Cyber Resilience Recognized by Gartner®: ESET's Prevention-First Approach

Cybersecurity
Progress. Protected.

Embracing Proactive Cybersecurity Mindset Pays Off

As digital transformation accelerates, organizations face growing complexity and an expanding attack surface. Cloud-first services, remote work, and AI-driven innovation are reshaping business operations—but also creating new vulnerabilities across endpoints, email, SaaS apps, and networks.

Threat actors are evolving fast, using sophisticated tactics like social engineering and AI-generated ransomware to bypass traditional defenses. Many organizations lack visibility into their attack surface, leaving them exposed and uncertain.

That's why a prevention-first cybersecurity strategy is no longer optional. It helps mitigate advanced threats, reduce breach costs, and ensure operational continuity.

This paper explores how we believe ESET—recognized by Gartner in endpoint protection platforms —empowers organizations to stay resilient and secure in a world where change is constant.

Why Proactive Cybersecurity Truly Matters

Let's be crystal clear: waiting for an attack to happen before taking action has not been a viable strategy for quite a long time. The threat landscape is evolving at a pace that demands foresight, agility, and above all—prevention. A proactive cybersecurity posture isn't just a technical choice; it's a strategic imperative.

The Evolving Threat Landscape: Prevention as a Necessity

It's hardly surprising that cyber threats are becoming more sophisticated, frequent, and damaging. The first half of 2025 saw a surge in social engineering attacks like ClickFix, which increased by 517% and now accounts for 8% of blocked threats across Windows, Linux, and macOS.

Infostealers like SnakeStealer have overtaken legacy malware, doubling in detections and now representing nearly 20% of all infostealer activity.

But perhaps the most alarming development is the emergence of AI-generated ransomware. ESET's discovery of PromptLock—the first ransomware powered by generative AI—marks a turning point.

This malware autonomously generates malicious scripts in real time, deciding whether to exfiltrate or encrypt data based on predefined prompts. The implications are profound: attackers no longer need teams of developers; a well-configured AI model is enough to launch complex, adaptive attacks.

Cost-Effectiveness: Prevention Saves Millions

The financial toll of cyber incidents is also staggering. According to CISA's Cyber Hygiene Services, early threat mitigation can reduce breach-related costs by up to 40% within the first 12 months, especially in large-scale incidents.

Such early threat mitigation is typically a preventive measure that subsequently helps organizations avoid the cascading expenses of breach remediation, legal fees, regulatory fines, and reputational damage.

IBM's 2025 report found that the average cost of a data breach reached $4.4 million. Costs were lowest for organizations using DevSecOps, AI-driven threat detection, and SIEM platforms. In contrast, shadow AI, supply chain breaches, and complex security systems drove costs higher—highlighting the value of streamlined, intelligent, and proactive cybersecurity.

Operational Continuity: Minimizing Downtime

Cyberattacks don't just compromise data—they disrupt operations, often bringing business to a standstill. And the financial impact of downtime varies dramatically across industries.

As Gartner notes, "Executive leaders need to start by understanding downtime costs and lost revenue. For example, operational downtime costs consumer packaged goods (CPG) organizations on average $40,000 per hour, while for automotive companies, downtime costs are up to $3 million per hour." We feel these figures underscore the urgency of proactive cybersecurity strategies that safeguard business continuity.

Solutions like continuous monitoring, endpoint protection, and incident response planning empower organizations to maintain essential functions—even under duress.

Cyber resilience, which blends prevention, detection, and recovery, is no longer optional: it's a strategic imperative to ensure that operations don't just survive an attack—they keep running through it.

Brand, Trust and Compliance: Building Confidence

Customers and regulators alike expect organizations to protect sensitive data. Proactive cybersecurity directly supports compliance frameworks such as the NIST Cybersecurity Framework and HIPAA, as well as regulations like SOX and CCPA, which mandate robust risk management, incident reporting, and technical safeguards.

HIPAA violations, for instance, can cost organizations up to $50,000 per violation, with annual caps reaching $1.5 million, while criminal cases may bring fines of $250,000 and prison time. Under SOX, executives can face fines of up to $5 million and 20-year sentences for knowingly filing false reports.

Meanwhile, the CCPA imposes penalties of up to $7,500 per intentional violation, a figure that can escalate quickly in large-scale breaches. Beyond avoiding these fines, however, proactive security builds trust. It signals to customers that their data is safe, their privacy respected, and their loyalty valued.

The Hidden Costs of a Reactive Approach

Delayed breach detection allows attackers to deepen infiltration, escalating the average cost to $5.1 million in 2025. Recovery becomes complex, requiring resource-heavy incident response and digital forensics, often supported by costly DFIR retainer services. Beyond technical remediation, reputational damage and customer churn are long-term consequences. According to IBM, the global average cost of a data breach reaches $4.4 million.

Cyber risk incidents can have significant operational, financial, reputational, and strategic consequences. Reputational damage from breaches undermines customer trust and brand equity, often resulting in long-term churn and diminished market competitiveness. These hidden costs make reactive strategies unsustainable.

Prevention-First Strategy

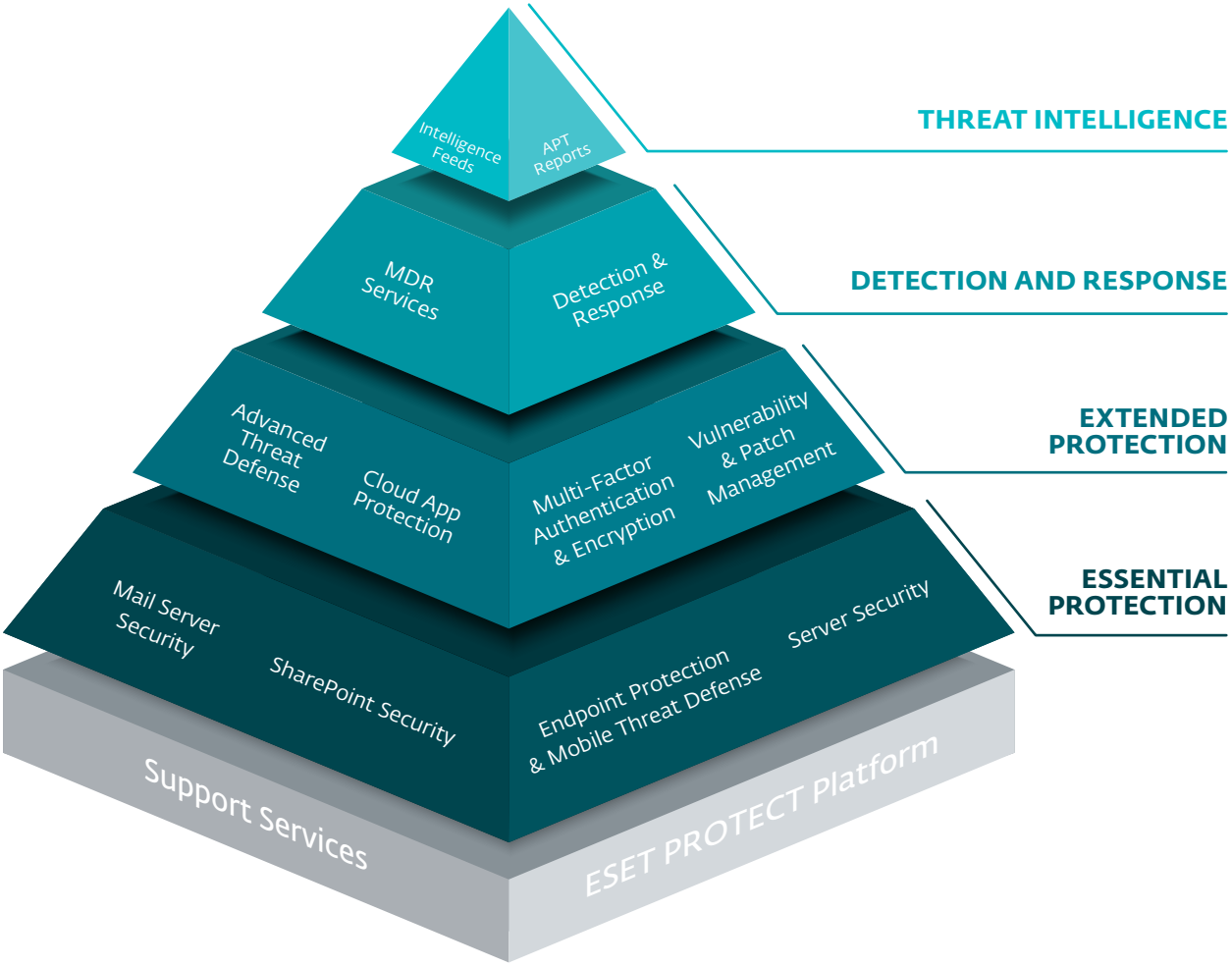
A lot can be achieved with a prevention-first strategy that addresses issues in a comprehensive way. However, effective prevention begins with robust endpoint protection. As the primary defense layer, it stops threats before they spread.

ESET's multilayered endpoint security combines advanced heuristics, machine learning, and cloud-based reputation systems to block ransomware, exploits, and AI-generated malware—making it the cornerstone of proactive defense.

Threat Intelligence is the second pillar of prevention, enabling early detection and strategic decision-making. Here comes ESET Threat Intelligence into play, which provides real-time feeds, APT reports, and deep visibility into emerging threats, helping security teams anticipate and neutralize attacks before they escalate.

Continuous monitoring and risk assessment ensure that threats are not only detected but also contextualized and swiftly addressed—making them the third key pillar of a prevention-first strategy. ESET MDR (Managed Detection and Response) offers 24/7 monitoring, threat hunting, and expert-led incident response, reducing detection time and minimizing business disruption.

Finally, there's zero-trust architecture that reinforces the human layer of cybersecurity. ESET Cybersecurity Awareness Training empowers employees to recognize phishing, social engineering, and insider threats, aligning with zero-trust principles by treating every access request as potentially risky, regardless of origin.



Together, these pillars form a resilient, intelligence-driven framework that shifts cybersecurity from reactive defense to proactive prevention.

Building Proactive Defense

The Core Pillar: Endpoint Protection

In a prevention-first strategy, endpoint protection is not just a layer—it's the foundation. Most threats originate at the endpoint, making it the first and most critical line of defense. ESET's approach to endpoint protection is powered by its proprietary ESET LiveSense® technology, a multi-layered framework that integrates advanced detection mechanisms including DNA detections, behavioral analysis, machine learning, and cloud-based reputation systems.

ESET's LiveSense® technology offers real-time, intelligent, and adaptive protection across all stages of the threat lifecycle. Combined with Intel-powered AI optimization, it delivers lightweight performance with low false positives which is ideal for modern, distributed workforces.

The Unifying Realm: ESET PROTECT Platform

The ESET PROTECT Platform—rated 4.6 / 5 as of September 30, based on 1000 reviews by users on Gartner Peer Insights™ review platform across product capabilities, integration, and support—extends, in our opinion, this endpoint-first philosophy into a centralized, cloud-native management console.

It automates key security workflows, integrates seamlessly with SIEM and XDR platforms, and supports complex environments—on-prem, cloud, and hybrid. With coverage across Windows, macOS, Linux, Android, iOS, and servers, it ensures consistent protection across all assets.

ESET offers subscription tiers tailored to specific threats—ransomware, phishing, insider threats, identity-based attacks, and more. For high-security environments, ESET PROTECT Platform supports air-gapped systems and strict data residency requirements. Gartner recognizes ESET as a Challenger in its 2025 Magic Quadrant™ for Endpoint Protection Platforms.

Automation & Advanced Tools

Automation is a key enabler of proactive defense as well. ESET Vulnerability and Patch Management and the recently launched Ransomware Remediation tool provide automated rollback and file recovery from secure backups, even when threat actors attempt to corrupt system restore points.

These tools reduce remediation costs and response time, reinforcing resilience, and help stop attacks from escalating into full-blown crises—giving security teams time to focus on prevention, not just cleanup.

Cloud Office Security

Customers can also rely on ESET Cloud Office Security which protects Microsoft 365 and Google Workspace apps—Exchange, OneDrive, SharePoint, Gmail, and more—against spam, phishing, and zero-day threats. Operating entirely in the cloud, it offers scalable, multitenant protection with sandboxing via ESET LiveGuard Advanced, ensuring business continuity and secure collaboration.

As a preventive layer, it blocks threats before they reach users' inboxes or cloud storage—reducing the risk of ransomware, phishing, and data loss. This is especially valuable in remote and hybrid work environments, where cloud apps are frequent entry points for attackers.

Recognition by Industry Analyst Firm

ESET's Endpoint Protection Platform continues to earn recognition from Gartner—an industry analyst. In various comparative and thought leadership reports, we feel ESET has been acknowledged as a trusted and capable cybersecurity provider, particularly for organizations seeking reliable, flexible, and well-supported endpoint protection.

ESET recognized in the 2025 Gartner Magic Quadrant

In the 2025 Gartner Magic Quadrant for Endpoint Protection Platforms, ESET was named a Challenger for its ESET PROTECT offering. In our opinion, this recognition reflects not only ESET's consistent execution but also its strategic vision in a rapidly evolving threat landscape.

We strongly feel this recognition in the Magic Quadrant demonstrates ESET's commitment to delivering value through innovation, operational excellence, and a deep understanding of customer needs.

According to Gartner, Challengers offer mature endpoint protection products that effectively meet the needs of EPP buyers. They also have strong market visibility, resulting in better Ability to Execute compared to Niche Players. However, Challengers are often late in addressing emerging needs, lack in-depth product integration and may have accumulated technical debt, affecting usability. They may also lack alignment with the market's direction, impacting their Completeness of Vision compared to Leaders. Challengers are practical choices, especially for customers who have established strategic relationships with them.

ESET as an Established Vendor in Gartner "Voice of the Customer" for Endpoint Protection Platforms 2025

Since its launch in October 2015, Gartner Peer Insights has collected over 300,000 verified reviews across more than 330 technology markets, offering buyers a unique peer-driven perspective on vendor performance. The "Voice of the Customer" is a document that applies a methodology to aggregated Gartner Peer Insights' reviews in a market to provide an overall perspective for IT decision makers.

This aggregated peer perspective, along with the individual detailed reviews, can also complement expert-generated research such as Magic Quadrants and Market Guides. It can play a key role in your buying process, as it focuses on direct peer experiences of buying, implementing, and operating a solution.

In the 2025 Gartner® Peer Insights™ "Voice of the Customer" report for Endpoint Protection Platforms, **ESET was named an Established Vendor in the overall Endpoint Protection Platforms market**. ESET has an overall rating of 4.8 out of 5, based on 68 reviews as of September 30, 2025.

We feel this recognition underscores ESET's exceptional performance and long-standing commitment to building solutions that effectively address cybersecurity challenges across industries. By focusing on customer needs, technical excellence, and operational reliability, ESET continues to deliver value to organizations of all sizes.

Peer Insights disclaimer: Gartner Peer Insights content consists of the opinions of individual end users based on their own experience with the vendors listed on the platform, and should not be construed as statements of fact, nor does it represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product, or service depicted in this content, nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

Trusted Across Industries and Regions

ESET is trusted by users across a wide range of industries and geographies. According to the 2025 Gartner Peer Insights "Voice of the Customer" report:

- 37% of reviews came from the public sector, government, and education
- 21% were from services and 10% healthcare
- The remaining 32% represented other sectors

ESET Recognized in Gartner Vendor Spectrum for Endpoint Protection Platforms 2025

A "Vendor Spectrum" document synthesizes Gartner Peer Insights' reviews into useful insights for enterprise IT buyers. It offers them a view of the vendor landscape in Gartner's research market, based on the vendor peer reviewers considered and selected in their buying process.

The vendors that are selected or considered most frequently in a market are included in the Vendor Spectrum graphic. This aggregated peer perspective can be used in conjunction with other Gartner-published research to aid the technology shortlisting and buying process. Vendors in the report are categorized into three groups:

- Targeted Selection
- Balanced
- Broad Consideration

ESET Recognized as a Balanced Vendor

In the 2024 edition of the Gartner Vendor Spectrum for Endpoint Protection Platforms, ESET was recognized as a Balanced Vendor—a designation given to vendors that in our opinion are frequently considered and selected relative to others in the market.

We believe this recognition confirms that ESET is consistently shortlisted and chosen by buyers evaluating endpoint protection platforms, reflecting both its technical strength and market trust.

This feedback reinforces that proactive defense is not just about technology—it's about value. ESET's approach combines cost efficiency, operational reliability, and customer intimacy, which we believe makes it a preferred choice for organizations seeking both protection and partnership.

Gartner Critical Capabilities for Endpoint Protection Platforms Report 2025

A Critical Capabilities document is a comparative analysis that scores competing products or services against a set of critical differentiators identified by Gartner. It shows you which products or services are the best fit in various use cases to provide you actionable advice on which products/services you should add to your vendor shortlists for further evaluation.

This report complements the Gartner Magic Quadrant by diving deeper into product functionality, deployment flexibility, and operational strengths, giving buyers a clearer picture of how solutions align with their unique needs.

ESET PROTECT: Tailored for Small and Midsize Organizations

ESET's solution is designed to deliver reliable protection without unnecessary complexity, making it ideal for organizations that prioritize efficiency, compliance, and continuity.

Flexible Deployment Options

ESET PROTECT offers a range of deployment models to suit different infrastructure needs:

- Hybrid management: On-premises and cloud-based options
- Global availability: North America, Europe, and Asia
- Low-connectivity support: Operates effectively in environments with limited or intermittent internet access

Core Strengths and Ideal Use Cases

ESET PROTECT stands out for its high protection efficacy, consistently delivering strong prevention and detection capabilities across diverse environments. Its cloud-based management console is both intuitive and powerful, enabling security teams to manage endpoints efficiently without unnecessary complexity.

What truly sets ESET apart is its mature hybrid management architecture. Whether deployed in the cloud, on-premises, or in a hybrid setup, ESET ensures continuity and compliance—even in low-connectivity or air-gapped environments. This flexibility makes it a dependable choice for organizations with strict regulatory requirements or operational constraints.

When it comes to use cases, ESET PROTECT is particularly well-suited for organizations that need reliable, lightweight endpoint protection without sacrificing performance or manageability. It's a strong fit for environments where data governance and regulatory compliance are non-negotiable, such as government, healthcare, and finance.

For businesses that don't require broad OS support but demand stability, simplicity, and security, ESET offers a compelling solution. Its ability to operate effectively in architecturally constrained or bandwidth-limited environments makes it ideal for distributed teams, remote offices, and sectors with strict infrastructure policies.

Conclusion

In today's dynamic threat landscape, cybersecurity is no longer just a technical challenge—it's a strategic business imperative. Organizations must move beyond reactive defense and embrace a proactive, prevention-first mindset to safeguard operations, data, and reputation.

We believe ESET, recognized by Gartner across multiple reports, offers a compelling blend of technical excellence, operational reliability, and customer-centric innovation. From its multilayered endpoint protection and threat intelligence to its cloud-native management platform and advanced automation tools, ESET delivers a unified solution tailored to modern needs.

Whether you're a mid-sized business seeking cost-effective protection or a global organization navigating complex regulatory environments, ESET provides the flexibility, trust, and performance required to stay ahead of evolving threats.

As the Gartner recognition shows, ESET is not just a vendor—it's a cybersecurity partner - one that helps organizations build resilience, reduce risk, and thrive in a world where change is the only constant.

Attribution:

Gartner, Inc. Magic Quadrant for Endpoint Protection Platforms. Evgeny Mirolyubov, Deepak Mishra, Franz Hinner. 14 July 2025.

Gartner, Inc. Voice of the Customer for Endpoint Protection Platforms. Peer Community Contributors. 23 May 2025.

Trademark disclaimer:

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. MAGIC QUADRANT and PEER INSIGHTS is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.

Objectivity disclaimer:

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

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

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

eset
Cybersecurity
Progress. Protected.