Trellix

DATA SHEET

Trellix Endpoint Detection and Response (EDR)

Powerful threat detection, guided investigation, and response—simplified

Key benefits

- Provides high-quality actionable threat detection without the noise
- Offers proactive insight on threats before the attack
- Performs analysis faster, so you can mount a more resilient defense
- Uses AI-guided investigations to provide analysts with machine-generated insights into attacks
- Maximizes the impact of your existing staff
- Is hosted in a low-maintenance cloud
- Simplifies deployment using Trellix ePO software or SaaS-based ePO
- Enables analysts to focus on strategic incident response without burdensome administration overhead

*Trellix Insights requires Trellix Endpoint Security telemetry (opt-in) to function properly. If you do not want to provide this telemetry, you should not choose this product, as you won't be able to receive full value.

Overview

Adversaries maneuver in covert ways, camouflaging their actions within trusted components already in your environment. They don't always install something tangible like malware, but they always leave behind a behavioral trail. Trellix Endpoint Detection and Response (EDR) continuously monitors and gathers data to provide the visibility and context needed to detect and respond to threats. But current approaches often dump too much information on already stretched security teams.

Trellix EDR helps manage a high volume of alerts, empowering analysts of all skill levels to investigate more alerts, more effectively. Unique to Trellix EDR is Trellix Insights,* the first technology to proactively prioritize threats before they affect your organization and simultaneously predict if your countermeasures will stop them, all while prescribing exactly what you need to do if they won't.

Strengthen, accelerate, and simplify EDR

Trellix EDR reduces mean time to detect and respond to threats by enabling all analysts to understand alerts, fully investigate, and quickly respond. Advanced analytics broaden detection and make sense of alerts. Artificial intelligence (AI) guided investigations and automation equip even novice analysts to analyze at a higher level and free more experienced analysts to apply their skills to the hunt, accelerating response time.

Detect advanced endpoint threats & respond faster

Without the right data, context, and analytics, EDR systems either generate too many alerts or miss emerging threats, wasting precious time and resources without improving security. Trellix EDR offers always-on data collection and multiple analytic engines throughout detection and investigation stages to help accurately surface suspicious behavior, make sense of alerts, and inform action.

Gain context and visibility

Endpoint event information is streamed to the cloud, providing the context and visibility necessary to uncover stealthy threats. Endpoint information is available for immediate inspection, real-time search, and historical search. Flexible data retention options support the varied needs of diverse security operations teams and organizations.

Obtain new, proactive context from Trellix Insights

Dashboard notifications or email alerts on prioritized campaigns are defined by the Trellix Intelligent Sandbox. You also get campaign information, local assessment of systems, prediction of potential impact to your EPP, and prescriptive guidance to prevent breaches. This allows analysts to get ahead of adversaries. It takes a fraction of time and resources to prioritize, predict, and prescribe compared to penetration testing with red/blue team exercises. These three Ps are automated, to notify your team about threats before the attack. What used to take weeks can take minutes, shifting your SOC team from reactive to proactive.

Uncover more with powerful cloud-based analytics

Analytics engines inspect endpoint activity to uncover a broad spectrum of suspicious behavior and detect threats—from file-based malware to fileless attacks—that have slipped by other security defenses. Cloud-based deployment enables rapid adoption of new analytic engines and techniques.

Think like an attacker

Behavior-based detection results map to the MITRE ATT&K® framework, supporting a more consistent process to determine the phase of a threat and its associated risk, and to prioritize a response.

Easily navigate

Alert ranking further helps analysts understand risk severity and an appropriate response. Flexible data display and visualization at this stage help analysts with different levels of experience easily navigate the data to quickly understand why an alert was raised and determine next steps: dismiss, respond, or investigate.

Respond with speed

Trellix EDR preconfigured responses enable immediate action. Your team can easily contain threats by killing a process, quarantining a machine, and deleting files. Analysts can act on a single endpoint or scale response to the entire estate with a single click.

AI-guided investigations

If immediate response to an alert and root cause of the incident is not obvious—and often it is not—security analysts must step outside their EDR solution and investigate to truly understand all the facets of a complex threat or campaign and the associated risk.

EDR solutions traditionally enable investigations by providing raw data, context, and search functions, but still require knowledgeable analysts to perform the inquiry and analysis. Experienced analysts often do not have time to validate and investigate numerous alerts, while inexperienced analysts may not know where to start.

With Trellix EDR, analysts at any level can take the next step and investigate. Rather than simply enabling an investigation with search functionality and data, Trellix EDR guides the investigation.

Dynamic investigation guides

Combining the expertise of Trellix forensic investigators with AI, investigation guides in Trellix EDR force-multiply the investigation process, exploring many hypotheses in parallel for maximum speed and accuracy. Unlike playbooks that automate scripted tasks for known threats, investigation guides dynamically adjust to each case, combining different investigation strategies and data. Trellix EDR automatically asks and answers questions to prove or disprove the hypotheses. Trellix EDR automatically gathers, summarizes, and visualizes evidence from multiple sources and iterates as the investigation evolves.

Broad data collection and local relevancy

The AI-powered investigation engine gathers and processes artifacts and complex event sequences—from endpoints, security information and event management (SIEM) systems, proactive Trellix Insights, and Trellix ePolicy Orchestrator software—to help make sense of alerts. Trellix EDR compares evidence against known normal activity for each organization and threat intelligence sources to improve local relevancy and reduce false positives. Investigations can originate from either Trellix EDR or SIEM alerts.

Different views for different users

The flexible data display applies the appropriate lens for users with different levels of experience, so all analysts can quickly understand how artifacts and events are connected without pivoting to multiple screens.

Phishing investigation

Trellix EDR easily plugs into security operations phishing investigation workflows. Suspicious emails can flow to Trellix EDR for inspection. If they're found to be malicious, Trellix EDR can quickly determine which machines across the organization may be affected.

Trellix EDR reduces the expertise and effort needed to perform investigations and increases the speed with which analysts can determine the risk of the incident and its root cause. At an organizational level, the benefits multiply. Each analyst can be more efficient, more cases can be dispositioned by junior analysts, and senior analysts can spend time on the highest value activities.

The right data at the right time for the task at hand

In addition to guided investigation, analysts and threat hunters can use the powerful Trellix EDR search and data collection capabilities and Trellix Insights proactive data to expand inquiries across systems, and look deeply into and across those systems.

Historical search

The comprehensive and always-on data collection feature streams endpoint event information from all monitored systems to the cloud. Analysts can search this centralized data—regardless of online or offline status of endpoints—to find indicators of compromise (IoCs) and indicators of attack that may be present along with deleted files.

Real-time search

For active incident inquiries, real-time search reaches out to endpoints across your estate to quickly query for up-to-the-moment information. Flexible syntax enables capabilities like simple queries for searching workstations. You can also run more complex searches that return more data from the workstation, such as identifying a user at the time of event, command-line execution, and when the suspected application was started. Trellix EDR can easily scale queries across the enterprise to tens of thousands of machines.

On-demand data collection

To support investigations, Trellix EDR can take a snapshot of an endpoint, capturing a comprehensive view of active processes, network connections, services, and autorun entries. Trellix EDR provides associated severity and additional information, such as hash, reputation, and the parent process/service/user that executed a suspect file. Enabled by a non-persistent data collection tool, snapshots can be captured on both monitored and non-monitored systems.

Trending campaigns

Orchestrated and targeted attacks (based on region or industry) are alerted from Trellix Insights, identifying IoCs to proactively search for with Trellix EDR. This empowers the analyst to execute proactive searches before the attacks occur.

Collaboration expands visibility, increases operational efficiency, and improves outcomes

Trellix EDR is a key component of an integrated security ecosystem. It extends endpoint protection capabilities and visibility while supporting the workflows and processes of the security team. You can also use the solution to help reduce mean time to detect and respond and increase operational efficiency.

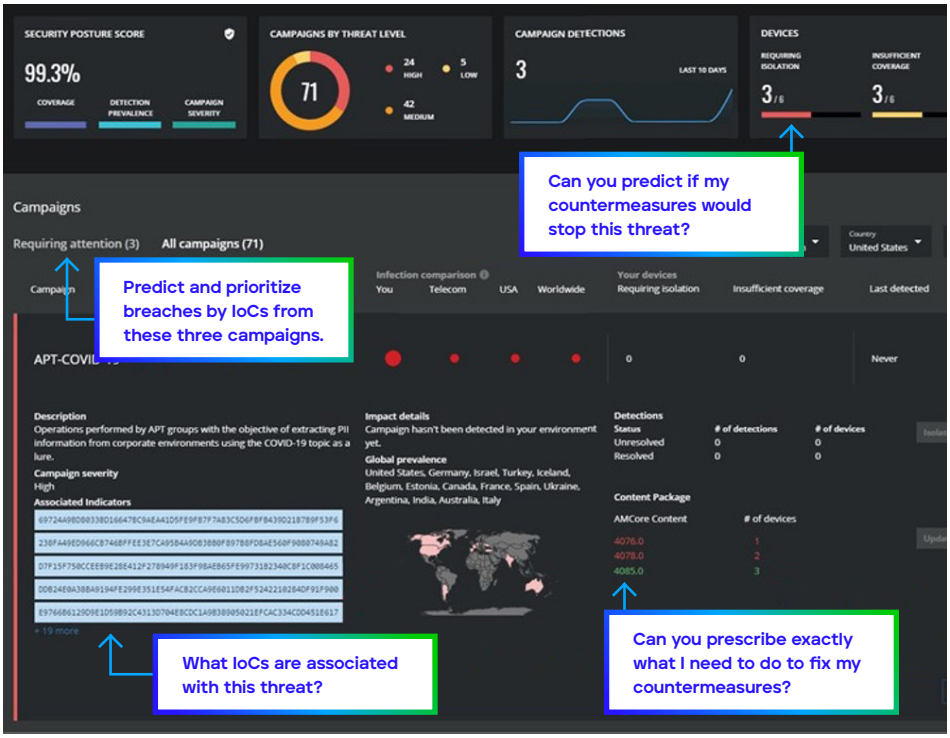

Figure 1. The Trellix Insights dashboard automatically surfaces threats that matter and guidance on what to do before the attack. It offers additional EDR insights to clarify and accelerate investigation efforts.

Correlate data from across the enterprise for complete visibility

Collaboration and easy integration with data sources beyond the endpoint are key to closing data gaps for multifaceted threat investigations. Tight integration with SIEM solutions, such as Trellix Enterprise Security Manager or third-party products, enables Trellix EDR to expand investigation capabilities and insights. It does so by correlating endpoint artifacts with network information and other data collected by the SIEM.

- Trellix EDR leverages the proactive context on new outside threats provided by Trellix Insights, accelerating investigation and remediation efforts.
- Trellix Insights alerts you to potential campaigns, prioritized according to whether they are targeting your sector or geographies. It predicts which endpoints lack protection against the campaigns and what to do to improve this threat detection. It also informs analysts of campaign attack operation and the objective of attack, and provides strategic and mitigation advice across countermeasures.

  Trellix Insights gives your organization a complete set of IoCs to proactively search for with Trellix EDR. Analysts can execute proactive searches or use other tools to carry out further research.
- If Trellix Insights telemetry shows that you might be affected by a campaign, it will pivot to Trellix EDR. Analysts pick up the IoCs in question, saving them the time and effort of copying and pasting IoC information manually. A complete set of campaign IoCs are provided with each campaign, greatly speeding investigation of potential breaches.

Support team collaboration and workflows

Trellix EDR plugs into current security operations workflows and supports collaboration by sharing investigation data and updates through security incident response platforms.

Scalable, simple deployment

Trellix EDR is available as a software as a service (SaaS) application. Management with Trellix ePO—the industry's foremost centralized security management platform—simplifies deployment and ongoing maintenance of Trellix EDR and your entire security infrastructure. Now available both on-premises and in the cloud, Trellix ePO offers management flexibility to fit diverse organizational needs.

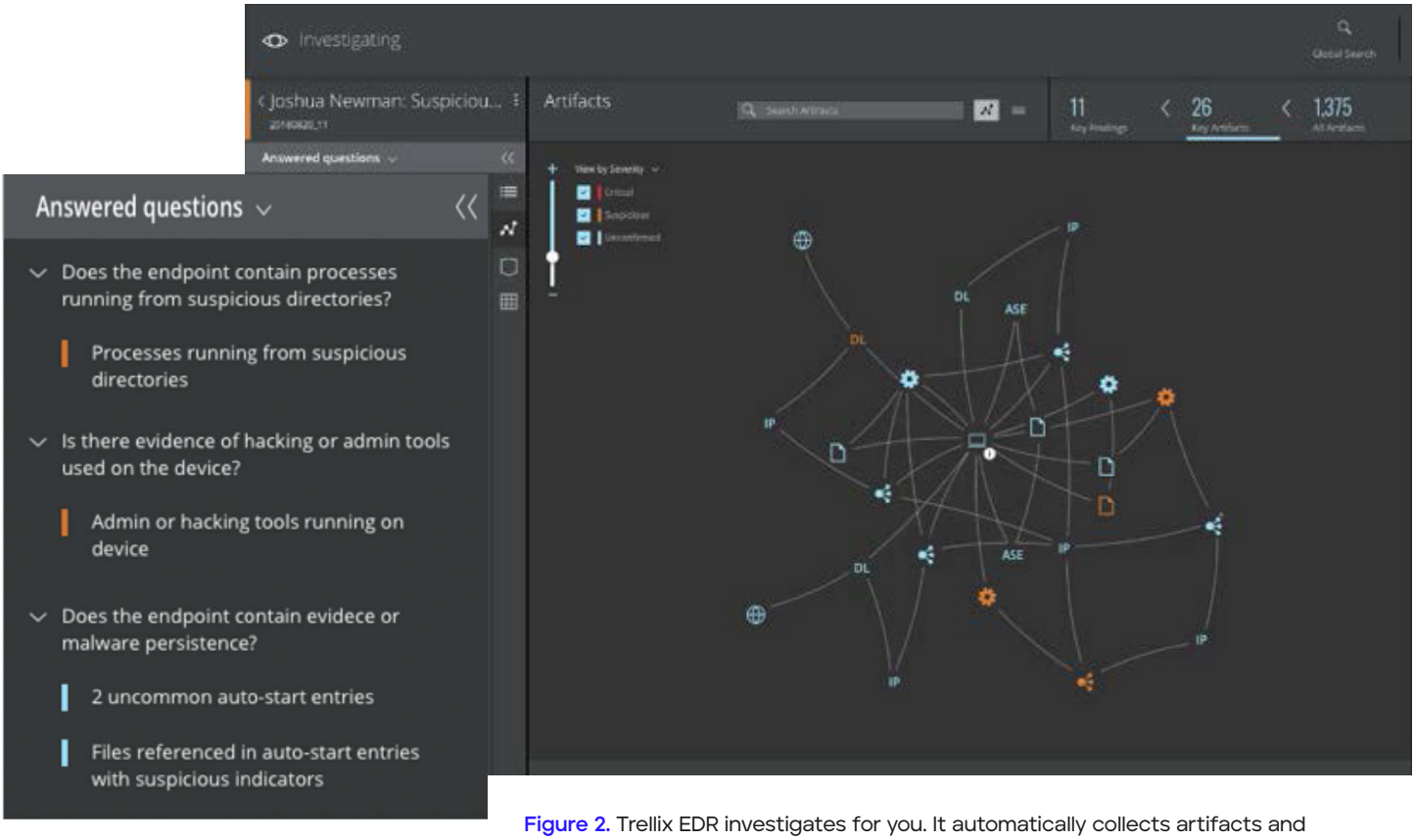

Figure 2. Trellix EDR investigates for you. It automatically collects artifacts and presents the key findings. This visualization clarifies relationships and speeds analyst understanding. Trellix EDR asks and answers the right questions to prove or disprove hypotheses.

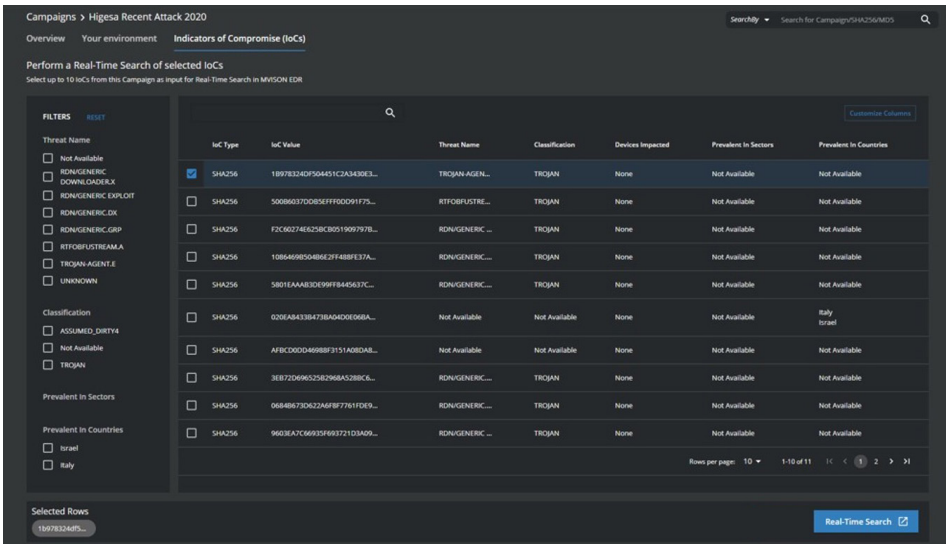

Figure 3. Trellix Insights offers IoCs of a high-priority threat, with an option to search in Trellix EDR.

Looking for managed endpoint detection and remediation?

Managed detection and response (MDR) denotes outsourced cybersecurity services designed to protect your data and assets even if a threat eludes common organizational security controls.

An MDR security platform is an advanced 24x7 security control that often includes a range of fundamental security activities, such as cloud-managed security for organizations that can't maintain their own security operations center. MDR services combine advanced analytics, threat intelligence, and human expertise in incident investigation and response deployed at the host and network levels. Our certified service provider partners offer 24x7 critical alert monitoring, managed threat hunting, advanced investigations, and threat disruption to significantly improve your threat detection and response efforts.

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com