elastic security

Elastic Security is the agentic security operations platform. Autonomous agents work across the SOC at machine speed while analysts stay in control of the decisions that matter. Composable skills for hunting, detection engineering, entity analytics, and investigation invoke each other and extend to external AI tools through Model Context Protocol (MCP), with every reasoning step visible.

Machine speed meets human judgment

Focus on building, not budgeting

Expertise you can see, edit, and verify

42%
Reduction in TCO[1]

74%
FTE hours reclaimed

36%
Reduction in annual risk

Agentic Security Operations Platform



Security built to secure, not tax

Unified SIEM + XDR + automation: zero per-endpoint fees, zero SOAR tax included.



Precise AI context

AI with precise context built on the Elasticsearch data and AI platform.



Total transparency

Nothing to hide: open detection rules and transparent AI that shows its work.



Hybrid visibility

Query everything, move nothing: ingest, correlate, and hunt across cloud or air-gapped environments.



Open frameworks

Open schema, open agentic frameworks: bring your own LLM and edit the workflows.



AI at every stage

Unify detection and response with AI-driven automation from triage to remediation.

 © 2026 elasticsearch B.V. All rights reserved.

Elastic Security: Help, Not Hype



Alert Zero: From Alert Queue to Validated Threats

Alert Zero is the SOC's version of inbox zero — a queue worked down to what actually matters, reached by agents and analysts together. Attack Discovery gets a SOC closer to that goal. It investigates like an analyst: hunting raw events, checking entity risk, and corroborating beyond the alerts that first fired before calling anything an attack, so teams open a short list of validated attacks instead of a wall of raw alerts. When it finds something the rules missed, it drafts an ES|QL rule to close the gap; an analyst approves before anything is saved. A separate alert analysis workflow works the noise from the other side, classifying alerts as true or false positives so Attack Discovery has a cleaner set to investigate.



Enhanced Endpoint Protection

Fewer alerts reach the queue when more threats are stopped on the device, so endpoint coverage is where prevention has to start. Elastic Security handles that with native, kernel-level sensors across Windows, macOS, and Linux that stop threats before execution. With built-in protections for ransomware, in-memory attacks, and behavioral anomalies; native automation; and a 100% malware protection rate from AV-Comparatives testing, everything is covered — nothing left to chance or budget.



Automation Across Your SOC

Elastic Workflows brings native automation to security operations, eliminating the need for a separate SOAR to buy, integrate, or maintain. Natural language authoring is now generally available and on by default, so analysts can build response automation by describing it in plain language. Human-in-the-loop approvals now reach tools like Slack, so an analyst can review and approve an escalation without leaving their workflow, and Visual Mode shows a workflow as a graph rather than raw YAML. When a detection fires, a workflow can trigger enrichment, case creation, and response — with humans making the decisions that need judgment.

 © 2026 elasticsearch B.V. All rights reserved.

Built by Security Users, for Security Users



Agent help, not hype

Machine speed meets human judgment with an agentic security operations platform.



Automation where your security data lives

AI with precise context built on the Elasticsearch data and AI platform.



Security made SIEMple

Master your data, wherever it lives, with a powerful SIEM built for the agentic SOC.



Defense for every endpoint

Protection across Linux, macOS, and Windows in any deployment — no weak link.



See, search, secure, and stop

Protect it all with extended detection and response (XDR).



Our best research, built in

Protections powered by expertise from Elastic Security Labs Threat Command.

Evaluated by the analysts



Leader in The Forrester Wave™: Security Analytics Platforms, Q2 2025[2]

Gartner

Visionary in the 2025 Gartner® Magic Quadrant™ for Security Information and Event Management[3]

IDC

Leader in the IDC MarketScape for Worldwide XDR Software 2025 Vendor Assessment[4]



100% perfect score in AV-Comparatives' Real-World Protection and Malware Protection Tests for all of 2025[5]

[1] *Analyzing the Economic Benefits of Elastic Security.*

[2] https://www.elastic.co/resources/security/report/forrester-security-analytics-wave

[3] https://www.elastic.co/resources/security/analyst-report/gartner-magic-quadrant-siem

[4] https://www.elastic.co/resources/security/report/idc-xdr-marketscape

[5] https://www.elastic.co/blog/av-comparatives-business-security-test-2025

 © 2026 elasticsearch B.V. All rights reserved.

elastic