Trellix

Trellix® Managed Detection and Response

Protection around the clock, surgical threat response, continuous optimization

Key Features

- 24/7 monitoring, analysis, detection, and response

- Blind spot detection and tuning of your Trellix ePolicy Orchestrator environment

- Continuous optimization of your Trellix EDR and Endpoint Security

- On-demand expertise from an elite team of Trellix security experts

Maintaining a 24/7 defense can be challenging and expensive. Without the right skills or staff to detect, respond, and manage your security, you can be left vulnerable.

Trellix Managed Detection and Response (MDR) delivers continuous threat monitoring, detection and response, using the GenAI-powered Trellix Security Platform.

Trellix MDR helps you reduce operational overhead, free up staff for more strategic projects, or upskill them with on-demand expertise.

Expert delivery and management

Whether you have an existing Trellix deployment, are just getting started, or need to complete your implementation—our service can be up in running in days. Trellix MDR analysts have a deep understanding of your Trellix Endpoint Security (ENS), Trellix Endpoint Detection and Response (EDR), Trellix Insights, and Trellix ePolicy Orchestrator (ePO) tools to rapidly implement, configure, optimize, and begin monitoring your environment.

When a potential threat is detected, it's immediately escalated to Trellix MDR's expert SOC analysts, who conduct an in-depth investigation. They determine the nature of the threat, respond to it, and make any changes necessary to your configuration, rules, alerts, or policies to strengthen your defenses against similar threats in the future.

Trellix

Key Benefits of Trellix MDR

24/7 Threat Management
Our experts maximize the value of your Trellix investment, providing end-to-end coverage, 24/7 monitoring, analysis, investigation, and remediation.

Reduce Response Detection Time by 50%
Using Trellix Wise, our GenAI capability, Trellix MDR is able to accelerate detection with AI-powered investigations. Wise automatically collects and correlates related breaches, artifacts, and more while providing detailed recommendations of next steps based on the nature and severity of the threat, greatly reducing MTTD.

Stay Ahead of New Threats
Trellix MDR leverages context on new outside threats provided by Trellix Insights, accelerating investigation and remediation efforts. Our analysts know of potential campaigns, prioritized by relevance to your sector or geography. They can even identify which endpoints lack protection against the campaigns and then take action to improve your threat security posture.

Get Help When You Need It Most
Trellix MDR includes access to an elite team of Trellix security experts who partner with you, help inform your strategy, and provide answers to your questions the moment you need them. They are available around the clock to provide strategic and mitigation advice across your security controls.

Extend Your Coverage
Trellix Endpoint Security covers more operating systems and OS versions than any other solution, allowing Trellix MDR services to provide broad visibility of your endpoints.

Figure 1: Trellix MDR unites the power of Trellix Endpoint Security, Trellix EDR, Trellix Insights, and Trellix ePolicy Orchestrator (ePO) with elite expertise, GenAI-powered detection, and 24/7 management.

Why choose Trellix MDR for your business?

Deep Focus on Uniting Protection and Detection:

Unlike other services, we measure ourselves on what we prevent, incentivizing our service to stay ahead of threat actors with continuous hardening of your defenses.

We use Trellix Insights, global threat intelligence, and IOC enrichment along with context from Trellix deployments around the world to update policies and close vulnerabilities before exploits can occur.

GenAI-powered Auto-investigation Speeds Response:

Security analysts typically step outside their EDR solution to investigate and truly understand all the facets of a complex threat or campaign. Trellix MDR analysts do not have to validate and investigate numerous alerts and can take the next step rapidly investigating with Trellix Wise™. Wise pre-investigates events, prioritizes events, guides investigations, correlates threat activity, and automates manual tasks.

Rapid Time to Value:

Trellix MDR integrates effortlessly with your existing Trellix Endpoint Security solution, and no new deployment is required. This streamlined approach ensures immediate protection and operational continuity, allowing Trellix MDR experts to focus on critical threat detection and response without disruption.
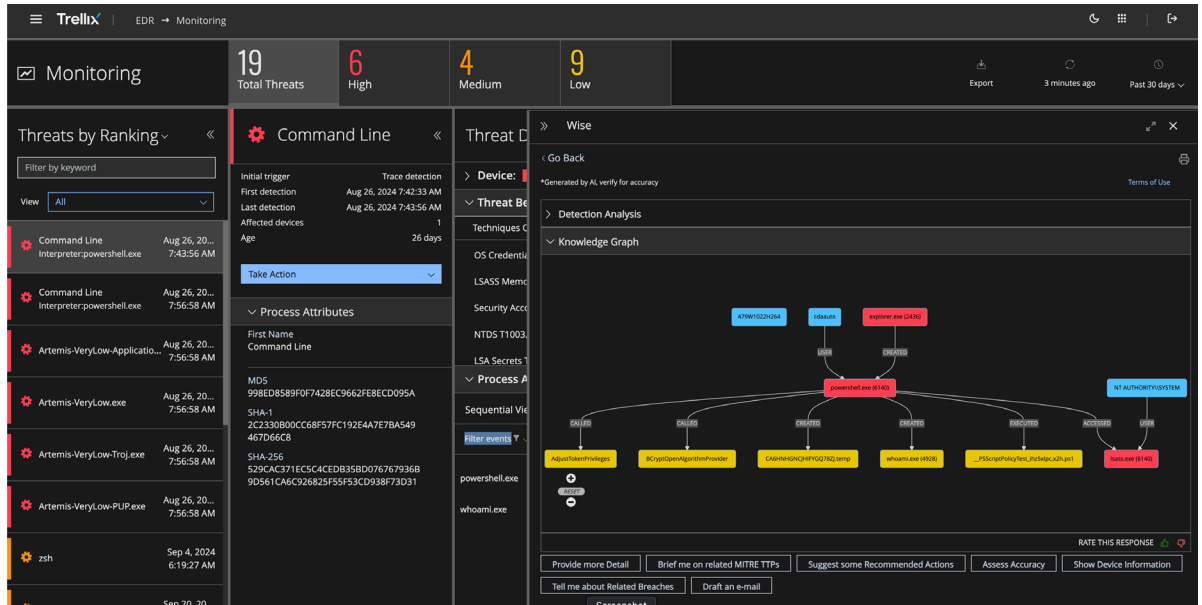
Figure 2: Trellix MDR uses Trellix Wise, our GenAI capability to speed detection and response times. It automatically collects artifacts, presents key findings visually to clarify relationships and speed understanding for Trellix MDR analysts.

Customer benefits

Based on third-party evaluation and Trellix proprietary data, Trellix MDR customers can realize significant savings while strengthening their security posture.*

- Recover 13 or more hours per week for more strategic projects and boost your productivity by 148%

- Reduce your risk of missed detections by 40% and as much as $1.95M in damages.

- Reduce your operating costs by as much as 90%

- Realize an ROI of 390% or more in the first year alone

- Save over $230K upfront by using Trellix MDR instead of implementing with in house resources

Experience the difference of expert-led threat detection and response—contact us now.

* Individual experiences may vary. Request an evaluation from a Trellix expert for a more detailed analysis