elastic

Elastic Security

Security teams have long used the Elastic (ELK) Stack to extract valuable security insights from their data. With Elastic Security, your teams can quickly find the data they need to prevent, detect, and respond to complex cyber threats at scale, minimizing risk and protecting your organization's reputation. All on a unified, open platform that's built for cloud.

Ready to search across years of data in seconds?

Start Free Trial →

Accelerate your security programs

Why do security teams choose Elastic Security? Speed, scalability, and the power of the open source community. By implementing Elastic Security within your security programs, your team is equipped with the technology driving many of the world's most mature security teams.

Eliminate blind spots

Elastic makes it simple to search, visualize, and analyze all of your data — cloud, user, endpoint, network, you name it — in just seconds. Add new data with one-click integrations, community-built plug-ins, and simple custom connectors.

Arm every analyst to succeed

Quickly grasp an unfolding attack by correlating all relevant data in one intuitive user interface. Glean insights with analyst-driven correlation and simplified host inspection. Seamlessly access internal and external context. Respond rapidly with a nimble UI, built-in case management, and a burgeoning set of external automations.

Search by the petabyte

Explore years of historical data in minutes — without breaking your budget. How? Elastic makes low-cost object stores like AWS S3, Microsoft Azure Storage, and Google Cloud Storage fully searchable. So equip analysts with an order of magnitude more data for search, threat intelligence matching, reporting, and more.

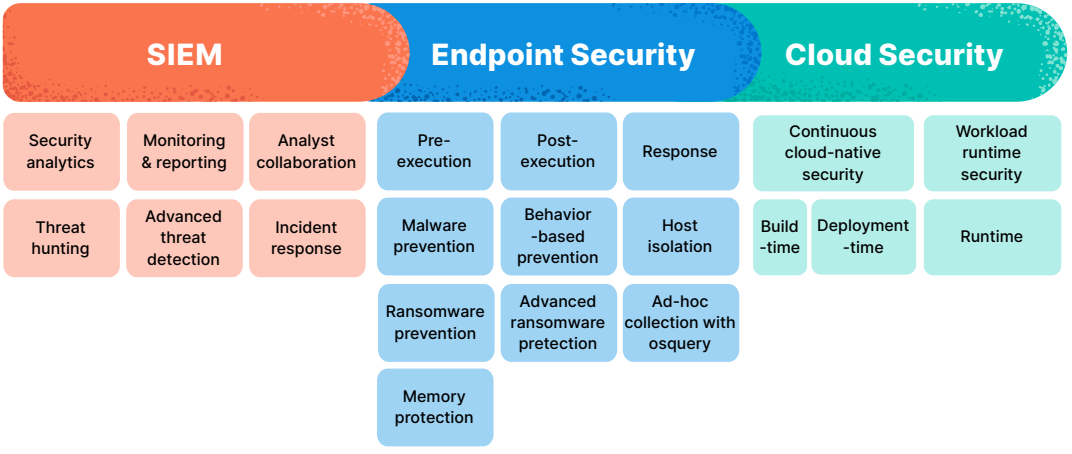
Stop threats at scale

Stop advanced threats with host-based behavior analytics and cross-environment ML. Prevent malware and ransomware on every OS. Automate detection with MITRE ATT&CK®-aligned rules developed by Elastic Security researchers. Advance program maturity by leveraging contributions from across the global Elastic community.

Limitless XDR

Elastic Security's Limitless XDR enables teams to see more, stop more, and scale security at the speed of business. Improve visibility, automate detection, and achieve comprehensive analysis across your environment with a consolidated approach.

Limitless XDR is a single approach for tackling top security use cases and modernizing how teams protect their organization.



Sky's the limit

What makes Elastic's approach to XDR limitless? Limitless data ingestion... limitless analysis... limitless protection... all provided with a scalable pricing structure based only on the resources you use.

Threat prevention & detection

Secure your organization against ransomware attacks, business email compromise, malware, insider threats, and more. Gain immediate visibility into corporate networks, cloud environments, remote workers, or SaaS applications.

Real-time, for real

Prevent breaches and ransomware threats before impact with built-in native endpoint security. Detect complex threats faster with deep visibility into endpoints and rich integrations, coupled with out-of-the-box analytics and machine learning capabilities. Take immediate action by invoking host response actions or trigger third-party orchestration workflows to minimize breach impact.

Solve for use cases such as:

- Malware prevention
- Ransomware prevention
- Lateral movement identification
- Anomalous network, OS, and file access behavior detection
- Host-based detection and prevention

Hunting, investigation, & incident response

Elastic Security enables security teams to address threats faster to minimize reputational harm, data loss, and impact to productivity. Get the most out of your security data to proactively find issues and accelerate response. Collaborate for greater impact, improved efficiency, and higher organizational resilience.

It's a marathon, and a sprint

Boost security operations with contextual insights to power smarter investigation and expedite triaging for root cause analysis. Power collaboration with built-in case management, a nimble UI, fast data search across petabytes of data, live endpoint visibility, and a burgeoning set of workflow integrations.

Solve for use cases such as:

- Incident investigation
- Incident case management
- Rapid response
- Host-based remediation
- Proactive threat hunting
- Automated incident response

Continuous monitoring

Files, operating systems, user activity, network and cloud infrastructure, apps, transactions... there's a lot to monitor in an environment. Your ability to protect across these vectors is only as effective as what you can see. Elastic Security adapts to meet your ongoing efforts to protect sensitive data at any level.

Always on

Gain crucial insights into system security and application performance with an integrated security and observability solution. Elastic Security eliminates blind spots by ingesting as many years of data as you need, normalizing it all, and analyzing it in seconds. The solution empowers you to gain rich visibility to get ahead of compliance and security issues faster.

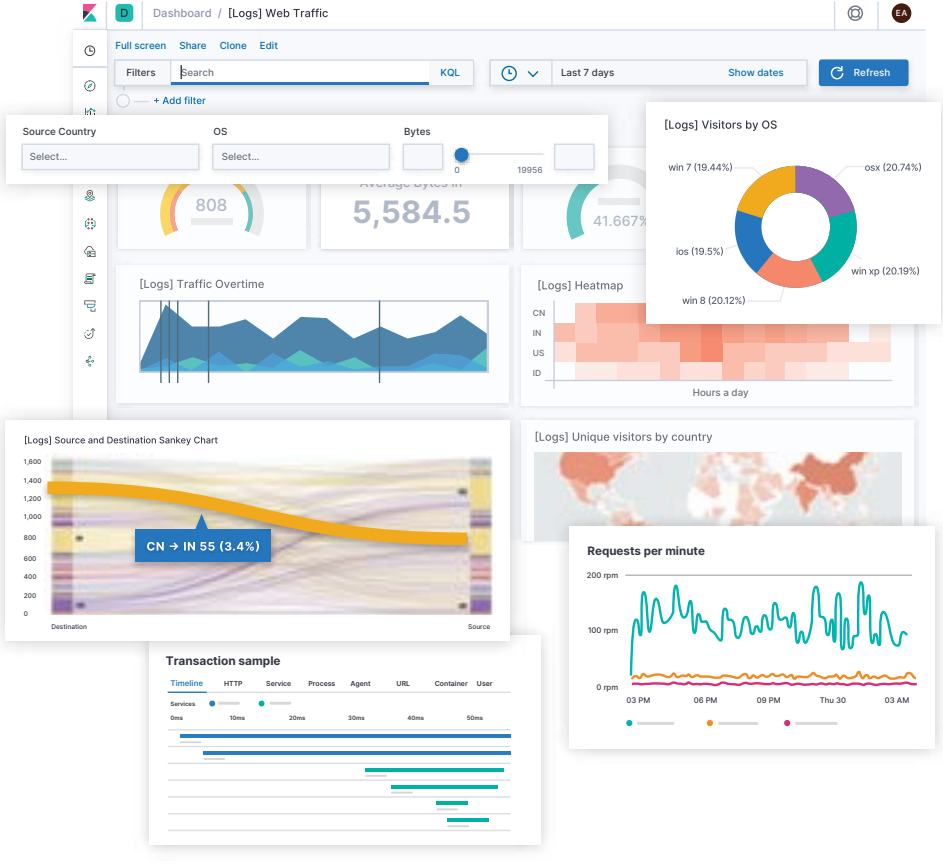
Solve for use cases such as:

- Context-aware asset visibility
- File integrity monitoring
- Cloud application monitoring
- Privileged user and VIP monitoring
- Network activity monitoring
- Critical asset monitoring

See your data, your way

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

Ingesting and normalizing your data is only the beginning of the story. Making sense of that data is where you achieve true visibility. Luckily, Elastic provides prebuilt features to help you excel in both.



License to scale

An effective security practice requires data at scale. Don't let a complex pricing model interfere with your mission.

No matter your use case, data volume, or endpoint count, you'll pay only for the resources you use. Do more with your data without concerns of a nickel-and-dime pricing structure.

Validated by the best

AV comparatives FORRESTER® Gartner MITRE

Let's take on your biggest security challenges

Want to check out Elastic Security for yourself?

Elastic Cloud is the best way to consume all of Elastic's solutions across any cloud — securely and at scale. Get started today with a free trial at **ela.st/elastic-security,** or visit the Amazon Web Services, Google Cloud, or Microsoft Azure marketplaces to deploy in minutes.