Trellix

SOLUTION BRIEF

Trellix® Managed Next-gen SIEM

Proactive defense, precision detection, rapid response

Key Features

- 24/7 monitoring, analysis, detection, and response
- Centralized data ingestion and analysis across all security feeds
- Unrivaled threat intelligence integration that boosts detection accuracy
- AI-powered analytics that enhance real-time threat detection
- On-demand expertise from an elite team of Trellix security experts
- Continuous optimization of your security posture
- Customizable, automated response actions tailored to your environment
- Simplified security operations and actionable insights for your team

Maximize your security investments

Securing your organization around the clock is a difficult and expensive challenge. Without the right staff or skills to manage threats, you're left vulnerable. Trellix Managed Next-gen SIEM solves this by providing continuous threat monitoring, advanced detection, and rapid response, all powered by our Trellix Security Platform and Trellix Wise™ GenAI capabilities. Part of the Trellix Managed Detection and Response (MDR) Services portfolio, it reduces operational overhead, frees your team for strategic work, and provides access to on-demand expertise.

Our managed service enables you to get the most out of your existing security tools, regardless of what you have deployed. We combine the power of the Trellix Next-gen SIEM with our unmatched expertise in three critical areas:

- **Integration with Your Tools.** Our Next-gen SIEM goes beyond simple data ingestion. It integrates with your entire security ecosystem, from on-premises to cloud platforms, using custom integrations and playbooks. This allows you to ingest more data and automate responses faster.
- **World-Class Intelligence.** Trellix is a leader in threat intelligence, trusted by organizations worldwide. Our AI enhances telemetry from your existing security tools, providing comprehensive threat coverage. We correlate multiple attack vectors—like network traffic, endpoint activity, and email—to connect seemingly unrelated events that might otherwise go undetected.
- **Unrivaled Expertise.** Our security operations center (SOC) provides 24/7 coverage, acting as a trusted partner to mature your security operations. Our analysts are experts in both your ecosystem and Trellix's products, enabling them to rapidly implement, configure, and optimize your environment.

Proactive security with Trellix Managed Next-gen SIEM

The Trellix Managed Next-gen SIEM continuously monitors your ecosystem in real-time, enabling early detection of anomalous behavior and potential threats. By highlighting critical alerts, it equips our expert analysts with automated playbooks for investigation and response. These capabilities are supercharged by Trellix Threat Intelligence and Trellix Wise, ensuring you benefit from top-tier analysis.

Our experts rapidly identify and analyze new threats, delivering the latest defenses. When threats are detected, our team conducts in-depth investigations and delivers tailored response actions using your existing tools, ensuring a seamless and precise mitigation. This collaborative approach manages threats with urgency and continually fortifies your security.

Broad data ingestion

Open and native integrations

Detections

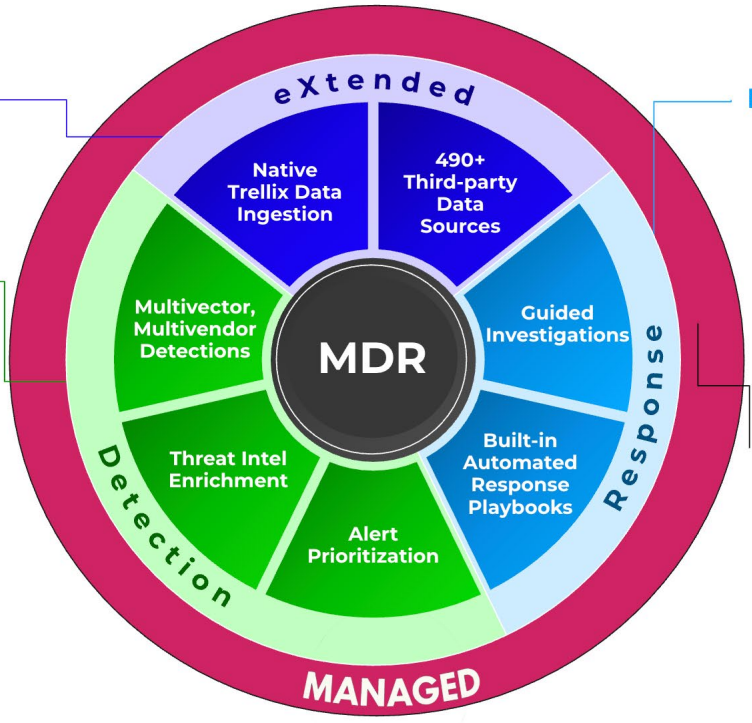
Analytics

Automated threat elimination

Noise suppression

Enrichment

Prioritization



Response

On-prem/cloud orchestration and response

AI guidance

Prebuilt, customizable playbooks

Managed

24x7 threat response

Expert-led investigations

Detection and Prioritization Across All Security Telemetry

We centralize and analyze all your security data, from every source. This comprehensive view, powered by advanced analytics and threat intelligence, allows us to rapidly detect and prioritize the most critical threats, cutting through the noise so you can focus on what truly matters.

Trellix MDR Key Improvements

Mean Time to Detect (MTTD): Significantly reduces the time to identify threats with 24/7 expert monitoring and advanced analytics.

Mean Time to Respond (MTTR): Accelerates threat containment and remediation through rapid, coordinated response actions**.**

False Positives: Drastically minimizes alert fatigue by leveraging expert analysis and intelligent correlation, focusing on real threats.

Security Team Efficiency: Frees up internal resources from mundane tasks, allowing your team to focus on strategic security initiatives.

Automated Responses for Faster Threat Mitigation

Our system provides automated response capabilities that are designed to help you neutralize threats faster. These preconfigured, intelligent actions can be triggered instantly upon detection, stopping attacks in their tracks and minimizing their potential impact with unparalleled speed.

A Complete Partnership for Protecting Your Organization

Our SOC experts streamline every incident using robust case management. Our service, when combined with Trellix Endpoint Detection and Response (EDR), is backed by a $1 million breach warranty and an incident response (IR) retainer, offering flexible access to critical services like incident response, tabletop exercises, and other specialized support. This demonstrates our commitment to delivering the highest level of security and accountability. With Trellix, you get a complete security partnership.

How Trellix Managed Next-gen SIEM impacts your security operations

Trellix Managed Next-gen SIEM delivers significant operational efficiency, saving customers over 4,000 hours annually, based on typical security tool usage with 50GB of daily data ingestion. This substantial time savings allows organizations to reallocate valuable resources.

Our 24/7 expert SOC analysts, backed by the industry's leading threat intelligence, ensure constant vigilance. They provide rapid, informed responses to any evolving threat, leveraging our advanced Trellix Security Platform to quickly identify and neutralize malicious activity.

This integrated approach dramatically enhances your security posture, reduces operational overhead, and liberates your internal team for more strategic initiatives. Ultimately, this leads to substantial cost savings and improved security outcomes for your organization.

Learn more about Trellix MDR services at trellix.com.