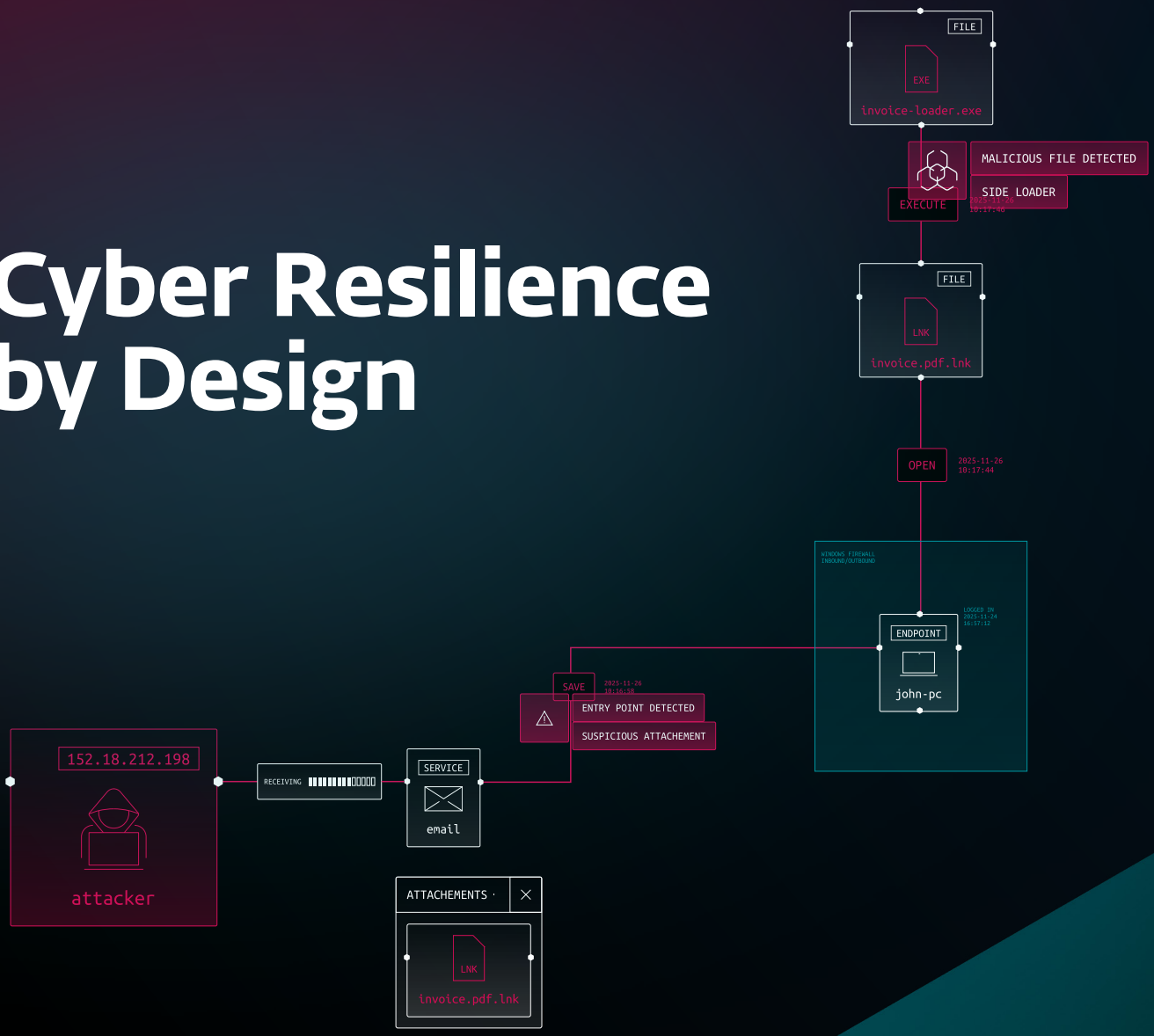
Cyber Resilience by Design



Cybersecurity
Progress. Protected.

If you work in security, you already know the uncomfortable truth: perfect security doesn't exist. When protection and detection fall short, it brings frustration and it's easy to feel like you're losing ground. The goal is to effectively anticipate what's coming, resist what matters, expose what's inside your environment, react fast, restore what's broken, and then keep going without letting incidents derail the business. That's cyber resilience in plain language.

This paper lays out a practical framework and roadmap, grounded in current data and realities. It walks you through how ESET does the magic as a technology enabler you can lean on, so you can spend more energy on processes, people, and business continuity.

Cyber Resilience: What's Really Going On?

Cyber resilience isn't about building a rigid fortress—it's about creating an adaptive system where technology, processes, and people interact dynamically to respond to change. The fact is that systems will fail and people will make mistakes. The question isn't if, but rather how prepared you are when it does.

So, what is cyber resilience, really? Think of it as your organization's ability to anticipate trouble before it strikes, spot it fast when it does, respond with precision, and restore what matters without grinding business to a halt. It's not just technology, it's processes, people, and the mindset that says: "We can take a hit and keep moving."

Industry thinking is also shifting in this direction. Increasingly, organizations are prioritizing resilience and recovery over the traditional goal of breach prevention. Rather than assuming incidents can be avoided entirely, leaders are designing systems to withstand failure, maintain operations under pressure, and recover quickly from disruptive events. This reflects a broader understanding of cybersecurity as risk management rather than risk elimination and reinforces the assumption-of-breach mindset that now dominates board-level conversations.

According to Gartner®, "by 2028, half of CISOs will formally rebrand their cybersecurity program as cyber resilience programs."

Gartner: *Predicts 2026: Cybersecurity Program Rebrands to Cyber Resilience, Arthur Sivanathan, Charlie Winckless, Will Candrick. [1 December 2025] ID: G00841555.*

The truth is that resilience isn't perfection. It's consistency under pressure which means doing enough, every day, so that when chaos comes knocking, you don't panic and you know what to do instead. The opposite of resilience is fragility. It takes hold when roles, responsibilities and priorities are unclear, tool stacks are rigid and tangled, teams drown in alerts and blind spots, identity controls are weak, and Zero Trust exists only as a presentation slide, not as a strategy.

Fragility is confusion about what to do first, what to fix, outsource, and what to own, which is a state leading directly to what we can call a paralysis. Hardly anyone is willing to be paralyzed when it comes to critical situations, right?

A resilient organization looks different. It knows likely scenarios, it also knows who does what, when, and how, across technology, processes, and people. It doesn't aim for "never breached." It aims for "never broken".

The Threat Picture of Why Resilience is Critical in 2026

If you think the cyber threat landscape is intense now, buckle up because 2026 is accelerating it further. Three forces are driving this shift: AI-driven threats, sprawling hybrid environments, and geopolitical turbulence. The world isn't getting safer, but organizations can still build cyber resilience if they understand what's changing.

First, let's talk about speed. AI-powered malware and autonomous attack chains now compress intrusion timelines from days to hours, sometimes minutes. Attacks adapt in real time, chaining exploits without waiting for human hands.

In November 2025, Anthropic announced it had identified and disrupted one of the earliest known cyber-espionage campaigns leveraging an AI agent to autonomously carry out operations in the wild. For businesses, this signals a future where attacks can scale and adapt at machine speed, making proactive resilience and AI-governed defenses non-negotiable.

Then there's the complexity problem. Hybrid infrastructures—cloud, on-prem, SaaS—introduce adaptive complexity, requiring integrated controls that evolve with changing environments. Every new integration is a new doorway, and attackers know it. Supply chain gaps in open-source packages, build systems, and commercial binaries show how trust without verification remains a liability.

At the same time, cloud misconfigurations remain one of the most exploited weaknesses in hybrid environments. Unsecured storage buckets, overly permissive IAM roles, and neglected API endpoints create silent entry points for attackers. Continuous posture management and automated compliance checks are essential to close these gaps.

60%

of all breaches

are driven by human element.

Source: *Verizon: 2025 Data Breach Investigations Report*

Let's not forget the human angle. Phishing remains the number one entry point, now turbocharged by generative AI that makes fake emails eerily convincing. AI-enabled scaling has fueled identity-based attacks, and Verizon's 2025 Data Breach Investigations Report confirms the human element drives 60% of all breaches. AI-assisted Business Email Compromise (BEC) tactics alone have resulted in record financial impacts, with the 2024 FBI's IC3 reporting $2.77 billion in annual losses.

These trends underscore the financial stakes: IBM's Cost of a Data Breach Report 2025 pegs the global average breach cost at $4.44 million, while organizations using security AI save nearly $1.9 million per breach. Rather than just a statistic, it can be a business case for speed and automation.

Finally, there's a regulation which is raising the floor. In the United States, the latest SEC's final rule on Cybersecurity Risk Management and Incident Disclosure adopted in 2023 requires public companies to treat cyber risk as a material business issue, mandating four-business-day disclosure for material incidents and annual transparency around governance and oversight.

For federal contractors, the Cybersecurity Maturity Model Certification (CMMC) 2.0, effective November 2025, ties contract eligibility to NIST SP 800-171 compliance, making sound cyber hygiene a precondition for business with the Department of Defense.

At the executive level, Executive Order 14028 (2021) and its reinforcement through Executive Order 14144 (2025) are setting the standard for Zero Trust architecture, software supply chain security, and mandatory incident reporting within the federal government—and signaling those expectations across private sector providers.

In Europe, the same trajectory is playing out through NIS2 and the Digital Operational Resilience Act (DORA). DORA, in force as of January 2025, imposes uniform requirements on ICT risk management, operational resilience testing, and third-party oversight for financial entities.

$1.9 million

per breach was saved when organizations used security AI.

Source: *Verizon: 2025 Data Breach Investigations Report*

NIS2, now transposing across member states, expands scope and enforcement, elevating executive accountability and harmonizing incident reporting obligations across critical sectors. Whether navigating US or EU frameworks, the signal is consistent: resilience is no longer optional, sector-specific, or purely technical—it is a regulated business obligation.

The bottom line is that the cyber resilience in 2026 means simplicity, visibility, readiness at machine speed, and compliance.

The Resilience Lifecycle: 6 Stages, 3 Dimensions

Cyber resilience isn't a single control or a shiny product either. You can think of it as a cycle, a rhythm your organization learns to live by. Six stages define this lifecycle, and each one touches three dimensions: technology, process, and people. Together, they form the backbone of continuity when unexpected happens.

Not every organization starts from the same place. Some will already operate advanced detection, orchestration, and intelligence capabilities; others may rely on only a small number of foundational controls such as endpoint protection and firewalls

The resilience lifecycle is not a linear maturity model that all organizations must fully implement to be considered resilient. Instead, it represents a set of outcomes that can be approached incrementally, based on organizational maturity, risk appetite, and available resources.

ANTICIPATE — Know Your Risk Before It Knows You

Anticipation begins with understanding your attack surface and the threats most likely to target it.

Technology such as external surface mapping, curated threat intelligence, and identity-risk monitoring provides early visibility, while processes like business-aligned risk assessments and realistic tabletop exercises prepare teams for credible scenarios.

People complete this picture: executives need clear briefings, risk thresholds, and decision triggers to act quickly. With attackers exploiting vulnerabilities at machine speed and AI-driven phishing → expanding rapidly, anticipation creates the time advantage that resilience depends on.

RESIST — Reduce Avenues of Compromise

Resistance focuses on closing the easy paths adversaries look for.

Technology enforces Zero Trust principles, from phishing-resistant authentication to granular access policies across cloud and on-prem environments, supported by Cloud Security Posture Management (CSPM) to maintain secure baselines and by tighter management of both human and machine identities.

➜ Processes reinforce this posture through configuration standards, patching expectations, privileged access reviews, and growing emphasis on SaaS security. People remain essential, as embedded security expertise and adaptive, role-based training help ensure secure behavior is practiced consistently across the business.

EXPOSE — Reveal Hidden Risks

Visibility enables early detection of threats that evade preventive layers. Whether delivered through XDR capabilities or managed detection services, detection platforms should deliver strong identity and endpoint telemetry, tuned to catch ransomware precursors like credential theft and lateral movement.

High-fidelity telemetry from XDR, identity sources, endpoints, and cloud-native services helps uncover credential theft, lateral movement, and misconfigurations. Integrating Cloud-Native Application Protection Platform (CNAPP) and CSPM strengthens visibility across APIs, privileges, and multi-cloud workloads, while software supply chain monitoring reduces dependency-driven risks.

These technological capabilities are only effective when supported by processes that tune detections to frameworks like MITRE ATT&CK, maintain crisp SOC workflows, and reduce alert fatigue. Skilled human analysts transform

➜ telemetry into insight and help build knowledge for future scenarios.

REACT — Automate the First 15 Minutes and Get People Ready

When an incident occurs, reaction speed determines whether disruption is contained. Technology provides immediate response through SOAR playbooks or MDR services that isolate compromised assets, elevate authentication requirements, and verify backup integrity before human responders can intervene.

For organizations without in-house SOC or automation capabilities, these same response outcomes can be achieved through managed detection and response (MDR) services that provide continuous monitoring, expert-led investigation, and pre-built containment playbooks aligned to common attack scenarios.

Processes must be built around the tempo of modern attacks, with predefined communication flows, escalation paths, and decision trees for regulatory or legal engagement. People play a decisive role: clearly assigned responsibilities, regular drills, and well-understood authority lines ensure teams operate with confidence when seconds matter most.

RESTORE — Fast, Clean Recovery

Resilient organizations assume they will face a potentially catastrophic incident.

➜ The real question is whether systems can continue operating, whether roles and responsibilities are clear under pressure, and whether recovery paths are known and tested. All this matters as much as the underlying technology.

Recovery demonstrates whether resilience truly works. Technology such as immutable backups, tested restore paths, cloud failover options, and integrity checks ensures systems return to operation without reintroducing risk. Processes align RTO and RPO with business impact, define supplier failover plans, and codify recovery exercises for ransomware, SaaS compromise, and partner outages.

Frameworks from SEC, CIRCIA, NIST and CISA support continuity when third parties fail. People complete the restoration effort by coordinating across legal, finance, communications, and customer-facing roles, providing clarity and stability at a time when trust matters most.

➜ **Go On** — Learn and Adapt

Adaptation ensures resilience improves rather than stagnates. Technology supports this through post-incident analysis, platform consolidation, and retiring redundant tools to reduce operational drag.

Processes translate lessons learned into policy updates, prioritized backlog items, and governance improvements with clear ownership. The human dimension remains fundamental: teams require psychological safety and sustainable workloads to perform effectively over time.

One Forrester research report on security team toxicity states that "engaged, healthy, psychologically safe, and collaborative security teams experience fewer breaches." Forrester also reminds that "teams that lack this psychological safety report more breaches, including 3.5 times more internal incidents than the global average."

Real-world Barriers (And Tips How to Tackle Them)

Cyber resilience sounds great on paper, but reality has a way of complicating things. Organizations face a handful of stubborn obstacles that can derail even the best intentions. Let's unpack some of them and see how to tackle each.

The first thing is the budget problem since most enterprises juggle sprawling tool stacks. "According to a Gartner survey of 162 large enterprises, conducted between August and October 2024, organizations use an average of 45 cybersecurity tools." [1]

That's not resilience, that's chaos. Every extra console creates a tangled web of interdependent tools that drives up cost and introduces blind spots, making consolidation essential. Focus on what matters most—let it be things such as identity controls, exposure management, and backup/restore capabilities—and nail those before chasing niche tools.

"Fifty-eight percent of CISOs cite budget restrictions as one of the most significant challenges impacting their cyber resilience efforts. As such, elevating cyber resilience is more likely through reallocation than through net new investment."

Gartner: *Cyber Resilience in the Boardroom: 3 Messages CISOs Must Deliver, Christopher Mixter, Leigh McMullen, Christine Lee. [4 December 2025] ID: G00838385.*

Then comes an alert overload which drowns SOC teams in noise, forcing them to chase false positives while real threats slip through. Like we already discussed, the answer isn't more alerts, but smarter ones. Tune detections around known ransomware chains, identity misuse, and SaaS anomalies, and lean on governed AI to cut false positives.

Besides, human factors remain the wildcard because people click links, reuse passwords and have oftentimes poor understanding of possible threats. The solution lies in short, scenario-based training that feels real, not theoretical. GenAI can supercharge these programs with adaptive simulations and personalized nudges.

Another trap worthy of attention is Zero Trust gaps. Many treat Zero Trust as a product you can buy, but nothing can be further from truth. In fact, Zero Trust functions as an operating model: IBM describes it as a security strategy for modern hybrid environments, leveraging tools such as segmentation, identity-and-access controls and visibility which were the tools that constituted the model itself from the very beginning.

[1] Gartner Press Release, Gartner Identifies the Top Cybersecurity Trends for 2025, March 3, 2025.

Building a Resilient Organization

What you can do in-house and what to outsource? Start by assessing your maturity with clear eyes. Map your current capabilities against the six stages of resilience. If you don't have the staff for 24×7 monitoring, don't pretend you do—outsource detection and response to specialists who can.

On the other hand, if identity hygiene and patching are your weak spots, keep those in-house. They're "cultural," in a sense, meaning they refer to practices and behaviors deeply embedded in your organization's way of working, and depend on people's habits, values, and day-to-day decisions rather than just technology. Identity hygiene and patching are also operational and too close to the core of your business to delegate.

In house focus:

- **Identity & Access Hygiene:** Multi-factor authentication, privileged access management, passwordless strategies—these are deeply tied to organizational culture and daily operations.
- **Patch & Configuration Management:** This is critical for reducing attack surface; it also requires close coordination with internal teams which makes it wise to keep in-house.
- **Backup Strategy & Recovery Drills:** Ownership ensures trust and alignment with business priorities.

Outsource candidates:

- **Managed Detection & Response (MDR):** Continuous monitoring and threat hunting often require scale and expertise beyond most internal teams.
- **Threat Intelligence & Takedown Support:** External providers have broader visibility and faster takedown capabilities.
- **Incident Response Surge Capacity:** For major breaches, external IR teams bring specialized skills and speed.

The distinction comes down to culture, scale, and trust. Identity hygiene and patching rely on internal behaviors and processes, making them hard to outsource effectively. Continuous monitoring and threat intelligence, on the other hand, benefit from vendor scale and global visibility. Backup and recovery are too sensitive to delegate fully, requiring direct control to ensure alignment with business priorities.

This split also reflects what the data is telling us: Accelerated threats and growing supply chain complexity require continuous monitoring paired with strong hygiene. As Gartner notes,[2] this “rapid expansion of threats continually challenges cybersecurity and supply chain teams to keep pace, while the growing use of GenAI among trading partners increases the risk of data breaches and intellectual property leakage.” This underscores the need to maintain vigilant monitoring and robust hygiene practices.

How ESET Supports Cyber Resilience as a Technology Enabler

Cyber resilience can't be delivered by any single vendor or control set. ESET’s role is focused on workplace security—endpoints, user devices, and the telemetry and response capabilities anchored there.

This does not replace identity management, SaaS governance, data loss prevention, or business process recovery planning, which remain essential components of a complete resilience strategy.

If you’re tired of stitching point solutions, the first step is a ready-to-go package: deploy quickly, administer simply, and raise visibility across endpoints, identity, and data, so your core controls are reliable and quiet. ESET can help you technologically in the four aspects:

[2] Gartner Press Release, Gartner Says Supply Chain Cybersecurity is at Peak of Inflated Expectations, September 29, 2025.

1. Anticipate

ESET Threat Intelligence (ETI) delivers curated threat reports and real-time feeds to inform decision makers, sharpen organizational risk assessments, and enhance readiness. It includes:

- Detailed analysis of APTs and actor profiles, zero-days exploits, botnets, TTPs, and IoCs.
- Data feeds in STIX/TAXII format and API access that integrate with SIEM and SOAR platforms for automated enrichment.
- Human-curated reports alongside monthly executive summaries and private APT briefing, enabling strategic threat forecasting and rapid informed action.

2. Resist & Expose

ESET's protection architecture focuses on preventing breaches and amplifying detection efficacy:

- ESET Endpoint Security uses multi-layered defense to stop diverse threats like ransomware, fileless attacks, and APTs, combining real-time behavioral analysis, cloud intelligence, threat hunting, and mobile security within an ESET PROTECT console.
- ESET Inspect, an XDR-enabling component of the ESET PROTECT Platform, combines endpoint EDR capabilities and extended telemetry to highlight anomalies, automate incident creation, enable granular detection rule tuning, and feed incidents into downstream investigation and response workflows.
- As of March 2026, ESET is extending its protection architecture beyond endpoints with the launch of Cloud Workload Protection (CWP). This enables customers to secure cloud workloads and perimeter configurations while generating cloud-native telemetry that strengthens both detection and exposure management across hybrid environments.
- Policy controls and tight configurations are enforced via ESET PROTECT Platform, including management agent settings, firewall and network access policies, and visibility controls that are all configurable through centralized policy templates.
- Full Disk Encryption (FDE), delivered through ESET Full Disk Encryption and centrally managed via the ESET PROTECT Platform, reduces the impact of endpoint loss or theft by protecting data at rest and supporting breach containment and regulatory defensibility.

3. React & Restore

ESET integrates incident response orchestration, investigative telemetry, and recovery-enabling controls:

- ESET Inspect plays a direct role in response by generating high-fidelity incidents, correlating endpoint telemetry, and supporting investigation workflows that inform containment and remediation actions across the ESET PROTECT Platform.
- API-backed integrations allow ESET PROTECT to automatically feed detections and incidents into SIEM/SOAR solutions (e.g., Microsoft Sentinel, BlockAPT) through automated connectors, enabling orchestration, containment, and response playbooks.
- ESET's Incident Management API supports incident detection, grouping, rule and exclusion management, status updates, and analyst commentary, enabling structured response workflows within external orchestration and case-management tools.
- For recovery scenarios, the Ransomware Remediation feature in the ESET PROTECT Platform can automatically create secure backups of files during suspicious activity and restore them if ransomware is detected, helping organizations recover affected data and reduce downtime after containment.

4. Go On

Operational visibility, metrics delivery, and learning feedback loops are crucial:

- ESET PROTECT provides a comprehensive reporting system through which you can generate pre-built or custom reports (PDF/CSV) and schedule automated delivery to stakeholders, including LiveGrid® and MDR-specific outputs.
- Integrations support board-level dashboards by automating delivery of threat metrics into SIEMs and business reporting tools; the LiveGuard module integrates reporting templates to track suspicious file activity.
- MDR as a service provides customers with structured response and outcome reporting through ESET PROTECT reports, tailored to executive and operational audiences.

The message is quite straightforward: ignore overly complex stacks. ESET can handle the technology side cleanly, so you can focus on processes and people, and keep the business moving.

Roadmap

This roadmap illustrates a representative journey, not a universal prescription. The actual path, and the pace at which organizations move through it, depends on their current maturity, business priorities, regulatory exposure, budget constraints, and decisions around outsourcing versus in-house ownership.

SHORT TERM
0-90 DAYS

1. **STRENGTHEN IDENTITY CONTROLS**

   Enforce phishing-resistant MFA that reduces takeover risk, review privileged and machine accounts and rotate exposed credentials.

2. **PROVE BACKUP & RECOVERY READINESS**

   Run a ransomware restore exercise and verify backup immutability and recovery times to ensure resilience.

3. **AUDIT EXTERNAL EXPOSURE**

   Gartner emphasizes that exposure management is foundational because it "prioritizes threats most material to your business." To put this into practice, inventory all internet-facing assets, SaaS identities, and third-party integrations, and remediate high-risk misconfigurations.

MEDIUM TERM
3-9 MONTHS

4. **OPERATIONALIZE ZERO TRUST**

   Zero Trust is a security concept and it requires a holistic approach. Start by micro-segmenting crown-jewel systems, enforcing continuous device posture checks, and applying session-level access controls.

5. **SECURE THE SOFTWARE SUPPLY CHAIN**

   Require Software Bill of Materials (SBOMs) from vendors, scan open source and commercial binaries, and monitor leaked developer secrets. SBOM and software integrity are key to supply chain resilience.

6. **STRENGTHEN CLOUD SECURITY POSTURE**

   Implement CSPM and CNAPP to continuously monitor cloud configurations, enforce compliance, and integrate findings into detection workflows. This reduces risk in multi-cloud and SaaS environments.

LONG TERM
9-18 MONTHS

7. **ESTABLISH AI GOVERNANCE**

   Mature AI governance delivers measurable ROI and reduces risk. To achieve this, start by formalizing policies, discovering and controlling shadow AI usage, and tracking efficiency gains alongside risk reduction.

8. **RUN RESILIENCE DRILLS AT SCALE**

   Conduct cross-functional exercises simulating ransomware, supplier failures, and AI-driven attack scenarios. Remember that such resilience drills improve organizational readiness.

9. **CONSOLIDATE SECURITY TOOLS**

   Reduce overlapping agents and consoles; invest in unified platforms for identity, endpoint, and analytics. As discussed earlier, platform consolidation simplifies operations and improves response.

Conclusion

Cyber resilience in 2026 is about continuity under pressure, not perfect security. It means anticipating threats, resisting compromise, responding fast, and restoring operations without disruption. Organizations face AI-driven attacks, hybrid complexity, and strict regulations, requiring a lifecycle approach across technology, processes, and people.

Practical steps include hardening identities, validating recovery, managing exposure, operationalizing Zero Trust, securing supply chains, governing AI, and consolidating tools.

If you want to cut through complexity, ESET can be your trusted technology partner which is ready to deploy, simple to run, and built to handle the heavy lifting so you can focus on people, processes, and business continuity.

EXPLORE ESET BUSINESS SOLUTIONS

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

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

eset
Cybersecurity
Progress. Protected.

© 1992–2026 ESET, spol. s r.o. – All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.