

Malware Analysis Platform

Clear classification for your threats in seconds

Immediately Get Clear Answers About Any Suspicious File

Intezer Analyze quickly classifies malware and unknown files making it an indispensable security analyst tool.



Does it contain malicious code?



What specific type of threat is it?



Is the threat similar to a previously handled incident?



How do I respond?

No more Trojan.Generic



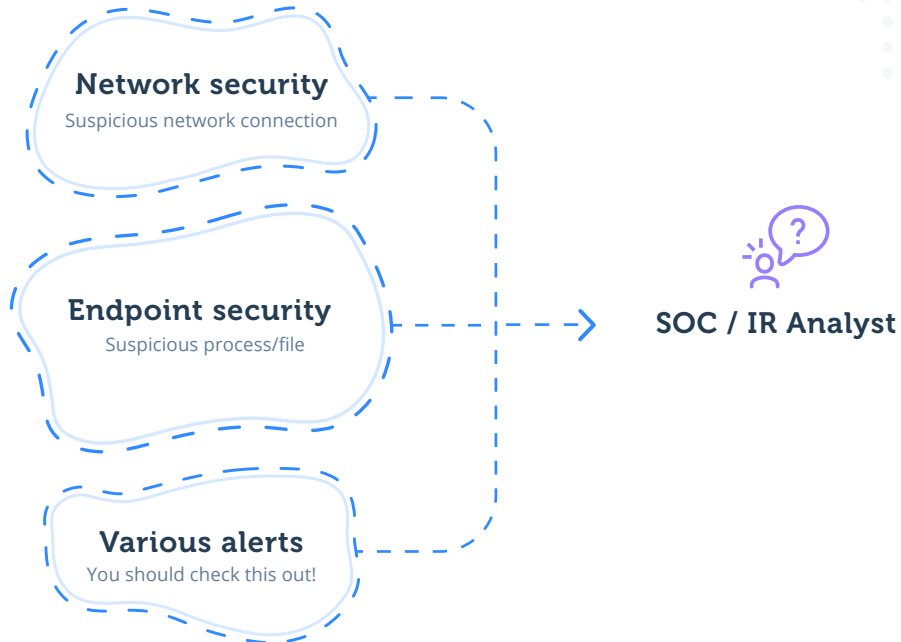
SC 2020
awards
EUROPE
FINALIST

Best Incident Response Solution

Analysis Tools Are Leaving Questions Unanswered

Current malware analysis tools often provide vague and generic results, leaving questions still unanswered.

Security Analyst Workflow



Threat Investigation Checklist



Is it a false positive?

What is the risk level and priority?

Is it related to a previous incident we had?

How do I respond and remediate?

Empowering Security Analysts in All Stages of the Response Cycle

Intezer is helping security analysts automate some of the most advanced and time-consuming assignments they face today, including reverse engineering, malware classification, and memory analysis.

Triage

Reduce false positives.
Highlight only malicious
and unique code

Rapid endpoint triage
and memory analysis

Malware Analysis

Quick malware
classification and
analysis

Differentiate between
[adware](#) and a [nation-
state attack](#)

Avoid duplicate work.
Understand if you are
dealing with a similar
threat your team dealt
with previously

Remediation

Determine malware
family to speed up
remediation

Classify malware to
dictate the appropriate
response

Threat Intelligence

Know what adversaries are
targeting you to make more
efficient security decisions
and investments

Attribute malware to
threat actor with high
confidence

Advantages

Specializing in malware classification

- Unlike Antivirus and EDRs, which mostly produce generic results (think **Trojan.Generic**) and only classify specific hashes, Intezer analyzes the code itself in order to classify the threat and identify variants from the same malware family.
- Many malware analysis solutions such as sandboxes are based on behavioral analytics. They tend to produce a lot of technical execution information and can be evaded by sophisticated attacks which are designed to behave normally.

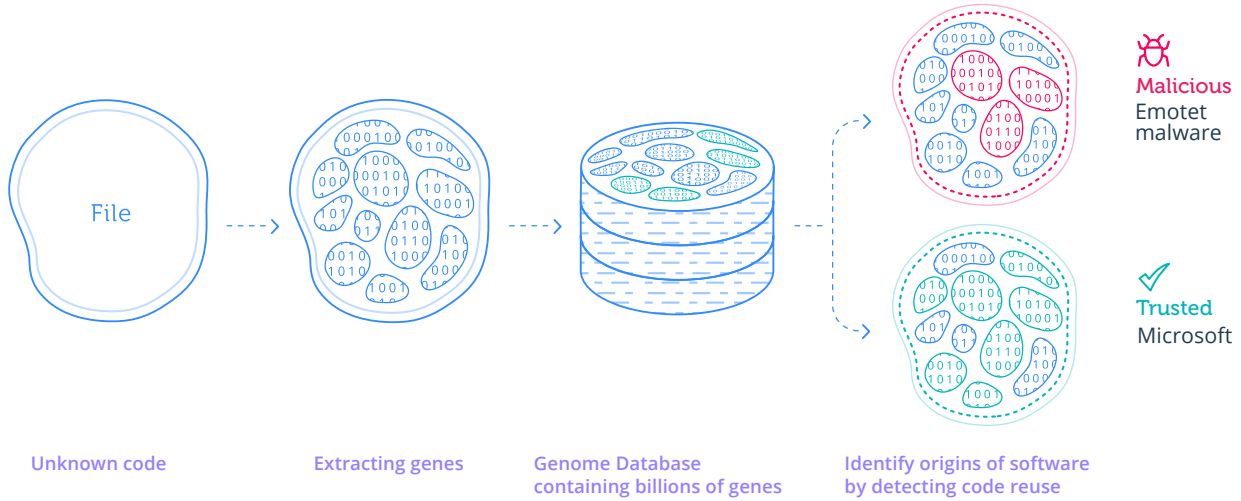
The only solution that enables malware classification at mass scale (massive pipeline or dataset of unknown files)

Accurate detection for APTs where other analysis systems fail

The only solution to classify in-memory threats from dumped processes and modules

Powered by Genetic Software Mapping Technology

Today's malware analysis solutions rely on behavioral analysis and signature-based techniques but they are struggling to provide context. Intezer classifies cyber attacks by divulging their code origins. Detecting code reuse between threats results in a much deeper understanding of any unknown or malicious file.



Creating a Globally Shared Immune System Against Cyber Threats

Intezer's unique Genome Database contains diverse code ranging from legitimate applications from trusted vendors to commonly spread malware and sophisticated APTs.



Tracing Major Global Cyber Events to their Source First

The technology behind Intezer Analyze has detected code similarities in high-profile nation-state attacks before leading engines and government agencies.



WannaCry










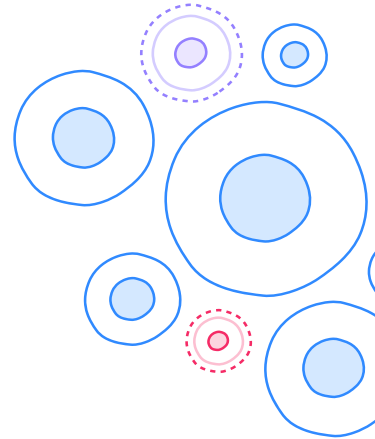
Turla



Winnti

Check out these features!

-  Custom number of file uploads per month
[Upload a file or search by hash!](#)
-  View code and string reuse
-  Download related samples
-  Conduct memory analysis on live machines
-  Accelerate RE with IDA Pro and Ghidra plugins
-  Track malware families to get updates on new samples spotted in the wild through code reuse detection
-  Classify and index files into your team's private Genome Database



IR Team Lead,
Fortune 500 company

Intezer's one-of-a-kind malware analysis technology based on code reuse detection is exactly what our IR teams needed to classify threats. Obtaining deep insights into every suspicious file in seconds saves precious time and efforts, enabling the team to focus on prioritizing and remediating attacks.



Our Partners



About Intezer

Founded by DFIR and Malware Analysis Experts

Intezer was founded by DFIR, malware analysis, and reverse engineering professionals who found that existing solutions were not providing them with the proper tools to detect and respond to modern cyber threats. This led them to develop a Genetic Software Mapping technology that is emerging as an advanced solution for classifying and responding to cyber attacks.



Alon Cohen | Chairman

Founder, former CEO of
CyberArk (NASDAQ: CYBER)



Itai Tevet | CEO

Former Head of IDF CERT
(Incident Response Team)



Roy Halevi | CTO

Former Cybersecurity
Architect at IDF



Intezer Overview

- HQ IN NEW YORK CITY
- CUSTOMERS INCLUDE FORTUNE 500 COMPANIES, GOVERNMENT ORGANIZATIONS AND FAST-GROWING TECH STARTUPS
- INVESTORS INCLUDE



OPENVIEW



Intezer is innovating threat detection and response by mapping the genetic origins of software. Intezer detects threats by identifying their code origins, with deep context for an effective response.

For more info, visit www.intezer.com or follow the company on Twitter at [@IntezerLabs](https://twitter.com/IntezerLabs).

