Trellix

SOLUTION BRIEF

Trellix Helix Connect

Multi-vendor/vector detections with AI-guided investigation and 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**

Point solutions and multiple collections of tools make detection and response lengthy, manual processes that allow threat actors to go undetected. Extended Detection and Response (XDR) solutions integrate data from multiple sources, analyzing it to deliver context for faster incident detection and response. But not all solutions offer the same level of context.

When you are evaluating a solution for your business it is important to understand how well a product performs integrations and analysis, and leverages data (whether from the vendor's technologies or from third parties). The ability to unlock the data you already own, as well as the data in the vendor's tools is the measure of how well a solution creates the "X" in XDR.

How does it work?

Trellix Helix Connect integrates data from security tools (Trellix native controls and 490+ third parties) to tell you the complete story of an attack. Data is ingested from multiple sources, then correlated by pre-built analytics and rules to create multi-vector, multi-vendor detections. New detections surface within hours of being deployed and 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 and hundreds more third-party components.

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.

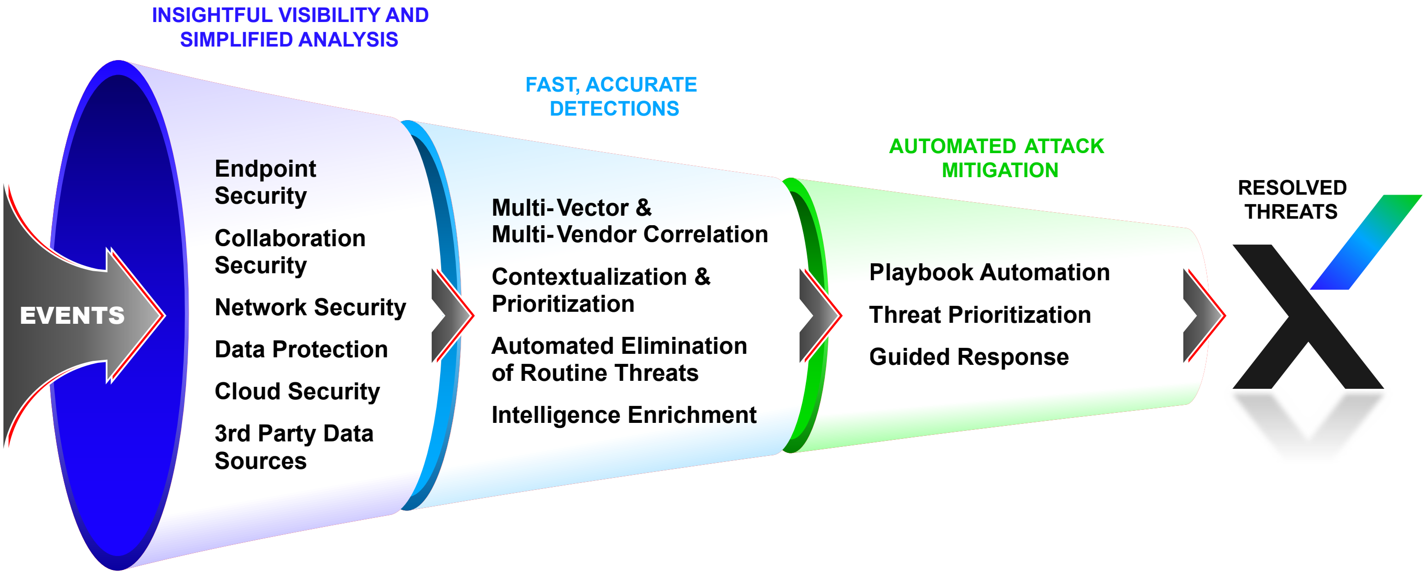
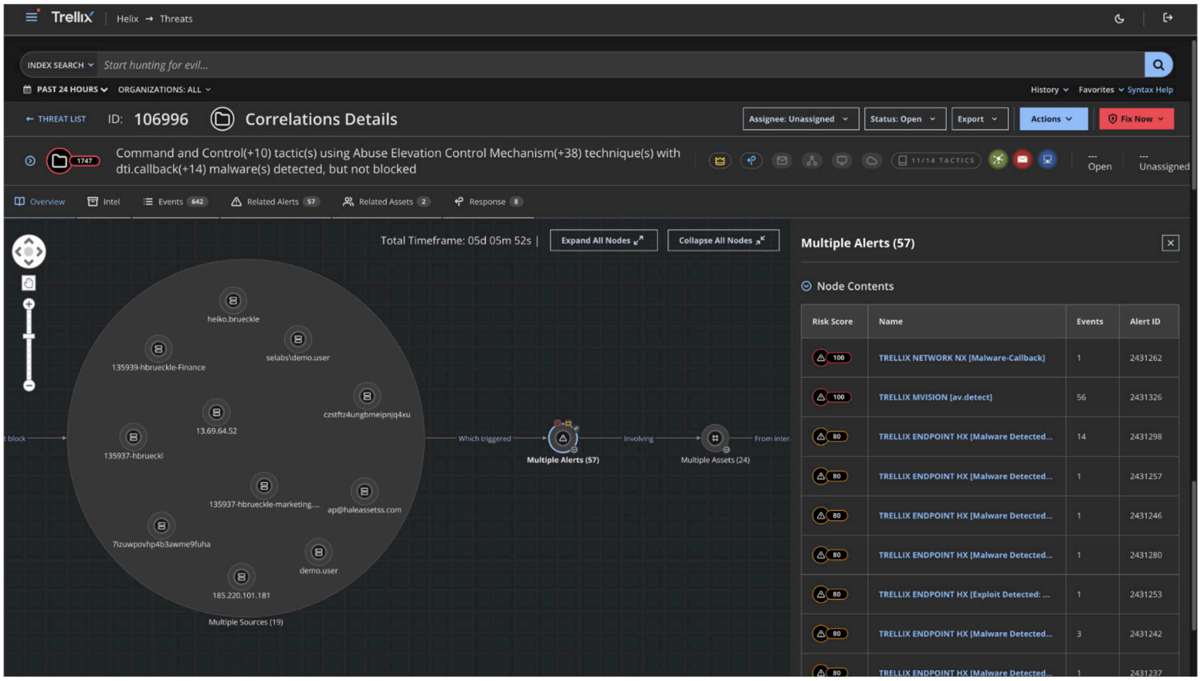

INSIGHTFUL VISIBILITY AND SIMPLIFIED ANALYSIS
FAST, ACCURATE DETECTIONS
AUTOMATED ATTACK MITIGATION
RESOLVED THREATS
EVENTS
Endpoint Security
Collaboration Security
Network Security
Data Protection
Cloud Security
3rd Party Data Sources
Multi-Vector & Multi-Vendor Correlation
Contextualization & Prioritization
Automated Elimination of Routine Threats
Intelligence Enrichment
Playbook Automation
Threat Prioritization
Guided Response

Figure 1: Data is ingested, correlated, and contextualized with threat intelligence. Built-in playbooks provide an integrated analyst experience with automated remediation.

What makes Helix Connect unique?

- **Depth of integrations:** We meet you where you are with 490+ integrations across 230 vendors to use more of the data you already own.
- **Out-of-the-box 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.
- **No disruptive requirements:** Helix Connect is open, with no native control requirements, allowing you to use and get more value from your existing tools or the Trellix XDR Platform.
- **Orchestration and automation for every analyst:** Helix Connect comes equipped to orchestrate and deliver automation across 250 third-party components. Augment your SIEM and enable more of your team to investigate threats with AI guidance and UI-driven, point and click automation.
- **Consolidated view of security in your environment:** Reduce manual pivots by using a unified analyst experience and spend 90% less time on non-response activities.



Trellix | Helix → Threats

INDEX SEARCH Start hunting for evil...

PAST 24 HOURS ORGANIZATIONS: ALL History Favorites Syntax Help

← THREAT LIST ID: 106996 Correlations Details

Assignee: Unassigned | Status: Open | Export | Actions | Fix Now

1747 Command and Control(+10) tactic(s) using Abuse Elevation Control Mechanism(+38) technique(s) with dti.callback(+14) malware(s) detected, but not blocked

11/14 TACTICS --- Open --- Unassigned

Overview | Intel | Events 642 | Related Alerts 57 | Related Assets 2 | Response 8

Total Timeframe: 05d 05m 52s | Expand All Nodes | Collapse All Nodes

Multiple Alerts (57)

Node Contents

Risk Score	Name	Events	Alert ID
100	TRELLIX NETWORK NX [Malware-Callback]	1	2431262
100	TRELLIX MVISION [av.detect]	56	2431326
80	TRELLIX ENDPOINT HX [Malware Detected...	14	2431298
80	TRELLIX ENDPOINT HX [Malware Detected...	1	2431257
80	TRELLIX ENDPOINT HX [Malware Detected...	1	2431246
80	TRELLIX ENDPOINT HX [Malware Detected...	1	2431280
80	TRELLIX ENDPOINT HX [Exploit Detected: ...	1	2431253
80	TRELLIX ENDPOINT HX [Malware Detected...	3	2431242
80	TRELLIX ENDPOINT HX [Malware Detected...	1	2431237

Figure 2: Helix Connect shows multiple alerts associated with a threat correlation at a glance.

What can Helix Connect 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.
- **Close security talent and skills gaps:** With more pre-built playbooks than competing solutions and the ability to customize them to your needs, Helix Connect 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.
- **Rapid time to value:** Helix Connect is ready out of the box and is deployed in under a week. Customers begin surfacing previously missed detections and new insights with a couple of hours of deployment. Competing solutions require weeks or months of detection engineering, integration work, or product replacements to use their XDR product. Helix Connect meets you where you are and is open and ready for any platform or environment, from cloud to on-premises or air-gapped environments.

Ready to learn more about Helix Connect? [Request a Demo.]