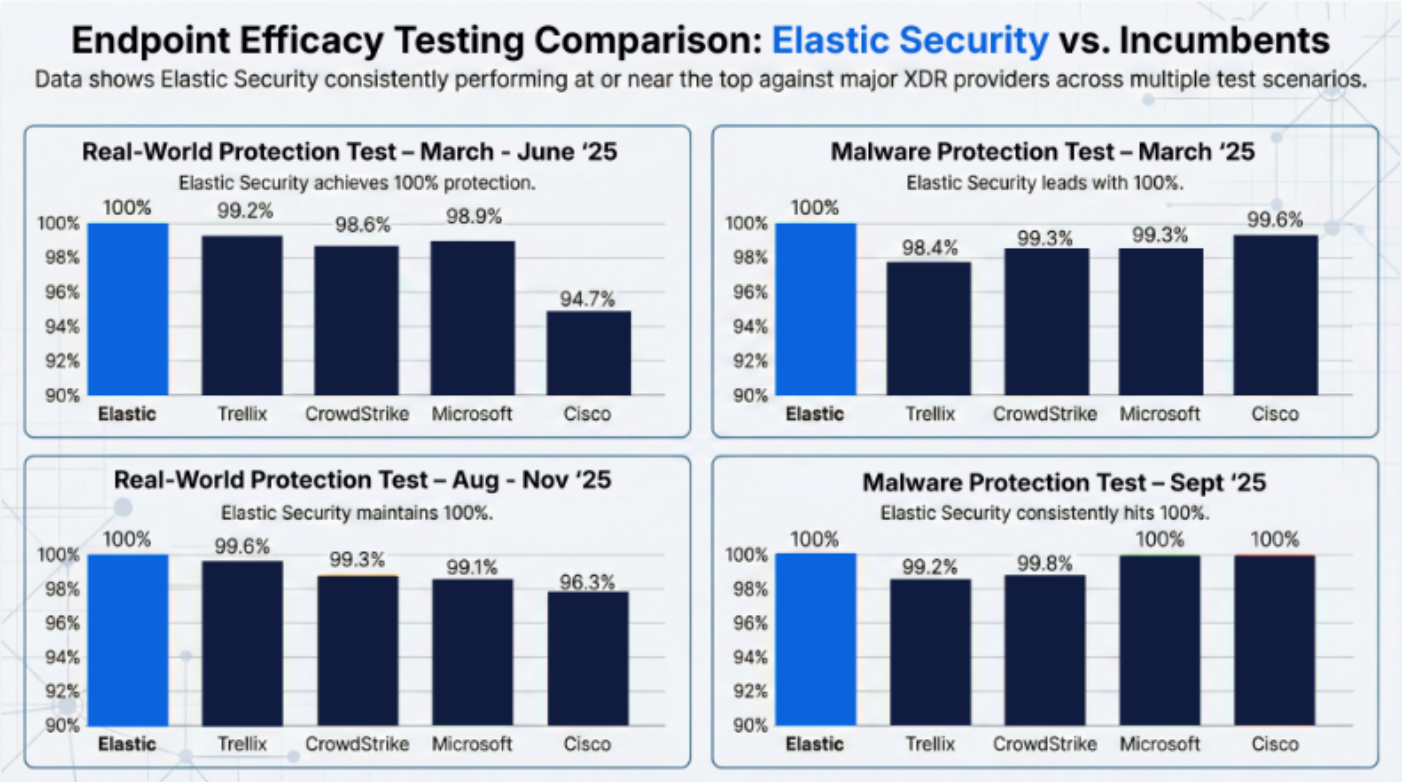
CyTech AQUILA Endpoint Agent (EDR, DLP, VDR)

AQUILA EDR leverages the core engine of **Elastic Endpoint Security**, which has been fully integrated and operationalized within the **AQUILA Cyber Monitoring and Response Domain**. This integration is not merely white labeling at the interface level. Instead, Elastic Endpoint telemetry, detection logic, behavioral analytics, and response capabilities are directly ingested into AQUILA's centralized monitoring framework. This enables our SOC to:

- Correlate endpoint telemetry with network, email, and other security domains
- Perform centralized detection, investigation, and response (DIR) workflows
- Enrich alerts with contextual threat intelligence
- Execute rapid containment and remediation actions from a unified console

By embedding Elastic Endpoint Security into AQUILA, we **strengthen endpoint visibility** while ensuring seamless interoperability across our broader cybersecurity domains. This approach enhances detection fidelity, reduces alert fatigue through correlation, and **improves mean time to detect (MTTD)** and **mean time to respond (MTTR)**.
As a result, AQUILA operates as a consolidated cybersecurity suite — delivering multiple security capabilities within a single platform, designed to support **SOC-driven operations**, **incident response readiness**, and **continuous threat monitoring**.
Please find below the images that fully reflect the standing of Elastic Endpoint Security into the real world.



The **Real-World Protection Test** is one of the most comprehensive evaluations in the industry. It runs 461 test cases that mimic online malware attacks a typical business user might encounter when surfing the internet.

- **Elastic result:** Blocked 461 out of 461 threats (100%)
- **The competition:** Elastic notably outperformed incumbents like Microsoft (99.1%), CrowdStrike (99.3%), and Cisco (96.3%), all of which allowed compromises during this test cycle.

Vendor	Blocked	User dependent	Compromised	Protection Rate [Blocked % + (User dependent %)/2][6]	False Alarms
Kaspersky	461	-	-	100%	0
VIPRE	461	-	-	100%	1
ESET	461	-	-	100%	6
Elastic	461	-	-	100%	13
Bitdefender	460	-	1	99.8%	2
Avast	460	-	1	99.8%	3
Trellix	459	-	2	99.6%	17
G Data	458	-	3	99.3%	6
K7	458	-	3	99.3%	15
CrowdStrike	458	-	3	99.3%	20
Microsoft	457	-	4	99.1%	2
Rapid7	454	-	7	98.5%	0
Sophos	451	2	8	98.0%	5
NetSecurity	452	-	9	98.0%	11
ManageEngine	449	-	12	97.4%	24
SenseOn	448	-	13	97.2%	0
Cisco	444	-	17	96.3%	3

Malware Protection Test

This test considers scenarios where malware pre-exists on the disk or enters the system via local area networks or removable devices.

- **Elastic result:** Achieved 100% detection rate
- **False alarms:** Scored a perfect result with zero false alarms on common business software

Vendor	Malware Protection Rate	False Alarms on common business software
Cisco, Elastic, ESET, G Data, Microsoft	100%	0
Bitdefender, Kaspersky, VIPRE	99.9%	0
Avast, CrowdStrike	99.8%	0
Rapid7, SenseOn	99.7%	0
Sophos	99.5%	0
NetSecurity	99.4%	0
Trellix	99.2%	0
K7	98.9%	0
ManageEngine	98.2%	0

Key Comparison Table

Aspect	Elastic Security	CrowdStrike Falcon	Microsoft Defender for Endpoint	SentinelOne Singularity	Bitdefender GravityZone
AV-Comparatives 2025 Protection Rate (Real-World + Malware Tests – Full Year Consistency)	**100% across both cycles** – Only vendor with flawless, unwavering 100% in both categories throughout 2025 (zero compromises)	99.3% (allowed some compromises in cycles)	99.1% (allowed compromises)	Not fully in main 2025 Business series (strong elsewhere)	Near-top but not consistent 100% streak
Key 2025 AV-Comparatives Win	Sole vendor standing: Perfect scores in Real-World (e.g., 461/461 blocked) & Malware – Consistent clean sweep confirmed	Solid but dipped below 100% in key tests	Solid but dipped below 100%	Excellent in other evals, but not the year-long 100% holder	High performer, but Elastic took the consistency crown
Gartner Magic Quadrant 2025 Position	Not in Leader quadrant (more niche/observability-integrated play)	**Leader** (top for vision & execution)	**Leader**	**Leader**	Visionary / Strong
Gartner Peer Insights Rating (Recent)	4.6/5 (smaller review base)	4.7/5 (3000+ reviews – massive user love)	4.4/5 (strong Microsoft ecosystem)	4.7/5 (top-tier automation)	4.8/5 (excellent value/satisfaction)

Aspect	Elastic Security	CrowdStrike Falcon	Microsoft Defender for Endpoint	SentinelOne Singularity	Bitdefender GravityZone
MITRE ATT&CK / EPR 2025	99.3% effectiveness in EPR (outscored some on detection/response)	100% in prior rounds, strong but not always top in every metric	Strong integration, but varies	High automation, often elite	Strong prevention
Core Strengths (Elastic Lens)	**Unmatched prevention consistency** + seamless SIEM/observability integration (ELK stack power for hunting/investigation) – No compromises in tests	Elite AI-driven EDR/XDR, managed hunting, breach prevention king	Deep Windows/Microsoft stack integration, cost-effective bundling	Autonomous AI response, rollback features	Lightweight, top user ratings, balanced prevention
Where Elastic Pulls Ahead	Pure block rate perfection in AV-Comparatives – If zero misses matter most, Elastic delivered where others didn't	Broader XDR/managed services dominance	Ecosystem lock-in wins for MS shops	Automation kings	Value/performance champ
Potential Drawbacks	Smaller standalone EDR footprint, setup complexity if not in Elastic ecosystem	Premium pricing, occasional ecosystem lock-in	Non-Windows gaps, occasional misses in tests	Pricing for scale	Less XDR breadth
Best Fit	Orgs prioritizing **flawless prevention + deep analytics/hunting** (Elastic users win big)	High-risk enterprises wanting top-tier managed EDR	Microsoft-heavy environments	Auto-response heavy setups	Balanced, lightweight needs

Summary

Elastic Security achieved outstanding results in the 2025 AV-Comparatives Business Security Tests, delivering a consistent 100% protection rate across both the Real-World Protection Test and Malware Protection Test throughout the year—the only vendor to maintain perfect scores with zero compromises. This performance surpassed competitors such as CrowdStrike (99.3%) and Microsoft (99.1%) in core prevention efficacy.

This proven foundation underpins solutions like **AQUILA EDR**, which is built directly on Elastic Endpoint Security's core engine and fully integrated into the AQUILA Cyber Monitoring and Response Domain. The integration extends beyond interface-level customization: Elastic telemetry, detection logic, behavioral analytics, and response capabilities are ingested natively into AQUILA's centralized platform.

This architecture enables **SOC** teams to:

- Correlate endpoint events with network, email, and other security domains
- Conduct unified detection, investigation, and response workflows
- Enrich alerts with contextual threat intelligence
- Perform rapid containment and remediation from a single console

The outcome is improved endpoint visibility, reduced alert fatigue through cross-domain correlation, faster mean time to detect (MTTD) and mean time to respond (MTTR), and a consolidated cybersecurity platform optimized for SOC-led operations, incident response preparedness, and continuous threat monitoring.

In summary, Elastic Security provides industry-leading prevention consistency and advanced analytics capabilities, while **AQUILA EDR** extends these strengths into a unified, operationally efficient SOC solution. This combination is well suited for enterprises seeking robust endpoint protection and seamless integration across security domains.

Source:

https://www.elastic.co/blog/av-comparatives-business-security-test-2025

Business Security Test 2025 (August - November) - AV-Comparatives

Business Security Test 2025 (March - June) - AV-Comparatives

Business Security Test March-April 2025 - Factsheet - AV-Comparatives

Elastic Security scores 100% in AV-Comparatives Business Security Test — Elastic Security Labs

Elastic - AV-Comparatives

Revision #2
Created 2 March 2026 06:07:48
Updated 17 April 2026 03:30:24