Threat detection and response solutions comparison checklist

See how OpenText Core Threat Detection and Response stacks up against the competition

Choosing the right threat detection and response solution can be challenging in a crowded market. This checklist simplifies the evaluation process by highlighting essential features, including adaptability, integration, and insider threat detection accuracy. Compare providers to understand how OpenText™ Core Threat Detection and Response stands out in delivering advanced, adaptive protection.

Key considerations	Description
AI behavioral analytics for detection	Detects subtle anomalies and patterns across vast data sets, identifying threats that traditional, rule-based methods might miss, ensuring proactive defense.
Insider threat detection	Monitors user behavior to uncover malicious or unintentional insider actions, protecting sensitive data and maintaining trust within the organization.
Seamless integration with Microsoft tools	Integrates effortlessly with Microsoft Defender, Entra ID, and other platforms, maximizing existing investments while streamlining operations.
Behavioral indicator of compromise (IOC)	Context-aware detection based upon correlation of behavioral anomalies provide clear, high-quality indicators of compromise enabling faster remediation of novel threats and advanced attacks.
Automatic false positive reduction	Filters out irrelevant alerts through advanced AI, allowing SOC teams to focus on genuine threats, improving efficiency and reducing alert fatigue.
Ease of deployment and ramp-up	Simplifies the onboarding process with minimal disruption, enabling organizations to quickly realize the benefits of advanced threat detection.
Integration effort	Reduces the time and complexity of connecting with existing security systems, ensuring smoother implementation and immediate value.
Value-add services	Advanced threat hunting, expert guidance, proactive support, and tailored solutions to maximize value while ensuring seamless integration and ongoing success.

Key considerations	Description
Adaptability	Automatically evolves with organizational changes, ensuring continuous relevance and effective threat detection without manual reconfiguration.
Process automation	Eliminates the need for frequent manual adjustments, reducing overhead for security teams and maintaining consistent performance.
SOC workload optimization	Reduces the burden on SOC teams by prioritizing critical alerts and automating mundane tasks, enhancing productivity and focus
High-context, natural language alerts	Provides actionable insights in plain language, simplifying decision-making and enabling faster responses from all levels of expertise.
Proactive threat detection	Identifies threats before they escalate, empowering organizations to stay ahead of attackers and prevent costly incidents.
Cost efficiency	Delivers advanced capabilities at competitive pricing, maximizing return on investment and lowering total cost of ownership.

https://www.opentext.com/products/core-threat-detection-and-response

Ready to see how OpenText Core Threat Detection and Response can help you outmaneuver advanced threats? Join our webinar and learn how to spot insider risks, reduce false positives, and ensure your SOC focuses on what truly matters.