ToolGPA

NOVEMBER 2026

# Elastic Security

## The Insider's Guide

SIEM with built-in endpoint protection, billed by data volume




**Every plan, grade, refund rule and rival among antivirus apps, read from Elastic Security's own pages.**

Made by Elastic · checked Nov 13, 2026 · toolgpa.com

1.8
GPA




# Contents


**01 Welcome**
What it is, who it suits, its grades and the ten things to know first

**02 What it costs**
Every plan, the free plan, ways to pay less and how prices have moved

**03 What it does**
Its main features, where it runs, what it works with and who makes it

**04 Where it stands**
Its grades against its category, and whether to keep it or make your own

**05 The alternatives**
The tools it is most often weighed against, side by side

**06 Quick answers**
The questions people ask about it, each answered in a line or two

**07 About ToolGPA**
Who made this guide, what else is on the site, and how to cite it


ToolGPA put this guide together from Elastic Security's own pages, its app-store listings and our grades. Every fact in it is on Elastic Security's page too, where it is kept up to date. Checked Nov 13, 2026.

# Welcome

What it is, who it suits, its grades and the ten things to know first

**1.8**

GPA, above 6 of the 56 other antivirus apps we grade

Elastic Security is a security operations platform that combines SIEM, endpoint protection and response, and workflow automation on the Elastic stack. The endpoint agent, Elastic Defend, covers Linux, macOS and Windows, and the cloud service is billed by the data it ingests and retains.

To get you started, here are **8 things to know about Elastic Security**, taken from its own pages and our grades.

> **Response actions, tamper protection and Device Control sit in the dearer Complete tier.**
>
> From our report card of Elastic Security

**1** **Best for security teams that want a SIEM with endpoint protection**

Elastic Security is a SIEM with endpoint protection built in, billed per GB of data ingested and retained rather than per device.

**2** **You can try it first**

Free trial of Elastic Cloud; length not stated on the pages read

**3** **It runs on 4 platforms**

Web, Windows, macOS and Linux.

**4** **Endpoint protection with Elastic Defend**

The agent applies behavioral protections on Linux, macOS and Windows, and the vendor says they work offline. Ransomware, memory and behavior prevention are in the entry tier.

**5** **SIEM and detection rules**

Prebuilt detection rules, triage, investigation and hunting. Elastic Security Labs writes the rules and publishes them openly on GitHub.

**6** **AI-assisted triage**

Attack Discovery correlates alerts into attack chains, and an AI Assistant helps analysts; both come with the higher Complete tier.

**7** **A 1.8 GPA, above 6 of 56**

That is against the other antivirus apps we grade, on value, the free plan, features, ease of use and platforms.

**8** **Keep it**

To replace Elastic Security you would be making an engine that recognises new malware as it appears. That is not a weekend's work, with an AI app builder or without one.

## Elastic Security at a glance

| | |
|---|---|
| PRICING<br>Free trial | FREE PLAN<br>No |
| FREE TRIAL<br>Free trial of Elastic Cloud; length not stated on the pages read | RUNS ON<br>Web, macOS, Windows, Linux |
| MADE BY<br>Elastic | CATEGORY<br>Antivirus & Malware Protection |
| OUR GRADE<br>1.8 GPA, weak | |

# The report card

## Best for security teams that want a SIEM with endpoint protection

Elastic Security is a SIEM with endpoint protection built in, billed per GB of data ingested and retained rather than per device. Response actions, tamper protection and Device Control sit in the dearer Complete tier. The bill follows how much data you send, which is hard to predict.

TOOLGPA REPORT CARD — **Elastic Security** — Graded Nov 13, 2026

| SUBJECT | GRADE | COMMENT |
|---|---|---|
| **Value for money** | C | No plan price: the page says from $0.09 and $0.11 per GB ingested, plus retention, so what you pay depends on your data and cannot be set against per-seat prices. |
| **Free plan and trial** | D | A free Elastic Cloud trial is offered but its length is not stated on the pages read, so it earns a D. |
| **Features** | C | Endpoint protection, detection rules and AI triage, but response actions, tamper protection and Device Control are Complete only. It is also a SIEM, not a plain antivirus. |
| **Ease of use** | D | It is a platform for a security team: agents, data ingest and detection rules to tune. No store rating is on record. |
| **Platforms and integrations** | B | Web console and agents for Windows, Mac and Linux, with AWS, Azure, Google Cloud and Kubernetes integrations. No phone apps. |

**Grade point average** — Weak, out of 4.0 **1.8**

An A is worth 4 points, a B 3, a C 2, a D 1 and an F nothing. The GPA is the average of the five.

## Who Elastic Security is for

- ✓ Fits if you have a security team that wants SIEM and endpoint data in one place
- ✓ Works for teams that want detection rules published openly on GitHub

## Who it is not for

- ✕ Not for you if you want a flat price per device, because the bill follows GB ingested and retained
- ✕ Pricey if you send a lot of data, since ingest and retention charges still apply
- ✕ Skip it if you want a simple antivirus: this is a platform to run
- ✕ Tight if you need response actions or Device Control, which are Complete tier only
- ✕ Watch out: AI triage comes with the higher Complete tier and the trial length is not stated

# Good to know

## Good for

- ✓ Security teams that want SIEM and endpoint protection in one data store
- ✓ Organizations that already run Elastic for logs or search
- ✓ Teams that want published detection rules they can read and edit

## Worth knowing

- ⓘ Serverless pricing has two tiers, Essentials and Complete, billed per GB ingested and retained; the page says as low as $0.09 and $0.11 per GB ingested, with no plan price to list.
- ⓘ Per-endpoint fees no longer apply as of March 23, 2026; ingest and retention charges still do.
- ⓘ Advanced endpoint features such as response actions, tamper protection and Device Control are in the Complete tier only.
- ⓘ This is a platform for a security team, not a consumer antivirus; the cost follows how much data is sent in.

# What it costs

Every plan, the free plan, ways to pay less and how prices have moved

Elastic Security's current pricing could not be confirmed from its own site.

> **A free Elastic Cloud trial is offered but its length is not stated on the pages read, so it earns a D.**
>
> From our grade for free plan and trial

We could not confirm Elastic Security's current prices from its own site, so this guide lists no plans. elastic.co has them.

# What it does

Its main features, where it runs, what it works with and who makes it

4

Places it runs: Web, macOS, Windows and Linux

SIEM with built-in endpoint protection, billed by data volume. Here is what it does, as its own site describes it, and what it covers: AI features, workflow automation, malware protection.

> **Endpoint protection, detection rules and AI triage, but response actions, tamper protection and Device Control are Complete only.**
>
> From our grade for features

### Endpoint protection with Elastic Defend

The agent applies behavioral protections on Linux, macOS and Windows, and the vendor says they work offline. Ransomware, memory and behavior prevention are in the entry tier.

### SIEM and detection rules

Prebuilt detection rules, triage, investigation and hunting. Elastic Security Labs writes the rules and publishes them openly on GitHub.

### AI-assisted triage

Attack Discovery correlates alerts into attack chains, and an AI Assistant helps analysts; both come with the higher Complete tier.

### Workflow automation

Scripted automation and AI agents run together in Elastic Workflows, so a playbook can call an agent when a step needs judgment.

### Long-term data retention

Data is kept in a searchable store billed per gigabyte retained, so older logs can be queried without restoring an archive first.

### Where it runs

Web · macOS · Windows · Linux

### What it works with

AWS · Azure · Google Cloud · Kubernetes

Elastic Security is made by Elastic.

# Where it stands

Its grades against its category, and whether to keep it or make your own

**6/56**

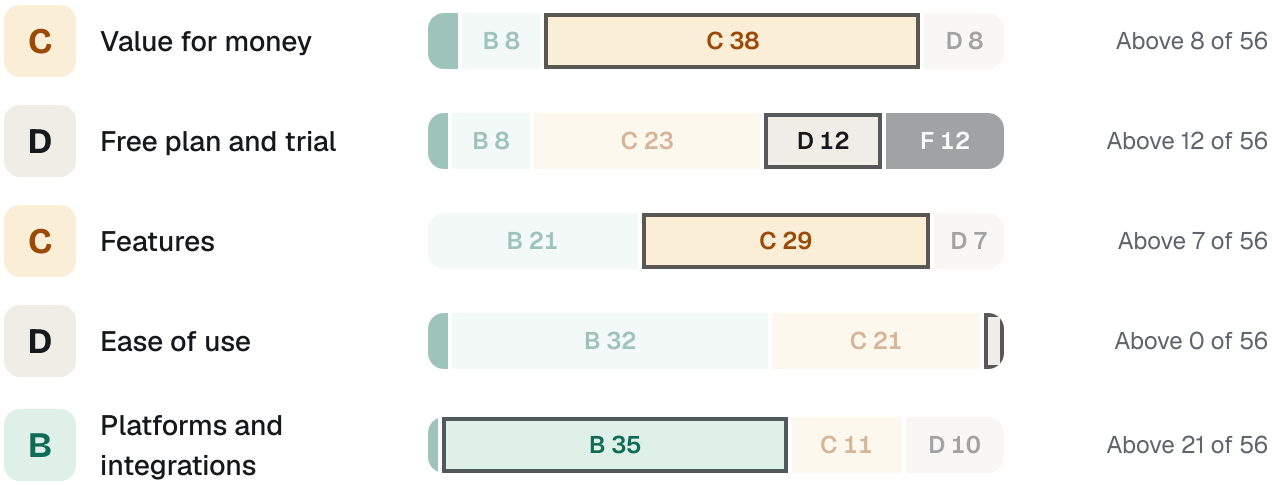
Other antivirus apps it is graded above

Elastic Security's GPA of 1.8 is higher than 6 of the 56 other antivirus apps we grade, and level with 7.

It stands best on platforms and integrations (B, above 21 of 56) and worst on ease of use (D, above 0).

## Each grade against the category

Every bar is all 57 antivirus apps we grade, cut by the letter each got. Elastic Security's own letter is outlined.




## Keep it, or make your own?

Whether this is something you could build for yourself with an AI app builder, and what you would give up.

## Keep it

To replace Elastic Security you would be making an engine that recognises new malware as it appears. That is not a weekend's work, with an AI app builder or without one.

That makes this kind of software worth paying for, not this one in particular: 43 of the 56 other antivirus apps grade higher.

### What you could not

- ✕ An engine that recognises new malware as it appears.
- ✕ Connections to other products, each kept working as those products change.
- ✕ Apps for macOS, Windows and Linux that stay in step with each other.
- ✕ AI features, unless you pay a model provider for each request yourself.

**What this rests on.** Elastic Security's listing: what it does, where it runs, what it plugs into and what it costs. It is a judgement about the kind of software this is. We have not built a replacement for it, and making your own means looking after it too. How we decide, and every tool's verdict.

# The alternatives

The tools it is most often weighed against, side by side



CrowdStrike Falcon Go, Huntress and Rapid7 InsightIDR

The 3 tools Elastic Security is most often weighed against, with where each one differs from it.

2.2 GPA

## CrowdStrike Falcon Go

Free trial · from $59.99/yr

Small-business antivirus with USB device control and mobile protection.

- Only Elastic Security lists a web app.
- Only CrowdStrike Falcon Go lists iOS and Android apps.
- Elastic Security also covers workflow automation.

Elastic Security and CrowdStrike Falcon Go compared in full

---

2.0 GPA

## Huntress

Free trial · from $8.99/mo

Managed endpoint detection and response with a 24/7 human SOC.

- Elastic Security also covers workflow automation.
- Huntress also covers reports.

Elastic Security and Huntress compared in full



1.4
GPA

## Rapid7 InsightIDR

Paid

Rapid7 SIEM and threat detection, now sold as Incident Command.

- Only Elastic Security lists Windows, macOS and Linux apps.
- Elastic Security also covers workflow automation.
- Rapid7 InsightIDR also covers reports.

Elastic Security and Rapid7 InsightIDR compared in full

# Quick answers

The questions people ask about it, each answered in a line or two

**10**

Questions, each answered in a line or two

The short version of everything above, for when you only need the answer. Each one is told in full in its part of the guide.

### Is Elastic Security free?

No, Elastic Security is a paid product, but you can try it first. Free trial of Elastic Cloud; length not stated on the pages read.

### What platforms does Elastic Security work on?

Elastic Security is available on Web, Windows, macOS and Linux.

### Does Elastic Security have an Android app?

No Android app was listed when its pages were read on Nov 13, 2026. Elastic Security is listed for Web, Windows, macOS and Linux.

### Does Elastic Security have an iPhone app?

No iPhone app was listed when its pages were read on Nov 13, 2026. Elastic Security is listed for Web, Windows, macOS and Linux.

### Is Elastic Security open source?

Elastic Security is not described as open source on its own site, as read on Nov 13, 2026.

### What does Elastic Security integrate with?

Elastic Security's listing names AWS, Azure, Google Cloud and Kubernetes.

### Who makes Elastic Security?

Elastic Security is made by Elastic.

### What are the alternatives to Elastic Security?

The closest alternatives to Elastic Security in our directory are CrowdStrike Falcon Go, Huntress and Rapid7 InsightIDR.

### How does Elastic Security compare with other antivirus apps?

Elastic Security's GPA of 1.8 is higher than 6 of the 56 other antivirus apps we grade, and level with 7.

### Could I make my own version of Elastic Security?

To replace Elastic Security you would be making an engine that recognises new malware as it appears.

## Where this guide comes from

The prices, plans, platforms and features were read from Elastic Security's own pages on Nov 13, 2026, and the grades were given on Nov 13, 2026. Graded from this listing, whose facts were read from Elastic's own pages on 13 November 2026. Not based on using the product, and shorter than our full reviews.

Every tool we list gets five grades, A to F, each with its reason, and a GPA that averages them. How each is decided is at toolgpa.com/grades. This guide is ToolGPA's own work; it is not made, paid for or approved by Elastic. Prices change, so check elastic.co before you buy.

elastic.co/security
elastic.co/pricing
elastic.co/pricing/serverless-security

PART 07 · ABOUT

# About ToolGPA

Who made this guide, what else is on the site, and how to cite it

**7,721**

Tools graded, in 95 categories

ToolGPA grades software the way a school report grades a pupil: five subjects, a letter for each with the reason written beside it, and a GPA that averages them. Prices, plans and platforms are read from each maker's own pages and dated, so you always know how fresh a figure is.

Every grade, review and ranking on ToolGPA is our own judgement. No company can pay for a grade or change one. Every tool on the site has a guide like this one, free to download and pass on. It all lives at **toolgpa.com**.

| 7,721 | 95 | 739 | 579 |
|---|---|---|---|
| tools graded | categories | price changes on record | apps priced in 12 countries |

## What else is on toolgpa.com

### Elastic Security, kept up to date

Everything in this guide, with prices and grades as they are today

toolgpa.com/tools/elastic-security

### How grades are given

The rules behind every letter and every GPA

toolgpa.com/grades

### Value charts

What each tool costs against what it scores, for every category

toolgpa.com/charts

### Compare

Any two tools side by side, plan by plan

toolgpa.com/compare

### Price changes

Every price rise and cut on record, each with its source

toolgpa.com/price-changes

### Prices by country

What apps cost on the App Store in 12 countries

toolgpa.com/prices-by-country

### Pay less

Every public discount: yearly billing, students, nonprofits

toolgpa.com/save

### Keep or make

Which tools are worth paying for, and which you could build yourself

toolgpa.com/keep-or-make

**Scan for the live page**

Prices and grades as they are today

### Quoting this guide?

Please name ToolGPA and link to the live page, so readers can check the figures for themselves:

```
ToolGPA, "Elastic Security: The Insider's
Guide", checked Nov 13, 2026.
https://toolgpa.com/tools/elastic-security
```

### Know someone choosing between antivirus apps?

Send them this guide:
toolgpa.com/tools/elastic-security/guide

ToolGPA elsewhere: youtube.com/@toolgpa

# See our other guides

The best-graded antivirus apps after Elastic Security, each with an Insider's Guide of its own.

### Antivirus & Malware Protection Insider's Guide

Every one of the 57 antivirus apps we grade, compared

### Avast Insider's Guide

Free antivirus for PC, Mac and phones, with paid Premium and Ultimate

3.0 GPA

### AVG Insider's Guide

Free antivirus for Windows, with paid Internet Security and Ultimate

2.8 GPA

### Bitdefender Insider's Guide

Antivirus suites for computers and phones, with a free Windows tier

2.8 GPA


ToolGPA

## Choosing software? Every tool graded, every price dated.

Compare tools at toolgpa.com ›



Everything in this guide is ToolGPA's own summary of what Elastic Security's pages, its app-store listings and public reviews said on the dates shown. Grades are our judgement under the rules at toolgpa.com/grades. Every grade, review and ranking on ToolGPA is our own judgement. No company can pay for a grade or change one. Elastic Security is a trademark of its owner, and this guide is not made, paid for or approved by Elastic. Prices and plans change: check elastic.co before you buy.