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 you can use robust security solutions — **Elastic SIEM** and **Elastic Endpoint Security** — directly from the makers of the technology that keeps the world's largest organizations ahead of threats.

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

elastic

Elastic Stack for security

Why do organizations power their security operations and threat hunting programs with the Elastic Stack? Speed, scalability, and relevance. By adopting Elastic security solutions within your SOC, your team is equipped with the technology trusted by security teams everywhere.

Collect at scale
Hints of a threat can come from anywhere, including places you weren't expecting. Centralize data from across your environment. Store petabytes of data and keep it searchable for years.

Monitor your attack surface
Monitor your data in near real-time on interactive dashboards. Drill down and pivot with direct access to underlying data and the structure of a purpose-built schema.

Explore anomalies with machine learning
Surface unusual events with machine learning-based anomaly detection. Equip threat hunters with evidence-based hypotheses. Find the threats you expected — and the ones you didn't.

Ask your data questions of all kinds
Query structured, semi-structured, and unstructured data. Perform ad-hoc searches across your enterprise and get results in seconds, all made possible by ingestion-time indexing.

Automate detection
Automate threat detection with correlation rules. Implement Elastic and community security rules and tailor them for your environment. If you can query it in Elasticsearch, you can alert on it.

Accelerate incident response
Reveal the root cause of an attack and the extent of a compromise. Gather forensic evidence and contextual data. Forward investigations to ticketing and SOAR platforms. Automate response with Elastic Endpoint Security.

elastic

Open source roots, enterprise-ready

Milliseconds matter
Monitor your environment with interactive dashboards. 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.

Security starts at the endpoint

Elastic Endpoint Security
Elastic Endpoint Security combines prevention, detection, and response into a single autonomous agent. It requires zero training, is 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.

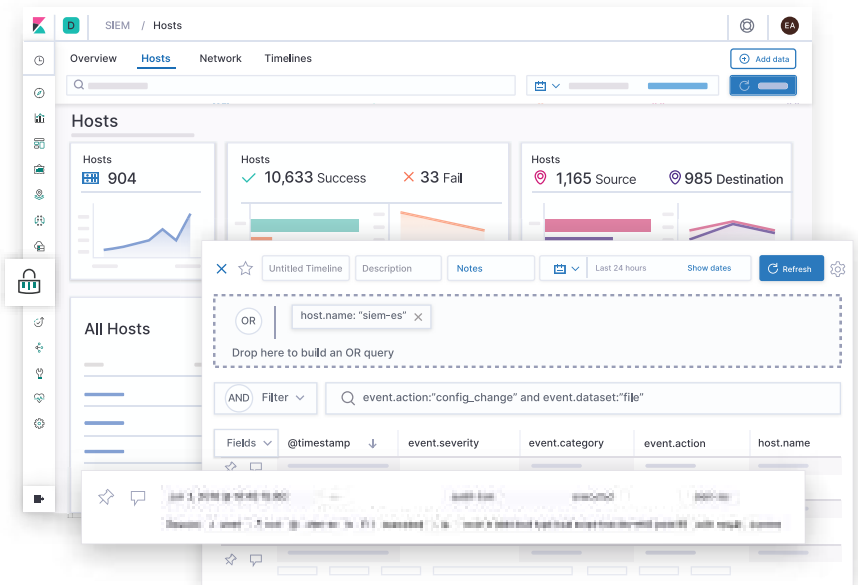
- **Fileless attack prevention:** Our injection protection stops in-memory attacks like reflective DLL and shellcode injection. We detect and can block suspicious and malicious Powershell scripts.

Validated by the best

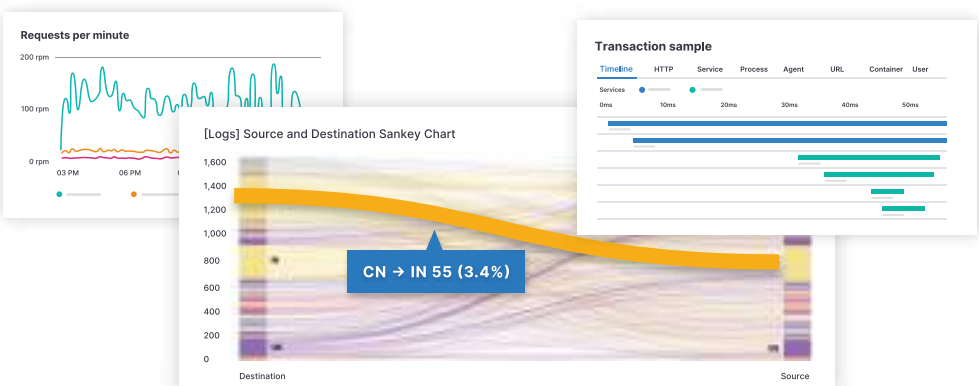
See your data, your way

Elastic SIEM app

The Elastic SIEM app provides an interactive workspace for analysts to triage events and perform initial investigations. Security teams use its interactive timeline to gather and store evidence, pin and annotate key data, and forward findings to ticketing and SOAR platforms.

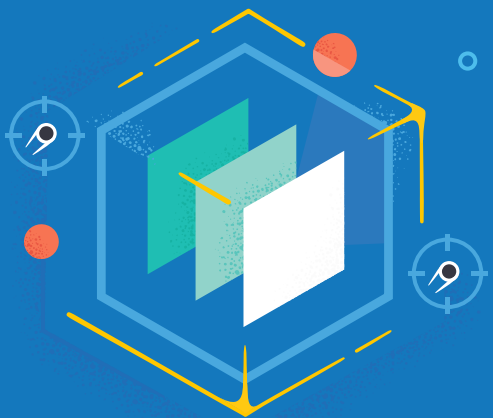


There's even more in Kibana for security analysts to love.



Full protection, no compromises

Prevent **Detect** **Respond**



We're bringing endpoint protection and SIEM into a single experience to provide optimal protection against cyber threats and streamline how you secure your organization.

Built on the Elastic Stack