Trellix

WHITE PAPER

Trellix Wise™: Bridging the Gap to the Agentic SOC

The road to true automation through a federated intelligence layer

Traversing the "Darien Gap" of security operations
In modern cybersecurity, you face a digital "Darien Gap"—a dense, impenetrable jungle between detection and remediation. On one side you have massive detection capabilities from fragmented vendors and on the other, a desire for remediation. But in between lies a jungle of "medium" and "low" alerts where sophisticated threat actors hide.

The reality: Human scaling has failed
Historically, organizations have ignored 90% of detections because they couldn't hire enough analysts to bridge this gap. Today, as adversaries use AI to automate attacks, ignoring the noise is no longer an option, but manual scaling is impossible.

Trellix Wise: The road to true automation
Trellix Wise is the GenAI-powered infrastructure that finally connects detection to remediation. It is the road through the jungle. Unlike legacy tools that require a rip and replace of your security stack, Trellix Wise is designed as a universal, **vendor-agnostic** infrastructure that snaps on top of your existing environment. Trellix Wise functions as the brain that queries your disparate security data without moving it, ensuring your data stays in your environment.

A federated engine

Federated data query sources
Trellix Wise doesn't just ingest data; it operationalizes it via real-time queries across your entire stack. It breaks down silos between:

- **Trellix Helix (or another SIEM):** Serving as the primary alert and detection source.
- **Splunk Enterprise / Cloud:** Turning security indexes and notable events into actionable findings.
- **OpenSearch / Elasticsearch:** Leveraging SIEM alerts and threat intelligence domains.
- **Other Data Sources:** Custom integrations that extend the "Agentic" reach to any environment.

AI-powered alert analysis

Trellix Wise uses intelligent auto-discovery to identify security indexes and field mappings automatically. It executes Level 3 investigations by generating and correlating queries across all sources:

- **Dynamic investigation:** It asks—and answers—the deep questions: *What were recent logins from this IP? What other rules fired for this source? Is this user traveling? What did they do after the password reset? Is this a known admin tool?*
- **Operationalize static intelligence:** Threat intelligence reports are usually static news that gather dust. Trellix Wise transforms our premier, customer-specific SecondSight threat hunting service into proactive live security controls. It looks beyond single malicious PowerShell commands and really understands the handwriting of an adversary, identifying the specific, unique order of PowerShell arguments and execution steps used by a threat actor.
- **From regex to GenAI pattern matching:** The era of writing hyper-specific regular expression (regex) rules and managing "silent" machine learning (ML) detections is over. These legacy methods are brittle, high maintenance, and prone to false positives. Trellix Wise uses GenAI to match complex behavioral patterns against known adversary TTPs instantly. By moving to pattern-based matching, your SOC analysts stop being rule-writers and start being strategic investigators.

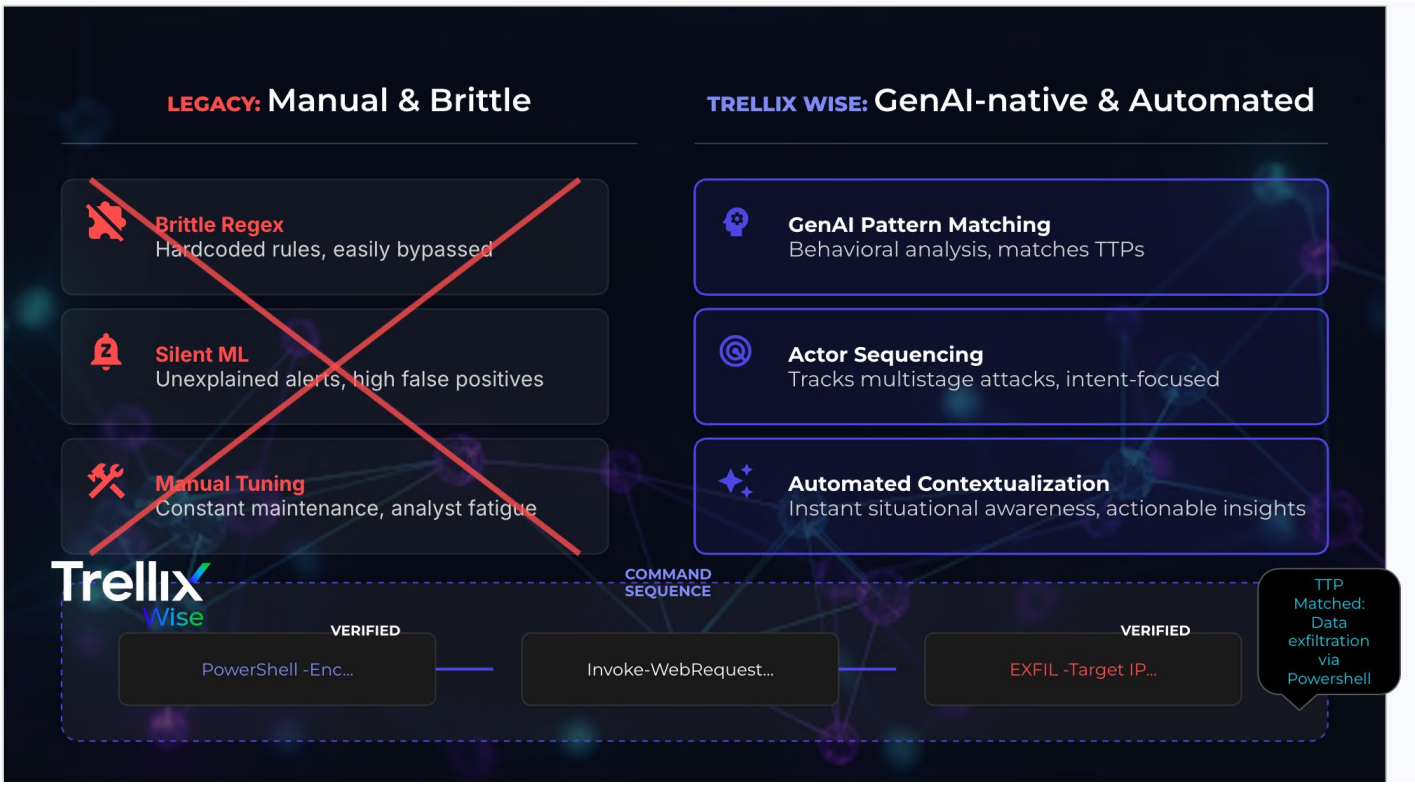

Figure 1: Trellix Wise helps you make the move to proactive, automated, contextualized, detection and response.

From verdict to automated action

GenAI confidence: The key to "auto-pilot"

A SOC can automate only what it trusts, and trust requires context. Every data source you add to Trellix Wise increases the confidence score. By correlating *"What happened," "Who was affected," "Is this expected," "Have I seen this before,"* and *"What should I do,"* Trellix Wise builds a confidence matrix that shatters the confidence ceiling of siloed tools, reaching the threshold required for "auto-pilot" remediation.

Figure 2: Confidence growth through multi-vendor aggregation.

Automated response actions

Once a verdict on an alert is reached (true positive vs. false positive), Trellix Wise triggers specialized response workflows:

- **Helix case management:** Auto-creates cases with full investigation timelines and enriched notes.
- **Hyperautomation (SOAR):** Executes playbooks to contain endpoints, block IOCs, or run custom automated tasks.
- **Webhook integration queues:** Routes verdicts to specialized teams—network queue (firewall/proxy), desktop queue (endpoint response), or IAM queue (identity/disable accounts)—via Jira, ServiceNow, or Slack.

Figure 3: Trellix Wise reads multi-source security data from its native location to provide automated analysis, high-fidelity verdicts, and intelligent response orchestration.

Proven business ROI

- **Recover 8 Hours:** For every 100 alerts Trellix Wise investigates, a SOC recovers 8 hours of manual labor.
- **Faster MTTR:** Reduce the risk to the organization by closing the loop on threats in minutes, not days.
- **Scale without headcount:** Empower junior analysts to perform like Tier 3 experts with guided, natural language frameworks.
- **Transparency by design:** Trellix Wise "shows its work," providing a full evidence trail so your team can audit every GenAI decision

Trellix Wise works across on-premises, air-gapped, and cloud environments. Start operationalizing your intelligence today.

Build the road to automation with Trellix Wise.