elastic

Elastic Security

Protect, investigate, and respond to threats with Elastic Security's unified SIEM & security analytics, cloud-native security, and endpoint detection & response (EDR) solution.

We help organizations modernize their security operations efforts across complex environments to solve continuous monitoring, threat hunting, advanced threat prevention, and investigation & incident response challenges.

All through a scalable solution that's built for cloud.

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 plugins, 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 provide analysts with an order of magnitude more data for search, threat intelligence matching, reporting, and more.

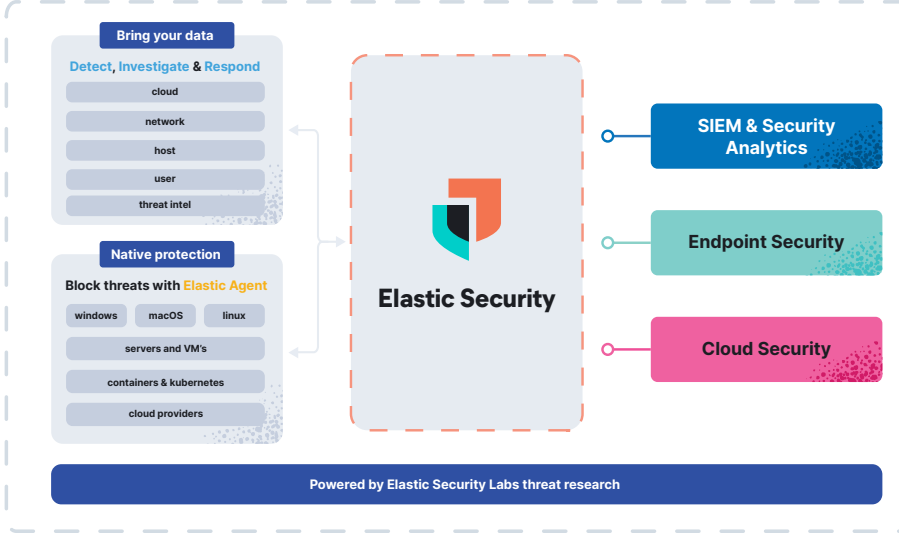
Stop threats at scale

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 Labs researchers. Advance program maturity by leveraging contributions from across the global Elastic community.

Security operations, modernized

Elastic Security 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.

Through a single solution, take on top security use cases and modernize how you protect your organization.



Sky's the limit

What makes Elastic's approach scalable? Limitless data ingestion... speed-of-thought analysis... automated protection... all available through a scalable pricing structure based only on the resources you use.

Automated threat prevention

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 with integrated SOAR workflows to minimize breach impact.

Solve for challenges such as:

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

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 challenges such as:

- Incident investigation
- Incident case management
- Rapid response
- Host-based remediation
- 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

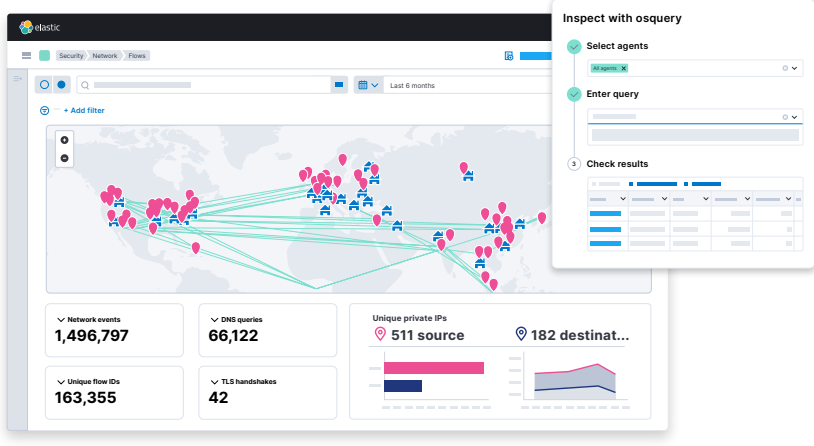
Gain crucial insights into system security and application performance with an integrated security and observability solution. Elastic Security eliminates blind spots by ingesting as many years of data as you need, normalizing it all, and analyzing it in seconds. The solution empowers you to gain rich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

Solve for challenges such as:

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

Threat hunting

Elastic offers the speed, valuable insights, and rich context required for effective threat hunting. Initiate hunts with insights gleaned from advanced analytics. Leverage petabytes of data, enriched with threat intel. Uncover threats you expected — and others you didn't.



Reduce dwell time & minimize damage

Waiting for frozen data to thaw wastes precious time. Elastic provides quick access to frozen data, enabling practitioners to dig into archives without a long wait. By surfacing rich context on the fly, analysts can confidently take rapid action to remediate threats. Threat hunters can query petabytes of logs in just seconds and quickly match fresh IoCs against years of historical data.

Solve for challenges such as:

- Anomaly detection
- Insider threat detection
- Threat intelligence enrichment
- Data exfiltration prevention
- Improved IT visibility

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

Gartner FORRESTER® IDC MITRE AV comparatives

Let's take on your biggest security challenges

We're here to help you keep your organization safe every step of the way. Our threat researchers at Elastic Security Labs actively investigate the latest malware, ransomware, tactics, activity groups, and leading security topics to equip you with cutting-edge insights and tools to defend your environment.

Check out Elastic Security for yourself.

elastic.co/security