elastic

Search. Observe. Protect.

Free and open Limitless XDR

Elastic Security equips security teams to stop threats quickly and at cloud scale, with the best-in-class platform for prevention, detection, and response.

elastic.co/security

What is Limitless XDR?

Visibility, Analytics, Response

While EDR is more readily implemented into a security team's existing toolset, XDR is far more effective at boosting teams' ability to monitor, detect, and respond across the organization's full attack surface. Wondering which solution is best for your organization's needs? Why not both? With Elastic Security's Limitless XDR, EDR is a key component — alongside SIEM and cloud security — of the comprehensive solution.

XDR Whitepapers videos, case studies, etc	https://www.elastic.co/explore/security-without-limits
Elastic XDR	https://www.elastic.co/what-is/limitless-xdr
SIEM for the modern SOC	https://www.elastic.co/siem/
Endpoint security	https://www.elastic.co/endpoint-security/

Agent and data onboarding

We can get your data in the system in a minute with a number of assets, such as dashboards, saved searches, and visualizations for analyzing data. https://www.elastic.co/integrations

The Elastic Agent with the Elastic Endpoint Integration, which protects your hosts and sends logs, metrics, and endpoint security data to Elastic Security. See Configure and install the Endpoint Security integration. https://www.elastic.co/guide/en/security/current/ingest-data.html

EDR: malware, ransomware protection

Malware Prevention is ML based and evaluates the binary when it sees it. Signatureless malware prevention puts an immediate stop to malicious executables on endpoints. In its latest round of testing, AV-Comparatives found that the Elastic Security machine learning model stops 99.6% of malware and triggers zero false positives on common business software.

Behavioral ransomware prevention detects and stops ransomware attacks on Windows systems by analyzing data from low-level system processes. It is effective across an array of widespread ransomware families — including those targeting the system’s master boot record.

How to use ransomware protection to stop threats at scale

Stop attacks with Elastic's signatureless anti-malware model | Elastic

Detections

Rules run periodically and search for source events, matches, sequences, or machine learning job anomaly results that meet their criteria. When a rule's criteria are met, a detection alert is created. Enable Elastic prebuilt rules to immediately start detecting suspicious activity https://www.elastic.co/guide/en/security/current/prebuilt-rules.html

Check our Github Repository: Elastic Security will develop rules in the open alongside the community, and we're welcoming your community-driven detections https://github.com/elastic/detection-rules
Create your own rules based on EQL, ML, IOC, Threahold with a simple wizard https://www.elastic.co/guide/en/security/current/rules-ui-create.html

Free training: Elastic Security: SIEM fundamentals

Docs: Detection and Alerts

Webinar: Security detection techniques with Elastic

MITRE ATT&ck Integration https://ela.st/tj-mitre-an

Advanced analytics with ML in security and logs

If your data is in Elasticsearch, it's ready for machine learning. The Elastic Stack processes data upon ingestion, ensuring that you have the metadata you need to identify root causes or add context to any event. https://www.elastic.co/what-is/elasticsearch-machine-learning

Docs https://www.elastic.co/guide/en/security/current/machine-learning.html

Free Book (incl Screenshots) https://events.elastic.co/machinelearningwithelastic

Log Catgeories https://www.elastic.co/guide/en/observability/current/categorize-logs.html

Log Anomalies https://www.elastic.co/guide/en/observability/current/inspect-log-anomalies.html

Free training https://www.elastic.co/training/elastic-security-fundamentals-siem

Webinar https://www.elastic.co/videos/training-how-to-series-security

Free Workshops https://events.elastic.co/emea-workshops-hub-page

Blogs https://www.elastic.co/blog/author/elastic-security-intelligence-&-analytics-team

VITAS: Mitigating risk through real-time threat visibility and prevention with Elastic Endpoint Security

VITAS Healthcare has been a pioneer in the hospice movement since 1978, with more than 12,000 employees, VITAS provides care to more than 17,000 patients daily across 65 sites throughout the US.

- Identify and mitigate risk, giving them insight into adversary behavior and techniques across the organization. The forensic data provided by Elastic Endpoint Security enables them to assess top attacks and malware specimens to ensure they have appropriate protections in place.
- Additionally, automated threat prevention controls greatly reduced the need to respond to threats by running third-party virus validation scans and performing cleanups that interrupt employee daily operations, saving VITAS about $62k a year in IT operation costs.

https://www.elastic.co/customers/vitas

ECI protects its financial services clients with cutting-edge security solutions from Elastic

ECI defends its financial services clients against security threats by quickly searching event logs and identifying irregular behavior with cybersecurity solutions from Elastic. ECI provides stability, security and improved performance for more than 1,000 customers worldwide with over $3 trillion in assets.

- Deployed real-time threat response technology, machine learning for automation, and a single, unified way to ingest data into the system. XDR (eXtended Detection and Response) is another addition for unifying the capabilities of SIEM, security analytics, and endpoint security.
- Has complete transparency through access to prebuilt Kibana dashboards, to examine activity relating to their business software, and track any irregular behavior — including insider attacks. This transparency is a key differentiator for ECI as is its competitive pricing model.

https://www.elastic.co/customers/eci-deploys-cybersecurity-from-elastic

Use Cases · Elastic Stack Success Stories | Elastic Customers

How to start with XDR?

Ready to take Elastic Security Solution for a test drive and see for yourself how you can use the Elastic Stack to store, search, analyze and protect data?

1. To start with Elastic Security, you only need an Elastic Stack deployment (an Elasticsearch cluster and Kibana). Getting started with the Elastic Stack Check feature specific requirements Elastic Security system requirements

2. To ingest data, you can use the Elastic Agent with the Elastic Endpoint Integration, which protects your hosts and sends logs, metrics, and endpoint security data to Elastic Security. See Configure and install the Endpoint Security integration. To enrich your data with Threat Intelligence

3. To get a clear overview of events and alerts from your environment and drill down into areas of interest use Elastic Security app - a highly interactive workspace designed for security analysts. https://www.elastic.co/guide/en/security/current/es-ui-overview.html

4. To protect your data from malware, ransomware, memory threat, malicious behaviour install elastic agent and activate elastic security module https://www.elastic.co/guide/en/security/current/configure-endpoint-integration-policy.html

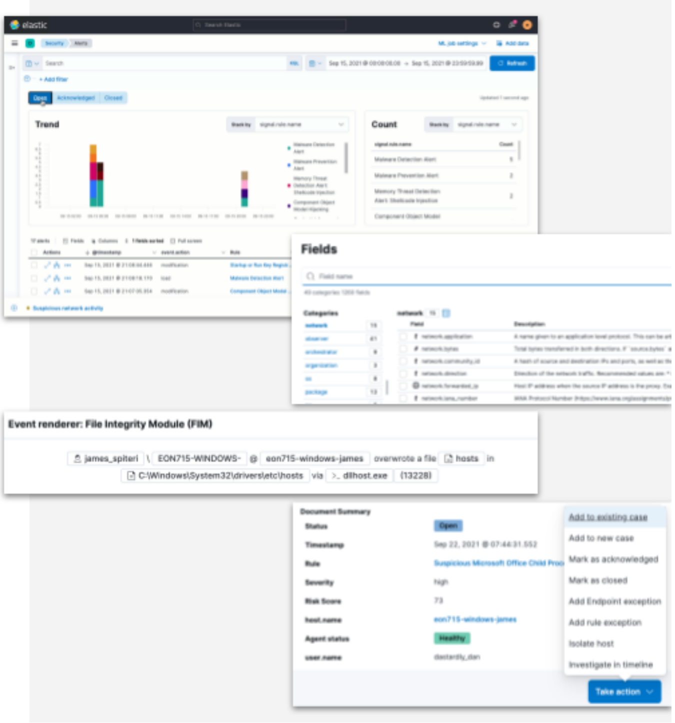
In this Quick Start guide, you'll learn how to configure your endpoints with Elastic Security so you can stream, detect, and visualize threats in real time on Elastic Cloud.
https://www.elastic.co/training/elastic-security-quick-start

Follow our best practices to design a solution that meets both the functional requirements and non-functional requirements (scalability, reliability, security, etc.) of your plan. After working through the success planning guide, apply your findings to your technical plan.
Guided journey | Elastic
Customer Success Framework Template | Elastic

Elastic Security XDR

Accelerate qualification and investigation

- **eliminates blind spots and makes it simple** to search, visualize, and analyze all of your data — cloud, user, endpoint, network, etc
- provides strong foundation for **search by petabytes** of historical data
- **automates key security processes** with OOTB **MITRE ATT&CK®**-aligned rules and stops advanced threats with behavior analytics and **cross-environment ML**
- allows to grasp quickly an unfolding attack by **correlating all relevant data** in **one intuitive user interface** and provides insights with analyst-driven correlation and simplified host inspection



Event renderer: File Integrity Module (FIM)

james_spiteri \ EON715-WINDOWS- @ eon715-windows-james overwrote a file hosts in C:\Windows\System32\drivers\etc\hosts via >_ dllhost.exe (13228)

Document Summary

Status	Open
Timestamp	Sep 22, 2021 @ 07:44:31.552
Rule	Suspicious Microsoft Office Child Proc
Severity	high
Risk Score	73
host.name	eon715-windows-james
Agent status	Healthy
user.name	dastardly_dan

Elastic Security

Prevent

Pre-execution prevention

- ❑ Malware prevention
- ❑ Ransomware prevention

Post-execution prevention

- ❑ Behavioral ransomware Prevention

Collect

Continuous visibility

- ❑ Kernel-level data collection
- ❑ Tailored host data collection
- ❑ Ad-hoc host analysis via osquery

Elastic Agent

Detect

- ❑ Alert triage and hunting workflows
- ❑ Insights, context, and recommendations
- ❑ Threat intel. integrations
- ❑ Prebuilt detections: use cases, rules, ML models
- ❑ Advanced analytics, interactive visualizations, root-cause analysis
- ❑ Fast and scalable search platform, open data schema, on-prem to multi-cloud

Elastic Stack

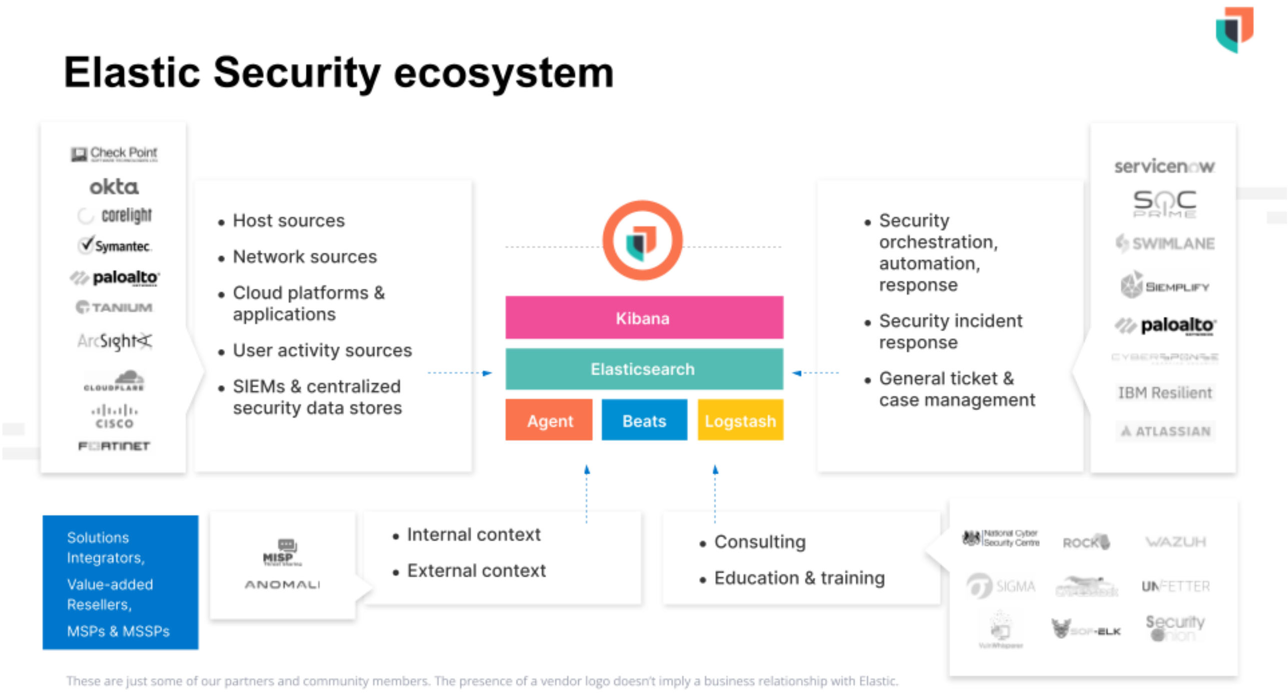
Respond

- ❑ Investigation & response workflows
- ❑ External alert actions: email, Slack, SOAR & ITSM platforms
- ❑ External case connectors: IBM, JIRA, ServiceNow, Swimlane
- ❑ Simple custom connections

Elastic Stack

- ❑ On-demand osquery inspection
- ❑ Remote host isolation

Elastic Agent



Elastic Security ecosystem

- Host sources
- Network sources
- Cloud platforms & applications
- User activity sources
- SIEMs & centralized security data stores

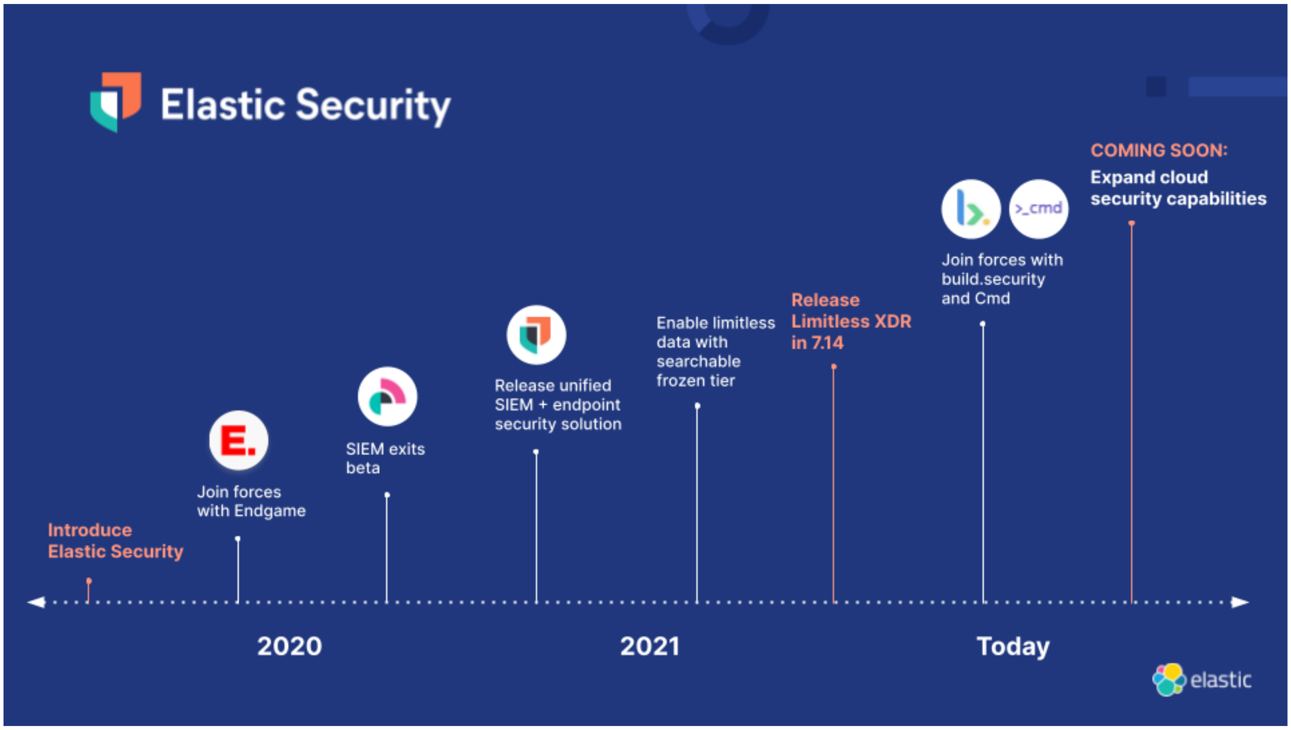
- Security orchestration, automation, response
- Security incident response
- General ticket & case management

Solutions Integrators,
Value-added Resellers,
MSPs & MSSPs

- Internal context
- External context

- Consulting
- Education & training

These are just some of our partners and community members. The presence of a vendor logo doesn't imply a business relationship with Elastic.



Elastic Security

Introduce Elastic Security

Join forces with Endgame

SIEM exits beta

Release unified SIEM + endpoint security solution

Enable limitless data with searchable frozen tier

Release Limitless XDR in 7.14

Join forces with build.security and Cmd

COMING SOON: Expand cloud security capabilities