



Search. Observe. Protect.

Elastic Security

Security teams have long used the Elastic (ELK) Stack to extract valuable security insights from all their data, enabling them to evolve quickly and solve complex security problems.

elastic.co/security

elastic.co



Elastic Security

State, local, and education IT leaders have long deployed the Elastic (ELK) Stack to reliably and security take data from various sources, in any format to then search, analyze, and visualize the data in real-time. This has allowed even the smallest security teams to evolve quickly and solve complex problems across their organizations.

Elastic Security builds on the power of the Elastic Stack to deliver pre-built capabilities that help security teams evolve even faster. The solution enables a unified, out of the box approach to security — with the inherent benefits of speed, scale, and relevance Elasticsearch is known for.

Prevent, detect, respond

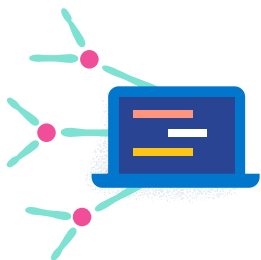
Why do government and education organizations rely on Elastic Security to stay ahead of adversaries? Speed, scalability, and a customized approach to security that is powered in part by contributions from the open source community. Validated by industry experts, Elastic Security helps prevent damage, reduces dwell times, and increases team efficiencies.





Eliminate blind spots

Elastic makes searching, visualizing, and analyzing across all your organization's data — IoT, OT, network, and endpoint — simple and instantly actionable. Protect your organization through global visibility and immediate insights, real-world validated detections, and an interface built for accelerated analysis and response. For organizations with limited budgets, a resource-based pricing model provides uninhibited data ingestion and storage for maximum impact within budget constraints.



Stop threats at scale

With the Elastic Security detection engine, automate threat detection and identify priority issues before damage occurs. Leverage machine learning to improve accuracy at scale across the entire organization. Align to the MITRE ATT&CK® framework and hunt for threats quickly and methodically.



Arm every analyst

With intuitive visualizations, Elastic Security makes it easy to determine root cause across host, network, cloud, user, or any other data source. Security teams can easily customize workflows and investigative drill downs while leveraging built-in case management and integrations with operations platforms to maximize efficiency and allocate resources to what's most important.

Free and open

Elastic Security is free and open to everyone so you can get started right away, validate a POC, and scale with a subscription after seeing the value for your team. With our customer-centric pricing approach, you can control costs and keep your priorities. Costs are calculated based on the amount of underlying server resources you use — no matter the use case or amount of data ingested — so you can maximize your budget and staff resources.

Want to check out [Elastic Security](#) for yourself? Try a 14-day free trial on Elasticsearch Service at ela.st/sec.

