OpenText Core Threat Detection and Response

Detect insider risks, novel attacks, and advanced persistent threats before they impact your organization

Benefits

- Remove your security blind spots
- Improve threat hunter efficiency and effectiveness
- Detect insider threats and other advanced attacks sooner
- Reduce alert fatigue with fewer false positives

Insider threats continue to pose a costly and persistent risk despite substantial cybersecurity investments. While external attacks often dominate attention and budgets, malicious insider actions and the misuse of stolen identities frequently go undetected, resulting in an average annual loss of $16.2 million. Effectively addressing insider threats demands specialized security solutions that detect and mitigate harmful actions and identity misuse.

In a recent survey of cybersecurity professionals, 90 percent of respondents report insider attacks as equally or more challenging to detect than external attacks, highlighting the complexity of insider threats.[1] Worsening the challenge is the shortage of cybersecurity staff needed to prevent and troubleshoot security issues.

Addressing insider threats requires **specialized security technologies designed for proactive detection and mitigation** of both insider actions and identity misuse. Whether it's negligent employees, advanced persistent threats, malicious insiders, privilege escalation, novel attacks, or lateral movement, your biggest threats are likely already inside your organization. Today's ever-evolving landscape has cybersecurity professionals facing many challenges:

1 CSO Online, Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive, 2023

- Security operations center (SOC) teams are overwhelmed by alert fatigue, leaving them drowning in false positives and making it difficult to spot legitimate threats.
- Traditional security tools leave gaps, resulting in significant insider threats going unnoticed.
- Already-strained resources are spending too much time sifting through noise instead of neutralizing real threats.
- SOC teams, who typically deploy as many as 20 different security tools, face disconnected systems, impeding effective communication and exposing gaps in your defense.
- Hampered by a cybersecurity skills gap, security leaders are unable to hire the necessary number of threat hunters with the skill sets to improve threat detection capabilities.

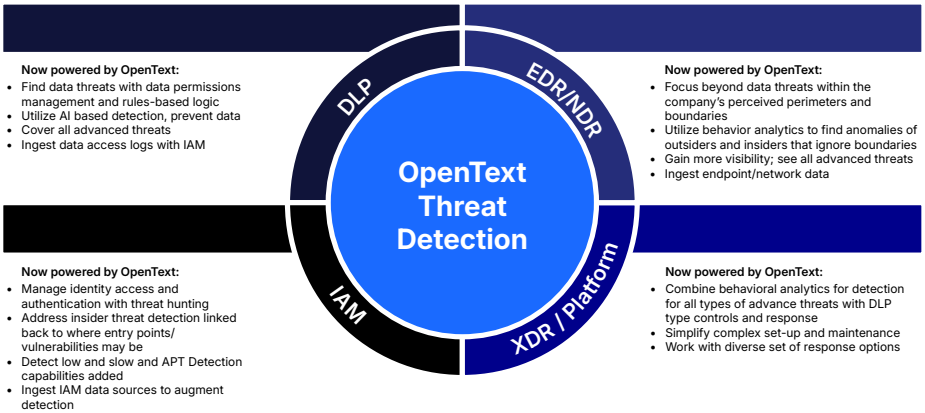
You need threat detection capabilities that give you time, insight, and confidence. The OpenText™ Core Threat Detection and Response solution enables your SOC team to identify critical threats faster, preempt costly damages, and stay ahead in a rapidly evolving threat landscape—all while reducing administrative burden.

Leveraging patented self-learning AI behavioral analytics that dynamically adapt to your environment, OpenText Core Threat Detection and Response uncovers elusive insider threats and the misuse of stolen identities by outsiders, while integrating with your existing security solutions.

- **Leverage adaptive insider threat defense:** Our AI solution seamlessly aligns with your specific environment and evolves with its changes, ensuring proactive detection of high-risk insider activity and unmatched protection against emerging insider threats.
- **Boost the ROI of existing security investments:** Integrate with your current security infrastructure to increase insider threat detection and boost the ROI of your security investments
- **Multiply your team's impact:** Talent shortages and mounting threats strain even the best SOCs. Our solution amplifies the effectiveness of your existing team with behavioral threat detection based on self-learning AI that identifies new threats automatically. In addition, automated threat hunting detects patterns of anomalous behavior and high-quality signals that uncover threats much earlier in the attack lifecycle.
- **Cost Avoidance:** By detecting advanced threats earlier in the attack lifecycle, OpenText Core Threat Detection and Response reduces (or eliminates) the costs of remediating an incident.

Your security resilience: Now powered by OpenText

Open XDR architecture with OpenText Threat Detection and response



Resources

See OpenText Core Threat Detection and Response in action

Try the click tour ›

Visit the product page

Learn more ›

View the launch details

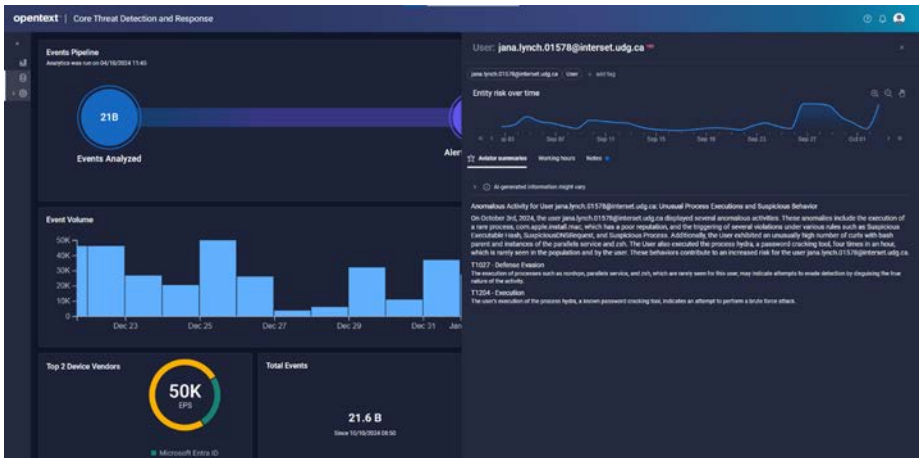
Read the blog ›

As cyberthreats continue to evolve, OpenText Core Threat Detection and Response ensures that organizations are equipped to detect and respond to even the most sophisticated attacks.

- **Remove your security blind spots:** Attackers may not always break rules, but they will always act abnormally. Gain visibility into your organization's unique user and entity behaviors with AI precision, ensuring that no anomaly goes unscrutinized and no advanced attack goes uncovered.
- **Improve threat hunter efficiency and effectiveness:** Not all alerts are created equal. Avoid the noise of traditional cyber tools and empower your threat hunters with high-quality, context-rich leads.. Focus on real, immediate threats and remediate incidents in days not months. OpenText Threat Hunting Service team has a more than 80-percent success rate in detecting Red Team attacks using our behavioral analytics capability.
- **Early detection of insider threats and other advanced attacks:** Your biggest threat may already be inside! Identify and neutralize insider threats before they wreak havoc on your organization. From data exfiltration and privilege escalation to subtle, prolonged attacks, behavioral analytics detects anomalies missed by rules and thresholds alone.
- **Reduce alert fatigue with fewer false positives:** Your security shouldn't be built to fit someone else. Your AI-powered security automatically adapts to changes across your organization that would require manual updating with rule-based tools. Significantly reduce false positives with security that knows you, allowing your security team to concentrate on legitimate threats, not noise.
- **Seamless integration with Microsoft security tools:** Leverage the Microsoft Defender for Endpoint, Entra ID and Copilot data you already collect and unlock deeper insights into threat activities, all while enhancing your existing security investments.
- **Simplify threat detection and response:** Reduce complexity in your SOC with behavioral threat detection based on self-learning AI that identifies new threats, summarizes risky entity behavior and provides additional context

Security reimagined

OpenText Core Threat Detection and Response represents the next evolution in threat detection, leveraging industry-leading behavioral analytics to identify insider threats with greater speed and accuracy. By transforming how organizations detect and respond to threats, OpenText Core Threat Detection and Response eliminates security blind spots and boosts SOC performance with true unsupervised machine learning. Seamlessly integrating with Microsoft Defender for Endpoint, Entra ID and Copilot, OpenText Core Threat Detection and Response delivers unparalleled threat detection capabilities.



Analysts, threat hunters, and security management get a high-level view of their environment along with a list of high risk leads on which to quickly follow up.

Features	Description
Adaptive, behavior-driven analytics	Automatically adjusts its detection baselines, learning from your organization's evolving workflows. As roles, technologies, and business processes change, the solution continuously refines what "normal" looks like, ensuring more accurate detection and fewer false positives.
Seamless integration with existing investments	Meshes seamlessly with your established ecosystem for enhanced visibility and fewer blind spots—without disrupting operations or forcing you to overhaul your technology stack.
High-context, actionable alerts	Provides context-rich insights in clear language when suspicious behavior is identified. SOC analysts no longer waste time deciphering cryptic alerts or investigating benign anomalies, improving response times and reducing the risk of insider-driven breaches from all levels of expertise.
Reduced SOC workload and alert fatigue	Filters out the noise and prioritizes high-risk incidents, empowering analysts to focus on genuine threats. This improves efficiency and enhances analyst morale and effectiveness, contributing to a more proactive and resilient security posture.
Scalable and future-proof	Scales and adapts its behavioral models as your organization grows, positioning your team to stay ahead of risks and evolving insider threat tactics. OpenText's expert services and ongoing innovation delivers a solution designed to address today's challenges and tomorrow's unknowns.
Risk scoring for threat prioritization	Prioritize high-risk threats like malicious insiders, with behavior-based risk scoring, reducing alert fatigue and helping teams respond to the most critical incidents in days, not months.

opentext™