

# Cybersecurity in an AI-Turbocharged Era



**Bill Mylchreest**

**National Partner Account Manager**

Bill.Mylchreest@eset.com



**Victoria Smith**

**Enterprise Sales Rep**

Victoria.smith@eset.com



**Walter Taylor**

**ESET Account Executive**

Walter.taylor@eset.com



**Kevin Wood**

**ESET Account Manager**

Kevin.wood@eset.com



## Today's Agenda:

- ✓ **Gen-AI** impact on the cyber threat landscape
- ✓ Fighting back with an AI-augmented, **prevention-first cybersecurity** approach
- ✓ Limitations of modern AI in cybersecurity
- ✓ How the **ESET AI approach** works to overcome today's challenges

# DEFINITIONS WE WORK WITH:

**Artificial Intelligence (AI):** A generally intelligent machine that can learn and make decisions **independently**, based on inputs from its environment – without human supervision.



**Machine Learning (ML):** The field of computer science that gives machines the ability to find patterns in vast amounts of data, by sorting them and acting on the findings

**Large Language Models (LLMs):** Machine learning models that can comprehend and generate human language text by analyzing massive data sets of language



# ESET Has Been Tracking AI and ML In Cyber Crime for Decades

## What we predicted in 2018:

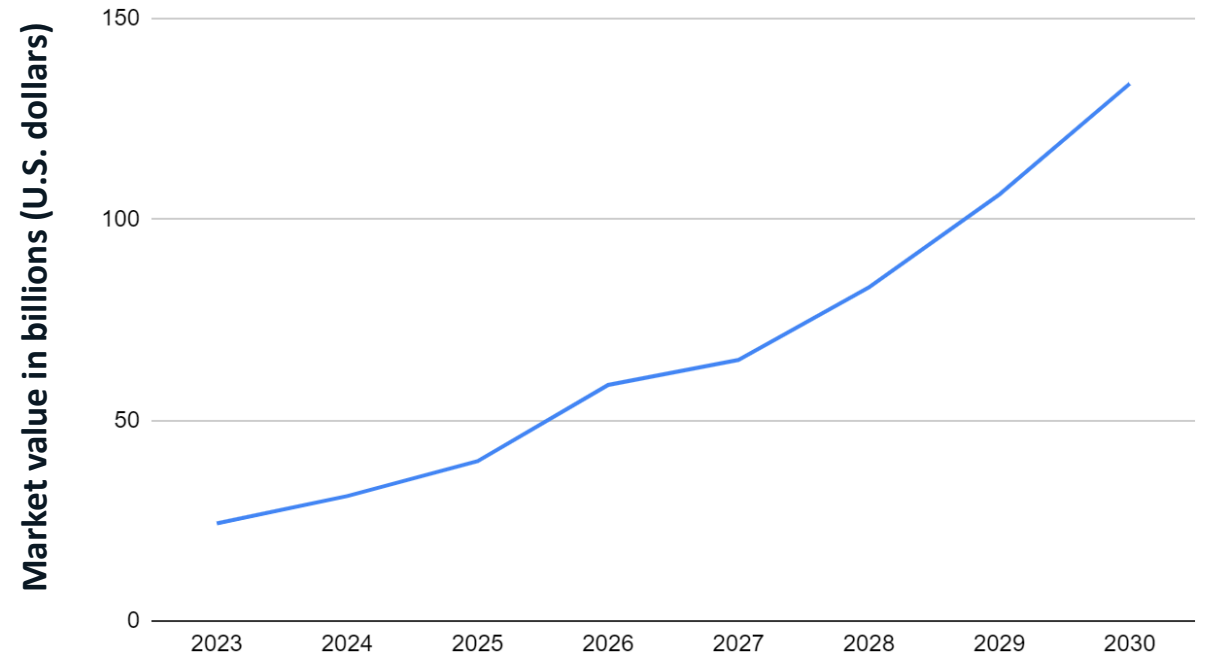
- ✓ **Humanlike social engineering**
- ✓ Targeted spearphishing campaigns
- ✓ **Malware optimization**
- ✓ Victim selection and targeting
- ✓ **Fast vulnerabilities research**
- ✓ **New malware generation**
- ✓ Self-destructive mechanisms to thwart investigation and analysis
- ✓ **Decreasing the time of an attack**
- ✓ **Collective learning of (IoT) botnets**
- ✓ False flags

# Projected Growth in Value of AI Cybersecurity Market Worldwide

Market value of

**\$134B**

By 2030



# AI's Profound Impact on the Threat Landscape

## Four Key Takeaways



Digital Security  
Progress. Protected.

# Massive Increase in Volume and Scale



1,265% increase in malicious phishing emails (CNBC)

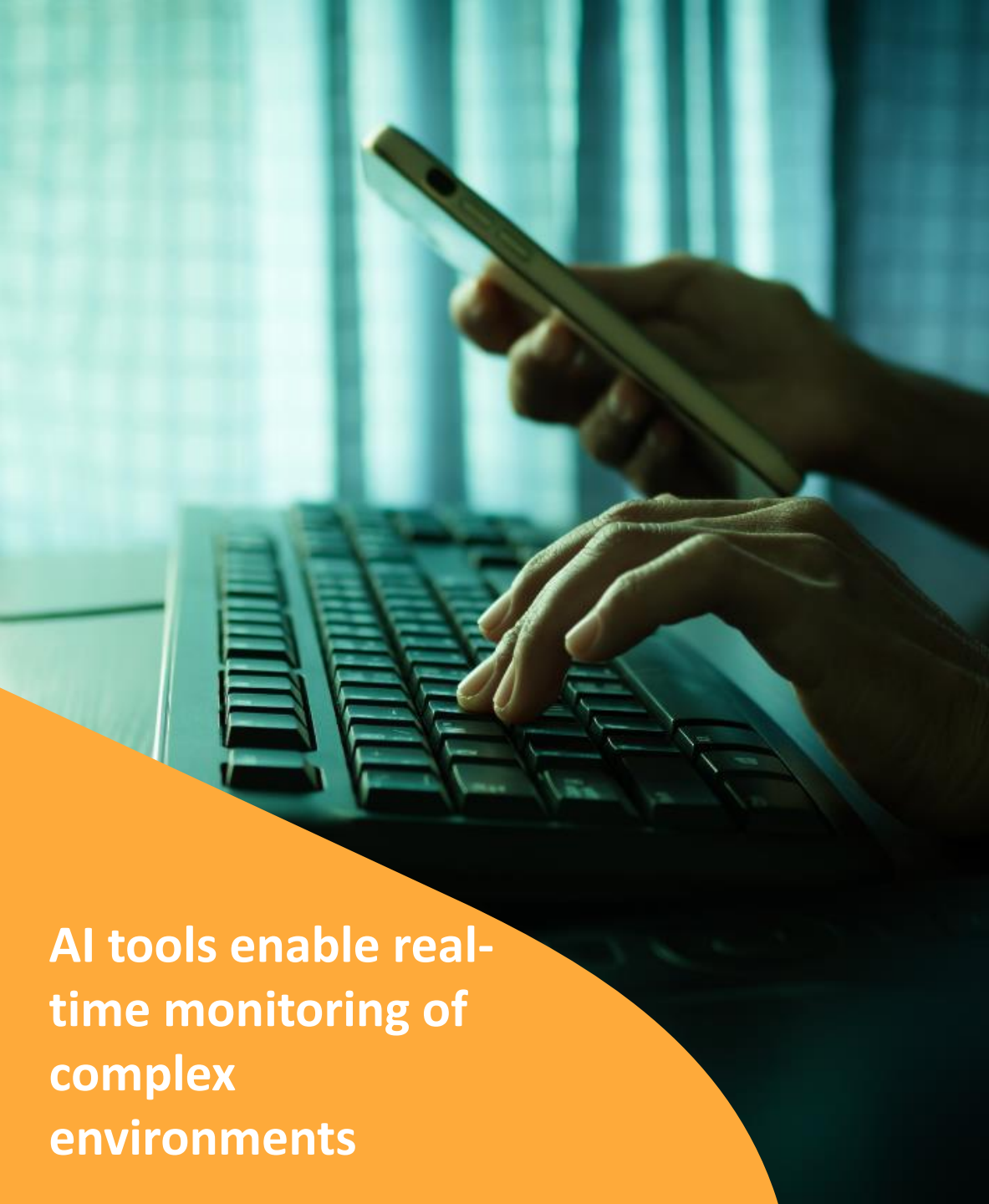
967% rise in credential phishing since Q4 2022 (CNBC)

1760% Surge in Business Email Compromise Attacks  
(Security Today)

Gen-AI tools streamline new malware creation by automating tedious assignments like debugging, code optimization, and rewriting libraries.

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





**AI tools enable real-time monitoring of complex environments**

# Improved Attack Success Rate



Human-like language for more convincing content

Better attack evasion tools

Lower barrier to entry for new adversaries – AI gives midlevel attackers tools to up their game!

Gen-AI tools utilize LLMs to create more convincing, human-like content, leading to higher attack success rates for experienced attackers and those entering the game.

Data-collecting and detection-thwarting botnets analyze every victim for signs of monitoring.

# Ability to Shift Public Perception



1 in 5 Americans receive their daily news from social media

64% of adults said “fake news” caused confusion on basic facts

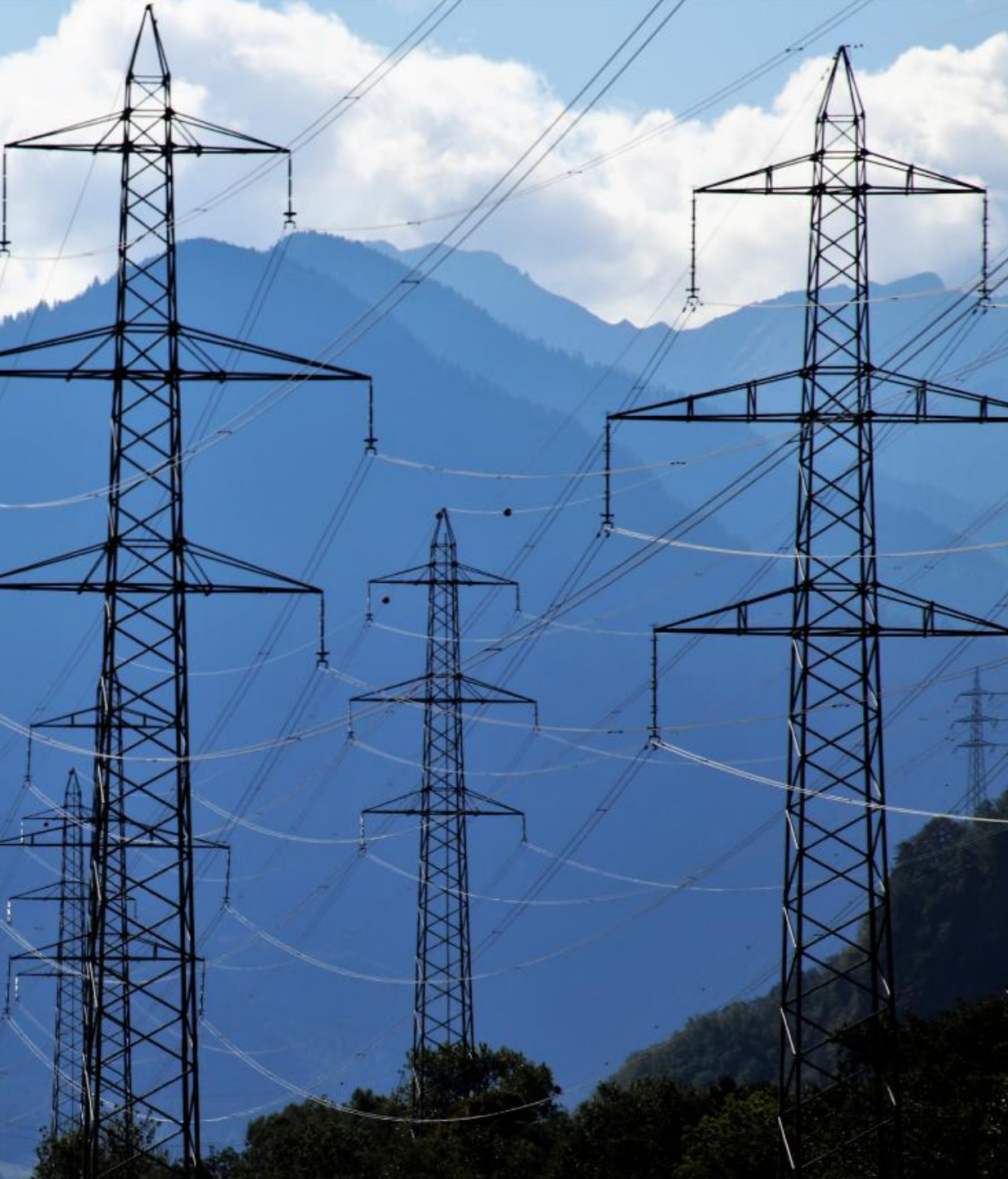
23% of adults have knowingly or unknowingly shared “fake news”

(NCSC.org)

Gen-AI enables large-scale disinformation campaigns that have the proven ability to shift public perception.



People can only  
detect a fake image  
60% of the time



# Emergence of Cyber Physical Attacks



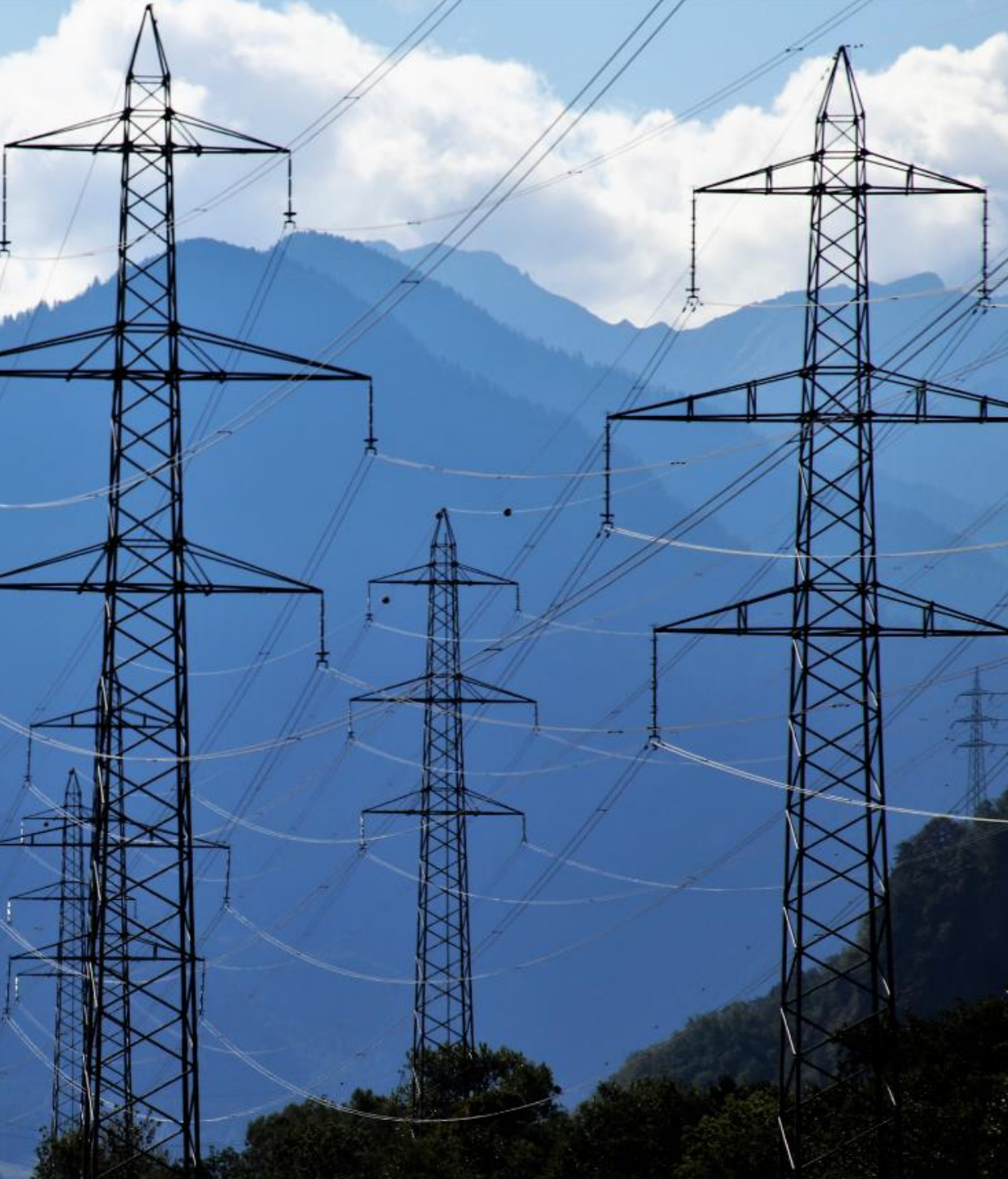
AI used to target critical infrastructure inside the U.S.

Simulated cyberattacks can damage equipment and cause destruction

86% of organizations have adopted Industrial Internet of Things (IIoT) (Forbes)

The FBI recently warned of real-world attempts to infiltrate IIoT systems using gen AI models with the intention to override physical systems and destroy essential infrastructure. (CNBC)





# Future (potential) AI assisted attacks

- Nation state advisories will use advanced tools
- Potential risk of sophisticated attacks against critical infrastructure
- Attacks may morph automatically depending on defenders' responses



## Sci-Fi or Near Future?


- ✓ **Planting false flags:** sending forensic threat hunters on a wild goose chase
- ✓ **Improved victim selection:** AI combing through vast data sets looking for the weakest entry point
- ✓ **Vulnerability hunting:** sifting through vast data on unpatched software, known CVEs, and notoriously insecure backdoors
- ✓ **Learning botnets:** could be used for more sophisticated operations like vulnerability hunting or information harvesting, not just DDoS
- ✓ **AI Poisoning:** intentionally compromising a training dataset used by an AI model to manipulate the operation of that model

# Fighting Back

Leveraging AI to Bolster a Proactive and Adaptive Defense Strategy



Digital Security  
Progress. Protected.



Pioneering  
heuristics since  
late 1990's

## Real-Time Attack Detection

- ✓ Improved threat scanning and sandboxing
- ✓ Streamlined incident response
- ✓ Dynamic map of interconnected items and events
- ✓ Advanced AI antispam and anti-phishing



## Improved Threat Hunting

- ✓ Processing vast amounts of data to identify attacks by correlation of various indicators
- ✓ Monitoring and analysis of network traffic for malicious or anomalous patterns



## Actionable Intelligence

- ✓ Prioritize alerts to avoid fatigue
- ✓ Mine intelligence feeds and distill into easy-to-understand format
- ✓ In-product AI to optimize settings and avoid misconfigurations
- ✓ Boost user awareness with better training materials and easily digestible infographics



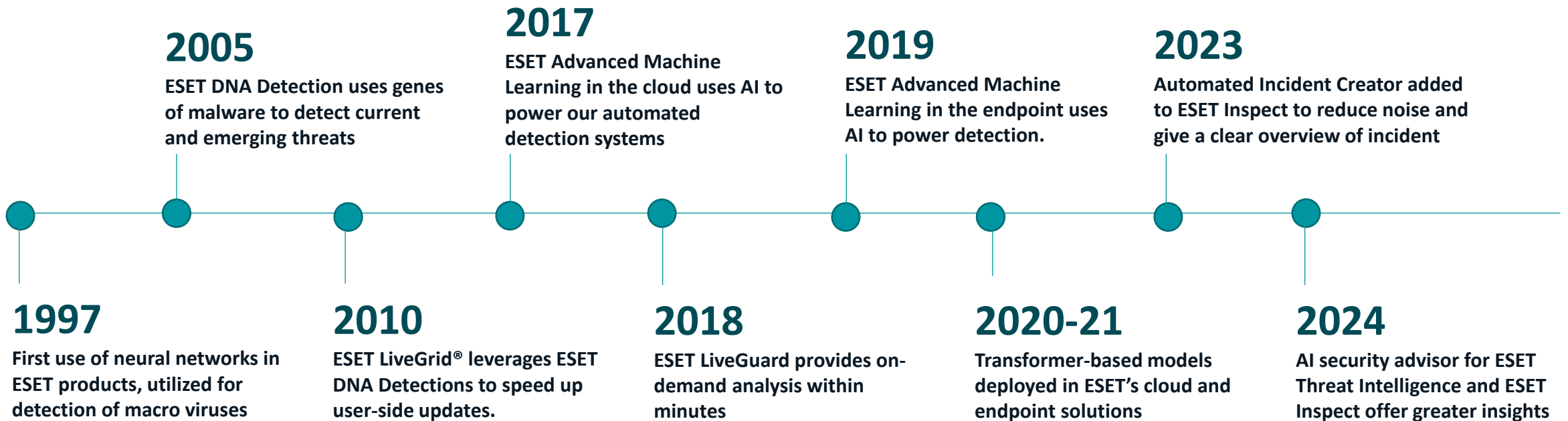
# ESET + AI

Enhance detection rates, aid threat hunting, and minimize false positives

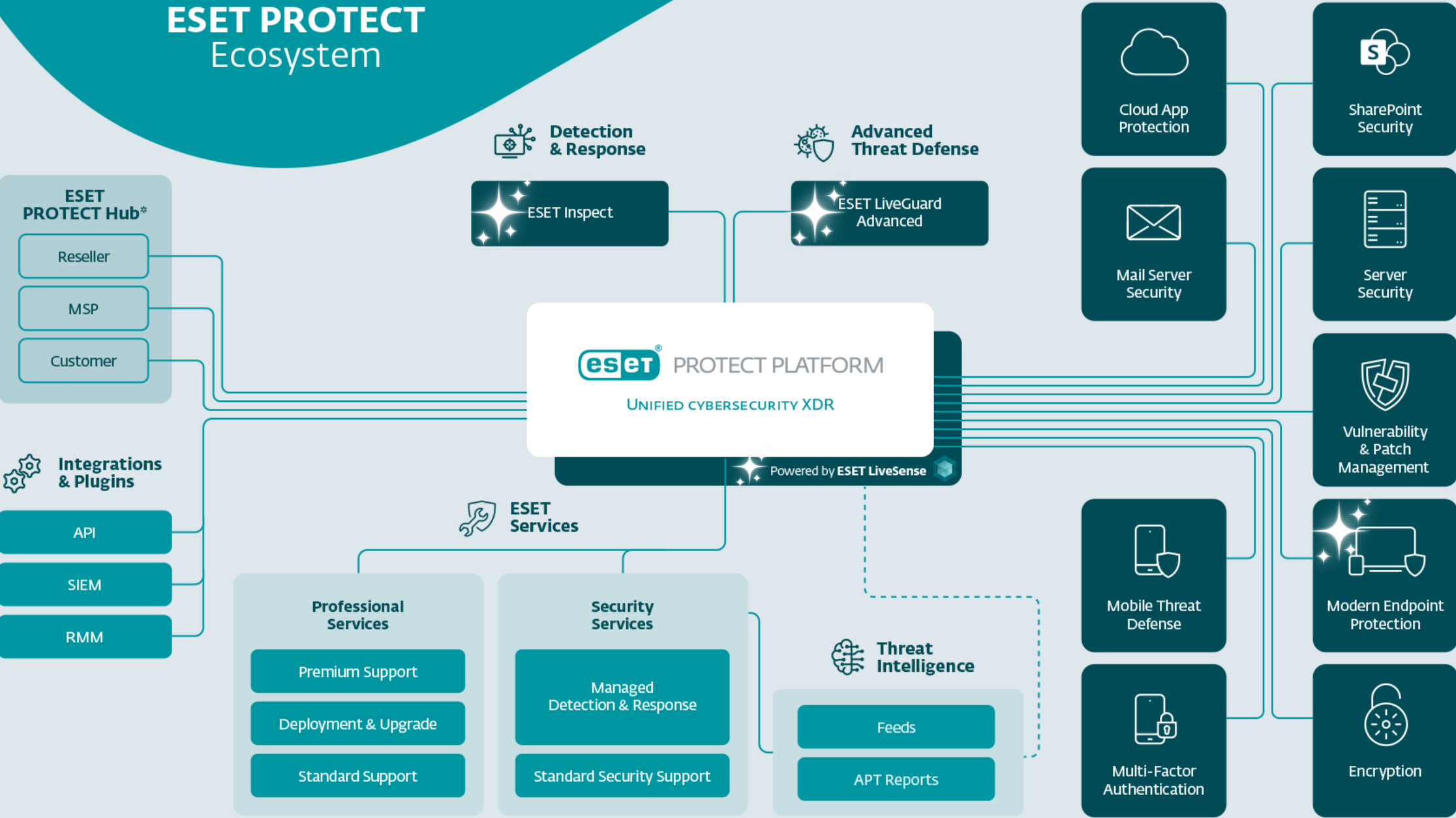


Digital Security  
Progress. Protected.

# ESET has been using AI for over 25 Years



# ESET PROTECT Ecosystem





# ESET LiveSense®

The figure below shows some of ESET's core technologies and indicates approximately when and where they can detect and/or block a threat during its life cycle in the system.

## PRE-EXECUTION LAYER

Reputation  
and cache

Network Attack  
Protection

UEFI Scanner

Advanced Machine  
Learning

Brute-Force Attack  
Protection

Device Control

DNA Detections

In-Product Sandbox

## EXECUTION LAYER

Ransomware Shield

Script Scanner  
& AMSI

Advanced Memory  
Scanner

Exploit Blocker

Deep Behavioral  
Inspection

## POST-EXECUTION LAYER

LiveGrid® Protection

Secure Browser

Botnet Protection

## Enhanced Detection Rates



## Aid in Threat Hunting

# ESET PROTECT Elite



**Console** ⓘ  
[Learn more](#)



**Modern Endpoint Protection** ⓘ  
[Learn more](#)



**Server Security** ⓘ  
[Learn more](#)



**Mobile Threat Defense** ⓘ  
[Learn more](#)



**Full Disk Encryption** ⓘ  
[Learn more](#)



**Advanced Threat Defense** ⓘ  
[Learn more](#)



**Cloud App Protection** ⓘ  
[Learn more](#)



**Mail Server Security** ⓘ  
[Learn more](#)



**Vulnerability & Patch Management** ⓘ  
[Learn more](#)



**Extended Detection & Response** ⓘ  
[Learn more](#)



**Multi-Factor Authentication** ⓘ  
[Learn more](#)



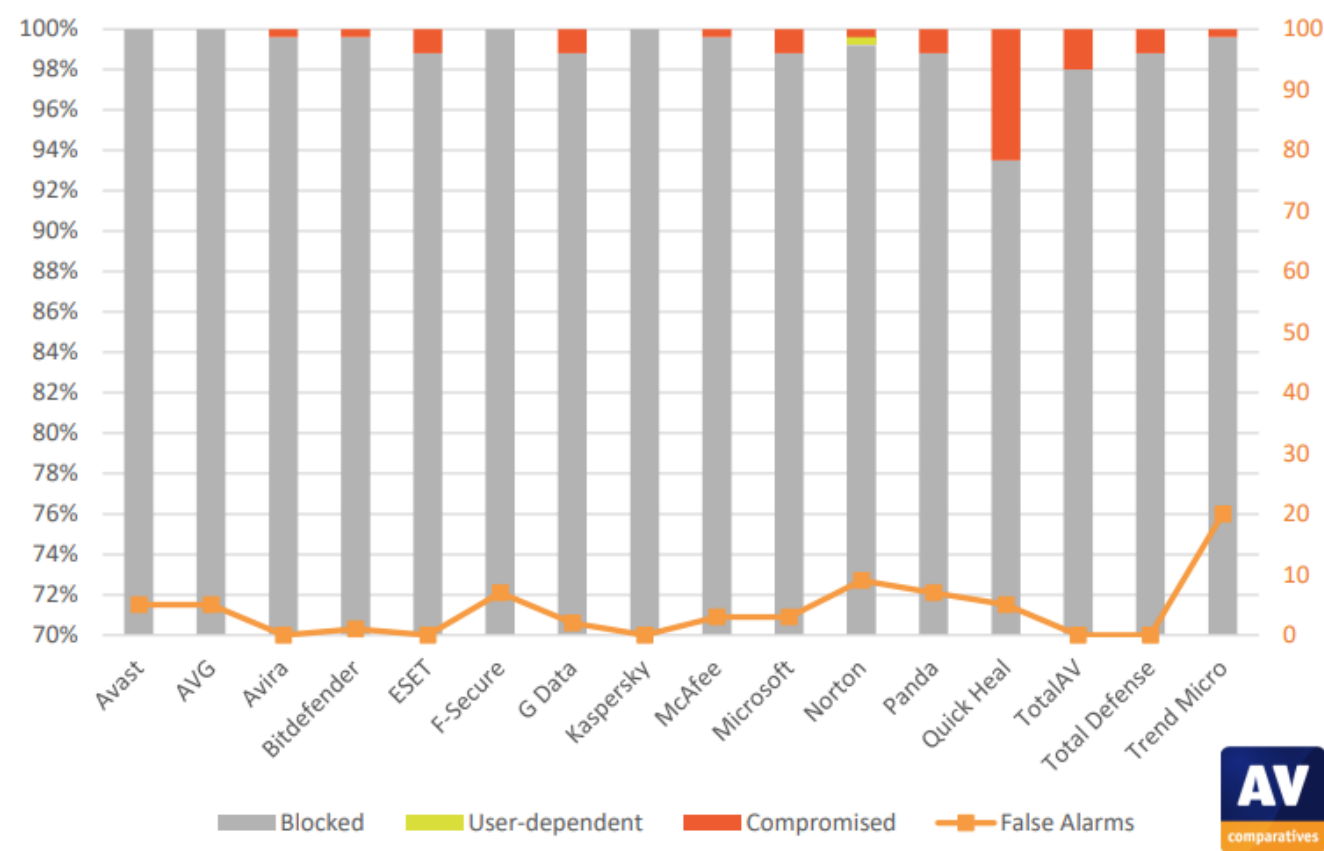
**MDR Ultimate Service**



**Premium Support Advanced**

# Real-World Protection Test

## March 2024 by AV-Comparatives



### Minimize False Positives



False Positives 2023 winner according to AV-Comparatives 2023 Summary Report



# How ESET MDR can help

Managed Detection & Response Service combines AI and human expertise to achieve unmatched threat detection and rapid incident response **without the need to maintain in-house security specialists.**

security

AI

detection

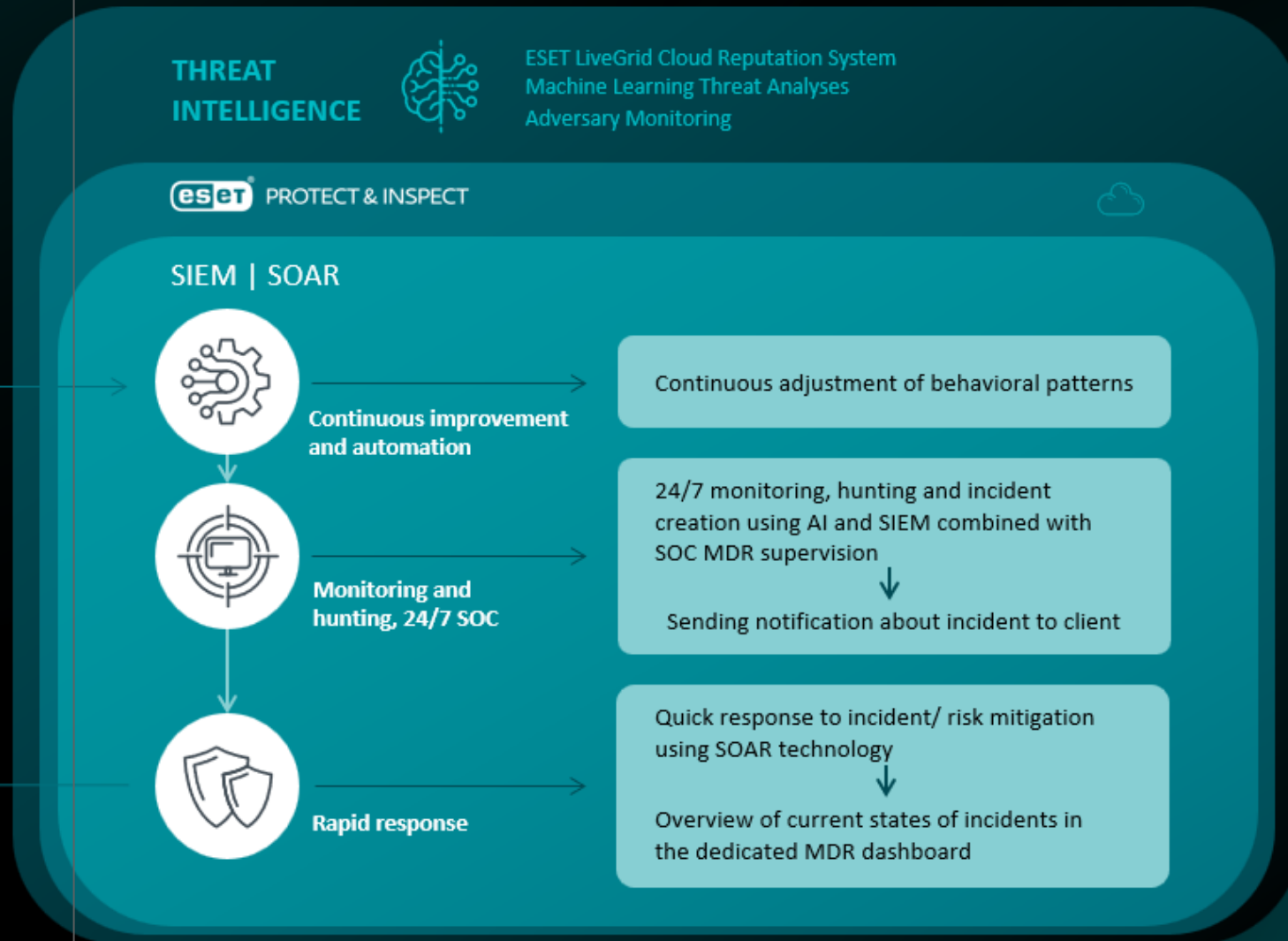
service

expertise

maintain

response

# How ESET MDR works



# About ESET



30+ years in  
the market



Private company,  
no debt



Always focused on  
technology



Biggest European  
Union vendor



Growing year-over-  
year since its  
inception



Owned by original  
founders



Strong values



Progress. Protected.

# Questions?



Digital Security  
**Progress. Protected.**



# Thank you for listening

[Request Live Demo](#)

[Request Business Trial](#)

[Contact Sales](#)



Digital Security  
Progress. Protected.