, SOAR, and vulnerability assessment in a single, unified platform, and provides a natural upgrade path to Core MDR or MDR Complete when you want to add 24x7 expert coverage.

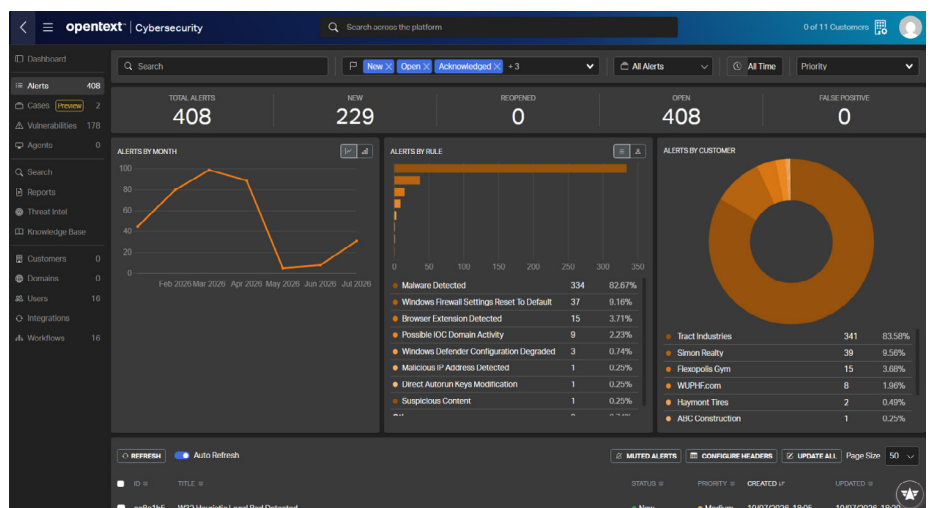
Catch attacks earlier with MDR Complete. Precursor activity, such as brute force sign-in attempts, obfuscated PowerShell, or possible data exfiltration triggers automatic SOC escalation, providing customers with earlier intervention before an incident becomes a breach.

Win and keep compliance-driven customers. Continuous monitoring, documented response, dashboards, and customizable reports give you evidence-ready documentation for audits, contracts, and cyber insurance requirements.

MDR Complete is the right fit when you have:

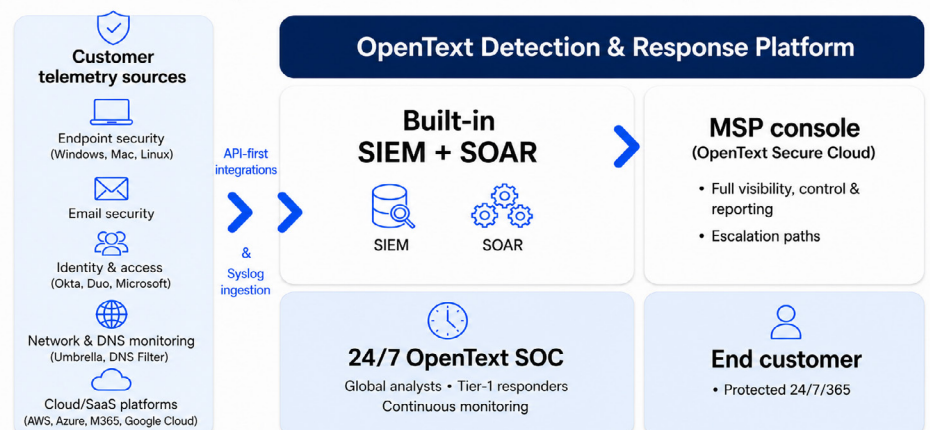
- Limited internal security expertise, with IT generalists covering security alongside everything else.
- A growing customer base you need to protect without scaling headcount in step.
- A desire to standardize security service delivery across every customer on one platform.

MDR Complete helps keep operational overhead low. The SOC manages the alert categories that consume the most analyst time, so a small team can deliver a big-team security service.



OpenText MDR console: Multi-tenant visibility into alerts, cases, and response across your customer base

How it works: OpenText Core MDR and MDR Complete



Feature	What it delivers
24×7×365 SOC monitoring and triage	Global analysts provide continuous eyes-on-glass coverage, validating alerts and prioritizing high-fidelity incidents around the clock.
Threat hunting	Expert-led hunts surface stealthy behaviors and weak signals that existing tooling alone might miss.
Tier-1 initial response	The SOC executes non-disruptive containment autonomously and escalates disruptive actions to the MSP with context and recommendations.
Expanded alert coverage (MDR Complete)	Extends SOC escalation to the categories that demand deeper analyst time and judgment: identity and access attacks, script-based attacks, network and IOC threats, data exfiltration risks, and risky or untrusted browser extensions.
35+ API integrations	Deep API integrations at no additional cost across endpoint, messaging, identity, DNS, cloud, network, and MSP service management tools. These integrations unify visibility and support bidirectional workflows and response actions across the stack.
Unified agent and installer	A single lightweight agent installs side by side with existing endpoint tools; tier upgrades and downgrades are entitlement changes with no reinstall and no deployment script edits.
Syslog ingestion	The Compliance Storage add-on enables ingestion from hundreds of syslog-capable sources, such as firewalls, switches, and servers, for log retention and compliance reporting.
Built-in SIEM and SOAR	Part of the base subscription, not add-ons; correlate endpoint, identity, cloud, and network events, with OpenText Threat Intelligence (BrightCloud) enrichment.
Co-managed, multi-tenant console	MSPs retain full visibility into alerts, cases, and response, with per-tenant playbooks, escalation paths, and notification preferences.
Reporting and compliance support	Dashboards, incident tickets, and customizable report templates provide evidence-ready documentation for audits, contracts, and cyber insurance.

Resources

Managed Detection & Response - MDR | OpenText Cybersecurity

[Visit product page ›](#)

OpenText EDR & MDR Integrations: API-First Power with Flexible Log Ingestion

[Learn more ›](#)

ARS Technology drives 20% YoY growth through OpenText Cybersecurity partnership

[Read the success story ›](#)

OpenText Cybersecurity

[See full suite of products ›](#)

Core MDR vs. MDR Complete at a glance

	Core MDR	MDR Complete
Positioning	For MSPs with in-house security expertise: the SOC handles the “Big 3” so your analysts can focus on threats that need deeper investigation	For MSPs without dedicated security staff: the SOC also absorbs the alert categories that demand the most analyst time and judgment
24×7×365 monitoring, triage, and threat hunting	Included	Included
Notification and initial response	Malware, ransomware, and phishing-related domains (DNS-based)	Everything in Core MDR, plus identity and access attack detection, script-based attack detection, network and IOC threats, data exfiltration risk alerts, and risky or untrusted browser extensions
Platform coverage	Windows, Mac, Linux	Windows, Mac, Linux
Telemetry retention	Rolling 60 days (Compliance Storage add-on available)	Rolling 60 days (Compliance Storage add-on available)
Optional add-ons	Incident Response Retainer; Cyber Resilience Program	Incident Response Retainer; Cyber Resilience Program

OpenText Core MDR and MDR Complete help MSPs deliver enterprise-grade security operations without building and staffing a SOC. With a co-managed approach, MSPs retain visibility and control while the OpenText SOC handles 24×7 monitoring, investigation, and initial response. Choose the level of SOC support that fits your business and scale your security practice with confidence.

Ready to deliver around-the-clock SOC-grade protection to every customer? Start with a supported evaluation and onboarding plan tailored to your MSP environment, with no annual commitment. [Book a demo](#) or contact your OpenText account representative to get started.