Trellix

SOLUTION BRIEF

Trellix Wise: GenAI for your biggest security operations challenges

Key Features

End alert fatigue
Wise automatically investigates all your alerts, raising the most important to the top with automatic escalations and alert scoring.

Make the right decisions, faster
Detect threats others miss, including those leveraging AI, with deep, automated EDR investigations across 1.5 petabytes of threat intelligence data and multi-vector controls.

Close security talent gaps
Make GenAI content creation accessible to everyone with everyday language while upskilling teams with prompts built on a decade of real-world expertise.

Prove ROI rapidly
Keep track of the hours Wise has saved and easily demonstrate increases in efficacy and efficiency with built-in reporting and dashboards. Recover 8 hours of SOC work for every 100 alerts Wise investigates, enabling you to go from response to prevention and keep more threats out.

The same problems seem to face security teams every year — missed threats, growing alert volumes, and talent gaps. These only increase as data continues to explode, security jobs remain unfilled, and collections of point tools fail to detect sophisticated threats before business impacts occur.

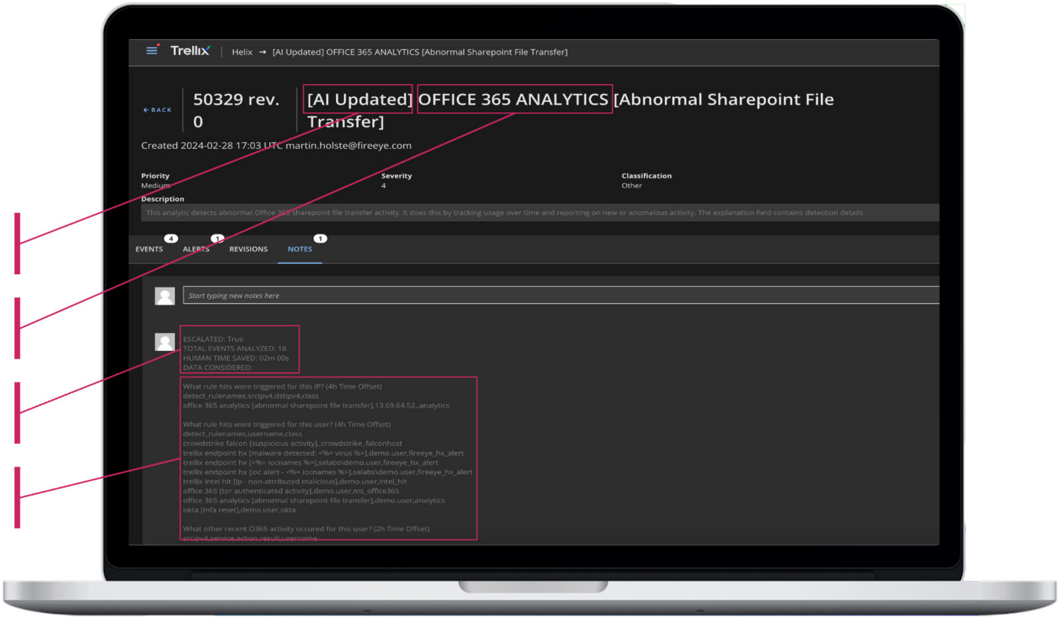
Those problems finally have an answer with Trellix Wise. Trellix Wise helps customers transform their security operations through **analytics, AI, and automation.** With Wise, teams can automatically investigate **all** of their data, eliminate false positives, automate remediation, and use conversational AI to perform threat hunting no matter their current level of expertise.

Never miss an alert again

Most security staff only look at about 10% of alerts due to the large volumes generated by their security tools and high volumes of false positives. With Trellix Wise, we finally have an answer to alert fatigue. Wise automatically investigates every alert, using the full context of your data to decide when teams need to take action. Instead of being overwhelmed by alert volumes, teams now have opportunities to dig deep and find advanced AI-enabled attacks. Wise is built on over a decade of AI modeling and 25 years in analytics and machine learning.

Deep dive into data with AI-powered investigations

Once an incident is identified, Trellix Wise will automatically call upon our rich endpoint detection and response (EDR) data. Leveraging 33 machine learning (ML) models across Endpoint, Email, Network, and Sandbox products, Wise makes decisions and surfaces detailed explanations for security teams.   Alert scores are raised so analysts see and prioritize them properly. This is hours of work typically done by 3 to 5 people, delivered in seconds!



Auto-investigates every alert

Leverages our integrations + ML AI for detection

Makes decisions and records stats on time saved

Provides detailed explanation of decision

Trellix
Helix → [AI Updated] OFFICE 365 ANALYTICS [Abnormal Sharepoint File Transfer]
← BACK
EVENTS 4
ALERTS 1
REVISIONS
NOTES 1
Start typing new notes here

50329 rev. 0 | [AI Updated] OFFICE 365 ANALYTICS [Abnormal Sharepoint File Transfer]

Created 2024-02-28 17:03 UTC martin.holste@fireeye.com

Priority: Medium
Severity: 4
Classification: Other

Description: This analytic detects abnormal Office 365 sharepoint file transfer activity. It does this by tracking usage over time and reporting on new or anomalous activity. The explanation field contains detection details.

```
ESCALATED: True
TOTAL EVENTS ANALYZED: 18
HUMAN TIME SAVED: 02m 00s
DATA CONSIDERED:

What rule hits were triggered for this IP? (4h Time Offset)
detect_rulenames,srcipv4,dstipv4,class
office 365 analytics [abnormal sharepoint file transfer],13.69.64.52,,analytics

What rule hits were triggered for this user? (4h Time Offset)
detect_rulenames,username,class
crowdstrike falcon [suspicious activity],,crowdstrike_falconhost
trellix endpoint hx [malware detected: <%= virus %>],demo.user,fireeye_hx_alert
trellix endpoint hx [<%= iocnames %>],selabs\demo.user,fireeye_hx_alert
trellix endpoint hx [ioc alert - <%= iocnames %>],selabs\demo.user,fireeye_hx_alert
trellix intel hit [ip - non-attributed malicious],demo.user,intel_hit
office 365 [tor authenticated activity],demo.user,ms_office365
office 365 analytics [abnormal sharepoint file transfer],demo.user,analytics
okta [mfa reset],demo.user,okta

What other recent O365 activity occured for this user? (2h Time Offset)
srcipv4,service,action,result,username
```

Fig 1: Trellix Wise uses built in Machine Learning, AI, and GenAI to make decisions in seconds.

The Trellix Wise Difference

- 3x the number of third-party integrations offered by competing solutions to apply GenAI value to more of the environment and find advanced threats with complex kill chains.
- Auto-triage of threats leveraging a large data ecosystem with 1.5 petabytes of telemetry data to make the right decisions with the right data.
- Real-time/real-world operational threat intelligence using 60 billion queries a day on malicious activity from 660 million endpoints.

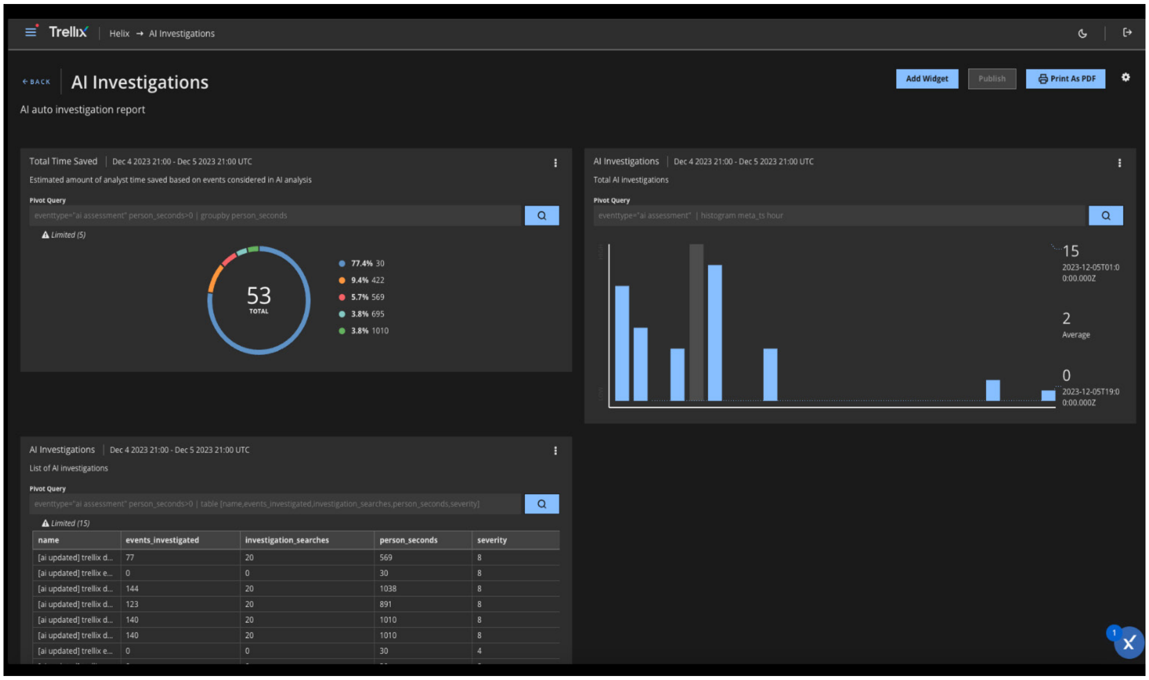
Make threat hunting accessible and upskill your staff

Threat hunting and setting up automated actions are no longer dependent on acquiring highly skilled analysts. With Trellix Wise, users of any level can interact, create automation, and hunt for threats using common language queries. This can be almost anything like “only escalate alerts from Sales on Fridays” or “always escalate alerts if an asset is public facing and there have been more than 10 failed login attempts.”

As Trellix Wise performs analysis it offers details on what it finds and remediation actions to take so even the least experienced team member can investigate, respond, and learn on-the-job threat hunting.

Prove value rapidly

It can be hard to know how rapidly or how much return you are getting from any given security investment. Trellix Wise keeps track of the time it is saving so you can view within the user interface or report to leadership teams gains in efficiency and effectiveness. You can see the total time saved by AI, the number of events, and the speed and severity of investigations in graphical and list format reports.



AI Investigations

AI auto investigation report

Total Time Saved | Dec 4 2023 21:00 - Dec 5 2023 21:00 UTC

Estimated amount of analyst time saved based on events considered in AI analysis

Pivot Query: eventtype="ai assessment" person_seconds>0 | groupby person_seconds

Limited (5)

AI Investigations | Dec 4 2023 21:00 - Dec 5 2023 21:00 UTC

Total AI investigations

Pivot Query: eventtype="ai assessment" | histogram meta_ts hour

AI Investigations | Dec 4 2023 21:00 - Dec 5 2023 21:00 UTC

List of AI investigations

Pivot Query: eventtype="ai assessment" person_seconds>0 | table [name,events_investigated,investigation_searches,person_seconds,severity]

Limited (15)

name	events_investigated	investigation_searches	person_seconds	severity
[ai updated] trellix d...	77	20	569	8
[ai updated] trellix e...	0	0	30	8
[ai updated] trellix d...	144	20	1038	8
[ai updated] trellix d...	123	20	891	8
[ai updated] trellix d...	140	20	1010	8
[ai updated] trellix d...	140	20	1010	8
[ai updated] trellix e...	0	0	30	4

Fig 2: Trellix Wise keeps track of the time it saves you and displays it graphically in our UI.

Solve today's biggest security challenges with Trellix Wise

Don't put off changes that can make a real impact to your efficacy, efficiency and make better use of your current resources. Trellix Wise connects hundreds of security tools and can be implemented in on-premises, air-gapped and cloud environments. With Trellix Wise, your organization can finally solve some of your most common challenges:

- **Automatic alert investigation in <3mins:** Ensure all alerts are triaged, scoped and assessed in **<3mins.**
- **Decrease MTTD:** Triage, scope and **investigate 90% more alerts, saving the work of 5 analysts/day.**
- **Improve MTTI:** Automated incident containment and streamlining investigations, summarizing events with risk scores and recommendations.
- **Improve MTTR by up to 300%:** Using AI-powered responses that reduce risk to your organization with faster, accurate responses.
- **Leverage current resources better:** With automated and accelerated workflows, security content creation, and natural language AI interactions.

Learn more about Trellix Wise at trellix.com/platform/wise/.