Trellix

DATA SHEET

Trellix Insights

The first endpoint to extended detection and response (XDR) security capability to help you get ahead of adversaries

Key benefits

Predict and prioritize threats that matter

Proactively identify and prioritize threats likely to hit your organization based on industry, geography, threat actors, and your enterprise's security posture.

Reduce mean time to detect and resolve from months to hours

Streamline workflows with rich actionable context and analysis. Progress quickly with intuitive guidance.

Be more proactive and spend more time preventing

Gain more actionable intelligence on a threat before an attack. Understand how your security posture stacks up against the threat. Obtain prescriptive recommended countermeasures.

Boost security operations defensive performance

Empower security teams of various experience levels with intuitive guidance in an advanced defensive playbook to respond to what matters. Bring security to life, so you can quickly adapt and learn.

Overview

The evolution and pace of cyberthreats are constant stress points for organizations. Enterprises have reacted to them by increasing security budgets amid a shortage of security expertise, but they still can't keep up with modern adversaries who are constantly updating their arsenal of tools, tactics, and techniques.

Most current security options rely on siloed intelligence requiring human and manual intervention. These may address immediate threats, but the increasing numbers and nuances of cyberattacks are bombarding security teams into a seemingly constant reactive posture. A threat intelligence platform (TIP) can offer a large data lake of threats to assess, but this requires manual integration and analysis cycles, producing limited actionability and remediation. Vulnerability management solutions can advise on existing vulnerabilities and their severity, but they offer limited insight into how your security posture can or cannot defend against current real-world threats.

The solution is Trellix Insights, with real-time intelligence that empowers proactive action. Comprehensive intelligence that has been distilled and analyzed by artificial intelligence and humans can provide prioritization into which threats are most likely to target your organization (a combination of deep learning and machine learning we call human-machine teaming). Trellix Insights predicts exactly how a threat would impact your overall security, and prescribes what you need to do to optimize your security stance.

Transform your security so you can be more proactive

Trellix Insights offers capabilities built into the Trellix management platform that uniquely align with and streamline risk and threat operations. These capabilities help you preemptively improve defensive countermeasures and accelerate response times while using fewer resources. Risk intelligence gathered and refined from one billion sensors assessed by proven advanced threat researchers empowers your enterprise to prioritize its defenses. Detection, remediation, preemptive accelerated response times, and significant risk reduction can be realized from one console.

In contrast, reactive cyberdefense strategies are limited to playing catch-up and fighting fires. Adversaries are devising campaigns designed to attack traditional defenses, testing reactive security products to see what techniques will breach their shields. Organizations need to address the entire attack lifecycle before and after they are hit.

Trellix Insights provides answers to risk-related questions for endpoints and beyond

- Are you at risk? What is your level of exposure?
- How do you prioritize the attacks that might hit your organization? How do you learn about them? What is your research process?
- How do you know which threats haven't yet hit your organization but are likely to?
- Even if you had a TIP, how would you prioritize all the attacks within the TIP database?
- How do you know about threats that have hit your peers?
- How prevalent is a threat in your industry and region?
- Is there a particular threat actor targeting your organization?
- How does your current security posture sustain a threat?
- What is your confidence in the complete threat landscape and why?

Gain complete attack lifecycle coverage

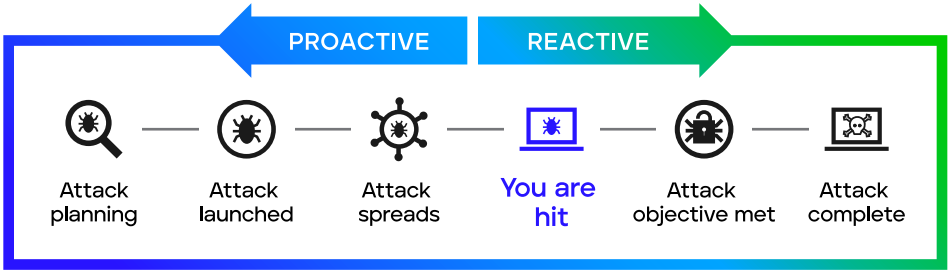

Figure 1. A typical attack lifecycle

At the end of the day, intelligence and actionable insights from a single console give you the best possible cybersecurity stance against the most likely threats, and boost confidence in your defenses. Assimilate critical threat information quickly (from weeks down to seconds). Trellix Insights accomplishes this by:

Automatically identifying global threats you haven't detected

Trellix Insights uses a massive reservoir of security intelligence from more than one billion sensors with optimized threat analysis powered by human-machine teaming. Machine learning detects never-before-seen threats that human analysts would likely miss due to lack of visualizing and processing. The human element of Insights leverages deep cybersecurity expertise and intuition to outmatch adversaries behind malicious code.

Increasing situational awareness so you can focus on what matters

Insights brings out the context behind the events and detections, showcasing the correlations between campaigns, threat actors, and TTPs. Your security operations team gains a better understanding of threats, with effective remedial actions. Preempt suspicious threats based on correlations with global telemetry, to strengthen defenses and prepare your team even before the attack occurs.

Improving readiness and preparedness for threats

You'll know precisely how your defenses stack up before threats hit. Trellix Insights proactively tracks and prioritizes local and global threats that are predicted to hit your enterprise.

Analyzing threats using machine learning

This capability allows you to determine how your specific comprehensive security posture derived from endpoint and cloud vantage points would perform. It then provides preemptive prescribed protection actions that you can take to quickly and easily block those attacks.

Significantly accelerate detection and response time

Trellix Insights helps your enterprise take the next critical proactive step to change and remediate your environment with prescriptive guidance and automated actions. Automation increases effectiveness against outside attacks, analyzing and comparing threats and proactively defending against them.

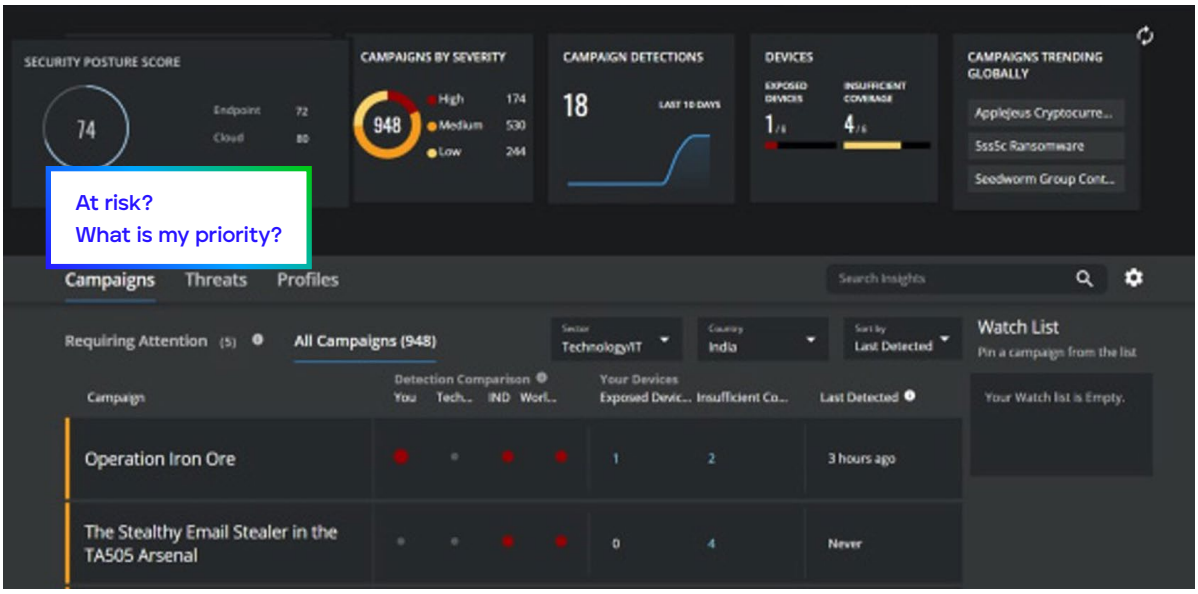

Figure 2. Drive proactive security with the Insights dashboard

Reduce mean time to detection and resolution from months to minutes

Human-machine teaming and advanced analytic capabilities are expanded to sift through enormous quantities of data and present actionable intelligence. Expanded detection capabilities preemptively accelerate response times and significantly reduce risk.

Advance with a comprehensive security posture

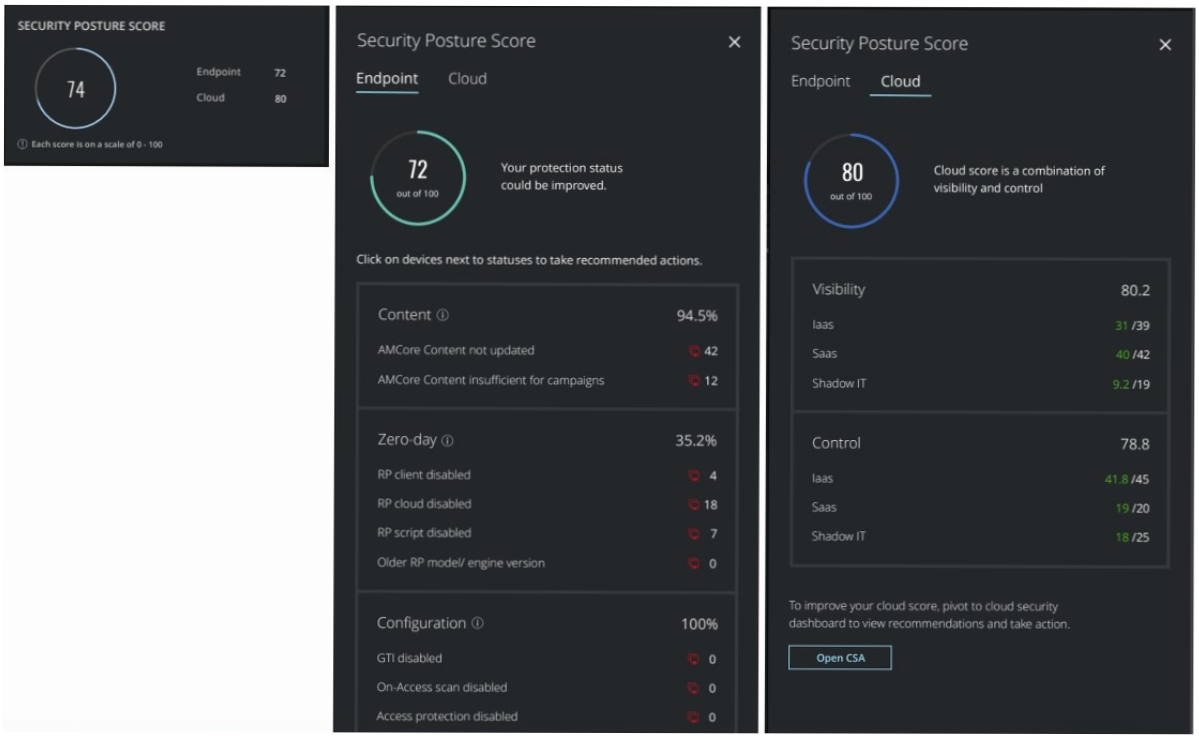

Figure 3. At-a-glance unified and actionable security posture scoring

Get a clear, understandable view of threats with prioritization and actionability

A comprehensive and unified security posture includes both endpoint and cloud assessment and allows you to focus on what matters across your environment. Guided response based on analyzed and prioritized intelligence and insight elevates even novice analysts. From the integrated console, quickly and easily respond by making changes to your configurations, isolating infected devices, updating policy, or pivoting to endpoint detection and response (EDR).

Reach actionable risk assessments

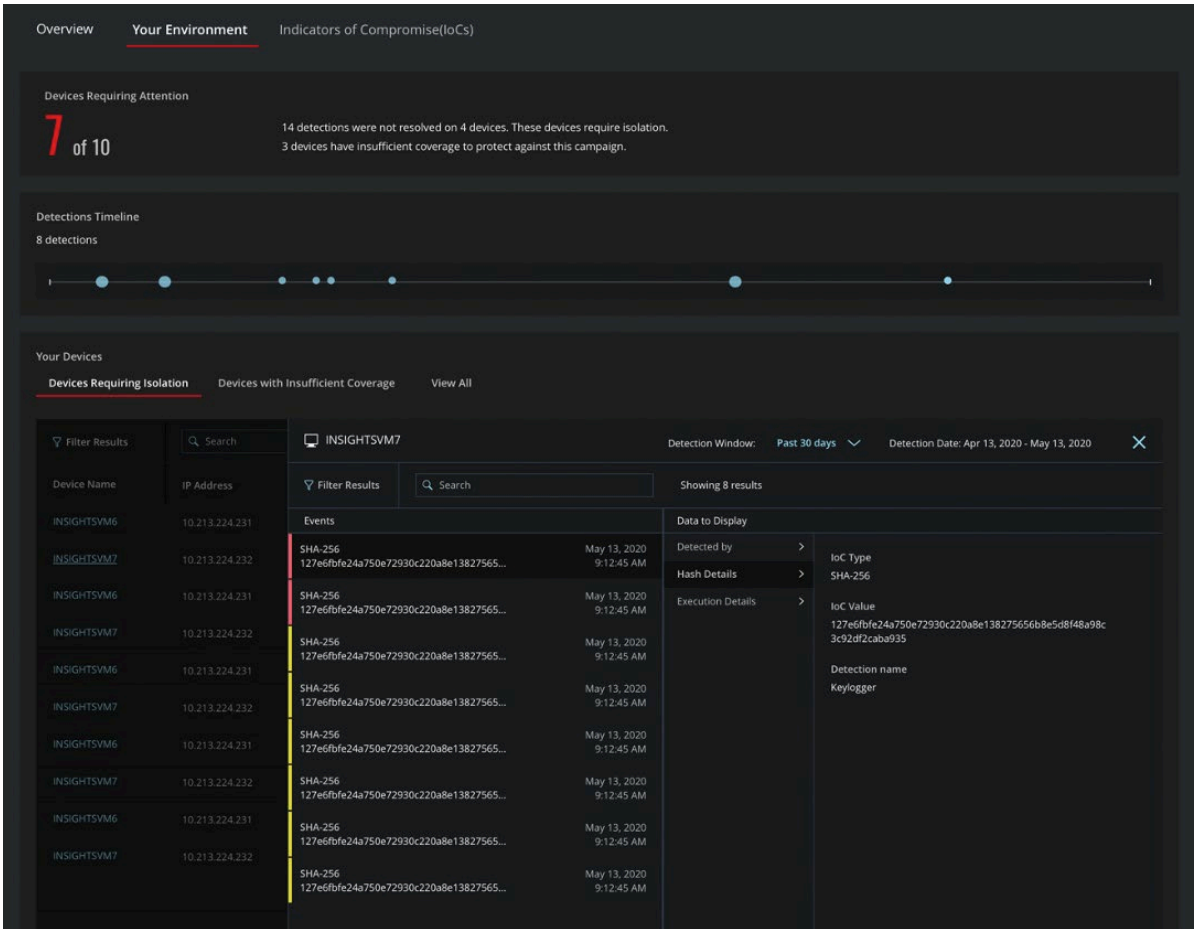

Figure 4. Know what requires attention in your environment to proactively counter a threat

Improve signal-to-noise ratio for threat indicators

Advanced analytics expand detection and help you make better sense of alerts. Insights threat analysis can easily pivot to Trellix EDR to search on additional context like indicators of compromise (IoCs) to reduce investigation cycles. Critical context on threat actors/crime syndicates behind the campaign is shared, including the tools they've used, the common vulnerabilities and exposures (CVEs) they've been associated with, the standard tactics/sub-techniques and the associated IoCs, and credible sources on the syndicate.

Empower SOC resources

Security teams are often overwhelmed by the immense volume of intelligence they must sift through to protect their environments. Limited resources and time inhibit analysis of threats and defenses. Using human-machine teaming, analytic capabilities are expanded—no matter the skill level of analysts—to crawl enormous quantities of data and present it as actionable intelligence.

Insights allows your enterprise to address its skills gap and empower security operations center (SOC) functions. Security teams are better informed so they can make better decisions.

- Insights gained from data intelligence allow security teams to customize and maximize your enterprise's defenses. This gives you optimum protection without the need to increase staff size or rely on higher levels of expertise. Insights offers more purposeful insights into Trellix EDR to reduce the length of the investigation cycle, providing the expertise and resources needed to carry out investigations. Analysts can verify the risk of the incident and root cause with increased speed and efficiency.
- Insights is the first tool in the industry to take advantage of a dynamic new Trellix Adaptive Defensive model, to deliver an advanced defensive approach for ransomware with the Trellix Adaptive Defensive playbook. The Adaptive Defensive model provides richer context and more intuitive, metrics-driven guidance than traditional solutions. Your SOC will be empowered to deliver better, more efficient security.
- Chief security officers (CSOs) can get the most out of their staff and products by freeing security analysts from mundane tasks and helping even junior-level team members become more effective. Organizations can reduce time spent on security management, streamlining their workflows to accelerate additional safeguards.
- Insights preemptively automates detection, response, and defenses on prioritized threats from a single console, alleviating the need for analysts to toggle between tasks. It accumulates and analyzes relevant data elements with actionable guidance in one place, placing it at the fingertips of security analysts when needed.

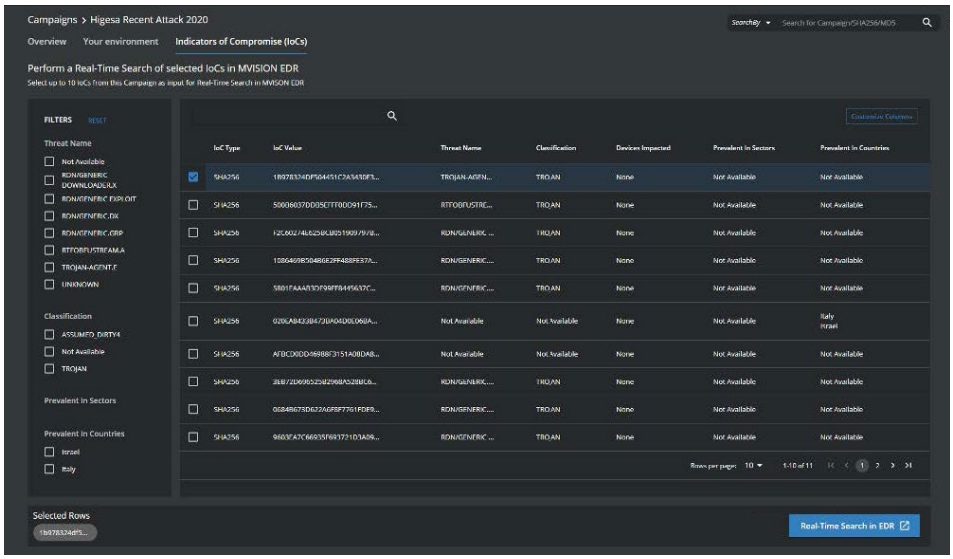

Figure 5. Dig deeper to understand threat events and determine your ability to defend your organization with an option to pivot to EDR capability.

Trellix Insights requirements

Insights is managed by Trellix ePO software 5.10 (on-premises, SaaS, and IaaS). It's optimized for use with our latest endpoint protection technology: Trellix Endpoint Security and Trellix Agent. To work effectively, Insights requires you to opt into Endpoint Security telemetry.

For more information, visit trellix.com.

Sample use cases

Problem	Solution	Outcome
Am I being targeted? Is this a new campaign variant?	Known threat assessment Severe threat group or actor assessment Selected retrospective attack analysis Comparative protection efficacy reporting User IoCs retrospective attack analysis.	Answer the questions: Am I at risk? Is there a specific threat actor targeting me?
What is my overall security posture?	Unified security posture from endpoint to cloud	Assess and act on my comprehensive security hygiene
Can my current protection configuration protect me?	Local protection posture check	Assess my current security posture
What specifically do I have to change to be protected?	Local protection posture check	Prescriptive guidance on what to do
Can my other security functions isolate?	Publish to isolate or contain to other security functions	Send contain actions to other security functions to further mitigate the risk (via Data Exchange Layer [DXL])

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