ESET PRIVATE

Tailored Cyber Resilience at Scale

CYBERSECURITY™
MADE IN EUROPE

“Technology has changed the world. Protecting that technology has always been our world.”

Richard Marko
CEO of ESET

ESET is a science-driven global digital security company that protects millions of customers and hundreds of thousands of companies worldwide.

Europe's largest cybersecurity vendor

Based on Frost Radar™: Endpoint Security, 2025 (Frost & Sullivan)

The largest global EU-owned & based company with **over 30 years** of experience in the cybersecurity industry

1 bilion + protected devices / security solutions are based on real threats that pose risk to organization

Long-term and consistent **recognition** by leading analysts for innovative and effective cybersecurity solutions

High detection rates, **low false positive** and low performance impact

One of the strongest cyber threat **research teams** in the world

Social responsibility built on **strong values** and principled position against all forms of war, cyber or traditional

We work with **5** out of magnificent seven multinational enterprises

Strong partnerships & alliances

ESET PORTFOLIO

ESET HOME

1 billion+
Protected **retail** users
worldwide

+

ESET PROTECT

500,000+
protected **business** users
worldwide

+

ESET PRIVATE

Tailored cyber resilience
for **Enterprises**
and **Governments**

Trusted by Global Brands

MITSUBISHI MOTORS
Drive your Ambition

orange™

Canon

BVB 09

T

ESET PRIVATE

Tailored cybersecurity at scale. Precision-built for complexity, compliance, and resilience.

ESET PRIVATE delivers tailored cybersecurity at scale. Engineered for complex environments, it brings together expert advisory, advanced threat protection, and custom services to safeguard critical assets. Backed by strategic partnerships and intelligent technologies, it integrates seamlessly into operations and supports compliance. The result? Cyber resilience—purposefully aligned to your goals, sector, and growth.

KEY OFFERINGS

Air-Gapped Solutions

Cutting-edge protection to secure restricted networks from known and evolving threats. Benefit from flexible deployment, compliance support, and full control over your security stack.

Client Shield

From service provider to customer—multilayered protection across Android and iOS. Block malware, scams, and identity theft to reduce risk and support compliance. Strengthen differentiation and drive growth.

Scanning Solutions

High-accuracy scanning for large volumes of inbound data—combining advanced threat detection and flexible deployment. Ultra-fast and purpose-built for scale, it supports compliance with minimal impact on performance.

Advisory

Custom cybersecurity strategies to strengthen readiness, compliance, and awareness. It helps organizations proactively anticipate, withstand, and adapt to threats, while protecting continuity and core business needs.

Threat Intelligence

Dedicated threat intelligence with geopolitical and sector-specific insights. Delivers early warnings, focused adversary monitoring, and exclusive research collaboration to strengthen proactive defenses.

Managed Security

End-to-end managed security operations with 24/7 monitoring and incident response across multiple perimeters. Custom-built for your environment, it includes dedicated SOC teams and compliance reporting.

Industrial Security

End-to-end protection across the entire IT and OT environment. Purpose-built for critical infrastructure and legacy systems, it secures connectivity and reduces cyber risk without disrupting operations.

ESET® PRIVATE

Air-Gapped Solutions

Cutting-edge protection for restricted environments

Uncompromising security for restricted networks from known and evolving threats. Benefit from flexible deployment, compliance support, and full control over your security stack.

Air-Gapped Solutions

CHALLENGE

Working within air-gapped or highly restricted environments means defending critical systems without access to real-time internet updates or cloud-based intelligence. Teams must keep protection strong while operating solely with internal tools, controlled update flows, and disconnected infrastructure. This makes it harder to stay ahead of fast-moving threats and maintain reliable, uninterrupted operations.

Strict data-sovereignty rules and limited visibility further complicate security management. Ensuring safe update distribution, validating threats locally, and maintaining consistent control across all assets becomes demanding when every process must respect isolation policies. The core challenge is staying resilient, compliant, and up to date—while never exposing the environment to external risk.

SOLUTION

ESET PRIVATE Air-Gapped Solutions deliver advanced, self-contained protection built specifically for fully isolated environments. All analysis, detection, and decision-making remain strictly on-premises, guaranteeing confidentiality and ensuring that no data ever leaves the secure network. With internally controlled update mechanisms and local reputation evaluation, the environment stays protected against both familiar and emerging threats.

The solution provides unified visibility and operational control across all assets inside the air-gapped perimeter. Secure behavioral analysis, strict access management, and controlled data-handling workflows ensure that threats can be identified and contained quickly—supporting regulatory compliance and ensuring the uninterrupted operation of mission-critical systems.

Air-Gapped Solutions

CHALLENGE

Working within air-gapped or highly restricted environments means defending critical systems without access to real-time internet updates or cloud-based intelligence. Teams must keep protection strong while operating solely with internal tools, controlled update flows, and disconnected infrastructure. This makes it harder to stay ahead of fast-moving threats and maintain reliable, uninterrupted operations.

Strict data-sovereignty rules and limited visibility further complicate security management. Ensuring safe update distribution, validating threats locally, and maintaining consistent control across all assets becomes demanding when every process must respect isolation policies. The core challenge is staying resilient, compliant, and up to date—while never exposing the environment to external risk.

SOLUTION

ESET PRIVATE Air-Gapped Solutions deliver advanced, self-contained protection built specifically for fully isolated environments. All analysis, detection, and decision-making remain strictly on-premises, guaranteeing confidentiality and ensuring that no data ever leaves the secure network. With internally controlled update mechanisms and local reputation evaluation, the environment stays protected against both familiar and emerging threats.

The solution provides unified visibility and operational control across all assets inside the air-gapped perimeter. Secure behavioral analysis, strict access management, and controlled data-handling workflows ensure that threats can be identified and contained quickly—supporting regulatory compliance and ensuring the uninterrupted operation of mission-critical systems.

KEY BENEFITS

Air-Gapped Solutions

Proven Isolation & Full Data Control

Built for networks requiring absolute separation — already deployed in government, industrial, and critical-infrastructure environments.

Always-Updated Protection Without Internet

Uses a controlled, multi-stage offline update process proven to keep air-gapped systems protected against emerging threats.

Local Threat Decisions With High Accuracy

Runs on-premise reputation and threat validation that has consistently reduced false positives in large, offline deployments.

Safe On-Prem Analysis of Unknown Files

Delivers secure local detonation and behavioral analysis, used in restricted environments where sample sharing is not allowed.

Central Visibility Inside the Air-Gap

Provides a single consolidated view of all protected assets, simplifying operations in environments where visibility is typically fragmented.

Designed for Compliance & Audit-Readiness

Built around strict data-sovereignty and audit requirements, validated in sectors demanding full control and complete traceability.

Client Shield

Multiplatform, white-label protection to strengthen customer trust, reduce risk, and drive growth

From service provider to customer. Boost customer confidence, reduce digital risk, and unlock new revenue by integrating advanced cyber protection into the customer experience.

Client Shield

CHALLENGE

Organizations across industries must protect customers and their devices against rapidly evolving digital threats. Attackers increasingly target end-user environments with malware, phishing, fraudulent apps or remote-access tools—exploiting the weakest link in the digital interaction. Even well-secured companies remain exposed when customer behavior, device hygiene and external environments lie outside their direct control.

Today’s threats are no longer purely technical. Social engineering, manipulation, and behavioral exploitation are growing just as fast as malware and phishing campaigns. At the same time, users expect safe and seamless digital services without added complexity. Traditional perimeter security cannot protect the full customer journey, making end-user protection essential to maintaining trust and service continuity.

SOLUTION

ESET PRIVATE Client Shield provides a private, brand-aligned protection layer that safeguards customers directly on their mobile devices. It combines advanced threat detection with behavioral insights to stop malware, phishing, fraudulent interactions and manipulation techniques that attempt to exploit customer behavior rather than systems.

Instead of adding friction, the solution integrates smoothly into existing digital ecosystems and enhances security without disrupting the user experience. Organizations gain clear visibility into device and behavior-based risks, reduce fraud-related losses, and strengthen overall trust in their digital channels—all while keeping customer protection effortless and intuitive.

KEY BENEFITS

Client Shield

Real-Time Threat Blocking

Client Shield protects users directly on their devices, blocking malware, phishing and fraudulent activity before it reaches digital services. This closes critical gaps caused by unmanaged endpoints.

Identity Protection

Actively monitors for compromised personal data and instantly alerts users if their credentials or sensitive information are exposed in known data breaches.

Universal Network Coverage (Wi-Fi included)

Security persistently follows the user, ensuring mobile devices remain fully protected across public Wi-Fi, unsecured hotspots, cellular networks, and roaming connections.

Increased Trust and Confidence in Digital Channels

Providing visible protection under the organization’s brand increases user confidence and supports adoption of digital services. Customers feel safer across all interactions.

Seamless User Experience With Transparent Protection

The lightweight client runs quietly in the background, protecting users without adding steps or disrupting digital journeys. Security becomes seamless and invisible.

Measurable Reduction of Fraud and Operational Risk

Early identification of device and behaviour-based risks lowers fraud cases and investigation workload. Organizations save time, resources and maintain smoother operations.

Scanning Solutions

Peak-performance scanning—engineered for scale, accuracy, and security

High-accuracy scanning for large volumes of inbound data—combining flexible deployment with advanced protection against never-before-seen threats.

CHALLENGE

Organizations worldwide face unrelenting pressure to process and exchange massive volumes of files — whether from customer uploads, partner integrations, or automated data pipelines like backups and data lakes. At peak load, these environments can process thousands of files per second, creating security blind spots that traditional endpoint or server-based protection cannot effectively address.

At the same time, many enterprises operate in highly regulated or sensitive environments where public cloud solutions are not an option. Due to data privacy regulations, internal security policies, or isolated infrastructure requirements, these organizations need scanning capabilities that can be deployed on-premises or in air-gapped networks— without compromising performance or detection accuracy.

SOLUTION

ESET PRIVATE Scanning Solutions provide an enterprise-grade file scanning platform designed for high-throughput, security-critical environments. The solution combines ESET's proven detection technologies—including static analysis, machine learning, and behavioral prediction—into a scalable architecture that integrates seamlessly with your existing infrastructure.

Deployment flexibility is a core design principle: ESET Scanning Solutions adapts to your operational and compliance requirements, rather than forcing changes to your environment.

KEY BENEFITS

High-Performance Scanning Engine

ESET's core scanning engine is optimized for speed and efficiency. In many cases, threats can be identified by analyzing only the initial portion of a file, significantly reducing processing time. Deep archive inspection is supported, including archives nested up to 50 levels.

Advanced Machine Learning Detection

Machine learning and neural network models trained on extensive real-world malware datasets enable reliable detection of previously unseen threats, complementing traditional signature-based methods.

Flexible Deployment Options

Cloud-native service, fully containerized on-premises solution, or air-gapped deployment—ESET adapts to your compliance and infrastructure needs.

Seamless Integration

Integration is simple via a gRPC-based API or the ESET Anti-Malware SDK, which supports white-labeling so you can deliver scanning under your own brand.

Built for Scale

A multi-threaded architecture, smart file hashing, and dynamic load balancing ensure near-in-stant responses in high-volume environments.

Enterprise-Grade Support

Custom SLAs and 24/7 access to ESET's top-ranked enterprise support teams provide operational confidence and rapid issue resolution.

Threat Intelligence

Threat intelligence with context — early warning, adversary insight, and focused research

Dedicated threat intelligence with geopolitical and sector-specific insights. Delivers early warnings, focused adversary monitoring, and exclusive research collaboration to strengthen proactive defenses.

Threat Intelligence

CHALLENGE

Organizations face a rapidly evolving threat landscape, including ransomware, affiliate-driven eCrime, state-sponsored APT campaigns, phishing, fraud, and supply-chain attacks. At the same time, they struggle to translate vast volumes of generic threat data into decisions that reflect their specific business risk, sector exposure, and operational priorities.

Security teams are overwhelmed by fragmented intelligence that lacks context, while leaders require clear, decision-ready insight tailored to their organization, environment, and risk appetite—delivered without noise, delay, or ambiguity.

SOLUTION

ESET PRIVATE Threat Intelligence delivers tailored, decision-driven intelligence by combining proprietary telemetry, global research, and analyst expertise into context-rich outputs aligned to each customer’s environment and priorities.

Through advisory-led collaboration, it transforms intelligence into actionable recommendations tied to real business decisions, enabling organizations to:

- Detect threats relevant to your environment
- Anticipate adversary activity early
- Turn intelligence into clear decisions
- Align security with business risk
- Collaborate directly with ESET experts

KEY BENEFITS

Threat Intelligence

Decision-Driven Intelligence

Every output is built around your organization’s real decisions—not generic reporting—ensuring intelligence directly supports risk owners, security teams, and executives.

Customer-Tailored Context

Intelligence is continuously calibrated to your sector, geography, and technology stack, delivering relevance that standard feeds cannot provide.

Analyst-Led Expertise

Certified experts work alongside your team, combining proprietary telemetry, research, and tradecraft to deliver trusted, high-confidence insights with clear recommendations.

From Data to Action

Translate complex threat data into actionable outcomes—bridging the gap between intelligence and execution across SOC, risk, and leadership levels.

Predictive & Proactive Foresight

Forward-looking intelligence anticipates relevant threats and models their impact on your organization, enabling proactive defense instead of reactive response.

Exclusive Collaboration & Visibility

Gain access to unique telemetry and direct collaboration with ESET researchers, delivering insights and intelligence not available through standard market feeds.

Managed Security

SOC-as-a-Service with 24/7 threat monitoring and incident response

Custom-built, end-to-end managed security for your environment. Proactive monitoring and incident response cover multiple perimeters.

Managed Security

CHALLENGE

Keeping pace with today’s fast-moving cyber threats requires constant monitoring, expert analysis, and the ability to respond within minutes—not hours. Many companies rely on overstretched internal teams or fragmented tools that cannot deliver the continuous visibility needed across endpoints, networks, cloud platforms, and identities. This leads to blind spots, delayed reactions, and unnecessary risk exposure.

Building and maintaining a fully functional SOC in-house demands specialized skills in SIEM/SOAR, threat intelligence, digital forensics, and incident response. Recruiting and retaining this expertise is difficult and costly. Without a coordinated, always-on security operation, threats escalate more quickly, detection quality declines, and operational efficiency suffers.

SOLUTION

ESET PRIVATE Managed Services offer a seamless, fully managed security operations capability that strengthens cyber resilience from day one. With 24/7 monitoring, expert-driven detection logic, and rapid incident response, customers gain continuous protection supported by world-renowned threat intelligence. The service ensures the right alerts are identified faster—and addressed more effectively.

A structured deployment model ensures smooth and quick implementation. Once live, it continuously refines detection rules, updates playbooks, enriches telemetry, and adapts configurations to evolving threats and business needs. The result is a reliable, scalable, and intelligence-driven security operation delivered without adding pressure on internal teams.

KEY BENEFITS

Managed Security

Continuous 24/7 Monitoring & Rapid Response

Proactive detection and response across the entire perimeter, supported by L1–L3 SOC teams and custom playbooks for faster containment.

Tailored SOC Operations

Custom configurations, environment-specific rule sets, and detection logic aligned to each customer’s industry, risk profile, and infrastructure.

Direct Access to ESET Threat Intelligence

Integrated intelligence from ESET research centers makes it possible to stop threats even before they impact the customer’s system.

Optimization of ESET Products & Technologies

Superior configuration is a continuous process that ensures you consistently get the maximum value from every ESET product already deployed in your environment

Reduced Operational Burden & Lower TCO

Enhances existing security operations, lowering resource overhead and reducing total cost of ownership through consolidation.

Transparent Reporting & Governance

Regular incident reporting, compliance support, and governance sessions ensure clarity, accountability, and audit-ready documentation.

Industrial Security

Lasting cyber resilience for legacy systems and critical infrastructure

End-to-end protection across the entire digital infrastructure. Built to secure legacy systems and critical operations with minimal disruption, long-term support, and operational continuity.

Industrial Security

CHALLENGE

Industrial, healthcare, and critical infrastructure rely on long-lifecycle systems that must remain stable for years. Many of these devices run legacy Windows versions or platforms that cannot be upgraded without costly equipment replacement. As IT and OT environments converge, these systems with limited or restricted update capabilities become directly exposed to modern cyberattacks.

Attackers increasingly exploit this weakness and target them with ransomware, wipers, and stolen credentials. Operational downtime is costly and disruptive. Aging systems are difficult to patch and easy to exploit. Organizations need protection that avoids disruption and doesn’t require replacing long-lifecycle equipment.

SOLUTION

Lifecycle Solutions provides endpoint security for industrial and critical infrastructure environments where upgrades are difficult, and connectivity may be restricted or fully air-gapped. All solutions support controlled, on-site update distribution and operate without cloud dependency – ensuring operational continuity and regulatory compliance.

Long-Term Support (LTS) delivers a stable, on-premises product baseline maintained over a multi-year lifecycle. It ensures predictable, reliable protection without disruptive version changes or unexpected feature shifts.

Legacy Support (LLS) extends advanced security to environments running end-of-life operating systems, empowering organizations to safeguard essential systems even when modernization is impractical or cost-prohibitive.

KEY BENEFITS

Industrial Security

Real-Time Threat Detection

High-quality real-time detection that protects modern and legacy systems without disrupting operations.

Lightweight, Performance-Friendly Design

Security is designed to protect without degrading performance or impacting production continuity.

Predictable lifecycle stability

LTS / LLS minimize disruptive change by keeping validated versions supported for years.

One Management Platform

Control of both modern and legacy endpoints through a single, streamlined management platform.

Protect Legacy Systems

Maintains protection for systems that cannot be upgraded.

Air-gapped and restricted-network ready

Runs fully on-prem with no mandatory cloud connectivity or external dependencies.

Operating system Coverage for Legacy Support (LLS)

Endpoint Security

- Windows XP SP3
- Windows Vista
- Windows 7
- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows 10

Server Security

- Windows server 2003 SP2
- Windows server 2003 R2 SP2
- Windows server 2008 SP2
- Windows server 2008 R2 SP1
- Windows server 2012

Advisory

Expert-led strategy to strengthen resilience

Custom cybersecurity strategies to strengthen readiness, compliance, and awareness. It helps organizations proactively anticipate, withstand, and adapt to threats, while protecting continuity and core business needs.

Advisory

CHALLENGE

Organizations are continuously investing in cybersecurity tools, yet breaches, operational interruptions, and compliance gaps persist. The core issue is not technology alone—it is the absence of a unified, organization-wide approach that connects security with strategic priorities. Cybersecurity often remains fragmented, leaving leadership without clear visibility into risk exposure and without the ability to make timely, confident decisions.

At the same time, regulatory pressure and increasingly complex threat landscapes demand more than reactive security. Companies struggle to translate high-level strategy into practical execution, maintain consistent control across their environment, and ensure that leadership, operations, and the workforce are aligned in how they prevent, detect, and respond to incidents.

SOLUTION

ESET PRIVATE Advisory provides a structured, end-to-end approach that embeds cybersecurity directly into the organization’s governance, operations, and decision-making. Acting as a long-term strategic partner, ESET helps define clear accountability, establish executive-level ownership of cyber risk, and ensure that security investments directly support business outcomes.

We translate strategy into measurable execution by shaping architectures, operational processes and cross-functional coordination. Through tailored governance, capability development, and continuous operational support, we help organizations shift from reactive security to predictable and sustainable cyber resilience.

KEY BENEFITS

Advisory

Strategic Cybersecurity Alignment

Establishing cybersecurity as a board-level priority, assessing current maturity, defining risk ownership, and aligning security investments with business objectives.

Cyber Resilience & Continuity Planning

Structuring security architectures, governance models, and control frameworks that translate strategy into enforceable, scalable operations across the organization.

Incident & Crisis Readiness

Equip leadership and operational teams with the frameworks, playbooks, and muscle memory required to make fast, high-impact decisions under pressure—when time, clarity, and coordination are critical.

Continuous Risk, Threat and Supply Chain Integration

Continuously assessing evolving risks, regulatory requirements, and third-party exposure, helping to adapt strategies to maintain resilience over time.

Operationalizing Security within the Organization

Embedding cybersecurity into day-to-day operations, integrating controls and risk management into business processes and cross-functional workflows.

Long-Term Security Maturity Acceleration

Providing sustained advisory partnership that builds internal operations and governance. Organizations gain a long-term advantage: faster adaptation to new risks.


Cybersecurity
Progress. Protected.
Thank you!
https://www.eset.com/us/business/tailored-solutions/