elastic

Search. Observe. Protect.

Gaining holistic visibility with Elastic Security

elastic.co

Table of Contents

Why is visibility important?

Security requirements continue to evolve. Modern security teams are tasked with significantly more responsibility than managing the alert queue. They are aligned to the business, and therefore need to answer not only difficult and complex technical questions, but also questions that help inform investment decisions and even the strategic direction of the organization.

Consider the following global trends:

Digital transformation initiatives

Impact:

- New attack types and vectors: more information technology (IT), more operational technology (OT), Internet of Things (IoT), mobile
- Distributed workforce: more insecure connectivity/bring your own device (BYOD)

Requirement:

- Visibility needed across larger attack surface

New attack methodologies

Impact:

- Latest threat tactics/techniques can go undetected
- More time and resources needed to stay current

Requirement:

- Deeper visibility needed from existing data (e.g., behavioral insights)

Unified operations and cloud migration

Impact:

- More people working off the same data
- Highly distributed, inconsistent architectures

Requirement:

- Same or better visibility needed by more teams, at cloud scale

Accelerated pace of change

Impact:

- Unexpected infrastructure changes
- Exacerbates skills shortage/understaffed teams

Requirement:

- Greater efficiency, adaptiveness, resilience needed

The requirements above raise new questions and complicate the manner in which we answer existing questions. For example, from a technical perspective, questions that security teams may need to answer include:

- How secure are all of our endpoints and servers, legacy and new, on-prem and in the cloud?
- Where do we need to apply patches or install application updates?
- Who needs additional training on compliance or InfoSec policy?
- Have any unexpected “new user accounts” suddenly appeared recently?
- Do any employees appear to be targeted for phishing attacks?
- Do we have an actionable view of what’s happening on the network?
- Are there any unusual traffic patterns or email activity we need to investigate?
- Are there any misconfigured cloud assets containing sensitive data?
- Are there any unexpected changes to security policies in our cloud environment?
- How do we find visibility gaps that we’re not even aware of? (e.g., shadow IT services)
- How can we quickly and accurately verify whether suspicious activity is malicious?
- How can we get better at threat hunting so we’re not as reactive?
- How does the latest and greatest attack model/framework apply to our situation?

Part of the challenge in answering these questions is in the realization that none of them is a simple "one and done." Each of these questions spawns new inquiries. For example, take a basic investigation that may arise from delving into any of the above questions. In responding to an alert, your team might have to answer numerous follow-on questions to get the right supporting context:

- ✔ Is a system actually compromised?
- ✔ When was it compromised?
- ✔ What accounts and users are associated with that system?
- ✔ What login activity happened around the time of compromise?
- ✔ For that system, has there recently been any cleartext used for authentication?
- ✔ Does network activity show any evidence of beaconing to a C2 server?
- ✔ How rare is this thing that I'm seeing?

These only represent an example fractional subset of the broad range of questions that security teams might need to pursue.

From a business standpoint, the following types of questions might be top of mind:

- ✔ How do we align security efforts to a specific business requirement?
- ✔ How can we clearly communicate how effectively we are performing?
- ✔ How can we provide insights needed by business owners to make informed decisions?
- ✔ How can we demonstrate consistent improvements in our process, not just key performance indicators (KPIs)?
- ✔ How can we quantify and show that our investments are paying off?
- ✔ How do we measure the effectiveness of our security program?
- ✔ What corporate risks are presented by any of our new business initiatives?

Understanding where you stand on these issues is critical. First, you need the right visibility.

What exactly is visibility?

In security, visibility comes from data. What types of data and how much of it do you need? Since modern multistage attacks can exploit any vector or attack surface available, almost any data can be considered security relevant — event and audit logs, metadata, and other activity from IT and OT devices, services, and applications; host activity; user activity; network events; cloud activity; wire data; threat intelligence; social media feeds; and many other sources of data and enrichment.

Data can be structured or unstructured, static or dynamic, generated on-premises or cloud-based — but regardless of type or format, security teams share the common objective of using data to gain key insights and decide and act on those insights.

Merriam-Webster's primary definition of "visibility" is:

> **vis·i·bil·i·ty**
>
> *noun*
>
> the quality or state of being capable of being seen

Merriam-Webster's definition also includes:

- conspicuous
- accessible
- readily seen or referred to
- degree of clearness

Similar to Merriam-Webster's definition, in security, visibility is not limited to only "capable of being seen." That is fundamental, but security insights should also be conspicuous, accessible, readily seen, and clear enough to facilitate decisive planning and effective remediation.

Visibility, not one size fits all

Security teams have unique skillsets, processes, tools, and objectives. They can interpret “visibility” differently, depending on their function and which use cases they support. They have different requirements, barriers to overcome, and desired outcomes, as relates to:

- Getting the visibility they need
- Operationalizing that visibility

Teams typically face a common tradeoff — do they have the time, resources, and staff to tackle visibility challenges? If not, are they prepared to deal with the negative impact from compromising on achieving desired outcomes?

Put simply: **Is the heavy lift needed to get visibility, and to operationalize that visibility, worth it?**

In the table below, Column 1 includes key aspects of visibility each functional security team will need. Columns 2 and 3 describe some of the challenges in attaining that corresponding level of visibility. These are not small issues — gaining visibility and operationalizing that visibility can be daunting, expensive, and in some cases not feasible, depending on the capabilities of the underlying data fabric and supporting technologies (we’ll cover why in the next section).

As a result, unfortunately, too many security teams can relate to the pain points described in Column 4.

Visibility mapped to team functions

Monitoring	Key aspects of visibility needed	Primary challenge(s) in getting that visibility	Primary challenge(s) in operationalizing this visibility	Impact of not having visibility (or not operationalizing that visibility)
Compliance	Changes that result in out-of-compliance conditions (e.g., configuration, permission, logging level, default settings, disabled security features or controls)	Identifying in-scope assets; automating data collection; scaling and maintaining continuous compliance	Getting the right dashboard views; ensuring appropriate and timely corrective actions; reporting	Cannot clear compliance; review cycles are long and dragged out; fines; failed audits; skilled staff working on mundane tasks
Cyber hygiene	Weaknesses in security posture (e.g., misconfigurations, outdated patch levels/ security updates, vulnerabilities, uncleaned malware)	Maintaining inventory of assets; assessing possible vectors and ensuring adherence to best practices	Maintaining visibility as new initiatives roll out; prioritizing these relative to threats; ensuring stakeholder awareness	Cannot quantify and report on real-time state of risk; too much time spent maintaining appropriate level of compensating controls

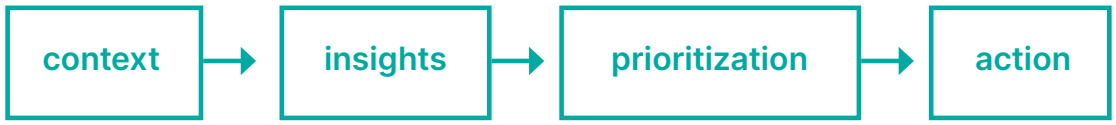
Threat detection

Alert triage	Relative prioritization; level of fidelity; clear understanding of how an incident impacts security posture; prescriptive actions/ recommendations	Adequate context (e.g., enrichment, gathering threat intelligence/ indicators of compromise (IoCs)/ indicators of attack (IoAs), related alerts)	Training tier I/ II analysts to understand how to interpret and escalate appropriately	Alert overload; alert fatigue; reduced number of incidents addressed properly; priority issues are missed
Verification	Intent, technique; tactic, target systems; accounts, objectives, outcome	Adequate and centralized context (i.e., all relevant data sources in one place, along with enrichments, threat intel, IoCs/IoAs, related alerts)	Training tier II/III analysts to know how to derive the right insights from a variety of data sources	Unnecessary escalations resulting in dead-end investigations, loss of focus on priority issues

Incident response	Key aspects of visibility needed	Primary challenge(s) in getting that visibility	Primary challenge(s) in operationalizing this visibility	Impact of not having visibility (or not operationalizing that visibility)
Containment and disruption	Root cause; tactics, techniques, and procedures (TTPs); vectors (e.g., associated C2 channels/ beaconing, target systems/accounts)	Adequate context (e.g., enrichment, gathering threat intelligence/IoCs, IoAs, related alerts, correlated activity)	Developing a formal, well-documented set of procedures; automating a response to be triggered from a high-fidelity alert	Inability to minimize risk and prevent further loss throughout the incident response process
Investigation/ scoping/ forensic analysis	Associated activity; root cause; impacted systems/ accounts (e.g., time and method of entry, infected systems, affected accounts, signs of lateral movement, whether data was exfiltrated, methods of persistence)	Speed of access to all centralized context (i.e., searching for evidence and quickly pivoting to downstream/ upstream events)	Enabling an intuitive, fast, accurate investigative methodology for any analyst, regardless of skillset or level of experience	Slow investigations (or inability to perform end-to-end investigations or scope incidents), resulting in inability to properly remediate and report on incidents
Implementing response actions and reporting	Current state of an investigation; assigned tasks; mitigation steps; remediations in progress; status of recovery	Difficult to establish a centralized view of all associated activities	Disparate tools, developers, and toolchain ops needed to integrate systems and customize workflows	Lack of efficiency in incident management and resolution; unresolved incidents; unmet service-level agreements (SLAs)

Hunting	Key aspects of visibility needed	Primary challenge(s) in getting that visibility	Primary challenge(s) in operationalizing this visibility	Impact of not having visibility (or not operationalizing that visibility)
Planning	Patterns/trends; anomalies; general awareness and understanding of the environment needed to form a crisp, clear, and narrow initial hypothesis	Establishing and maintaining a baseline of what is "normal" vs. "unexpected" — i.e., classifying whether or not something is an anomaly	Documenting and developing a formal operating procedure that leverages this deeper knowledge (not all people will know how to use it)	Hunting practice is inefficient or ineffective — skilled analysts on wild goose chases, time lost in looking for clues as scope creep sets in
Executing	Broad enough "spotlight" to help hunt teams gather and document critical clues as they proceed through their hunt	Ensuring data sources are not missing critical context; ensuring all data sources needed are readily accessible	Following a documented approach and hunt methodology that ensures teams will collect needed context and share in a usable manner, and can develop automations based on this context	"Reinventing the wheel" repeatedly; adding inefficiency and burning out skilled analysts who are carrying the bulk of the weight in supporting the hunt practice

Note that each team/function has its unique objectives to work toward. Ideally, they are all working in concert as they execute their respective portion of a common overall basic workflow:



Or, if you map this to a set of tasks that these teams must support:

Again, throughout this entire flow, there is the need for "process" — that is, not only getting the visibility, but also operationalizing that visibility.

Why is visibility hard?

We've established that visibility has different meanings for different teams. For each of these security teams to get the answers they need, they need access to the right data at the right time. This can sound as simple as indexing massive volumes of security-relevant data, but even with rigorous data preparation and architectural optimizations, teams run into limitations, resulting in issues with:

- Efficacy: they lack the specific context needed to achieve a desired outcome
- Scaling: they lack the adequate context needed for coverage across the organization
- Efficiency: context is siloed, resulting in failure to quickly meet common objectives

Why does this happen? Again, security teams are fundamentally solving two core problems, which require key attributes to address:

1. **Detecting and preventing priority issues across a multilayered ecosystem at scale**

   The goals of detection and prevention are to reduce dwell times and minimize damage without causing business disruption. The attributes of ***speed*** and ***accuracy*** are foundational to success here.

2. **Identifying and operationalizing the appropriate response to those issues**

   The goals of operationalizing are to help teams run efficiently and cost-effectively while enabling them to adapt and grow as quickly as needed. Therefore, operationalizing requires the attributes of ***flexibility*** and ***simplicity.***

These attributes are often in conflict with one another; security teams commonly balance tradeoffs in their tools and processes — "speed vs. accuracy" and "flexibility vs. simplicity."

There are a number of commonly used KPIs and metrics associated with each of these core problem areas:

KPIs and metrics

	Security KPIs	Business metrics	Attributes needed
Detection and prevention	Mean time to detect (MTTD)/mean time to identify (MTTI) (dwell time) Coverage (% of issues)	Damage from breach or data loss ($) Disruption to employee productivity (time) Revenue loss ($)	Speed, accuracy
Operationalizing an appropriate response	Mean time to respond (MTTR) (time required) Efficiency/productivity (# of staff required)	Cost to resolve/report incidents ($) Disruption to employee productivity (time) Revenue loss ($) Resources to add new use cases (time, staff, cost)	Flexibility, simplicity

The need for holistic visibility

In terms of visibility, the challenge is not achieving any one of these attributes, or even a subset of them, as that can typically be fairly easy in an isolated or relative context. The greater challenge is gaining ***holistic visibility*** — across all security-relevant data — while also gaining the benefits of speed, accuracy, flexibility, and simplicity, without compromise.

For example, when a security team uses a security tool that is native to a cloud infrastructure environment, they might benefit from speed and accuracy, but that tool may primarily focus on visibility of activity generated within that cloud environment. Will they be able to easily pull in bespoke data sources and integrate with other tools from across the rest of their environment, and run correlated detections and perform investigations across multiple environments, including on-premises and other clouds? Speed and accuracy for a portion of the overall security-relevant dataset should not come at the cost of coverage. Adequate context is needed

in order to properly respond to a threat in time to avoid damage, or to scope and report a breach within the timeframe required by a privacy mandate — not just within a cloud provider's infrastructure, but across the entire corporate environment.

Data silos = process silos

In most security architectures, the large number of specialized tools and functional teams, each with their own visibility requirements, can result in siloed operational processes. Even if one team can gain some benefit from a specific tool, another team may struggle to integrate their process with the insights or data from that tool, or may even find themselves in contention with other teams using different tools. This problem is compounded when considering the larger problem of collaborating with other ops teams across the organization.

For example, a security tool may lack the flexibility and simplicity to process all network firewall data the same way, regardless of vendor. Considering the skills gap, this is a critical advantage that security teams need in place to be adaptive and resilient while maintaining visibility.

They may also struggle to customize their workflows to meet their team's specific requirements, and to provide other ops teams access to the same data to view through a different lens so that those teams can, for example, answer observability questions from within the same platform — and vice versa, so that they can gain easy access to observability data to analyze in a security context. As organizations standardize at the data fabric layer, this is again another critical advantage needed to maintain visibility and consistency.

Holistic visibility challenges

We've explored a couple examples in depth. Let's now zoom out and take a look at all four of these key attributes in the context of the basic workflow elements from the previous section.

Note that each layer builds on the completeness and strength of the previous layer. By addressing the foundation — i.e., by ensuring we have a solid data strategy that can maintain speed, accuracy, flexibility, and simplicity as we scale — we can ensure that all security teams involved in the broader security operations function can gain holistic visibility, and also the ability to easily operationalize that visibility, without compromising on speed, accuracy, flexibility, or simplicity. It is critical to avoid those compromises, regardless of how each team prefers to analyze, visualize, and operationalize security use cases.

Challenges in gaining holistic visibility while maintaining speed, accuracy, flexibility, and simplicity

	Speed	Accuracy	Flexibility	Simplicity
Action (operations)	Not easy to perform real-time collaboration across all teams, leveraging common views and automation	Time-consuming and resource-intensive to verify and investigate, plan, and execute on best containment/ mitigation and response actions	Process silos resulting from multiple tools, incident response platforms, and case management systems	Requires investment in toolchain ops to enable higher degree of efficiency and collaboration across security operations
Prioritization (visualization)	Different, inconsistent visual methodologies for detection, triage, hunting, investigation, response	Need clearly prioritized alerting views, investigative drilldowns, and threat hunting workflows in one tool	Steep learning curve for less skilled analysts to filter and process results easily and to map according to any use case/ requirement	Not easy to customize views for any individual or team without a skilled developer
Insights (analysis)	Despite optimizations, pulling in adequate context results in slow searches and ad-hoc investigations; statistical methods converge slowly	Lack of research-validated out-of-the-box detections; too many false positives; difficult to take a behavioral-based approach to detection and correlation; need mapping to a framework	Difficult to enrich data from any source; developing custom detections/ models is challenging; difficult to integrate with other tools	Advanced machine learning (ML) and correlation methods require data scientist or seasoned threat hunter expertise to interpret and operationalize
Context (data)	Difficult to quickly access and search across a distributed environment	Cannot get enough context to adequately provide inputs needed for analytical methods	Rigidity prevents easy addition of new data sources quickly; heavy dependence on deployment/ environment	Data is not easy to normalize; high-volume data is not indexed and therefore not easily accessible

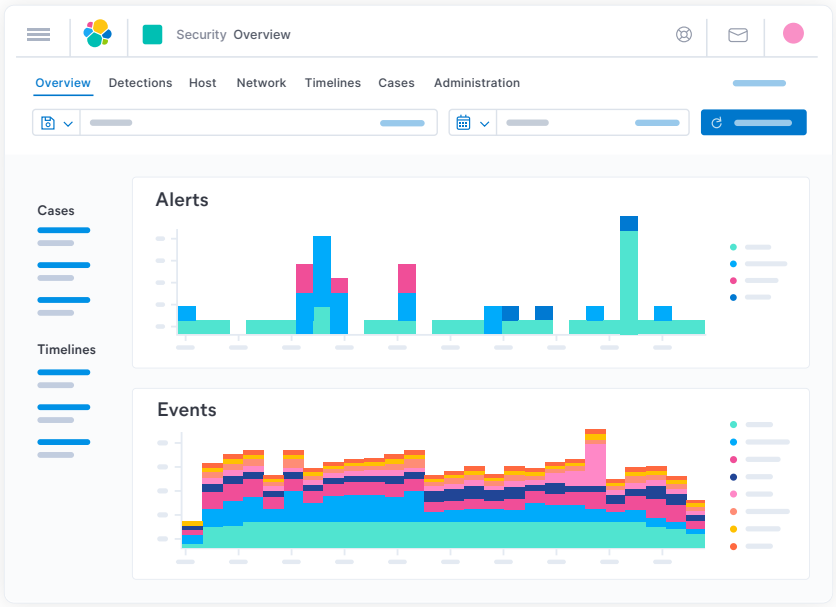
Gain holistic visibility with Elastic

It's one thing to know that a solid data strategy will provide the holistic visibility needed to help standardize operations and improve security team efficacy and efficiency. But how can you ensure success when the growth of data is so explosive? As we stated earlier, greater volumes and types of data are increasingly relevant to security.

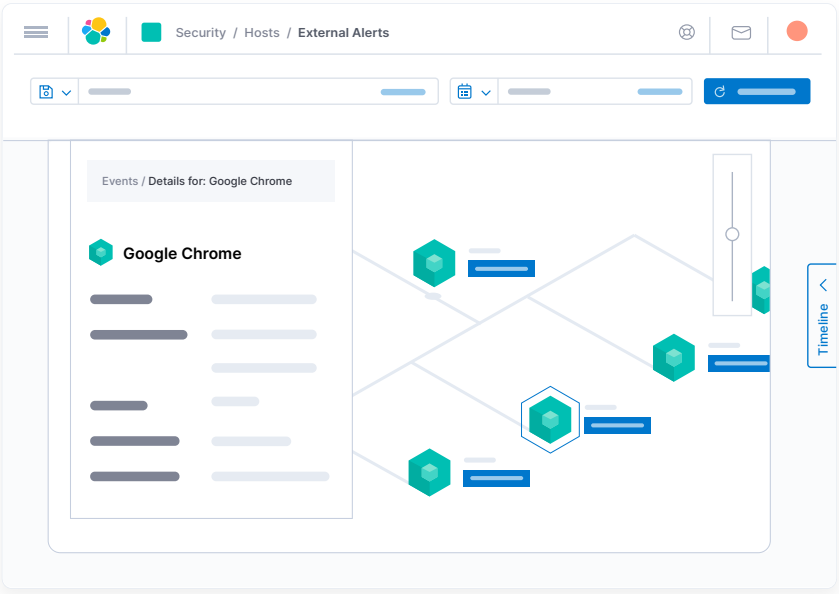
The most common and important way we interact with data is to search across it. At the most fundamental level, your security team's ability to quickly and accurately search at scale is the underpinning of success for your security program. If you solve the search problem — again, with speed, accuracy, flexibility, and simplicity — it is then relatively straightforward to build on top of that foundation — at the analytics layer, the visualization layer, and the operations layer. With this foundation, you can implement and scale virtually any security use case.

The Elastic Stack (formerly known as the ELK Stack) has been used for years by security teams as their data foundation for exactly this reason. At the heart of the Elastic Stack is Elasticsearch, known for its speed, scale, and relevance. Security teams have long used the Elastic Stack to extract valuable security insights from all their data. They can quickly search all data, structured and unstructured, from all different types of logs, static and dynamic forms, ad hoc inputs — any data that is searchable. This core advantage has enabled them to evolve quickly and solve complex security problems for a multitude of security functions, including threat hunting, security information and event management (SIEM), threat research, compliance, security monitoring and investigation, digital forensics and incident response, endpoint protection, antifraud, and more.

Elastic Security builds on the power of the Elastic Stack to deliver prebuilt capabilities that help security teams gain holistic visibility. The solution enables a unified, out-of-the-box approach to security. Again, search is the most important fundamental interaction with your data, and with Elasticsearch at its core, Elastic Security enables holistic visibility without compromise.



Elastic Security provides an ideal solution for gaining the holistic visibility you need and enables security teams to easily operationalize that visibility. With Elastic, teams can collaborate more effectively to protect critical assets, perform fast and accurate investigations, improve and formalize a threat hunting practice, and generally solve and operationalize any security use case at scale.



The advantages of Elastic Security for holistic visibility

	Speed	Accuracy	Flexibility	Simplicity
Action (operations)	Easily perform real-time collaboration across all teams, leveraging common views and automation	Timeline helps teams quickly verify and investigate, document, plan, and execute on best containment/ mitigation and response actions	Eliminate silos by leveraging integrations with Slack, JIRA, ServiceNow, IBM Resilient, Swimlane, Palo Alto, and more	Embedded case management plus integrations increases efficiency and collaboration across security operations
Prioritization (visualization)	Packaged SIEM visualizations (Alerts, Timeline, Cases) streamline operations across detection, triage, hunting, investigation, and response functions	Alerts are prioritized in a clean, extremely intuitive view; investigative drilldowns, enrichment, and threat hunting workflows enable teams to verify, scope, and prioritize accurately	Intuitive SIEM dashboards, Kibana, and Lens enable less skilled analysts to filter and process results easily, customize views, and optimize investigative workflow	Packaged SIEM visualizations enable straightforward interpretation of data; Kibana and Lens enable customization of data processing and visualizations without requiring a skilled developer
Insights (analysis)	Perform consistently fast searches regardless of number of data sources; leverage process tree visualization for fast investigations with deep endpoint context	Gain high fidelity with deep and broad enrichment; benefit from third-party-validated out-of-the-box detections designed to identify behaviors and resist evasion, mapped to MITRE ATT&CK®	Easily operationalize data enrichment; leverage out-of-the-box and/or develop custom detections/ models; integrate with other tools easily (malware detonation, threat intelligence, etc.)	Out-of-the-box ML jobs and advanced correlation methods help teams gain clear insights needed to plan and execute a hunt or respond effectively
Context (data)	Fast, federated search to quickly access and search across a complex, distributed environment	Include high-volume and non-traditional data sources and enrichment for high degree of coverage without compromising speed	Easily onboard new data sources using Elastic Agent, Beats, or Logstash, on-premises and in all major cloud environments	Normalize data with the Elastic Common Schema; index and easily access high-volume data sources without exorbitant cost

Security teams can protect users, applications, endpoints, and data with both out-of-the-box and user-defined capabilities. Advantages in indexing, distributed architecture, schema implementation, and threat prevention — built on the core tenets of platform flexibility and openness — deliver a foundational layer for security teams to build, customize, or simply use out-of-the-box packaged detections, ML, visualizations, and workflows, with broad support for a universe of technologies across your security, IT, and OT ecosystem.

Quickly and accurately answer hard questions, at scale

With this visibility, managers can improve team efficiency and incident handling efficacy and arm analysts with the skills and knowledge to be more effective security practitioners. CISOs can answer hard questions needed to ensure their teams are getting the most out of existing security investments to improve posture and reduce overall risk.

With Elastic, holistic visibility is not limited by a restrictive pricing model. What you pay is determined only by the amount of underlying server resources you use, no matter the use case or amount of data ingested. This translates to an operationally viable path to maturity and scale, without the need for constant license upgrades and increased spend for high volumes of data indexed resulting in delayed realization of value.

As an open source company, the Elastic team extends beyond our employee base. Elasticsearch, Kibana, Beats, Logstash, and the Elastic Security solution weren't built solely by us — they were built with contributions by the Elastic community. We leverage this approach to your benefit. For example, our world-class security research team develops detection rules in the open alongside the community, and we welcome community-driven detections to share collective knowledge and accelerate community learning to improve visibility for all.

About Elastic

Elastic makes data usable in real time and at scale for enterprise search, observability, and security. Elastic solutions are built on a single free and open technology stack that can be deployed anywhere to instantly find actionable insights from any type of data — from finding documents, to monitoring infrastructure, to hunting for threats. Thousands of organizations worldwide, including Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia, and Verizon, use Elastic to power mission-critical systems. Founded in 2012, Elastic is publicly traded on the NYSE under the symbol ESTC. Learn more at elastic.co.

Want to check out Elastic Security for yourself?

Try Elastic Security on Elastic Cloud (14 days free, no credit card required). Or, deploy it on-prem, where it's always free.

Start Elastic Security free