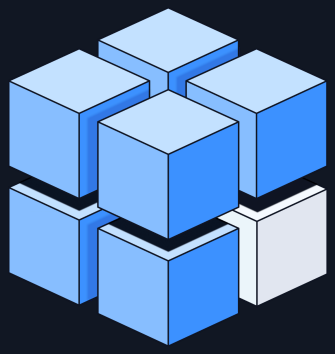
INTEZER

Your SOC, rewired for AI-driven attacks.

The AI SOC with forensic depth: Triage, Investigation, Response, and Detect and Hunt for every alert, so your team can focus on the decisions that matter.



Trusted by some of the world's most targeted enterprises

WYNDHAM HOTELS & RESORTS · hp · NVIDIA · Hilton · EQUIFAX · salesforce · MGM RESORTS · dpd

The challenge

- **Machine speed and scale:** AI-driven attackers log in with valid credentials and use your own admin tools, faster and at greater volume than a human-paced SOC can follow.
- **Hidden in low severity:** Teams and MDRs work by severity, so the low-severity alerts where real attacks hide mostly go uninvestigated.
- **AI without forensic depth:** verdicts built only on logs and other tools' conclusions still get re-verified by hand.

One AI SOC, with forensic depth

Intezer runs the full alert lifecycle on one platform, across four stages: Triage, Investigation, Response, and Detect and Hunt. Every stage is grounded in forensics, fused with AI and your organizational context. AI decides what to examine, forensics proves the findings, and each finding steers the next step. Every verdict carries its full evidence chain and tunes your detection rules.

What Intezer delivers

~1 min
average time to a verdict

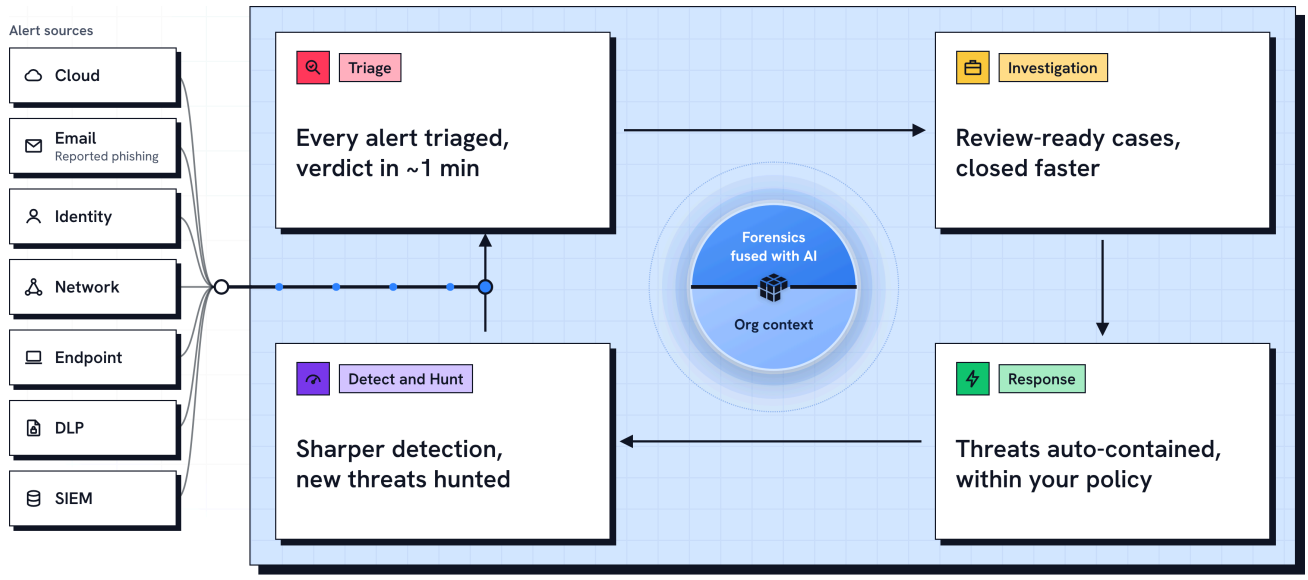
98%
verdict accuracy, evidence attached

<2%
of alerts escalated to your team

Unlimited alerts
pricing that doesn't climb with alerts

How Intezer works

The full alert lifecycle on one platform, with forensics fused with AI and org context at the center of every stage.



Why Intezer is different: forensics fused with AI reasoning

AI asks the questions, forensics proves the answers, and every verdict carries its full evidence chain.

AI reasoning

Steers every verdict

AI plans each analysis, picks the artifacts, logs and context that matter, and asks the next question.

Forensic depth

Down to the code

Memory analysis, reverse engineering and sandboxing turn artifacts into consistent, provable facts.

OrgBrain

Organizational context

Verdicts reflect your users, assets and stack, so normal work stays quiet and real anomalies stand out.

Why teams buy Intezer

Transition to agentic SOC

Outpace AI-driven attacks, with evidence behind every decision.

Replace your MDR

Full coverage, no black box, at a cost that doesn't climb at renewal.

Replace SOAR playbooks

Works out of the box: no playbook project, no scripting, no upkeep.

Fix detection coverage

Detection rules tuned in your SIEM and EDR, and new threats hunted.

Clear the alert backlog

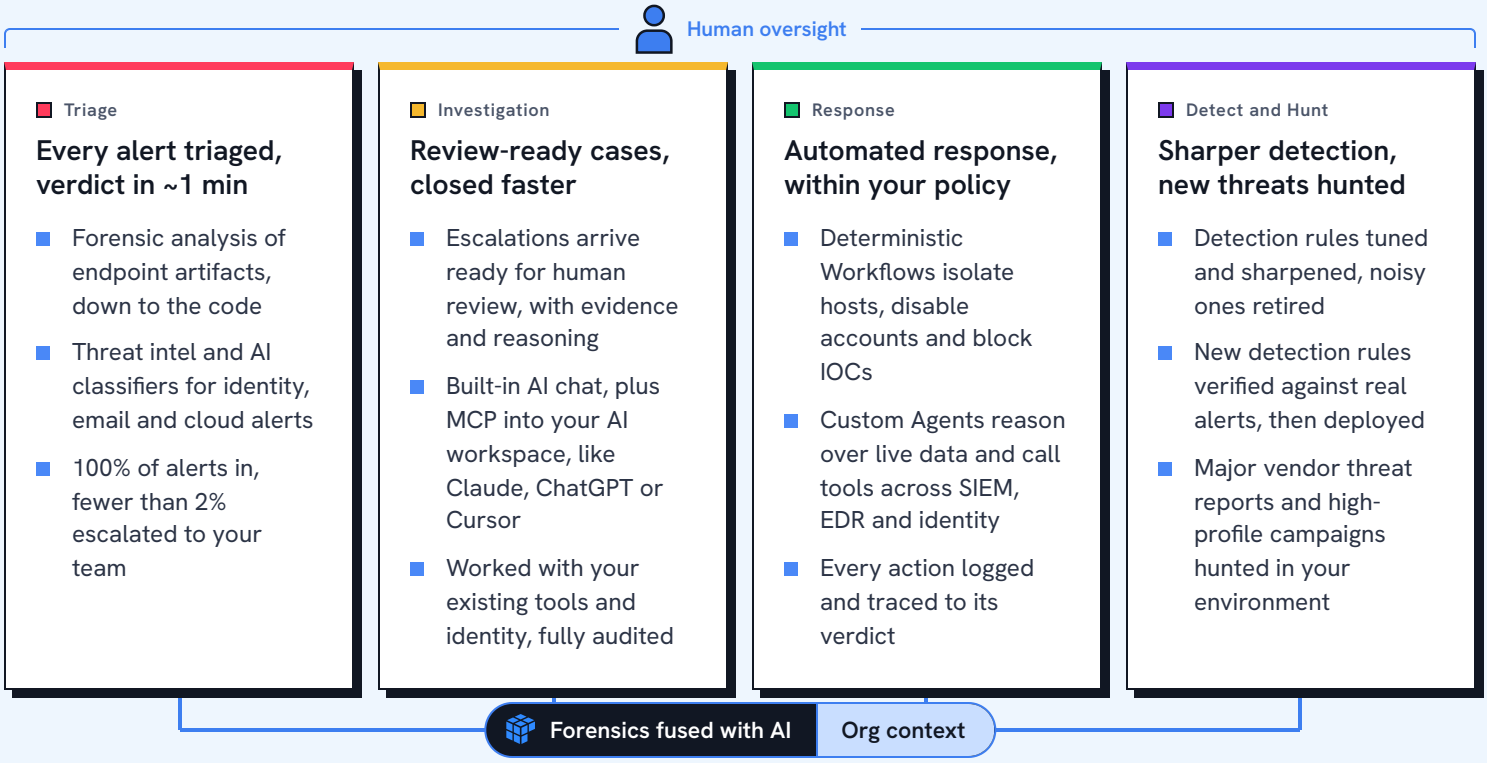
Every alert gets a verdict in ~1 min, and fewer than 2% reach your team.

Optimize your SIEM

Lower SIEM costs by cutting the logs that add no detection value.

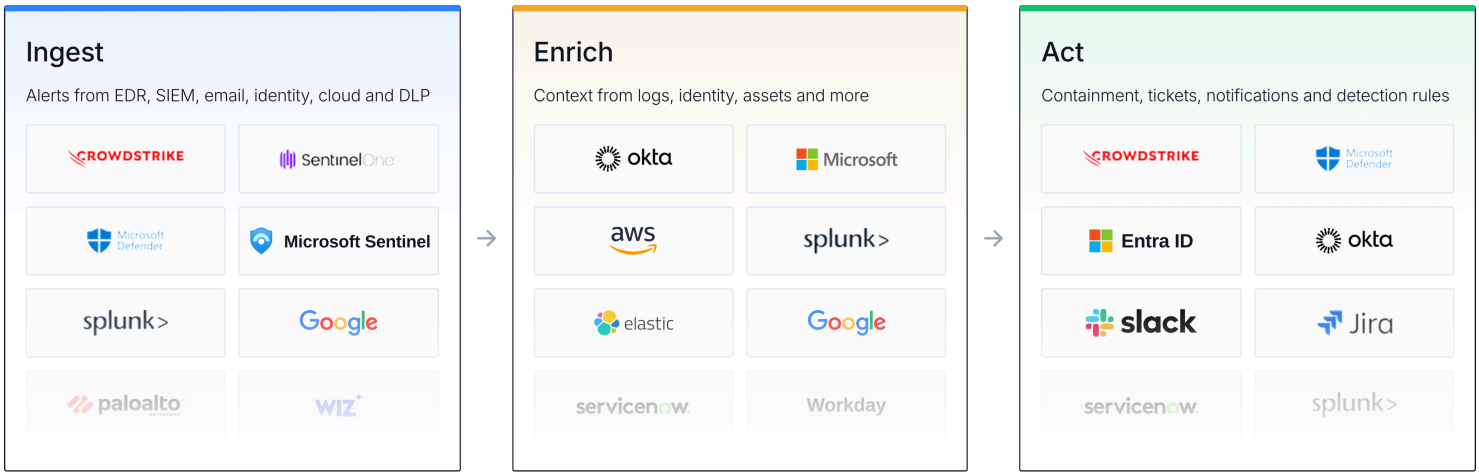
One platform, every stage

Four stages, each backed by forensics, AI reasoning and org context, and overseen by senior Intezer analysts.



Integrations across the enterprise stack

Intezer ingests your alerts, enriches them with context, and acts back through Workflows and detection rules.



> I've looked at a lot of security solutions over the years and the results from Intezer are amazing. Intezer integrates with all the modern security platforms, so teams have every alert fully investigated while enabling a fast time to respond. This technology is transformative for the efficiency and effectiveness of security operations.

Branden Newman
CTO MGM RESORTS

150+
customers, 75% of them enterprises

2,500+
hours of tier-1 SOC work saved at DPD

$2M
saved a year at RSM

Built for enterprise security teams

Audited controls
SOC 2 Type II audited, GDPR and CCPA compliant, and independently pen-tested, with reports in our Trust Center at trust.intezer.com.

Your data, protected
Data encrypted with restricted key access, deleted when you leave, and governed by our AI Quality and Governance Policy.

Expert-led setup
Each connection is set up with you and approved before it goes to production or a staging review.

Guardrails on every action
Automated response runs only within the guardrails you set, and every action is on record with its evidence.

Predictable pricing
Priced per endpoint, not per alert or AI token, so cost stays predictable as alert volume grows.

Intezer Oversight
Senior Intezer experts supervise verdicts, detection rules and hunts, and can confirm every escalation 24/7.

See every alert investigated

Bring your noisiest alert source. We'll show you how every alert is investigated, the evidence behind each verdict, and how threats are auto-contained within your policy.

Request a demo