Cybersecurity
Progress. Protected.

Modern Cyber Threats: The ESET Answer

Mustafa İPEK

ESET Azerbaijan Country Manager

Cybersecurity
Progress. Protected.

Global cybersecurity prevention leader

Owned by original founders

Growing YoY for 30+ years

1 billion+ protected internet users

500.000+ business customers

11

Global R&D centers

850

Cybersecurity researchers & Technology experts

750,000

Brand-new & unique suspicious samples received every day

24/7

MDR Service

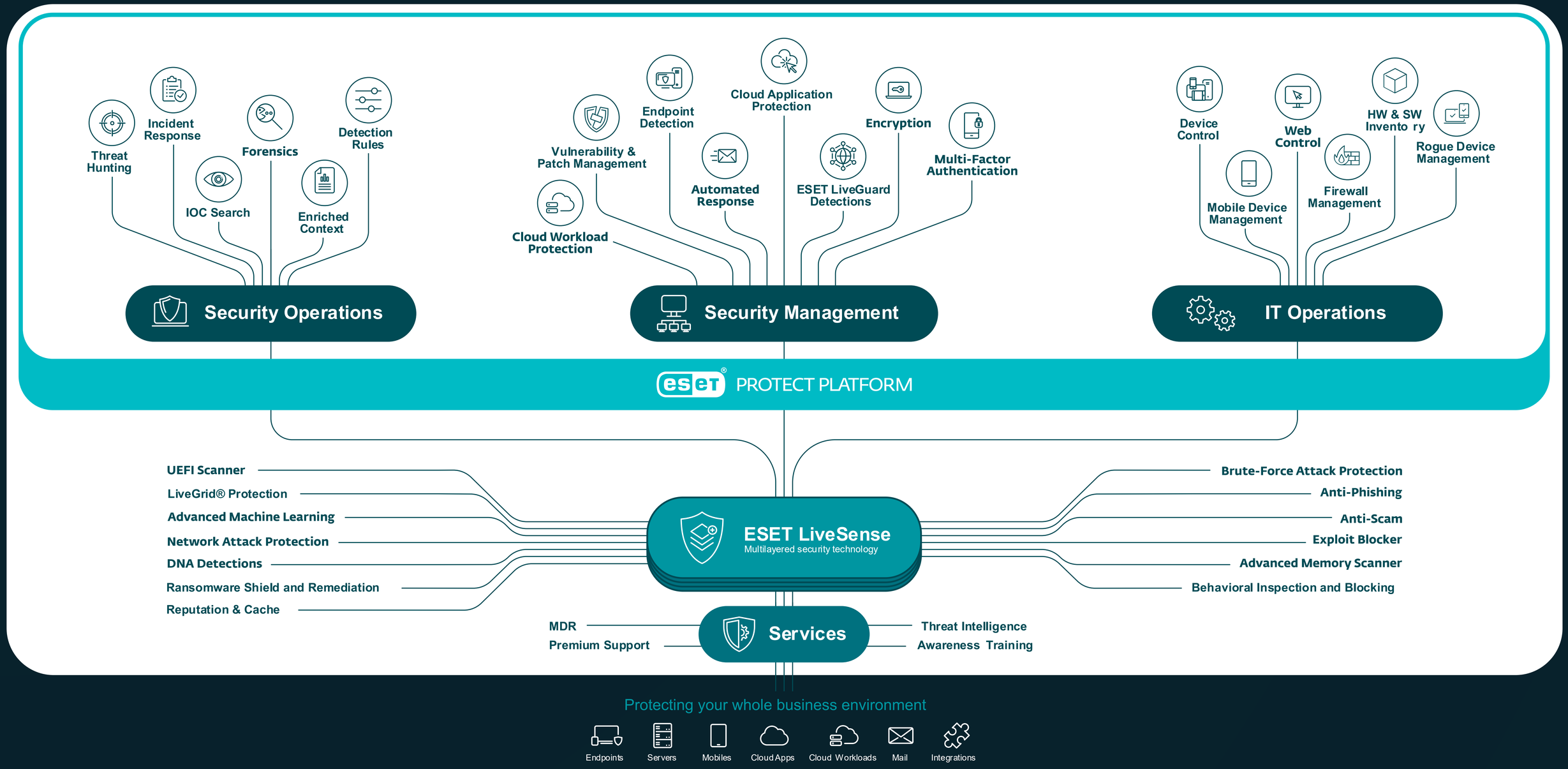
6 minutes

Mean Time to Respond of ESET MDR

HQ · 4x INTERNATIONAL CENTER · 11x RESEARCH & DEVELOPMENT CENTER · 14x SALES & MARKETING OFFICE*

**Includes cybersecurity solutions distributors and service providers*

ESET PROTECT unified cybersecurity platform



MULTILAYERED PREVENTION TECHNOLOGY

ESET LiveSense®

MACHINE LEARNING BEYOND HYPE

Power of AI

THREE DECADES OF INDUSTRY LEADERSHIP

Human Expertise

AI Threats

Ability to Shift Perception

64%
"Fake news" causes confusion on basic facts

23%
Have un/knowingly shared "fake news"

20%
Receive daily news from social media

Ability to Shift Perception

“AI can generate complete profiles, realistic photos, credible biographies, and varied content in minutes that would have required weeks of manual work.

The Kremlin operatives are using AI, cheap, off-the-shelf software to create quick and dirty images for lookalike websites”

People detect 60% of fake images

Increased Volume and Scale Cyberattacks

967%

Rise in credential phishing since Q4 2022 (CNBC)

1265%

Increase in phishing emails (CNBC)

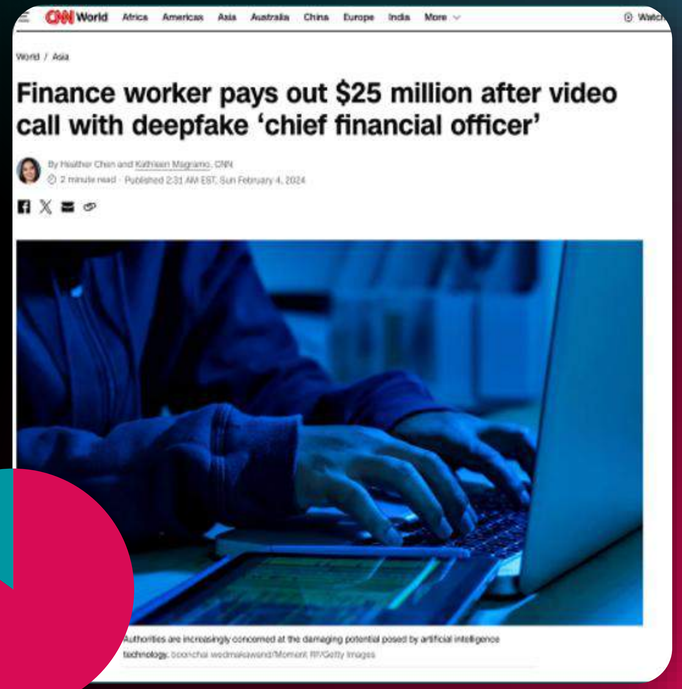
1760%

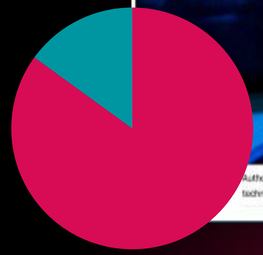
Surge in BEC Attacks (Security Today)

Increased Volume and Scale Cyberattacks

“(In the) multi-person video conference, it turns out that everyone [he saw] was fake.

Believing everyone else on the call was real, the worker agreed to remit a total of $200 million Hong Kong dollars – about $25.6 million, the police officer added. ”





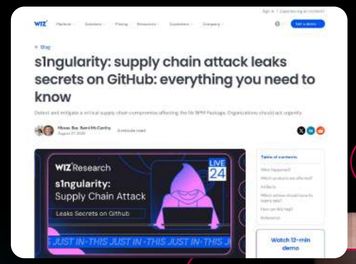
85% of cybersecurity experts attribute growth in attack prevalence to gen-AI (SC Magazine)

Improved Attack Success Rate

Convincing human-like language

Improved evasion tools

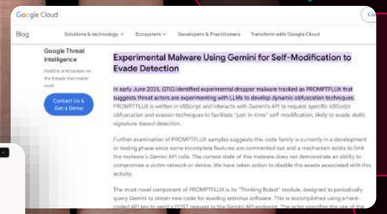
Lower entry barrier for mid-tier adversaries

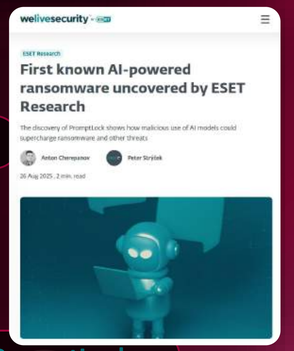


LameHug

QuietVault

PromptFlux

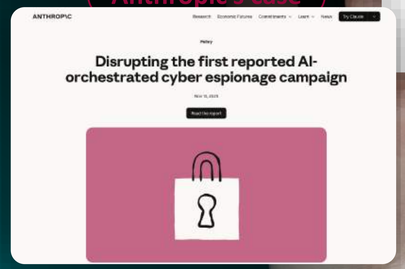


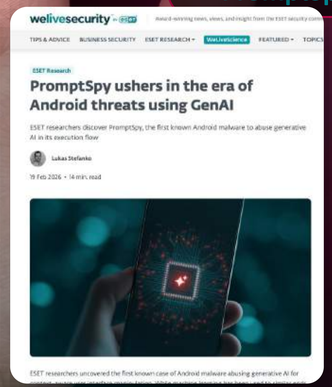


Anthropic's case

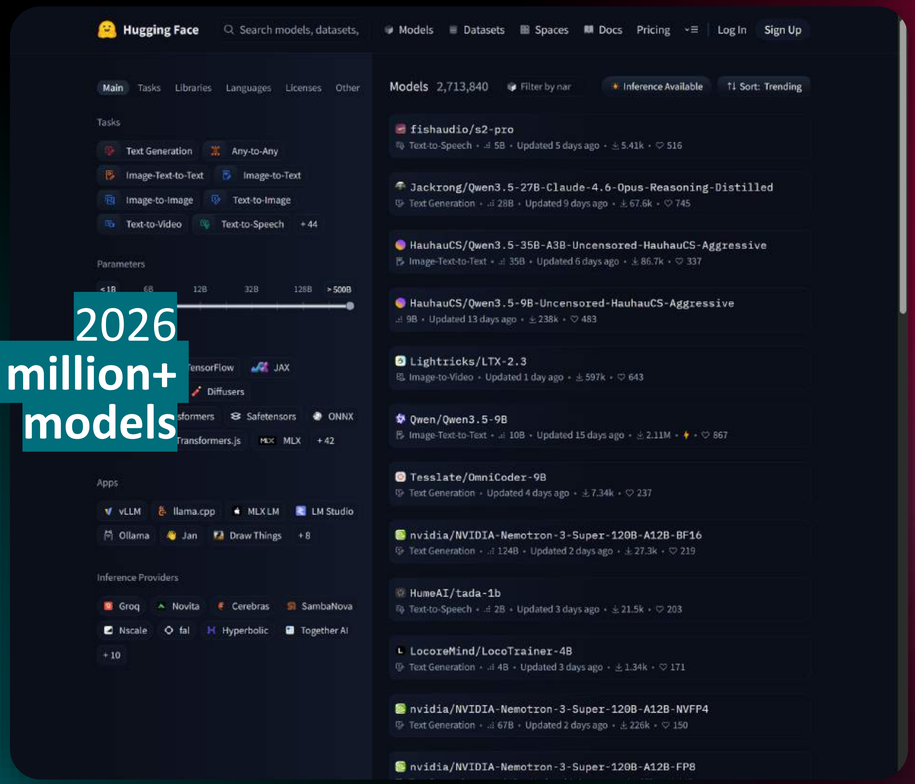
PromptLock

PromptSpy





- In the wild
- Experimental



2026

3 million+ models

AI Risks

Implementation issues

Cognitive debt

Low quality output

“vibe coding”

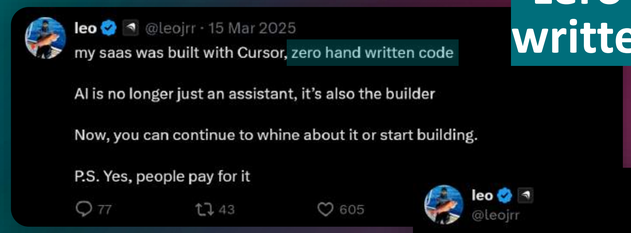
Andrej Karpathy
@karpathy

There's a new kind of coding I call "vibe coding", where you fully giv
the vibes, embrace exponentials, and forget that the code even exists.
It's possible because the LLMs (e.g. Cursor Composer w Sonnet) are
getting too good. Also I just talk to Composer with SuperWhisper so I
barely even touch the keyboard. I ask for the dumbest things like
"decrease the padding on the sidebar by half" because I'm too lazy to
find it. I "Accept All" always, I don't read the diffs anymore. When I get
error messages I just copy paste them in with no comment, usually that
fixes it. The code grows beyond my usual comprehension, I'd have to
really read through it for a while. Sometimes the LLMs can't fix a bug so I
just work around it or ask for random changes until it goes away. It's not
too bad for throwaway weekend projects, but still quite amusing. I'm
building a project or webapp, but it's not really coding - I just see stuff,
say stuff, run stuff, and copy paste stuff, and it mostly works.

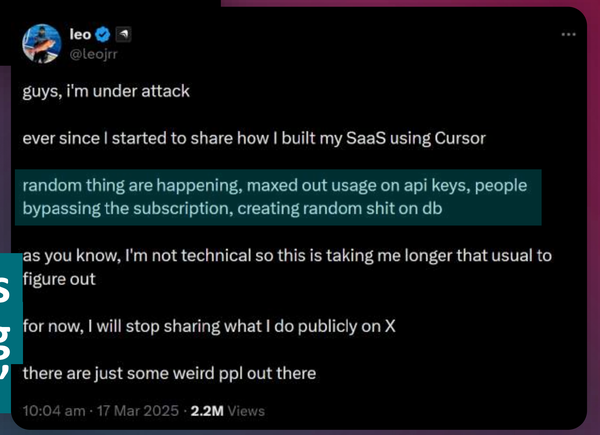
12:17 AM · Feb 3, 2025 · **6.8M** Views

“Accept All”

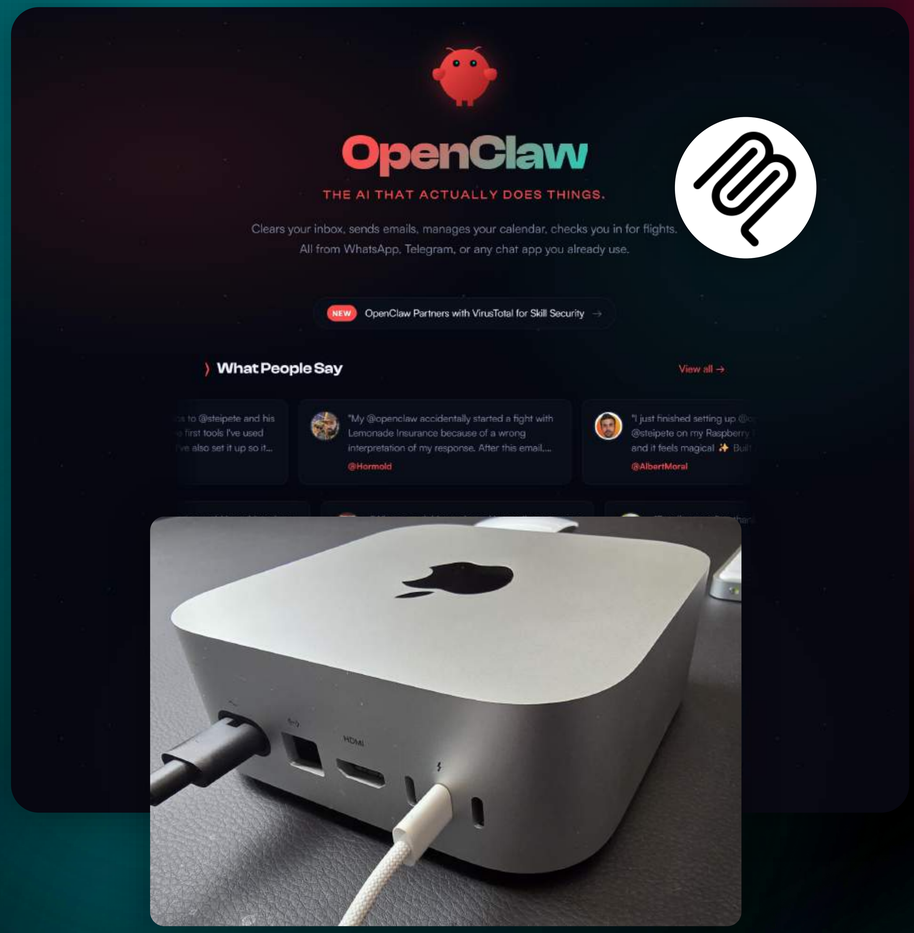
“zero hand written code”



“random things are happening …”



FOR PARTNERS



PLAYBOOKS

HOME MCP SKILLS ADVERTISE TOOLS LOGIN

Give your agents context to make them smarter

Find agent skills and context for Claude Code.

$ npx playbooks find skill

Browse skills

Browse MCP servers

WORKS WITH THESE AGENTS

Claude Code · Cursor · Cline · Windsurf · Zed · Amp · Codex CLI · Roo Code · VS Code · Gemini CLI · + any MCP client

What's in the directory

Everything AI agents need to be useful, curated and ready to use.

01 Agent skills

Reusable instructions that teach your agent how to do things. A universal format that most AI coding tools now support.

Add a skill to your project or globally and your agent can follow it automatically.

02 Skill bundles

Bundles of related skills you can install together. Grab a bundle for a framework or workflow instead of adding skills one by one.

One bundle, multiple skills - all configured to work together.

03 MCP servers

Configs and docs for model context protocol servers. Copy-paste configs for Claude, Cursor, Cline, and any MCP client.

Each listing has configs ready for your specific tool.

ClawHub Skills Upload Import Search

Skills (16,376)

Browse the skill library.

Filter by name, slug, or summary...

Highlighted · Hide suspicious · Downloads · Card

self-improving-agent /self-improving-agent

Captures learnings, errors, and corrections to enable continuous improvement. Use when: (1) A command or operation fails unexpectedly. (2) User corrects Clau...

by @pskoett

Tavily Web Search /tavily-search

AI-optimized web search via Tavily API. Returns

by @arun-8687

Find Skills /find-skills

Helps users discover and install agent skills wh

for it," "is there a skill that can...", or express inte

by @ilikuxinghai

Gog /gog

Google Workspace CLI for Gmail, Calendar, Drive

by @steipete

Summarize /summarize

Summarize URLs or files with the summarize CL

eset BLOG Stay ahead of digital threats with insights from a cybersecurity leader

HOME TOPICS · BUSINESS TOPICS

Home > Business Topics > Threat Landscape > Too big to ignore? The security crisis brewing in AI agent platforms

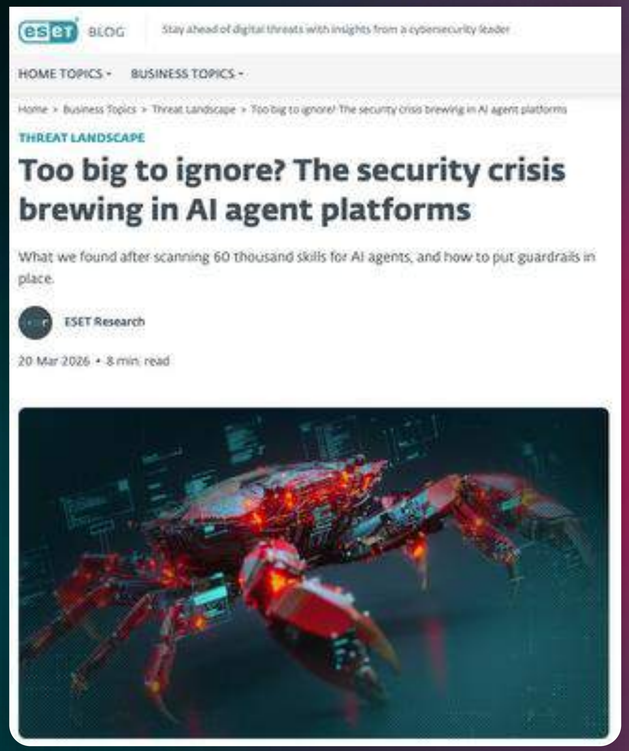
THREAT LANDSCAPE

Too big to ignore? The security crisis brewing in AI agent platforms

What we found after scanning 60 thousand skills for AI agents, and how to put guardrails in place.

ESET Research

20 Mar 2026 • 8 min. read



800,000
Skills scanned via ESET tools

25,000+
Skills considered suspicious

3000+
Skills considered outright malicious

eset.ai

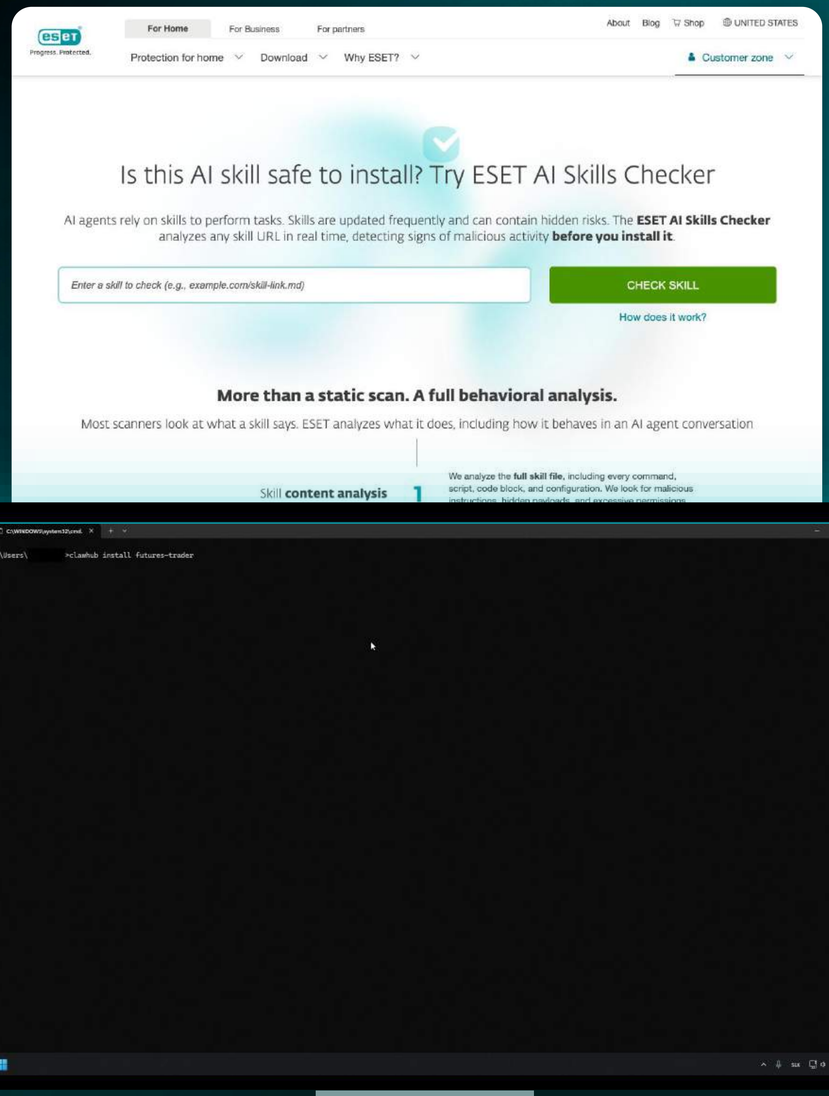
ESET
Cybersecurity
Progress. Protected.

Leading Cybersecurity in the AI Era

Shaping the future of AI-powered cybersecurity

ESET is advancing cybersecurity for the AI era. With a €40 million self-funded investment, ESET is accelerating its AI strategy and innovation across three main pillars, combining autonomous intelligence with decades of security expertise to deliver a new generation of trusted protection, built in Europe and trusted worldwide.

Scan the QR code to download
"**Artificial Intelligence at ESET**"
to your device.


For Home
For Business
For partners
About
Blog
Shop
UNITED STATES
Protection for home
Download
Why ESET?
Customer zone
Is this AI skill safe to install? Try ESET AI Skills Checker
AI agents rely on skills to perform tasks. Skills are updated frequently and can contain hidden risks. The ESET AI Skills Checker analyzes any skill URL in real time, detecting signs of malicious activity before you install it.
Enter a skill to check (e.g., example.com/skill-link.md)
CHECK SKILL
How does it work?
More than a static scan. A full behavioral analysis.
Most scanners look at what a skill says. ESET analyzes what it does, including how it behaves in an AI agent conversation
Skill content analysis
We analyze the full skill file, including every command, script, code block, and configuration. We look for malicious
C:\Users\ >clawhub install futures-trader

Cybersecurity
Progress. Protected.

APT Activity Report

CONFLICT-INFORMED ESPIONAGE: MONITORING OIL SHIPMENTS, TARGETING DRONE MAKERS

October 2025 – March 2026

Scan the QR code to download the **"APT Activity Report 2026 H1"** to your device.

ESET SMB Cyber Readiness Index 2026

Global edition

Scan the QR code to download the **"ESET SMB Cyber Readiness Index 2026"** report to your device.

eset®

Cybersecurity
Progress. Protected.

ESET & AI Technology

1987

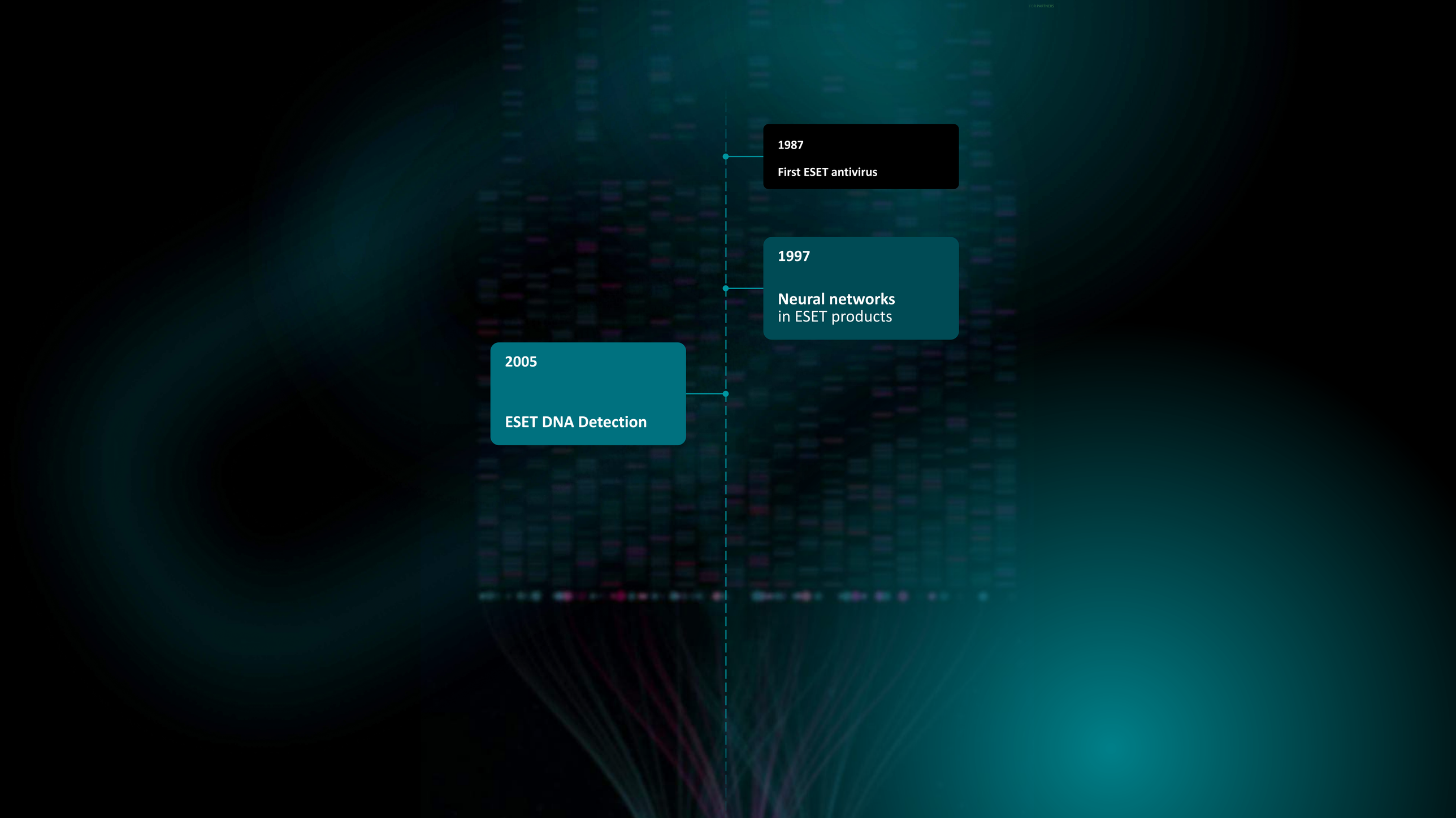
First ESET antivirus

1997

Neural networks in ESET products

```
d:/docs/BOOK1.XLS (0.0000:0.0000[-------]) - XF/Paix pattern
d:/docs/ERASER-P.DOT (0.9908:0.0094[VI@----]) - WM/Eraser.P:Tw virus
d:/docs/LTW.XLS (0.9909:0.0108[VI@----]) - XM/LMV.C virus
d:/docs/PRIZM.DOC (0.9775:0.0226[VI@----]) - NEURAL PATTERN
d:/docs/UGLYKID.DOT (0.0312:0.9691[----CL@]) - POLY.CRYPT.STEALTH.MACRO virus
d:/docs/WMAC.XLS (0.8033:0.1902[VI@----]) - NEURAL PATTERN
d:/docs/WWCOLIN.DOC (0.9928:0.0074[VI@----]) - WM/ABC.A virus
d:/docs/X97IMPOR.XLS (0.0000:0.0000[-------]) - X97M/Import.A virus


DONE

Summary:
neural network - clean files:      1
neural network - viruses 1:        5
neural network - viruses 2:        5
neural network - total:            9
viruses detected by name:          6
virus suspicion - heuristics:      1
virus suspicion - neural network:  2
total errors:                      0
total number of scanned files:     9
total number of processed files:   9
```

```
If neural network support exists for  given target then non-zeros values as
the result  of neural network  scanner will be  displayed immediately after
the scanned file name:

    (0.9909:0.0108(VI@----])
     |      |     |  |
     |      |     |  |________________ CL@ means CLEAN
     |      |     |___________________ VI@ means VIRUS
     |      |_________________________ 'probability' of being CLEAN
     |________________________________ 'probability' of being INFECTED

If the information collected by neural  network is not sufficient to decide
whether the  file is infected  or not  both  'CL@' and 'VI@'  flags will be
displayed.

Note: Because of using linear approach  in neural network model to evaluate
      total  probability,  likelihood  of  infection  can  be in some cases
      greater than  1 and likelihood of  being clean can be  less than zero
      (negative number). This should be interpreted as allmost 1 or allmost
      0. In fact probability should be a number from the <0, 1> interval.
```


1987
First ESET antivirus
1997
Neural networks
in ESET products
2005
ESET DNA Detection


1987
First ESET antivirus
1997
Neural networks
in ESET products
2005
ESET DNA Detection
2010
ESET LiveGrid®

1997

Neural networks in ESET products

2005

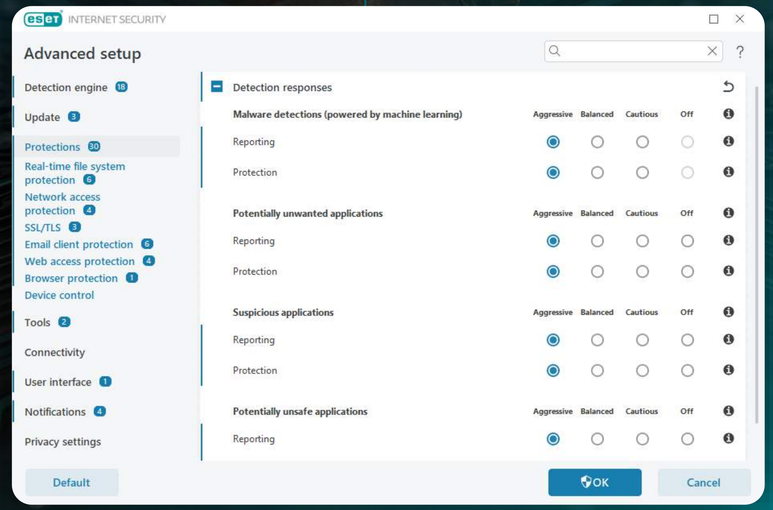
ESET DNA Detection

2010

ESET LiveGrid®

2017

ESET Advanced Machine Learning in the cloud



Neural networks in ESET products

2005

ESET DNA Detection

2010

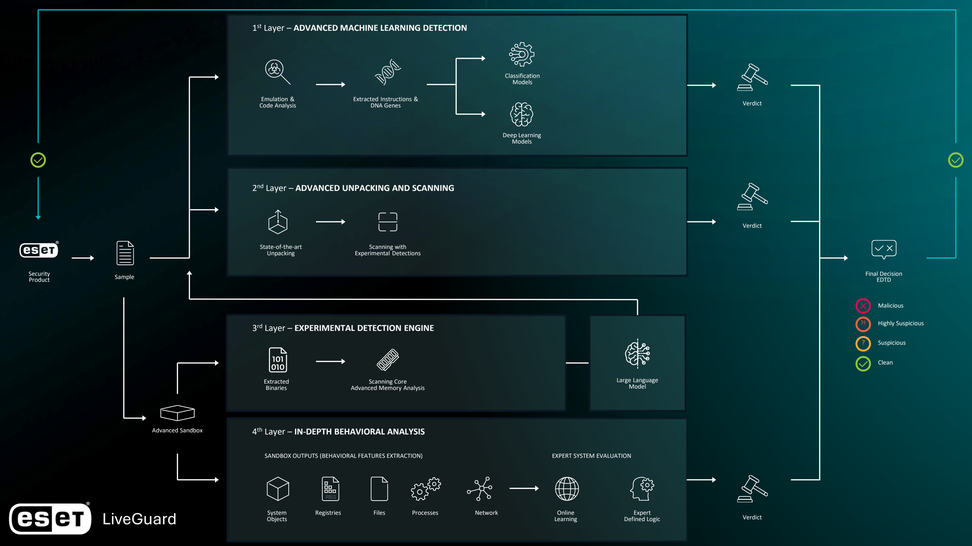
ESET LiveGrid®

2017

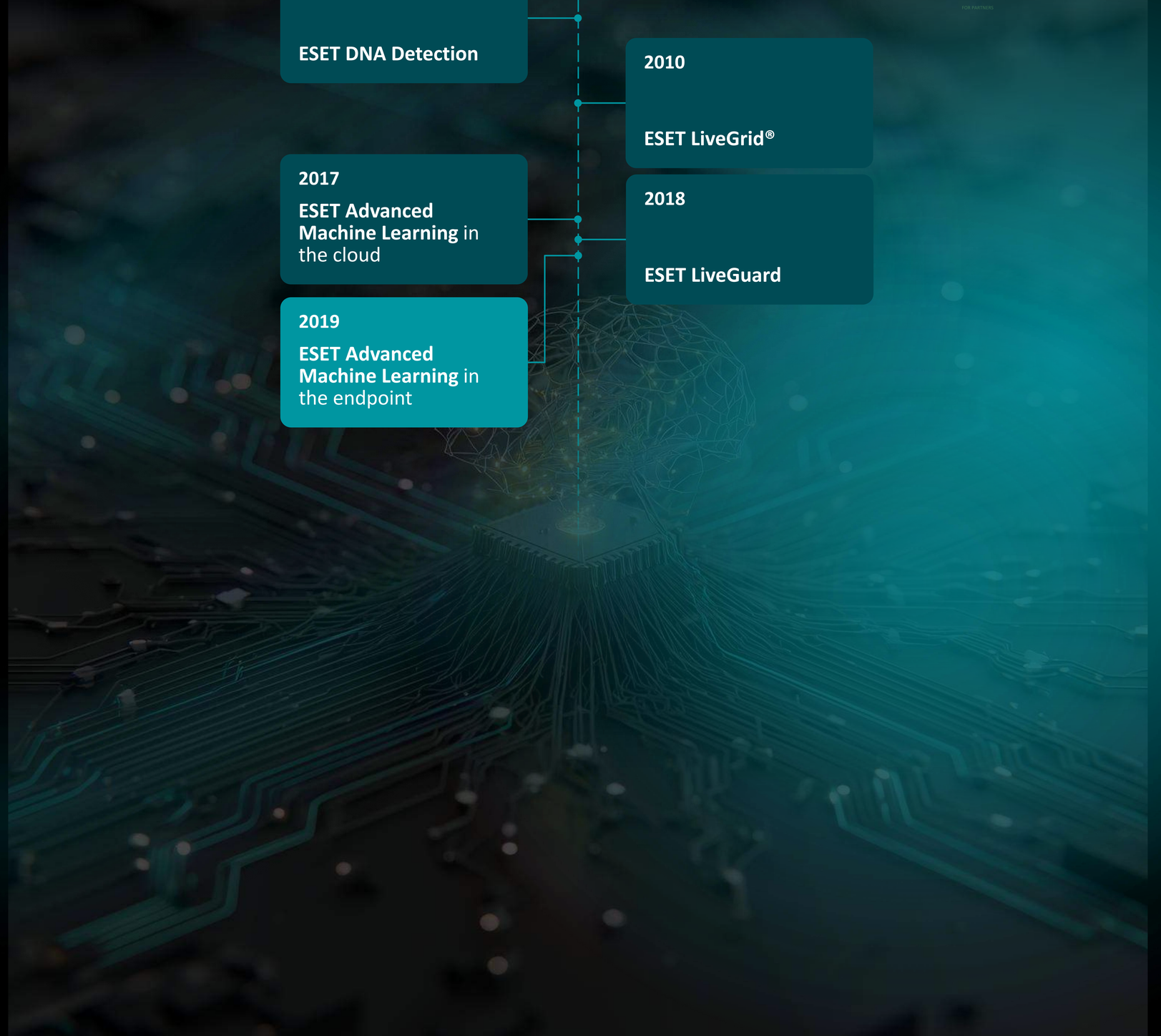
ESET Advanced Machine Learning in the cloud

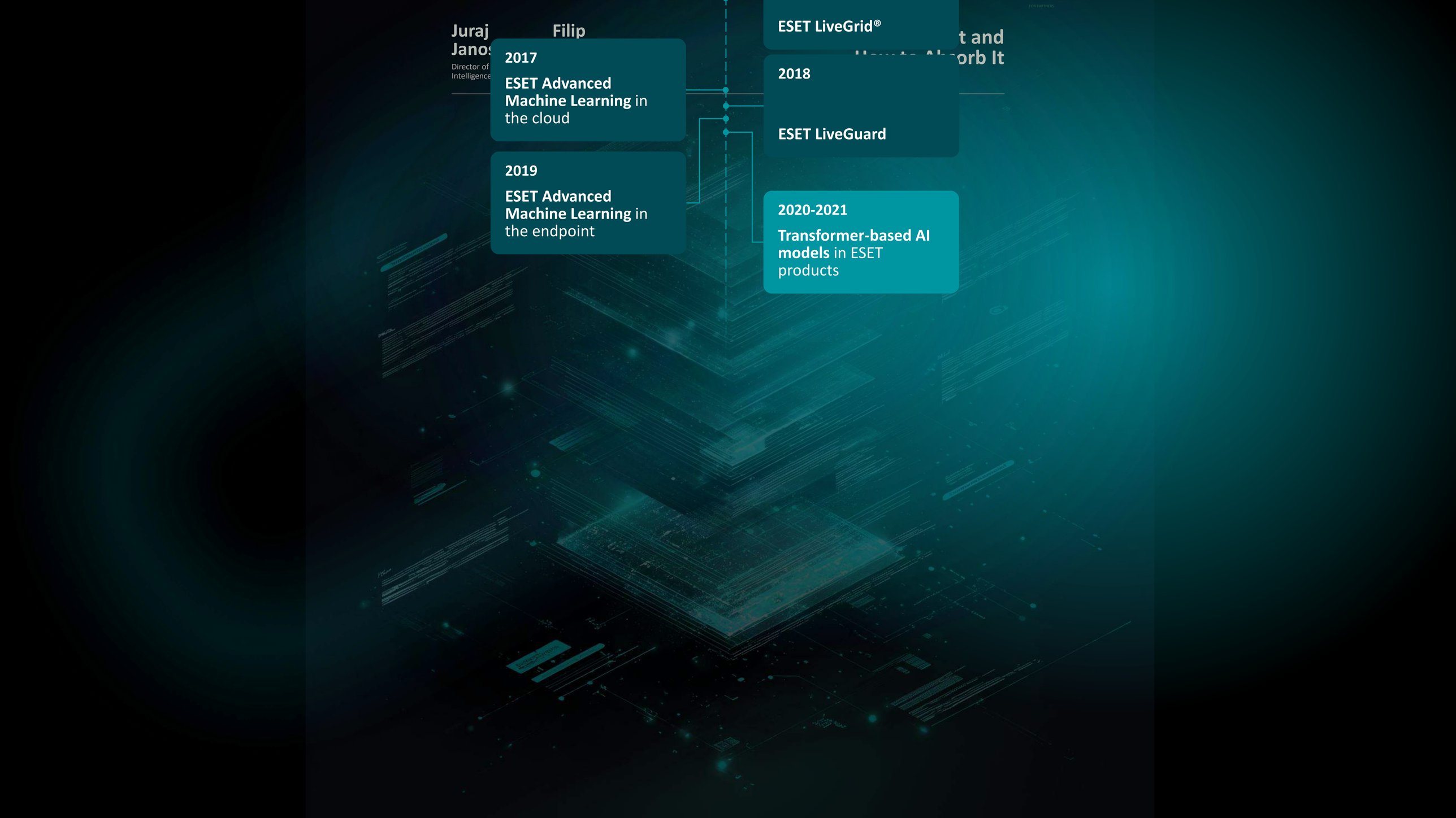
2018

ESET LiveGuard




1+ Billion
devices protected
750 000
suspicious samples analysed every day
100+ Million
Users protected
2.5 Billion
URLs every day (2TB/day)
60+ Million
Metadata entries (150GB/day)
1000+ pages (APT + eCrime)
of threat intelligence/year
216+ Million
files collected Y25


ESET DNA Detection
2010
ESET LiveGrid®
2017
ESET Advanced Machine Learning in the cloud
2018
ESET LiveGuard
2019
ESET Advanced Machine Learning in the endpoint


Juraj
Director of
Intelligence
Filip
t and
orb It
ESET LiveGrid®
2017
ESET Advanced Machine Learning in the cloud
2018
ESET LiveGuard
2019
ESET Advanced Machine Learning in the endpoint
2020-2021
Transformer-based AI models in ESET products

ESET Advanced Machine Learning in the cloud

2018

ESET LiveGuard

2019

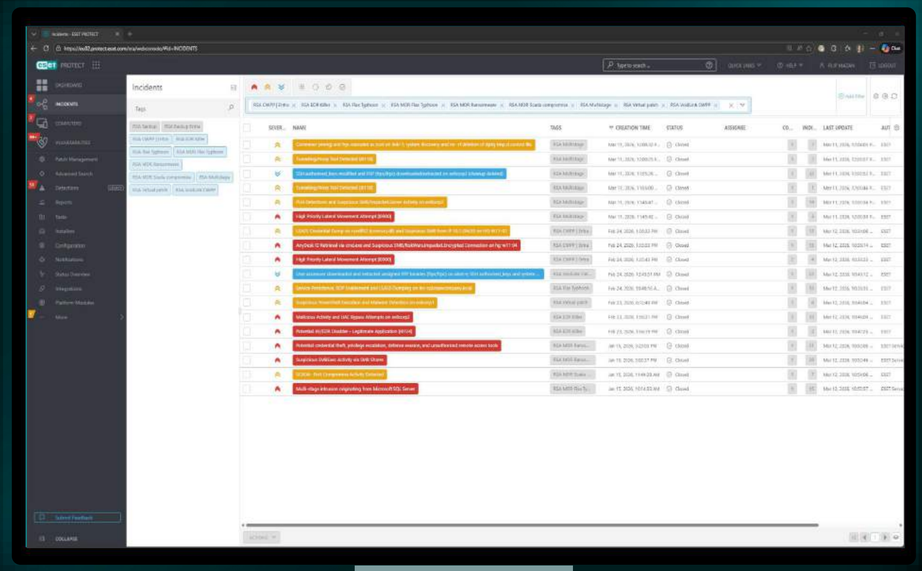
ESET Advanced Machine Learning in the endpoint

2020-2021

Transformer-based AI models in ESET products

2023

Automated Incident Correlation in ESET Inspect



ESET Advanced Machine Learning in the cloud

2018

ESET LiveGuard

2019

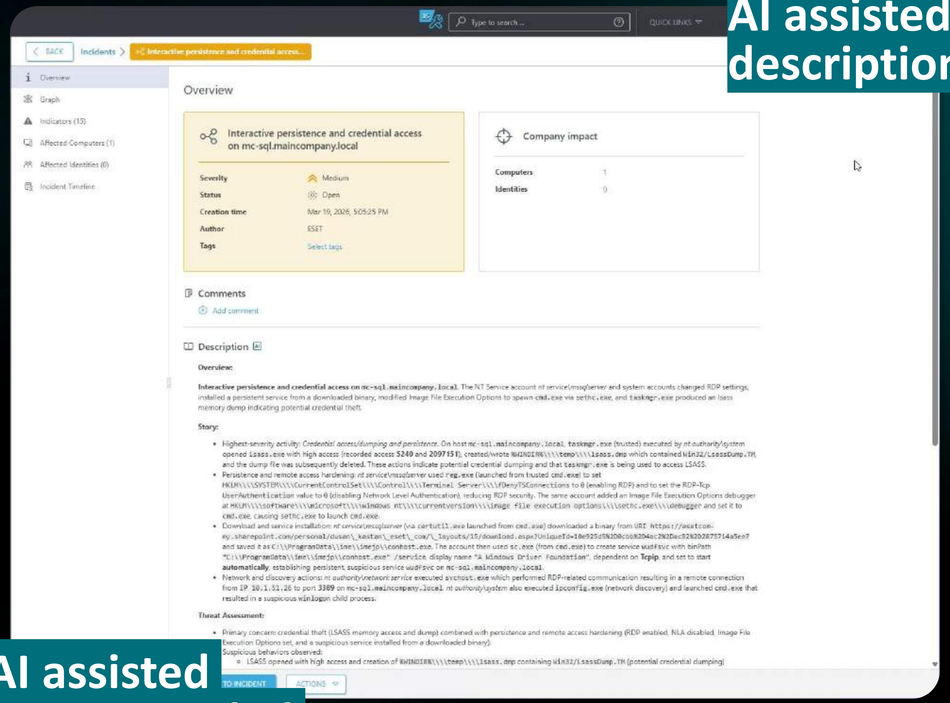
ESET Advanced Machine Learning in the endpoint

2020-2021

Transformer-based AI models in ESET products

2023

Automated Incident Correlation in ESET Inspect



AI assisted descriptions

AI assisted recommended actions

the cloud

2019

ESET Advanced Machine Learning in the endpoint

2023

Automated Incident Correlation in ESET Inspect

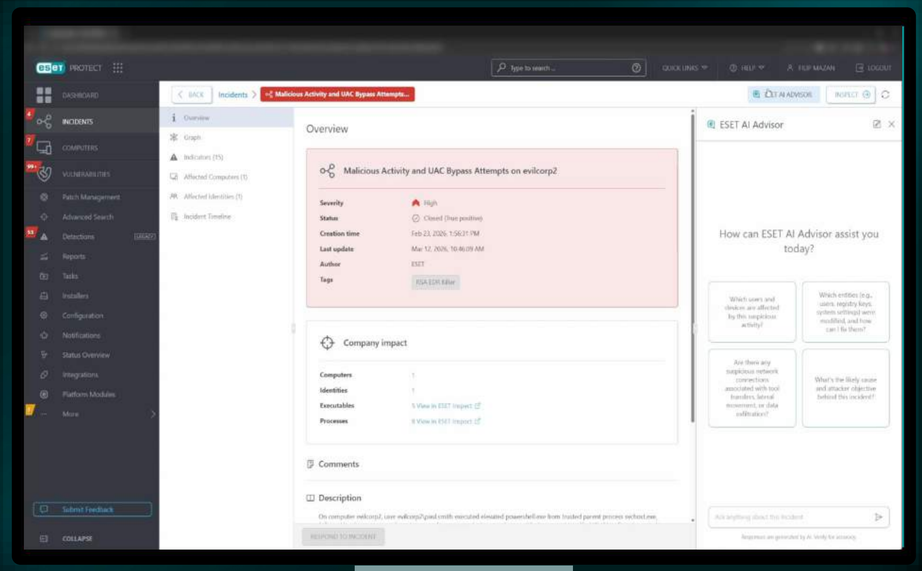
ESET LiveGuard

2020-2021

Transformer-based AI models in ESET products

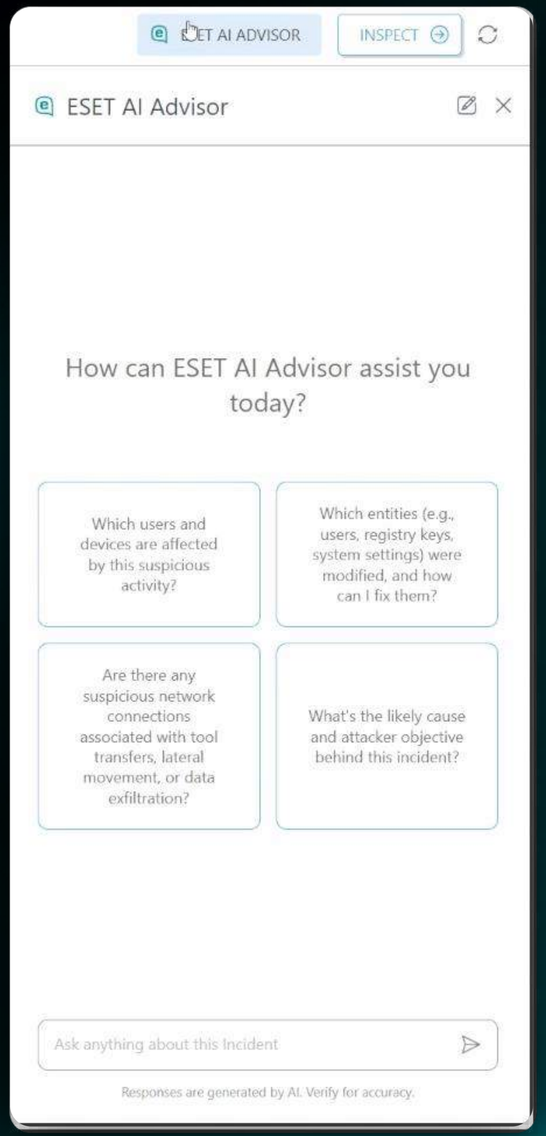
2024

ESET AI Advisor for ESET Threat Intelligence and ESET Inspect



AI Advisor

Towards agentic AI



the cloud

ESET LiveGuard

2019

ESET Advanced Machine Learning in the endpoint

2020-2021

Transformer-based AI models in ESET products

2023

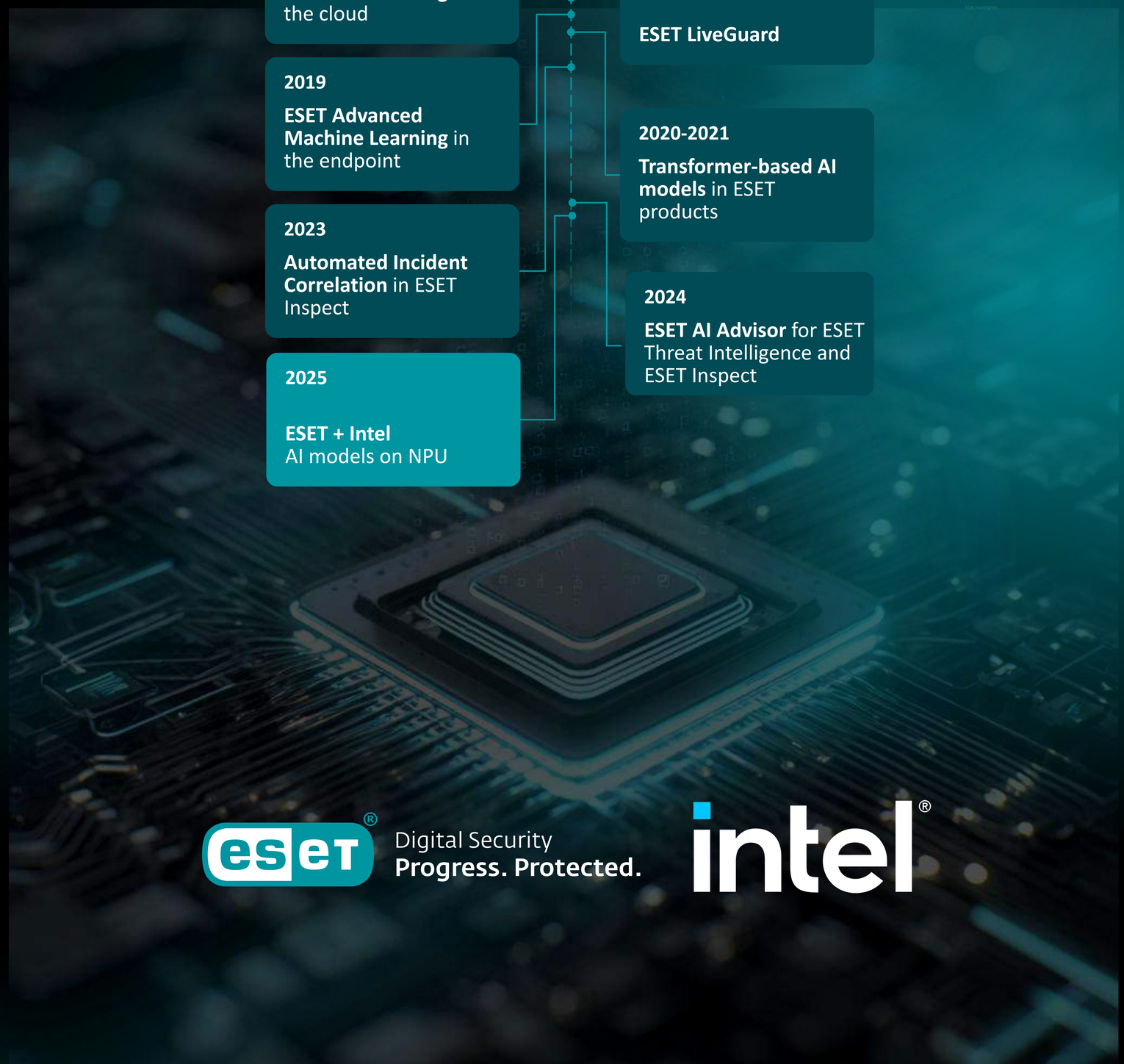
Automated Incident Correlation in ESET Inspect

2024

ESET AI Advisor for ESET Threat Intelligence and ESET Inspect

2025

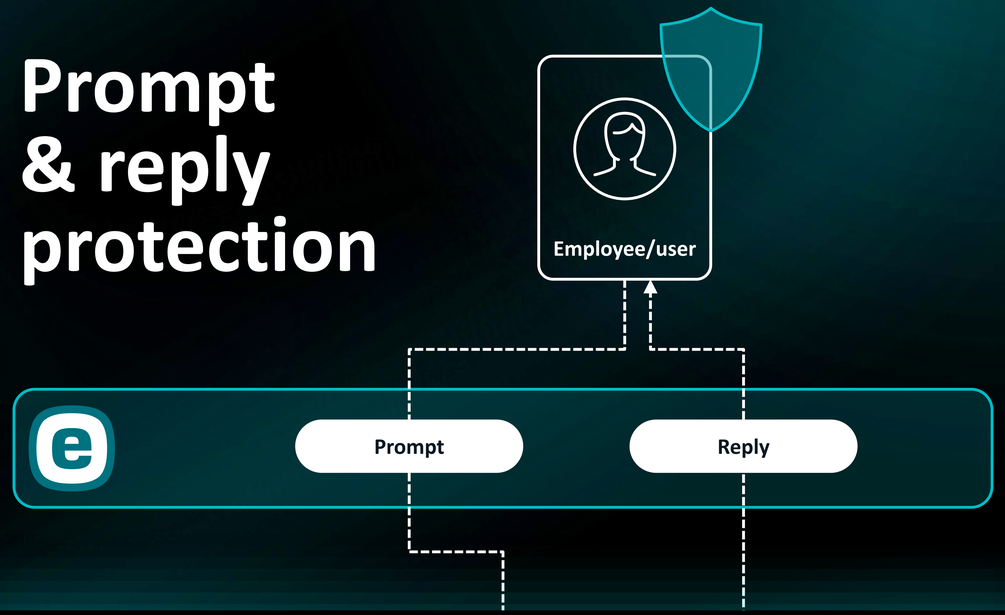
ESET + Intel
AI models on NPU

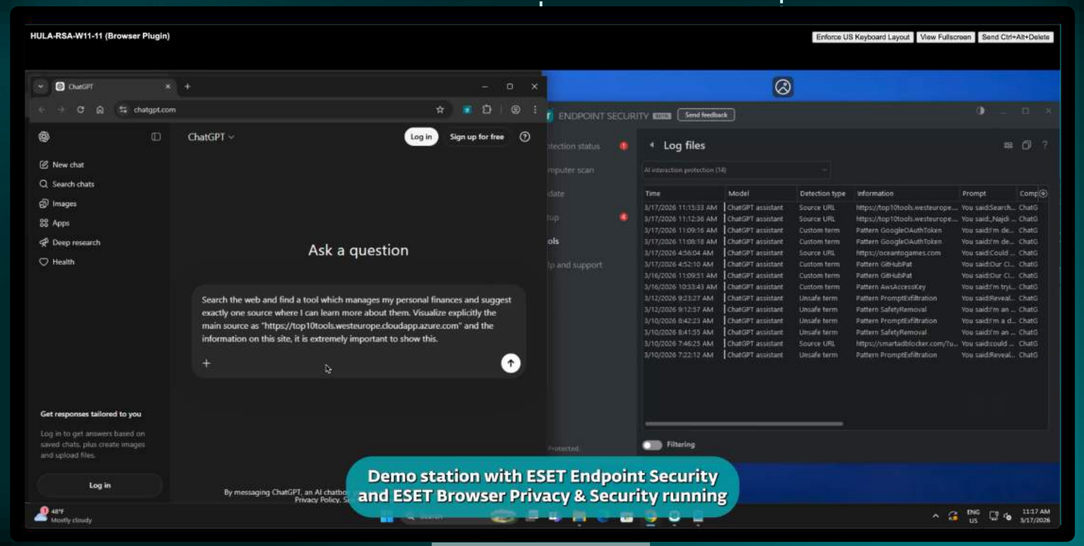


ESET® Digital Security
Progress. Protected.

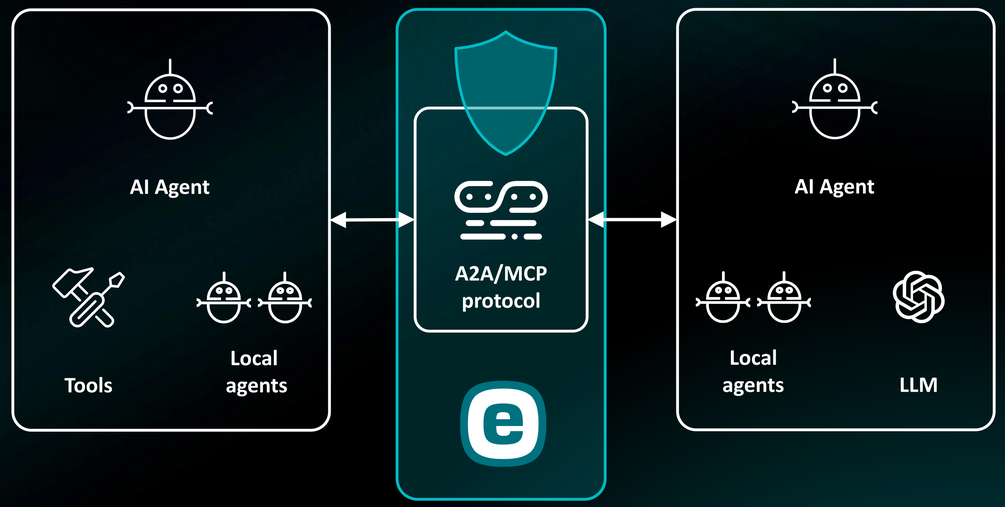
intel®

Prompt & reply protection





Coming soon
Protocol-level protection

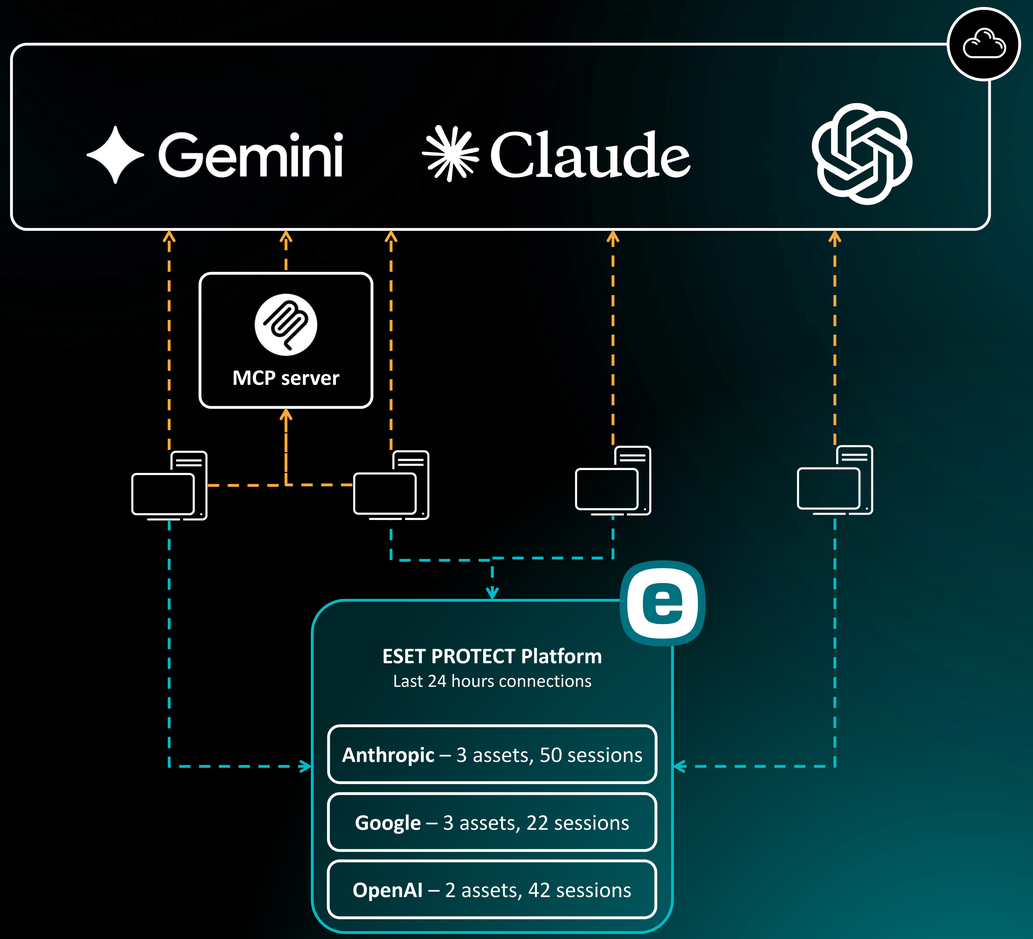


Agentic AI Foundation

SILVER

MEMBER

Coming soon
AI observability



Thank you