Trellix

SOLUTION BRIEF

Trellix® Helix

Accelerate incident management with AI-powered security operations, automated alert triage, and automated response

Native and Open Integrations

- **Endpoint Detection and Response (EDR)**
- **Identity Platforms**
- **Mobile Security**
- **Threat Intelligence**
- **Vulnerability Management**
- **Cloud Security**
- **Data Protection**
- **Network**
- **Cloud Security (e.g., CASB and CWPP)**
- **Email and Collaboration**
- **Fraud Detection**

Security Operations (SecOps) teams need to integrate, analyze and create context across multiple sources to reduce manual pivots. Only then can they put an end to data silos and create context for faster incident detection and response. But not all solutions offer the same speed and level of context.

Automation and AI are increasingly necessary for SecOps efficiency to combat machine speed attacks, help close talent gaps and surface low level signals that might be overlooked. However, automation has to be accessible, not just available to those with specialized coding experience in order to deliver rapid value. Similarly, AI has to go beyond simple chat-bot functionality to truly up-skill teams and make them more effective. Trellix Helix unites threat events from multiple controls so you can get the full story of an attack and reduce pivots across tools. It provides automation that is accessible to analysts of any level and GenAI that investigates, surfaces insights and speeds incident response.

How does it work?

Trellix Helix integrates data from security tools (Trellix native controls and 500+ third parties), Data is ingested from multiple sources, then correlated by pre-built analytics and rules to create detections inclusive of threat events across multiple tools (endpoint, network, email, cloud, and data) and across vendors. Events are prioritized by severity with 50% to 70% of false positives already removed. Built-in automation also removes routine threats and performs tasks like data enrichment, device containment, disabling users, and creating incidents for ticketing systems.

Trellix Wise™ then investigates every alert automatically, triaging them and prioritizing the most important alerts. This is hours of work done in minutes and alerts are enriched with Generative AI-created context and recommendations for incident responders.

AI helps users of any experience level perform investigations, threat hunting, and incident response. Several automation playbooks are included that have been built by analysts, for analysts, to further increase efficiency. Continuous machine learning, monitoring, and insights from the Trellix Advanced Research Center team ensure that the newest attack vectors, behaviors, and recommended changes are just a click away.

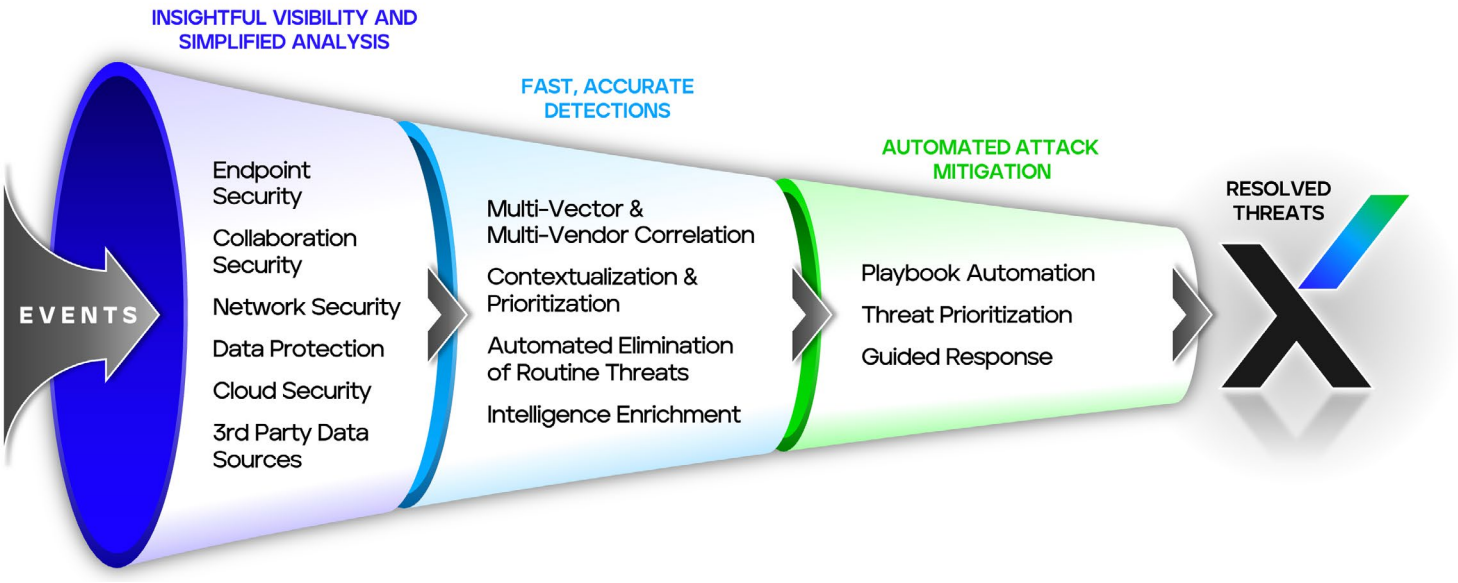

Figure 1: Data is ingested, correlated, and contextualized with threat intelligence. GenAI automatically triages and prioritizes alerts. AI and built-in playbooks perform automation and guide users. An integrated analyst experience reduces manual pivots and streamlines processes.

What makes Helix unique?

- **Depth of integrations:** We meet you where you are with 500+ integrations across 230 vendors to use more of the data you already own.
- **Out-of-the-box multi-vector detections:** Data is ingested in real time with over 2,000 rules and 50 analytics creating context without the need for months of detection engineering.
- **GenAI alert triage:** Investigate 100% of alerts, prioritize threats and get updates as related events are investigated.
- **No-code hyperautomation:** A drag-and-drop workflow builder lets analysts build automation easily without the need for coding expertise.
- **Designed for unique environments:** Deploy and manage based on your environment's requirements with support for cloud, hybrid and air-gapped environments.

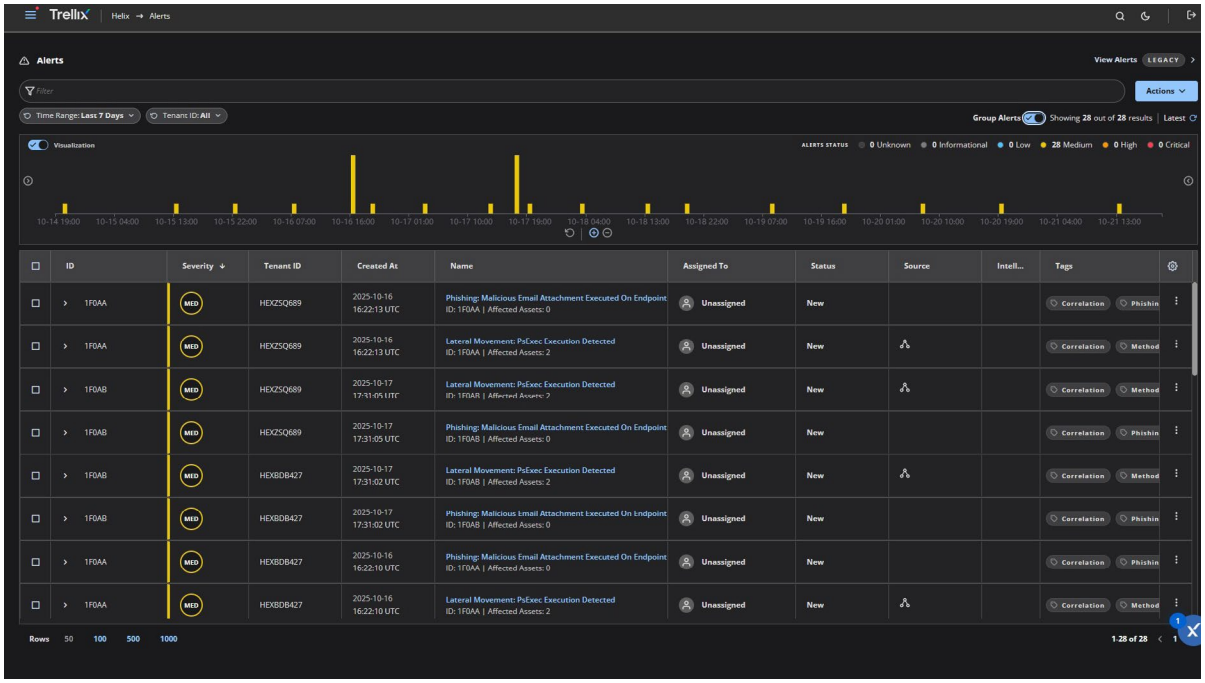

Figure 2: The Alerts area shows you a summary, status, the source and severity of events. Click to view the timeline, investigate, and take recommended actions.

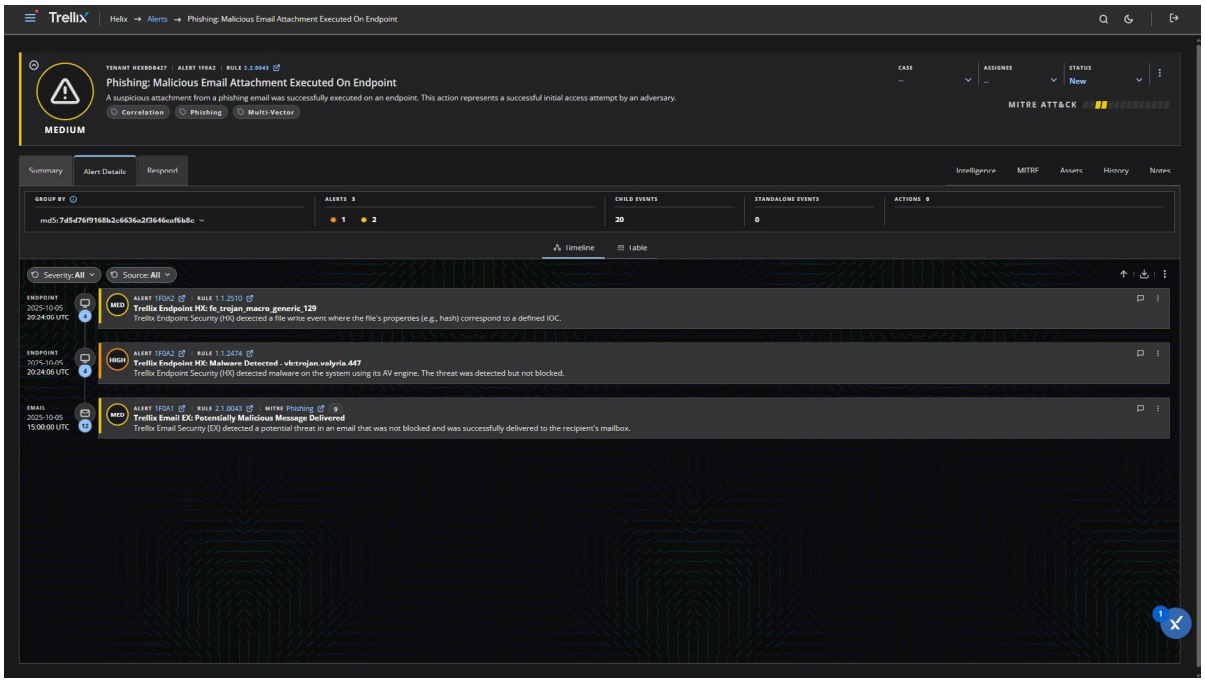

Figure 3: Helix shows multiple alerts associated with a threat correlation at a glance.

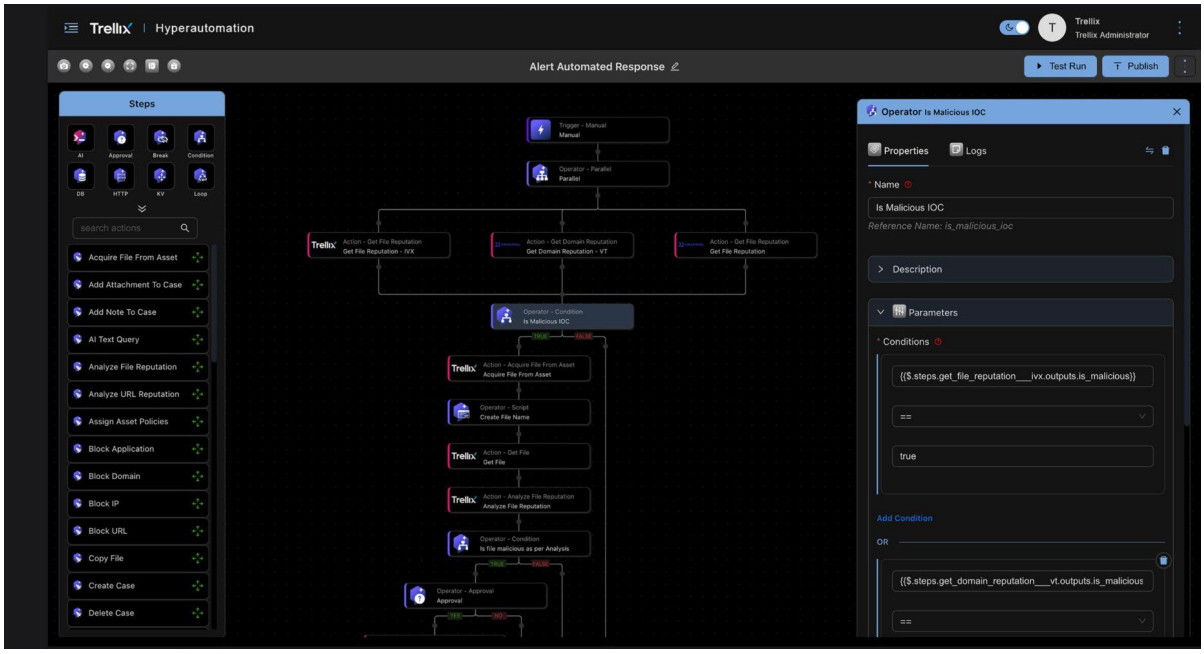

Figure 4: Trellix Hyperautomation is available with Helix and offers no-code automation for virtually any solution that offers an API.

What can Helix do for your business?

- **Speed your MTTD, MTTR:** Thanks to our deep analytics, AI, and user-friendly experience, the average time spent investigating threats and taking response actions is under 10 minutes. Your team can also eliminate pivots across point tools to boost efficiency by 20%!
- **Make your Security teams more efficient:** False positives waste a lot of time. We halt 50% to 70% of them before they arrive and prioritize the alerts that matter by severity, saving you hours or days.
- **Recover time for more critical tasks:** GenAI alert triage recovers 8 hours of work for every 100 alerts investigated, and no-code hyperautomation helps you automate entire workflows.
- **Close security talent and skills gaps:** With more pre-built playbooks than competing solutions and the ability to customize them to your needs, Helix can help you upskill less experienced analysts. They can click through correlation details, leverage guided investigations, and be led through best practices to perform data enrichment or remediation steps, improving their expertise.

Ready to learn more about Helix? Request a Demo.