elastic

Search. Observe. Protect.

Elastic Security

The Elastic (ELK) Stack has long been used by security teams and organizations to conduct fast and effective threat hunting and SecOps. Now, by integrating two critical components of cybersecurity — endpoint security and SIEM — Elastic Security provides prevention, detection, and response capabilities for unified protection across your infrastructure.

Want to check it out for yourself?
Try an extended 30-day free trial of Elastic SIEM on Elasticsearch Service at **ela.st/siem**, or spin up your own open source deployment with no time or size restriction.

elastic.co

Elastic Security

Why do organizations power their endpoint protection, security operations, and threat hunting programs with Elastic Security? Speed, scalability, and the power of the open source community. By implementing Elastic Security products within your SOC, your team is equipped with the technology validated by industry experts.

Advanced enterprise protection

Outsmart adversaries with multi-layered protection

Real-time, autonomous prevention on the endpoint stops attacks across the MITRE ATT&CK® Matrix, with no end-user impact. Protect all your endpoints — Windows, macOS, and Linux systems — with signatureless protections powered by machine learning. Uncover any cross-environment attacks and suspicious outliers with Elastic SIEM.

Security at scale

Eliminate blind spots

Elastic makes searching, visualizing, and analyzing across all your data — IoT, OT, network, and endpoint — simple and instantly actionable. Resource-based pricing allows you to install across all your endpoints and ingest and store as much data as you need in Elastic SIEM — paying only for resources you use.

Accelerate your security program

Reduce mean time to respond

Intuitive visualization renders the origin, extent, and timeline of an attack with real-time analysis of file, registry, user, process, network, and DNS data. Analysts can gather and analyze data from hundreds of thousands of logs and endpoints in just minutes to determine root cause and take immediate action.

Drag-and-drop data visualization

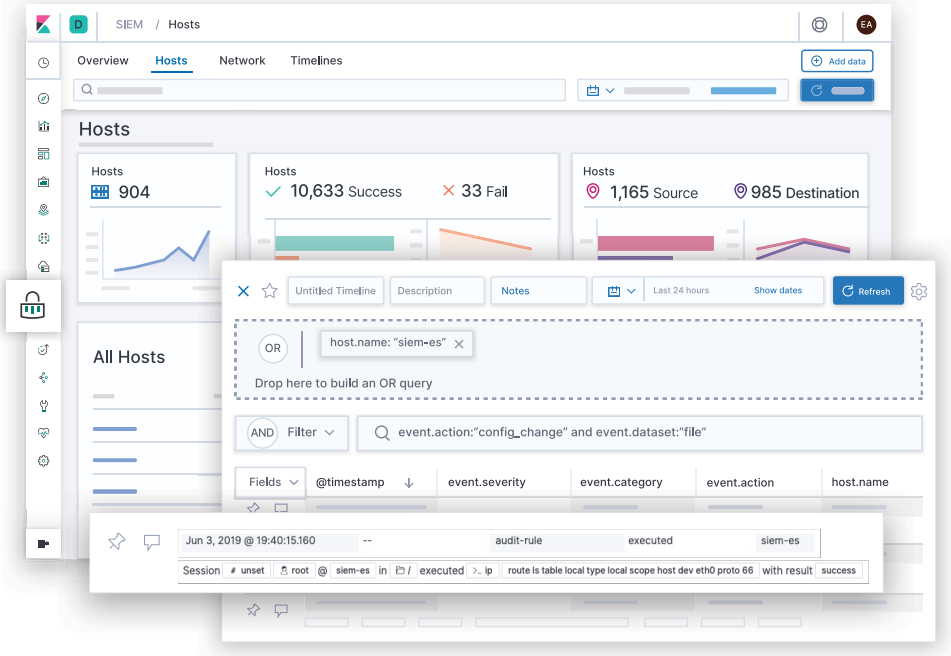
Visualize data in a snap

Using Kibana Lens, quickly check MTTD/MTTR, MITRE ATT&CK coverage, or whatever else your organization may need. Discover new ways to combine data traditionally used just for SecOps, APM, or business analytics. Simply drag and drop data fields to build new dashboards. Leverage smart suggestions for the most impactful way to display your data.

Elastic SIEM

See your data, your way

Elastic SIEM arms analysts to protect against true threats. Minimize dwell time with machine learning-driven anomaly detection, automated threat detection, and powerful threat hunting capabilities. Respond quickly with a flexible and intuitive interface that maximizes the power of every analyst.



Elastic Endpoint Security

As simple as antivirus, but way more powerful

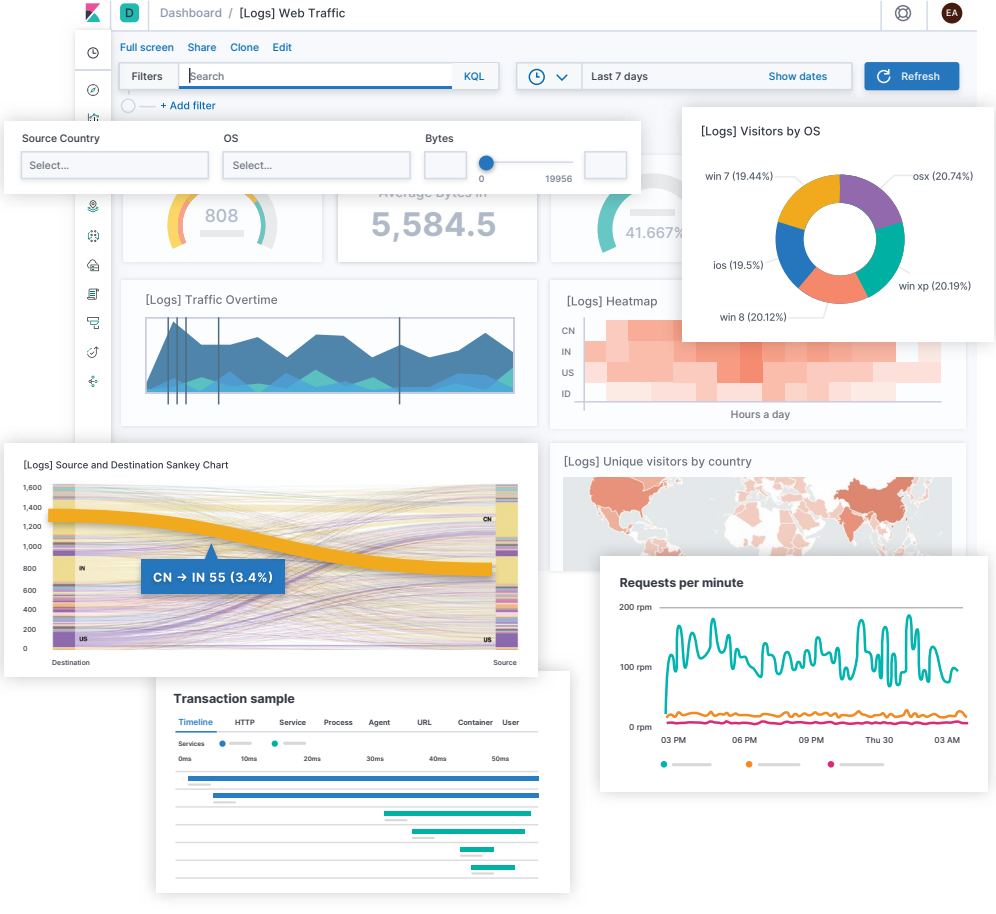
Elastic Endpoint Security combines prevention, detection, and response into a single, autonomous agent. It's easy to use, built for speed, and stops threats at the earliest stages of attack.

Elastic brings you the only security platform that makes advanced endpoint protection as simple as AV.

- **Malware and ransomware prevention:** Behavior-based ransomware prevention blocks attacks before full disk encryption, and MalwareScore™ for Windows and macOS is the machine learning-powered malware prevention with 99% block rate and zero false positives.
- **Phishing prevention:** The industry's only on-endpoint phishing prevention. Using machine learning to prevent malicious Microsoft Office documents and PDFs before they can execute.
- **Exploit prevention:** Block attempts to exploit vulnerabilities — even zero-day vulnerabilities and kernel exploits designed to elevate privileges — before any malicious code can execute.
- **Fileless attack prevention:** Our injection protection stops in-memory attacks like reflective DLL and shellcode injection. We detect and can block suspicious and malicious Powershell scripts.

Validated by the best

There’s even more in Kibana for security analysts to love.



elastic

Open source roots, enterprise-ready

Milliseconds matter
The quickest response can mean the difference between a minor incident and a major breach. Hunt for threats with a rapid succession of ad-hoc queries. Drill into and pivot through underlying data at will. And do it all with the technology fast enough for the sharpest analysts.

Establish a holistic view
Gathering all of your data is one thing. Being able to uniformly examine it is another. With the Elastic Common Schema (ECS), you can centrally analyze information like logs, flows, and contextual data from across your environment — no matter how disparate your data sources.

Secure. By design.
Don't let adversaries target your platform. Implement authentication and network traffic encryption. Create user roles and implement index- and cluster-level permissions. Manage access to Kibana saved objects like dashboards.

Security events are just the start
Have metrics? APM data? Documents with tons of text? Bring it all into the Elastic Stack to enrich your security analytics, enable new use cases, and streamline your infrastructure.

Make any infrastructure "home"
Streamline platform setup, administration, and maintenance. Deploy in the cloud or on-prem. Choose Elastic Cloud for simplified management and scaling or Elastic Cloud Enterprise to maintain complete control.

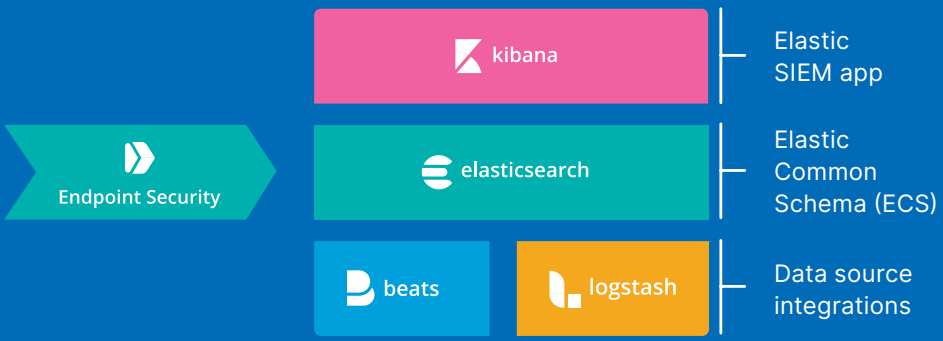
Retain the data you need
With average dwell times in excess of 90 days, long-term data retention is key. Elastic scales as big as you need, stores data for as long as you want, and makes searching through it simple and fast. And you'll only ever pay for the resources you use.

Integrate and collaborate
Extend the functionality of your solution with the Elastic Stack's broad set of REST APIs. Integrate with your legacy systems. Participate in Elastic's flourishing open source community.

Be in great company
The Elastic Stack powers many of the world's most demanding security applications. The technology is trusted by security teams at Barclays, Cisco, the US Air Force, and many other high-profile organizations.

Built on the Elastic (ELK) Stack

Built on the Elastic Stack and driven by the open source community, Elastic Security equips security practitioners to protect their organizations via global collection and analysis, field-proven protections, and an interface built for speed.

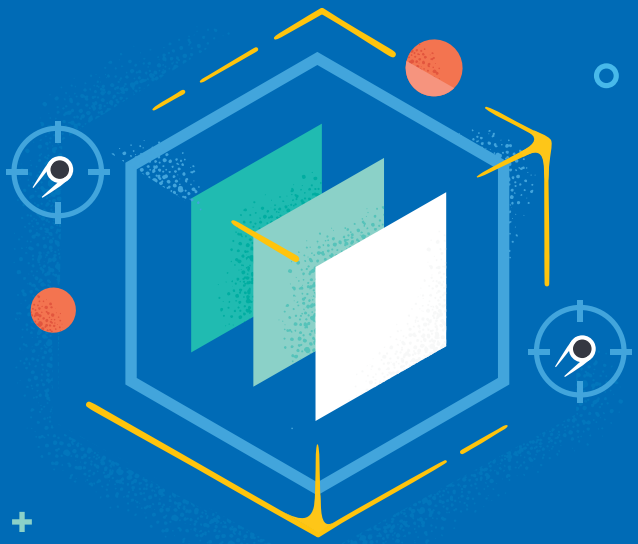


Pay only for the resources you use

Don't let a restrictive pricing model get in the way of best practices. What you pay is determined only by the amount of underlying server resources you use — no matter the use case, data ingested, or number of endpoints.

Enterprise protection, no compromises

Prevent **Detect** **Respond**



Elastic Security brings endpoint protection and SIEM into a single experience to streamline how you secure your organization.

elastic