Transform your security operations with embedded generative AI

Public sector security teams face a common problem: most security staff only review about 10% of security alerts according to Trellix's internal research, leaving critical threats buried in the noise.

Even after investing in comprehensive tools, many organizations simply lack the staff to investigate every potential threat. This problem of "too much data" creates dangerous blind spots, where early signs of a breach hide in plain sight among thousands of uninvestigated low-level alerts.

Trellix, powered by Amazon Web Services (AWS), addresses this gap by embedding generative artificial intelligence (AI) directly into security operations. Trellix Wise, the company's AI engine, automatically reviews all security alerts, analyzes real-time security data across systems to understand context, and takes the right actions. This helps public sector teams adopt generative AI quickly, investigate threats up to three times faster, and improve security operations without needing more staff.

Why Trellix for public sector security?

Broad integrated visibility

Trellix provides comprehensive platform coverage across email, network, and endpoint security, all connected through next-generation security information and event management. This gives Trellix's AI security platform a complete picture of the security environment.

Works within existing workflows

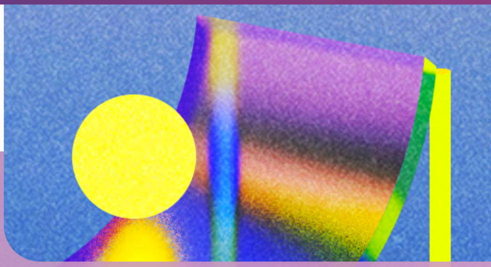
Trellix integrates with your current tools and processes, enhancing operations without retraining staff or changing systems. Analysts can also use natural language to investigate threats and act faster—no advanced expertise required.

Agentic AI that alerts—and then acts

Trellix's AI goes beyond simply flagging issues. When investigating a threat, it can automatically create tickets across systems to deactivate compromised accounts, quarantine devices, and implement network blocks, all within established security team workflows.

Multi-environment support

Trellix supports both cloud and on-premises deployments, including FedRAMP High environments and air-gapped networks, placing appropriate AI capabilities where they're needed while maintaining strict security boundaries.



Trellix *at a glance*

8 hours of security analyst work saved
per 100 alerts with automated investigation and remediation

Equivalent of a 10-person security analyst team
for organizations with 1,000 daily alerts—without the extra headcount

Improve alert response times by up to 300%
with automated context-based escalation

Automatic alert investigation in under 3 minutes
so all alerts are analyzed, scoped, and closed or escalated as necessary

Is Trellix right for my organization?

Ask yourself these key questions to determine if your teams would benefit from Trellix's AI-embedded security solutions:

1 **Do you investigate all of your security alerts, or only the critical ones?** If not, which alerts have you turned off due to alert noise? Security tools generate alerts for a reason: they're designed to detect potential threats. Turning them off or ignoring them compromises your security posture.

2 **Is your team spending time reformatting data rather than making security decisions?** The real value of AI isn't in summarizing information; it's in making intelligent decisions that save analyst time and improve security outcomes.

3 **Have you integrated your security tools across different data sources?** If your security tools can't easily access data from various systems (cloud, on-prem, third-party), you're limiting visibility. Trellix excels at connecting to existing data sources without requiring data duplication.

4 **Do you need to adopt AI quickly without disrupting existing systems?** Trellix embeds AI into your current workflows with minimal lift: no retraining, no replatforming, no complex customization. Most organizations can start seeing process improvements in days instead of months. Trellix Wise even keeps track of the time it saves your teams to prove AI value rapidly.

> *"Trellix Wise is the security Roomba: quietly, enthusiastically cleaning up while you focus on more important work."*
>
> *– Martin Holste, chief technology officer (CTO) for cloud and generative AI, Trellix*

How AWS powers Trellix's AI platform

Optimized for scale and security
Trellix runs entirely on AWS to leverage best-in-class security features and scalability, including for FedRAMP High and hybrid systems.

Cost-effective and performant AI
With the flexibility of Amazon Bedrock, Trellix combines multiple AI models to select the best model for every task—balancing speed, complexity, and cost to support every customer need.

Built-in auditability
With native AWS security and logging tools and Trellix's own observability layers, all AI actions are trackable, helping organizations stay secure and compliant.

Moving forward with embedded AI

Public sector organizations don't need to reinvent their security strategy to benefit from generative AI. The most effective solutions are the ones that work quietly in the background while your staff addresses high priority needs.

Trellix CTO Martin Holste recommends leaders begin their embedded generative AI journey by asking: "Can AI do this for me?" This simple shift reframes how teams approach security tasks, freeing staff to focus on high-value work while AI handles the backlog.

To get started:

- ✓ Identify alert categories you've deprioritized due to noise or staffing constraints.
- ✓ Build guardrails on your AI solutions with identity-based access controls to ensure user data privileges and actions are appropriate, but avoid over-restricting how much data your AI solutions themselves can access.
- ✓ Audit your investigation workflows, particularly where handoffs and repetitive tasks frequently delay timely responses. Consider where AI can apply intelligent automation to remove obstacles and keep processes moving.
- ✓ Pilot embedded AI in one system and measure how it performs to build confidence. Track key performance indicators like time saved for your staff to investigate the same number of alerts, automatic escalations rates, and the scope of visibility you gain across your organization.

Embedded AI tools like Trellix Wise work best when they support the workflows you already rely on. As you explore AI adoption, look for tools that already fit your mission needs and processes to deliver generative AI benefits fast.

aws | Trellix

Explore how Trellix helps public sector organizations accelerate key productivity functions and improve protection with embedded AI tools.

Learn how Trellix Wise can address your biggest security challenges and discover why Trellix and AWS are better together →