OVERVIEW

THREAT INTELLIGENCE

Unique intelligence feeds and APT reports from the industry's top professionals

Progress. Protected.

Why add ESET to your CTI stack?

Understanding the current threat landscape and the tactics employed by cybercriminals provides a crucial knowledge advantage. This insight enables organizations to **fortify** their **internal defense systems effectively**. High-quality intelligence data is the cornerstone of any robust cyber threat intelligence (CTI) strategy.

For over 35 years, ESET has been a privately held, debt-free and consistently growing company. Our success is built on a "prevention-first" approach powered by AI and enhanced by human expertise. At the heart of our operations is our **unique Global Threat Intelligence, supported by an extensive R&D network led** by industry-acclaimed researchers. We take the time to truly understand cyber threats, enabling us to defend against them effectively.

No matter how advanced your current CTI solutions are, integrating **ESET into your stack will provide unparalleled value**. Our comprehensive threat intelligence feeds and detailed APT reports ensure you stay ahead of emerging threats, enhancing your existing defenses with actionable insights and cutting-edge research.

Leverage ESET's Unique Telemetry

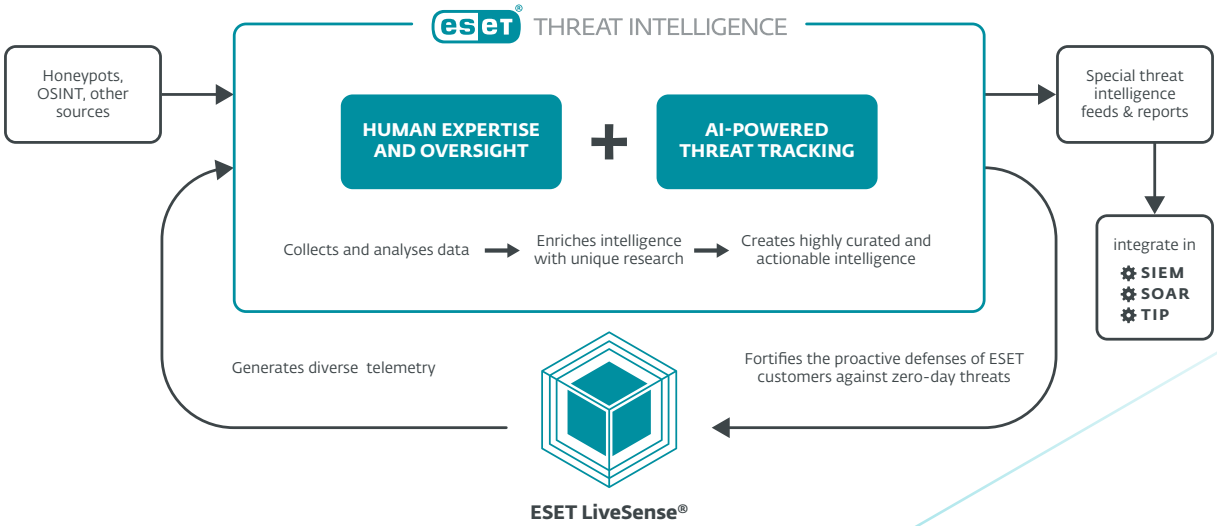
ESET's global presence, built over decades, provides us with a **rich and diverse intelligence library** from millions of nodes. Unlike many competitors, our telemetry is particularly strong in regions considered **"more interesting" from a geopolitical point of view** in the cyber defense world. This unique coverage translates directly into superior intelligence. By leveraging ESET's telemetry, you **gain access to high-quality, actionable insights** that enhance your threat detection and response capabilities.

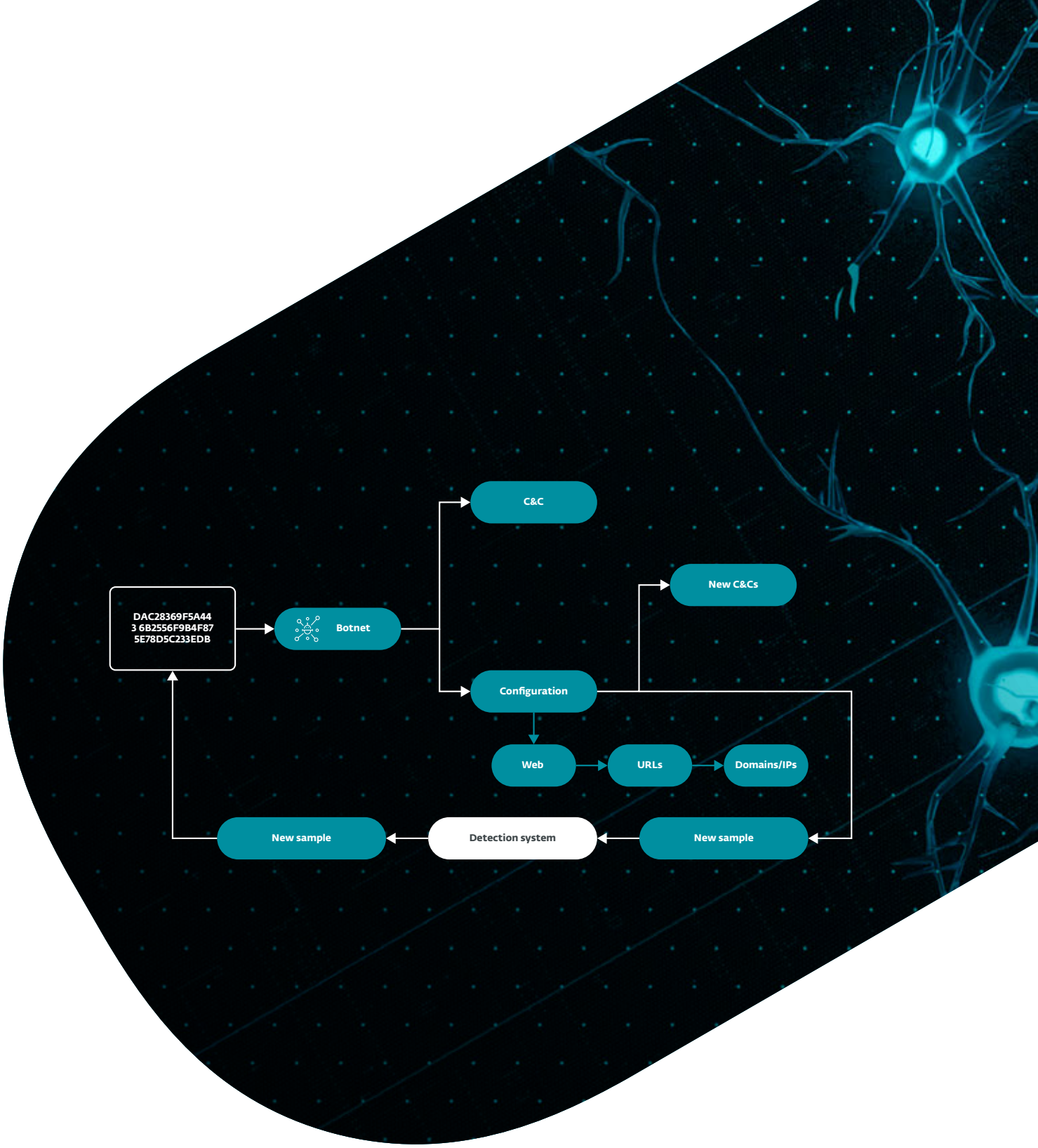
eset® Digital Security
Progress. Protected.

Unique, Enriched Intel for Actionable Insights

Threat intelligence is not just about collecting indicators and wrapping them up – ESET goes well beyond that. We employ advanced technology and extensive expertise to process and enrich our intelligence, ensuring it provides real value to your business.

1. **Comprehensive Telemetry:** Our intelligence starts with a wide range of telemetry generated by ESET LiveSense, our multilayered security technology integrated within the ESET PROTECT Platform. This ensures a broad and deep collection of data from diverse sources.
2. **Diverse Collection Methods:** In addition to LiveSense, we utilize various collection and monitoring methods, including honeypots, sensors, OSINT resources, web crawling (both clear and deep web), and Threat Tracking. This results in a significant volume of high-quality data.
3. **Advanced Processing:** Once collected, all data is processed through our robust backend systems, which leverage AI to classify and analyze the information automatically. This ensures that only the most relevant and actionable intelligence is surfaced.
4. **Expert Analysis:** Beyond automated processing, our skilled team of threat intelligence analysts and researchers plays a crucial role. They continuously study and analyze various threat actors, their motivations, TTPs (tactics, techniques, and procedures), and tools. This human verification adds an extra layer of depth and accuracy to our intelligence, going beyond what machine learning and automation alone can achieve.





The samples we receive via telemetry undergo in-depth behavioral and structural analysis. This process yields additional useful indicators, further enriching our threat intelligence. By meticulously examining each sample, we extract valuable insights that enhance the overall quality and effectiveness of our intelligence, providing you with a more comprehensive understanding of the threat landscape.

Superior Security via detailed APT Reports

Written in concise, actionable language to improve your organization's security posture, our APT reports provide detailed insights into malware campaigns, distribution, and actors involved. Access our MISP server and AI advisor, and book live sessions with ESET's top threat intelligence experts for comprehensive, actionable intelligence.

PUTTING OUR BEST RESEARCH AT YOUR FINGERTIPS

Our research team is well known in the digital security industry, thanks to our award-winning WeLiveSecurity blog. The team's excellent research and APT activity summaries are available, along with much more detailed information. ESET customers get an exclusive early preview of all WeLiveSecurity content.

ACTIONABLE, CURATED CONTENT

Reports provide a great deal of context for what is going on and why. Thanks to this, organizations can prepare in advance for what might be coming. Importantly, our experts make sure the content is easy to understand.

MAKE CRUCIAL DECISIONS FAST

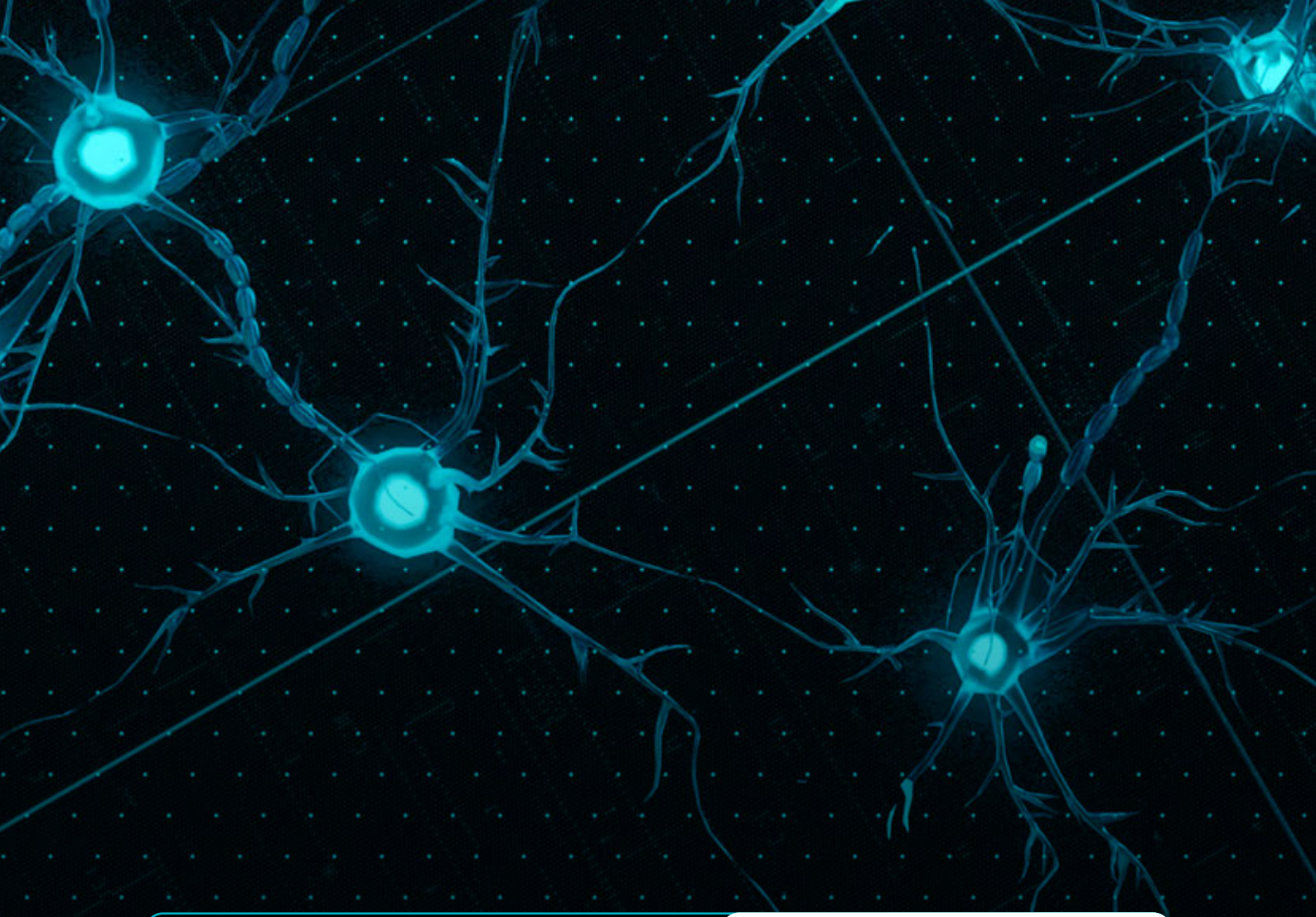
All this helps organizations make crucial decisions and provides a strategic advantage in the fight against digital crime. It brings an understanding of what is happening on the 'bad side of the internet' and provides crucial context, so that your organization can make internal preparations quickly.

ACCESS TO AN ESET ANALYST

Every customer ordering the APT Reports Premium package will also have access to an ESET analyst for up to four hours each month. This provides the opportunity to discuss topics in greater detail and help resolve any outstanding issues.

ESET AI ADVISOR

ESET AI Advisor uses advanced AI and APT expertise to provide on-demand insights and protective measures against cyberattacks. Available as a chatbot, it addresses security inquiries, offers APT summaries, compiles IoCs and TTPs, and generates YARA rules for swift threat understanding and prevention.



		APT Reports	APT Reports Advanced	APT Reports Ultimate
Bi-weekly Activity Summary	Reports summarizing the activity of all covered APT Groups as detailed above (two reports per month)	✓	✓	✓
Threat Analysis Reports	Customized or regular technical analysis of prevalent threats (~30 per year)	✓	✓	✓
Monthly Overview	Monthly compilation of information with an executive overview of threats	✓	✓	✓
Monthly Digest	Index and executive summary of the month's reports and events	✓	✓	✓
Pre-access to WeLiveSecurity	Pre-access to Threat reports and selected WeLiveSecurity articles	✓	✓	✓
APT IOC Feed	Full access to STIX/TAXII feed containing IOCs from the reports	✓	✓	✓
MISP Server Access	Full access to ESET MISP server containing all the information available in the reports	✗	✓	✓
ESET AI Advisor	Access to ESET AI Advisor providing insights and summaries of available APT reports	✗	✓	✓
Analyst Access	Analyst access via various platforms such as MS Teams and email, limited to four hours per month (non-cumulative, including preparation time)	✗	✗	✓

Clear and Concise Data Feeds

Enhance your threat landscape view with ESET's unique telemetry. We provide highly curated data feeds in JSON and STIX 2.1, seamlessly integrating into SIEM, TIP, or SOAR tools. Unlike many TI vendors, we pay really close attention so that **our feeds are meticulously filtered and assessed** to ensure their relevance. This enables automatic actions by existing security systems when needed, empowering threat intelligence analysts with a comprehensive view of the global threat landscape.

- Metadata-rich, detailed, and curated data with very low false positives
- We ensure data is low size, high relevancy, deduplicated, with confidence-scoring
- The result of advanced filtering, with insights by ESET researchers
- Market-leading, especially with botnet data
- Low maintenance requirements due to properly curated content
- Real-time feeds – only fresh and prevalent IoCs (Indicators of Compromise)

MALICIOUS DATA FEED

Gain valuable insights from this real-time feed, which provides information on newly discovered malware samples, their characteristics, and IoCs. By leveraging this data, you can proactively block malicious files before they cause harm. The feed includes details such as file hashes, timestamps and identified threat types.

RANSOMWARE FEED

Combat ransomware with real-time data on prevalent samples. Our feed provides insights into active ransomware families, enabling proactive blocking. Stay ahead of threats and protect your organization from data breaches and costly disruptions.

BOTNET FEED

Leverage insights from ESET's proprietary botnet tracker network with the Botnet feed. This feed comprises three sub-feeds: botnet, Command and Control (C&C), and targets. It provides essential data, including detection details, file hashes, last communication timestamps, downloaded files, IP addresses, protocols, and targeted information.

APT IOC

Benefit from valuable information from ESET's proprietary APT feed, which provides insights into Advanced Persistent Threats (APTs) based on ESET research. This feed is exported from ESET's internal MISP server and includes data that is detailed further in APT reports. While it's part of the APT reports offering, the feed can also be purchased separately.

DOMAIN FEED

Block domains considered malicious including domain name, IP address, and the date associated with them. The feed ranks domains based on their severity, which lets you adjust your response accordingly, for example, to only block high-severity domains.

URL FEED

Take advantage of the meticulously crafted URL feed, which focuses on specific addresses. It provides detailed information related to each URL and includes data about the domains hosting them. The feed results are curated to display only high-confidence findings, accompanied by human-readable explanations for any flagged URLs.

IP FEED

Receive actionable data from this feed, which provides information on malicious IPs. The data structure closely resembles that of domain and URL feeds. Use it to identify prevalent malicious IPs, proactively block high-severity ones, detect less severe IPs, and investigate further based on additional data to assess potential harm.

ANDROID THREATS FEED

This feed provides real-time information on prevalent Android threats and their IoCs, enabling proactive blocking. Created from ESET telemetry, it updates in near real-time with daily deduplication.

ANDROID INFOSTEALER FEED

A focused subset within Android threats, Android infostealer feed provides specific details about current and prevalent Android infostealer samples, along with associated data. By leveraging this information, you gain insights into the infostealer families active in the wild. More importantly, you can proactively block them before they inflict any harm.

SCAM URL FEED

Stay ahead of scams with real-time data on fraudulent URLs. Our feed covers electronic shops, investment scams, dating scams, and cryptocurrency scams. Created from all ESET URL sources in near real-time; deduplication happens every 24 hours.

CRYPTOSCAM FEED

Stay ahead of crypto scams with real-time updates on scam domains, URLs, and associated data. Our feed, sourced from ESET's extensive telemetry, provides early, targeted information to help you proactively block threats and protect your assets.

MALICIOUS EMAIL ATTACHMENTS FEED

Email is a prime target for attacks. Our feed provides real-time data on malicious email attachments sourced from ESET's extensive email scanning telemetry. Stay ahead of threats with up-to-date, actionable insights to protect your organization.

PHISHING URL FEED

Stay protected with real-time data on prevalent phishing URLs. Our feed, sourced from ESET's phishing URL database, updates near real-time with daily deduplication. Prevent data breaches by identifying and blocking deceptive sites before they cause harm.

SMISHING FEED

Stay protected with real-time data on SMS phishing (smishing) domains, URLs and associated data. Our feed, sourced from ESET's extensive telemetry, updates near real-time with daily deduplication.

SMS SCAM FEED

Protect against SMS scams with our real-time feed on malicious domains and URLs. Updated near real-time from ESET's extensive telemetry and deduplicated daily, this feed helps you identify and block sophisticated threats.

Experience the power of ESET Threat Intelligence

Schedule a demo with us today and discover the unparalleled value ESET Threat Intelligence can bring to your organization. With a 100% renewal rate, our satisfied customers are a testament to the effectiveness of our solutions. Let us show you how we can enhance your cybersecurity defenses.

Not ready for a demo call yet?

Start by creating a preview account in the ESET Threat Intelligence portal to explore feeds and APT reports.

This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats with our AI-Native, prevention-first approach. We combine the power of AI and human expertise to make protection easy and effective.

Experience best-in-class protection thanks to our in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers.

ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat hunting capabilities with a broad variety of security services, including managed detection and response.

Our highly customizable solutions include local support and have minimal impact on performance, identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

ESET protects your business so you can unlock the full potential of technology.

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200
countries and territories

12
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 9,000 endpoints

Allianz Suisse

protected by ESET since 2016
more than 4,000 mailboxes

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 32,000 endpoints

ISP security partner since 2008
2 million customer base

RECOGNITION

AV comparatives
APPROVED
Business Security
JUL 2024

ESET is a consistent **top-performer in independent tests** by AV-Comparatives and achieves best detection rates with no or minimal false positives.

Leader
FALL
2024

ESET consistently achieves top rankings on the global G2 user review platform and its solutions are **appreciated by customers worldwide**.

kuppingercole
ANALYSTS

ESET is **recognized as a Market Leader** and an Overall Leader in MDR, according to the KuppingerCole Leadership Compass 2023.