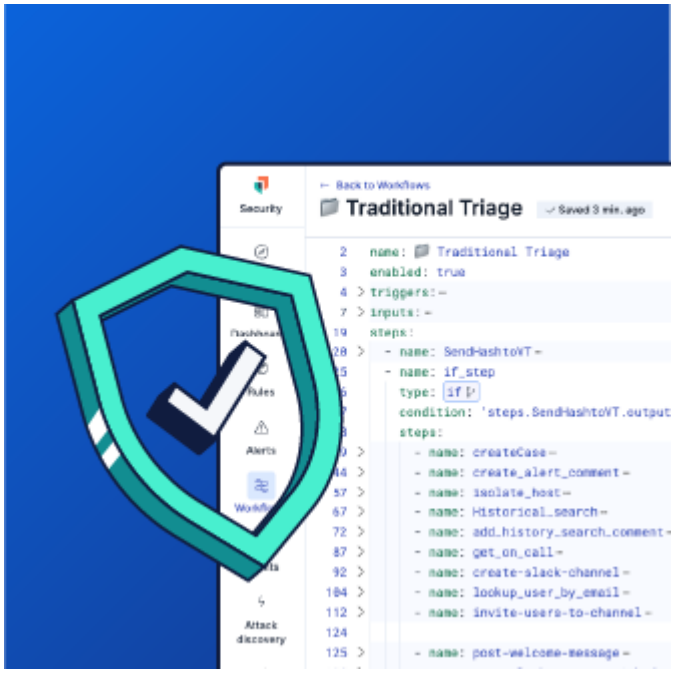
Agentic security operations from Elastic Security

Archived: 2026-04-05 18:26:16 UTC

Built to secure, not to tax. Move on from a security industry built to sell: per-endpoint fees, rehydration penalties, and endless add-ons. Try the only agentic security operations platform that includes everything you need to prevent threats.

- 

Elastic Workflows

End the automation tax. Built-in playbooks and AI reasoning shut down threats faster. No SOAR required.

Explore Workflows

Analyze critical context and stop attacks instantly with a single platform that includes world-class XDR with your SIEM.

- **Cloud security**

  Address threats and vulnerabilities across your multi-cloud environments (AWS, Azure, and Google Cloud) — with one UI and zero agents. Go beyond CDR by correlating across domains and keeping data ready for analysis.

- **AI for security**

  Automate your triage, investigation, and response workflows with grounded, contextual, and transparent AI. Surface critical threats, analyze user and entity behavior, and empower every analyst. Built-in controls ensure secure, compliant data handling.

PACKAGING OPTIONS

Adopt it all, or go at your own pace

Our agentic security operations platform meets you where you are — and takes you where legacy platforms can't.

- **Elastic Security**

  Everything you need — SIEM, XDR, native automation, and integrated AI — in one platform. No extra SKUs, no bolt-ons, no compromises. Just a single experience built for the way analysts think, hunt, and respond.

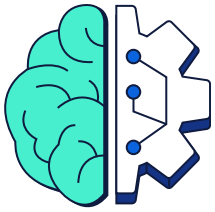
- **Elastic AI SOC Engine (EASE)**

  A package of AI capabilities that allows you to adopt Elastic Security on your schedule, without a full rip-and-replace. Bolster your existing SIEM, XDR, and other alerting tools with AI that plugs into your data and workflows — and expand to the full platform when you're ready.

DIFFERENTIATORS

Built different — for defenders

Elastic adapts to your data, your environment, and your budget. Run on any combination of cloud or on-prem systems, including on AWS, GCP, and Azure.



GENERATIVE AI & ML

Context is the multiplier

Elastic brings AI into the SOC with machine learning (ML) and GenAI that aid in threat detection, triage, and investigation by adding context from your environment — and showing you the logic, the source, and the path behind every decision.

OPEN DETECTION RULES

Transparency you can trust

Backed by an active community, all detection rules are open source and reviewed by Elastic to ensure full transparency and trust. Inspect, use, and customize with confidence — 2.3K GitHub stars and counting.

OPEN SOURCE PLATFORM

Open and extensible

Enterprise-grade, community hardened, and built on open source Elasticsearch that's trusted by developers worldwide. Ingest any data, build custom pipelines, and integrate with your tools. Our open architecture gives you full visibility and control.

XDR AT SCALE

Detection that goes the distance

Elastic extends detection across your ecosystem — including third-party endpoints — correlating petabytes of data at real-time speed. Built-in investigative and response tools help you trace events, pivot between related activity, and respond quickly to threats.

FEDERATED SEARCH

We don't defy (data) gravity

Go beyond fragmented data silos with a true data mesh architecture. Cross-cluster search and searchable snapshots enable fast queries across structured and unstructured data, wherever it resides, in the cloud or on-prem, even in low-cost object storage like S3.

COST-EFFECTIVE

Pay for usage, not for features

Affordable open source technology with usage-based pricing, no per user or endpoint fees, and a data lake that decouples storage from compute — so you can retain all the data you need without breaking the bank. No hidden costs, no surprises.

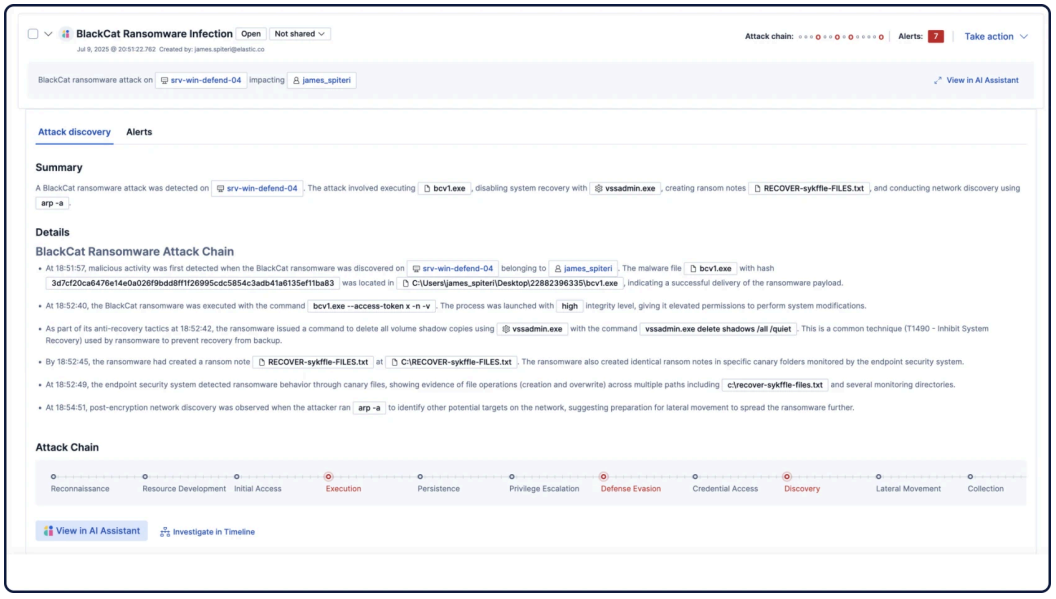
DETECT, INVESTIGATE & RESPOND

From data to answers, at speed and scale

Elastic Security powers the full security operations lifecycle, leaving threats nowhere to hide.

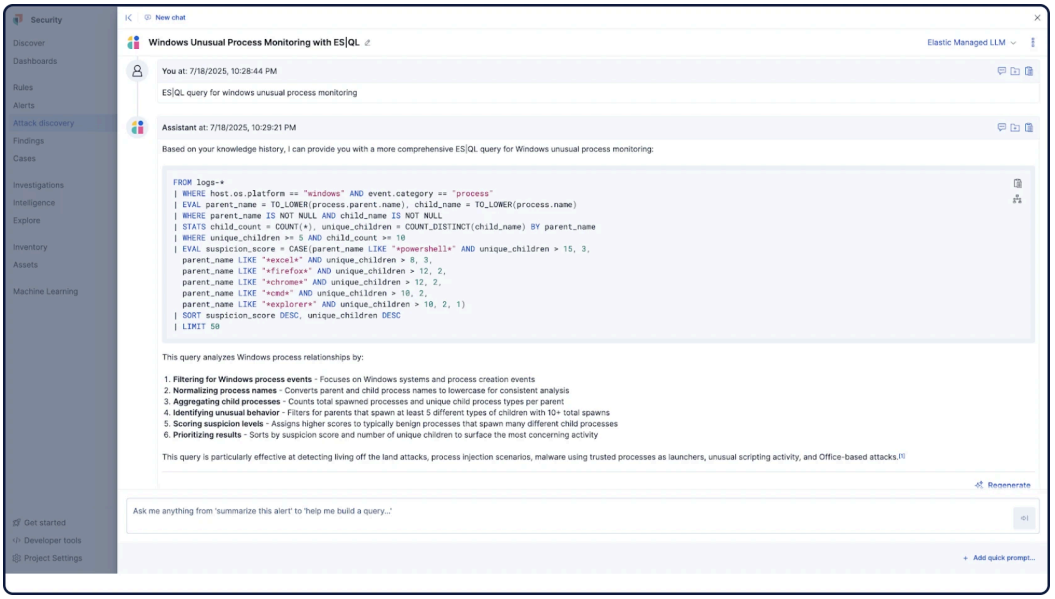
- **Agentic attack discovery**

  Attack Discovery mirrors the way analysts think — correlating alerts, behaviors, and attack paths with retrieval augmented generation (RAG)-based context to automatically surface threats and guide triage and investigation.

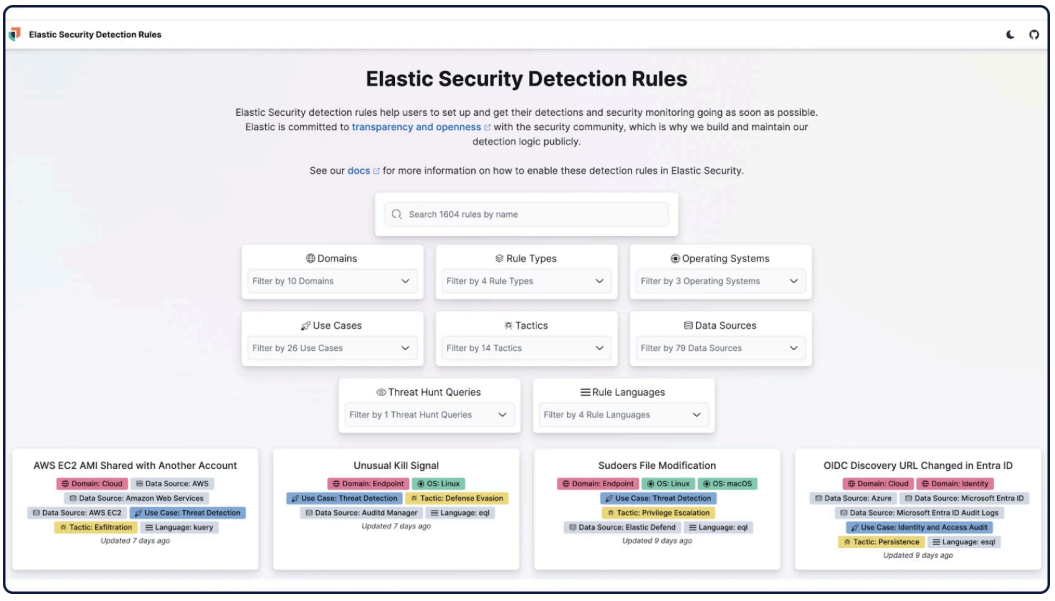


- **Built-in conversational AI**

  Much more than a bolt-on chatbot, Elastic AI Assistant integrates relevant environmental context (e.g., past incidents, response playbooks, backup firewall configurations, and threat research) to summarize, explain, and recommend next steps.

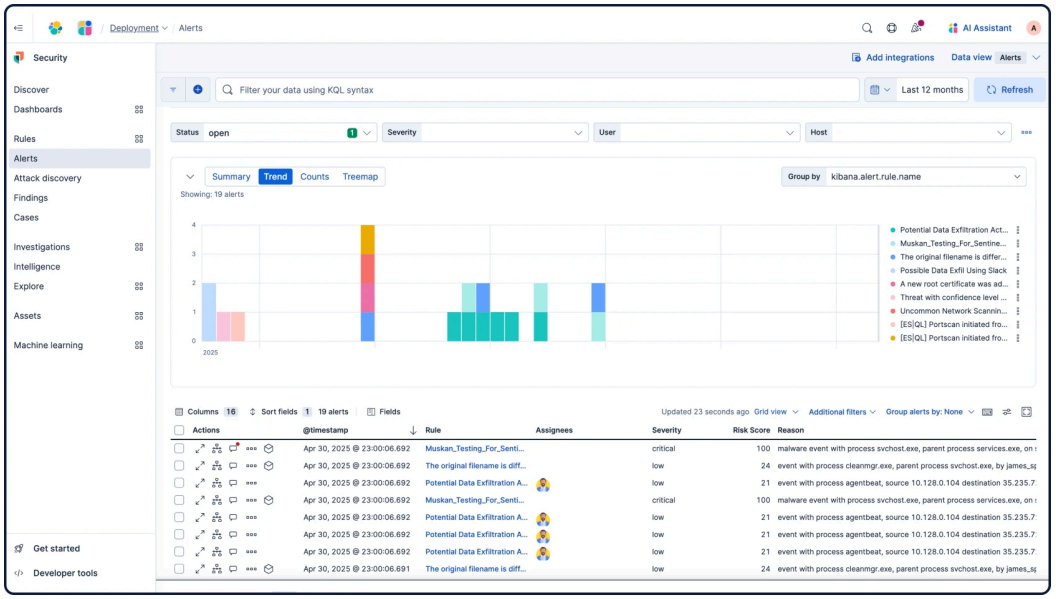


- Activate rules developed by Elastic Security Labs and continuously updated in an open repo. Elastic controls merging, so you get transparency with trust.



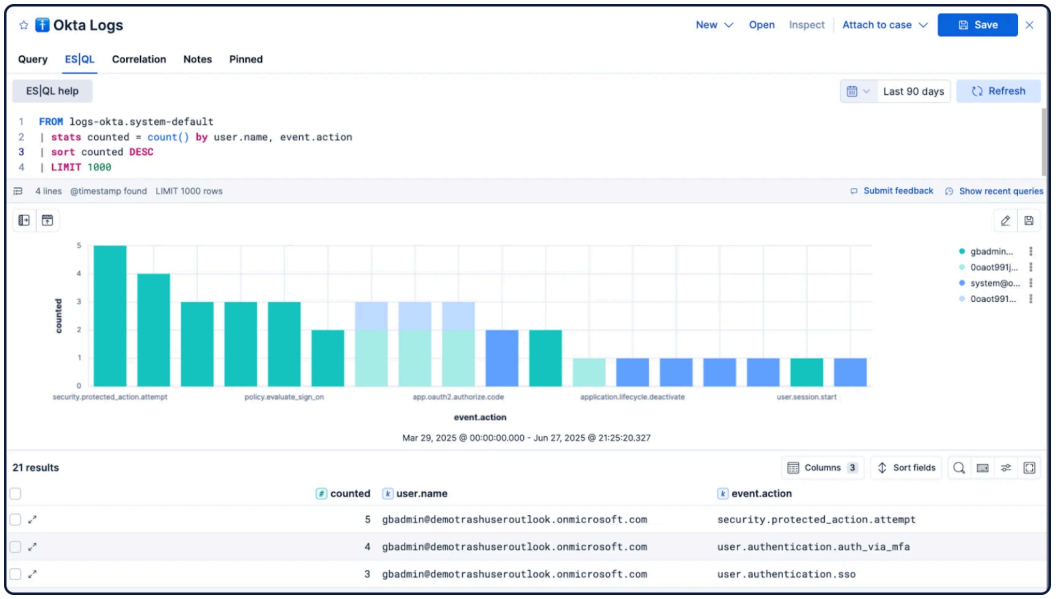
- **Automatic anomaly and threat detection**

  Run machine learning on both real-time and historical data to be alerted to critical anomalies, identity risk, and active threats. Choose from turnkey ML jobs, including UEBA, or easily customize models for your use cases — no PhD needed!



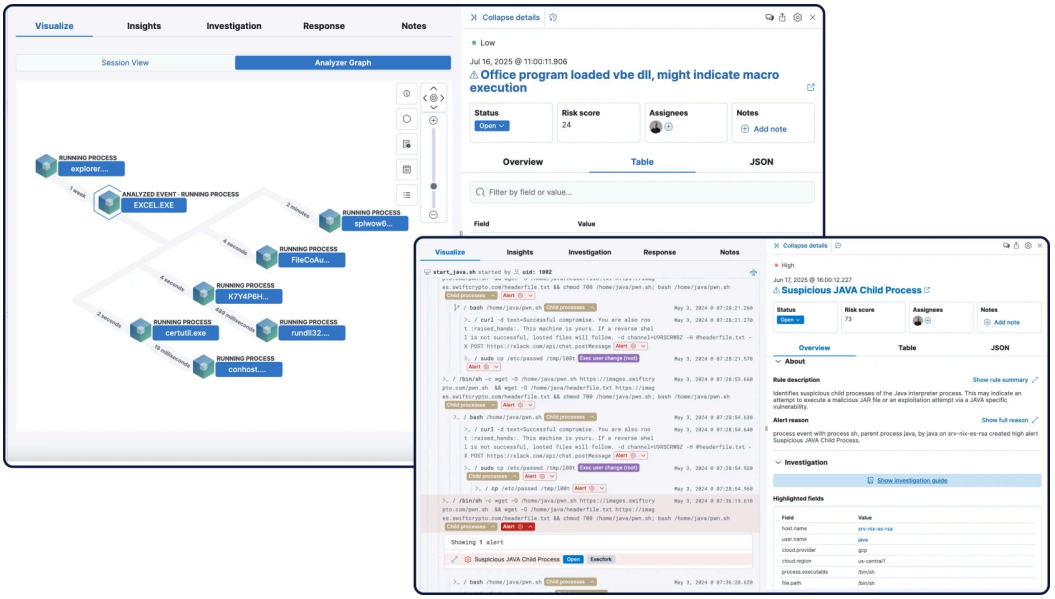
- **Scalable security analytics**

  Elastic handles petabytes of data. Enrich events, uncover connections, and retrace attack paths with fast, flexible ES|QL queries. Pivot instantly and analyze data in place — no backhaul delays or extra cost.



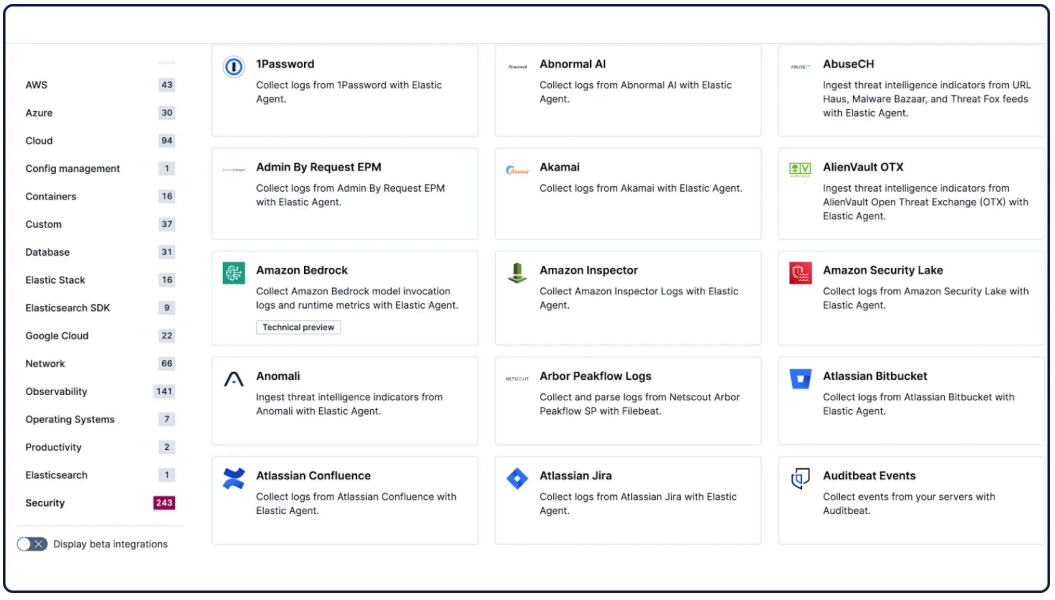
- **XDR: Cloud and endpoint protection**

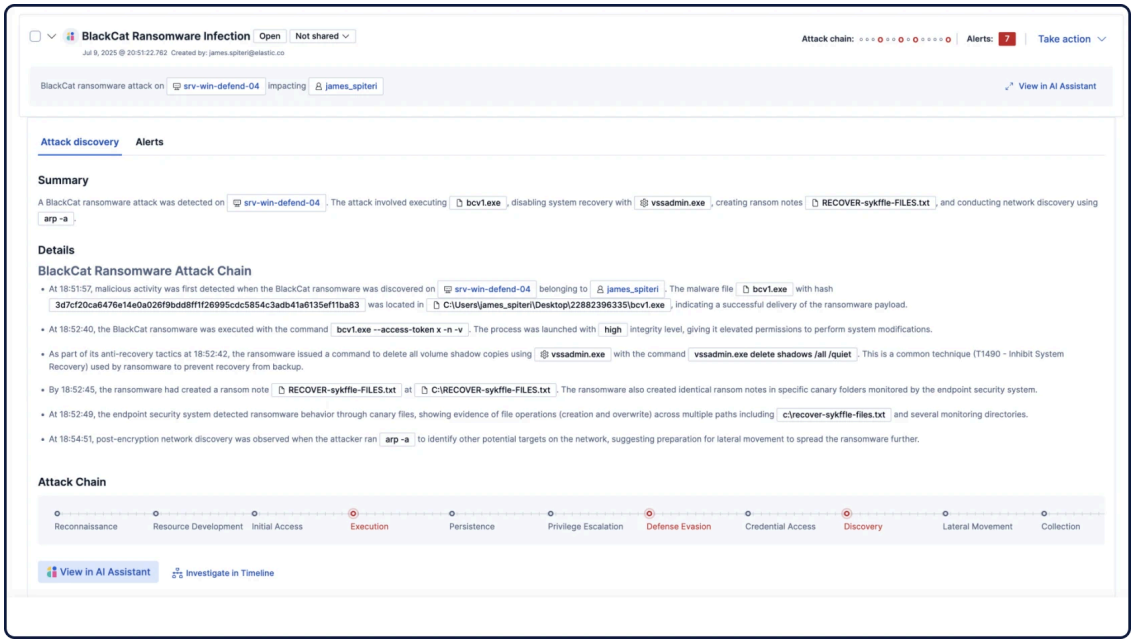
  Prevent ransomware and malware, gather telemetry, and take action with Elastic Agent and third-party endpoint security tools. Gather it all into our SIEM for a unified view of your entire attack surface, including your cloud infrastructure.



- **Hundreds of prebuilt integrations**

  Parsing is our job. Stopping threats is yours. Get immediate visibility into security-relevant data across your environment with our prebuilt integrations — or build custom integrations in minutes with AI-driven Automatic Import.





You're in good company

- **Customer spotlight**

PROFICIO

Proficio boosted SOC efficiency and achieved 60% growth with Elastic. Using the AI Assistant for cost-effective triage at scale, it cut investigation time by 34% and unlocked $1M in projected savings over three years.

- **Customer spotlight**

UOL turbocharges its security operations, achieving 80% faster incident resolution and seamless threat management, all powered by Elastic Security.

- **Customer spotlight**

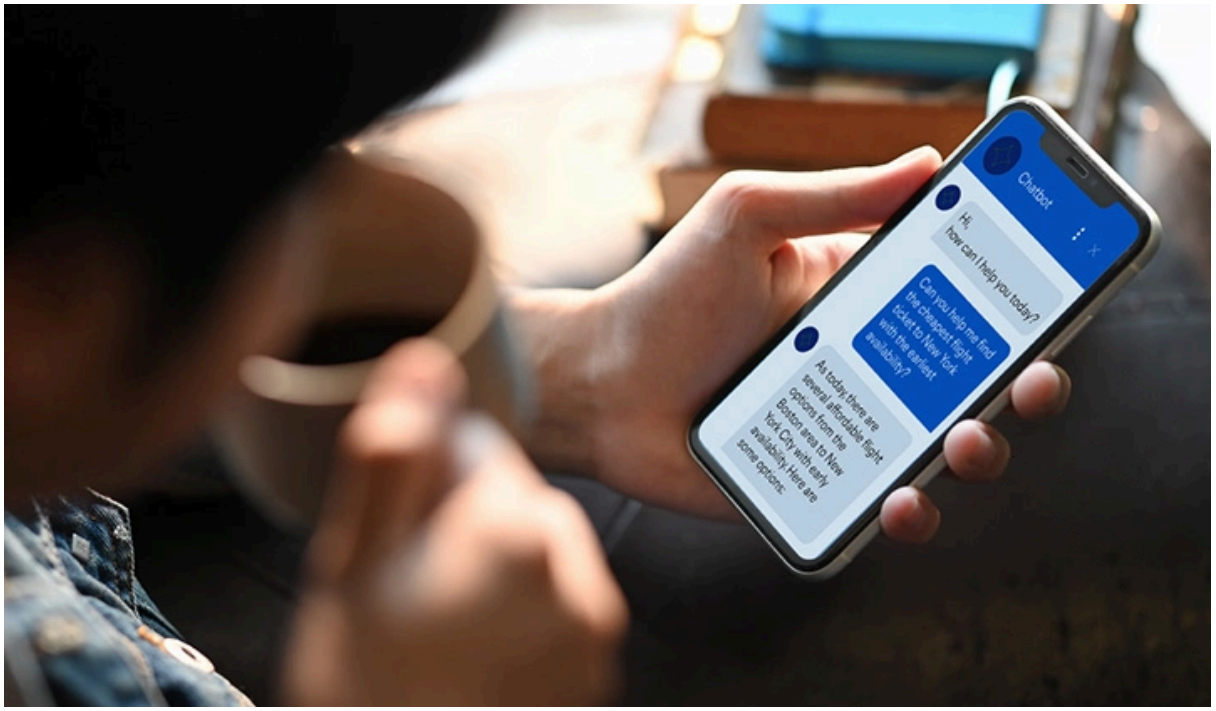
By replacing multiple tools with Elastic Security, Texas A&M automated and streamlined key processes, freeing up 100+ analyst hours every month and reducing response times by 99%.

Join the chat

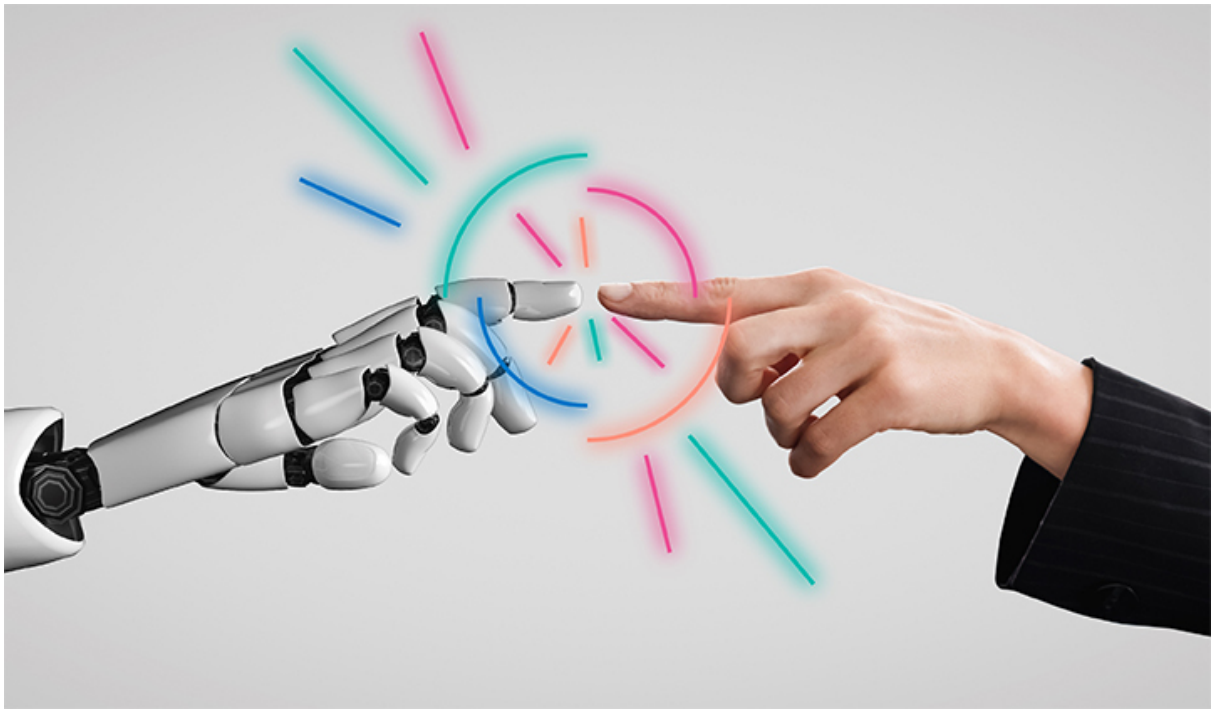
Connect to Elastic Security's global community — from open conversations and collaboration to hardening our product.

- 

Ask questions, get answers, and be heard in our open forum.

- 

Talk shop. Swap notes. Shape the future of Elastic Security.

- 

  Explore our detection rules and suggest enhancements.

- 

  Dive into Elastic. Learn, explore, and connect with peers.

Frequently asked questions

▶

What is the Elastic Security solution?

▶

Why Elastic Security?

▶

Is Elastic Security free and open?

▶

Why are businesses switching from Splunk to Elastic?

▶

What is Search AI Lake?
