Softtek®

Cybersecurity Reinvented:

When AI Plays Both Sides

Trust is proven under pressure

An organization can detect a threat accurately and still suffer its consequences while deciding how to respond. Between the alert and the action lie approvals, tools that do not share context, and teams that need to piece together what has happened. Artificial intelligence is shrinking the time available to work through that sequence. Under these conditions, even technically advanced defenses can be slow to act, and that gap matters far more than the number of solutions deployed.

AI is changing the balance between attack and defense by reducing the effort required to research a target, personalize a scam, or adapt a malicious operation. As those tasks become less costly, adversaries can multiply their attempts and sustain pressure more persistently. Their advantage comes as much from sophistication as from the ability to experiment and try again without the constraints that legitimate organizations face. For businesses, this raises the cost of every delay and calls into question a security model built on successive manual interventions.

It would be a mistake to conclude that the answer is to remove controls in order to compete on speed. A company must protect information, honor its commitments, and prevent defensive decisions from unnecessarily disrupting the business. That responsibility requires deciding in advance how control will be exercised. Requiring human approval for every decision may seem prudent, but it also means accepting that a threat can advance while someone gathers the information needed to intervene.

At Softtek, we believe the opportunity for AI lies in transforming how security operates. Its ability to connect signals, add context, and prioritize threats must be matched by an organization capable of taking action. An assistant that speeds up analysis loses much of its value if the response remains held back by the same dependencies. Investment should shorten the entire path from understanding a risk to containing it, with clearly defined responsibilities and criteria shared across security and the business.

This is where defensive automation and the gradual introduction of agentic capabilities have a clear role to play. Working within established policies and thresholds, systems can coordinate actions such as blocking access or isolating compromised resources without waiting for each step to be performed manually. The aim should be to embed specialists' expertise in the way defenses operate, even when the pressure exceeds their capacity to address every alert. The quality of that coordination will matter more than the level of autonomy a tool claims to offer.

This evolution requires particular attention to the role of people. Automating repetitive tasks frees experienced professionals to investigate behavior that is difficult to interpret, review decisions, and improve responses. It would be a waste to use AI to generate more information for the same overstretched teams to review. Its contribution should be evident in a lighter workload and more time for work that calls for judgment, business knowledge, and professional accountability.

Yet AI is also expanding what we need to protect. Models, the data they use, and the agents involved in business processes introduce new dependencies. Each addition must come with a clear understanding of the information it can access and the actions it can perform. A company can strengthen its defenses with AI while simultaneously increasing its exposure through poorly coordinated adoption elsewhere in the business. Both decisions belong in the same strategic conversation.

In our view, this is one of the most important implications of agentic AI: delegating work requires clarity about the authority being delegated. An agent needs permissions appropriate to its role, and the organization must be able to assess its activity as the context changes. Zero trust has a concrete application here, extending verification and the principle of least privilege to non-human identities. The legitimacy of an initial access request offers little assurance if it subsequently allows an agent to operate with excessive privileges.

Autonomy therefore warrants scrutiny that goes beyond a system's ability to execute. Before authorizing an automated response, it is important to understand its implications for the affected services and the conditions under which it should be stopped. Isolating a system may contain an attack, but it can also disrupt an essential operation. Designing an intelligent defense requires considering both effects and retaining the ability to intervene. Speed adds value when it is grounded in a sound understanding of the risk and the business it is intended to protect.

This responsibility must be shared from the design stage of AI initiatives. If business teams decide where to automate, technology teams decide how, and security is then asked to protect the result, a coherent approach will be difficult to achieve. The CIO and CISO need to participate in the decisions that determine exposure, alongside those accountable for the affected processes. Working together allows the boundaries of automation to be defined around real consequences and prevents every disagreement from becoming an operational delay.

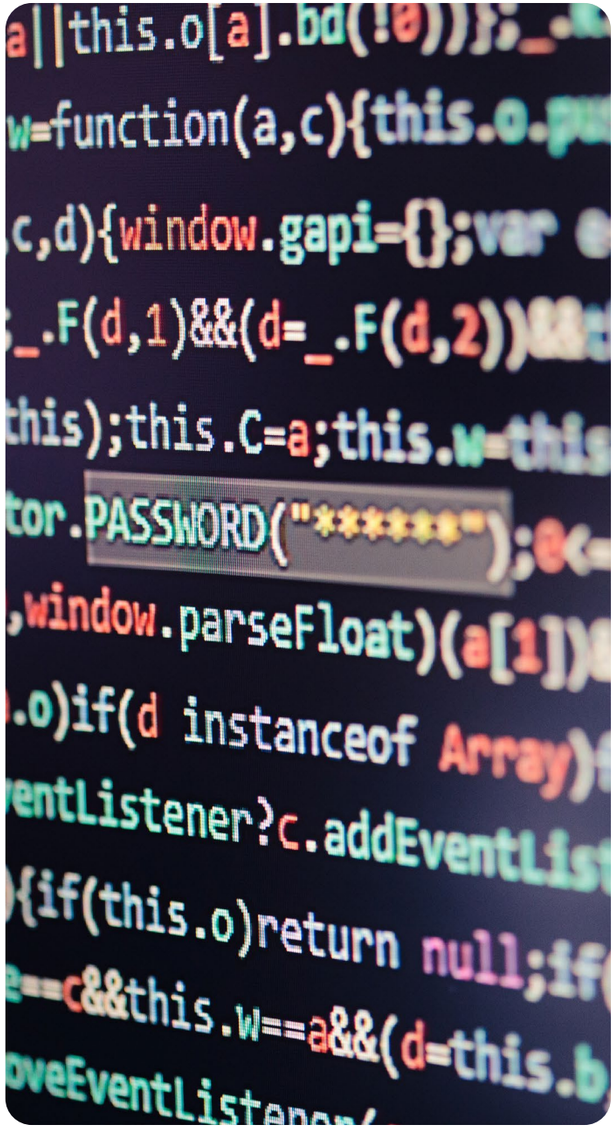
Technological ambition must also allow for the possibility that defenses will be breached. The more connected and automated an operation becomes, the more important it is to understand its dependencies and prepare for an orderly recovery. Resilience means deciding which services must remain available, how to contain the spread of damage, and which operations to restore first. These decisions need to be rehearsed before a crisis; advanced detection capabilities do not remove the need to verify that the business can continue operating under pressure.

This is why we believe the success of AI in cybersecurity should be judged by its effect on business operations. How quickly a threat is contained, how far compromised access can reach, and how an essential service is restored are useful measures for deciding where to invest. They also help distinguish genuine improvement from a convincing technology demonstration. Leadership needs to understand where exposure has been reduced and which risks remain, supported by evidence that allows priorities to be adjusted.

The transformation will need to proceed gradually, addressing the disconnects that prevent organizations from making full use of the intelligence already available. Where context, integration, or clear accountability is lacking, adding autonomy can amplify existing weaknesses. It makes sense to begin with well-defined decisions, test how the system behaves, and expand its scope as evidence shows that it responds as expected. That discipline allows organizations to gain speed on a foundation they understand and can govern.

At Softtek, we see cybersecurity as a prerequisite for an ambitious approach to AI. A company that understands the limits of its systems, can intervene in their decisions, and has tested its ability to recover has a stronger foundation for innovation. That is where the trust required to delegate processes is built: in the ability to take responsibility for their consequences.

AI offers businesses an extraordinary capacity to act. The task of leadership is to match it with an equally strong capacity to protect what is at stake. That will be the measure of progress: how far a company can advance with security capable of sustaining it, even when conditions are no longer favorable.

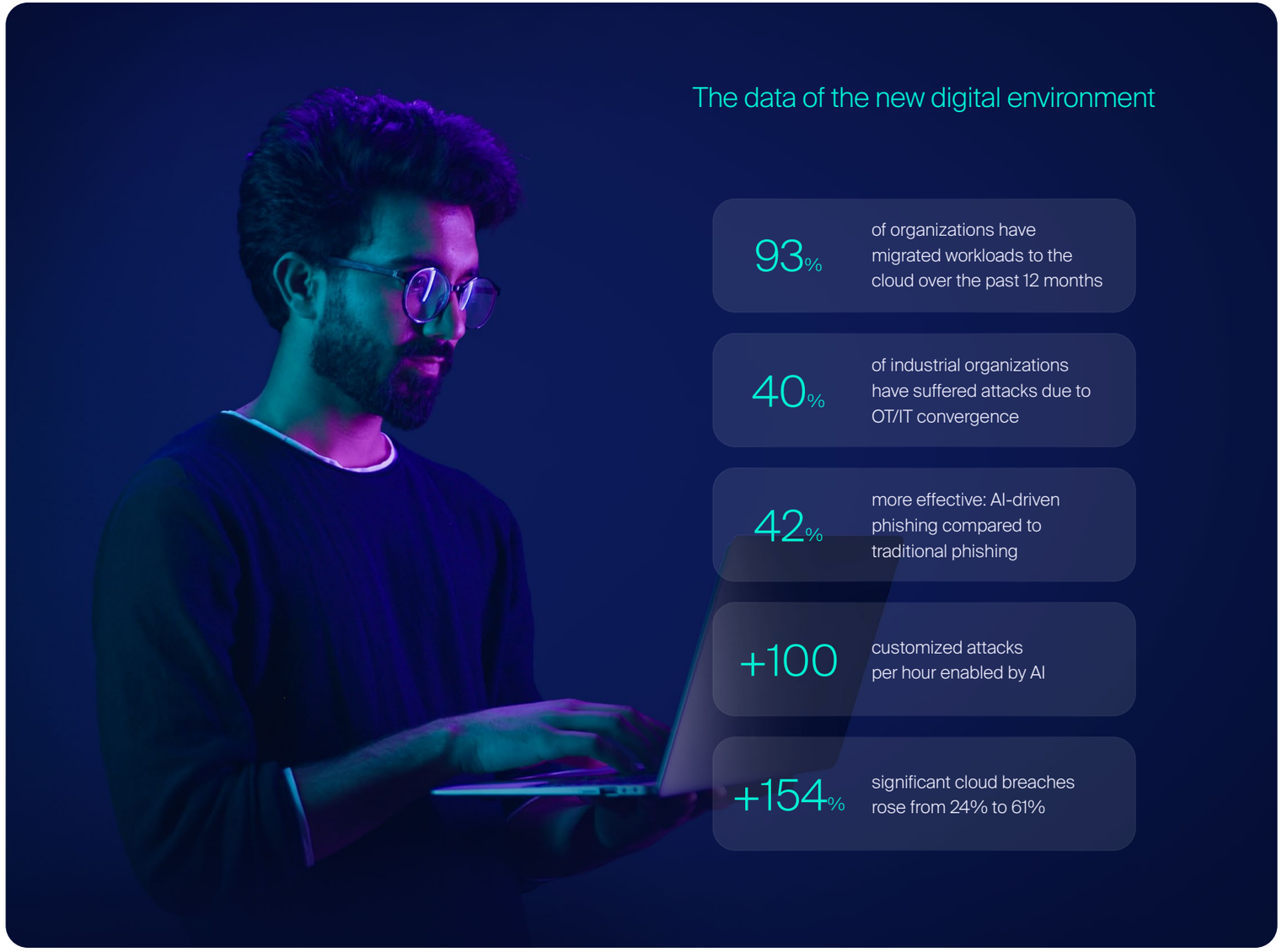


A new digital reality paves the way for a new approach to cybersecurity

Why have the foundations of cybersecurity changed

For years, cybersecurity has been built on a set of assumptions that, at the time, allowed for the protection of systems, containment of incidents, and reasonably effective risk management. Back then, the digital environment was more limited, attacks were more sporadic, and time worked in the defender's favor. However, **in just a few years, that balance has been irreversibly broken**.

The acceleration of the digital environment driven by the mass **adoption of cloud, the hyperconnectivity of business ecosystems and, in a particularly disruptive way, by artificial intelligence**, has transformed the nature of risk. We are no longer facing an incremental evolution of the threat landscape, but rather a qualitatively different reality where many of the assumptions underlying traditional cybersecurity models are no longer valid.



Sources: Cisco | World Economic Forum | Blackberry

One of the most profound changes is the transformation of the attack itself

Artificial intelligence, particularly generative AI, not only expands the attack surface but also removes friction that previously limited the adversary's scale, speed, and persistence. The result is an environment of perpetual exposure, where risk shifts from being an isolated event to becoming embedded in normal business operations.

This is how the inflection point emerges, **cybersecurity no longer protects against incidents but must operate in a context where attacks are continuous, automated, and adaptive**. This change is clearly reflected in the domains organizations identify as most challenging to protect: identity, network, cloud and devices. These aren't new domains, but rather the core of today's digital ecosystem, where users, data, distributed infrastructures, and increasingly, artificial intelligence capabilities converge.

In these domains, the **attack surface and operational complexity grow simultaneously**, rendering approaches based on static controls, traditional segmentation, or implicit trust insufficient.

Areas companies consider most difficult to protect against new cyberattacks

- 31% NETWORK
- 29% IDENTITY
- 16% CLOUD
- 15% DEVICES
- 10% AI WORKLOADS

Sources: Cisco | World Economic Forum | Blackberry

Systemic complexity amplifies risks across the entire digital ecosystem

Compounding this structural pressure is **the convergence of factors that amplify the complexity of the environment**: rising geopolitical tensions, increasingly interdependent and opaque digital supply chains, and accelerated adoption of emerging technologies that introduce new dependencies and vulnerabilities.

Risk is no longer confined to the boundaries of the organization but **spreads across distributed ecosystems**, where an external failure can have a direct impact on business continuity.

Factors compounding the complexity of modern cybersecurity

Geopolitical tensions

The normalization of cyber conflict introduces persistent and risk-tolerant attacks, overwhelming defensive models designed for isolated incidents

Sophistication of cybercrime

Cybercrime has become industrialized, operating with efficient, automated, and continuous models in the face of defenses that are still reactive and fragmented

Supply chain interdependencies

Dependence on third parties expands the perimeter beyond direct control, enabling the adversary to scale impacts through a single weak point

The new reality

Digital skills gap

The shortage of talent turns dependence on human processes into a structural disadvantage against automated adversaries that operate without fatigue, at scale, and continuously

AI and emerging tech

AI accelerates attacks faster than organizations integrate it into defense, disrupting the balance between detection, decision-making, and response

Regulatory requirements

Compliance increases the operational burden but does not guarantee real control, creating a gap between documented security and effective capability that the adversary exploits

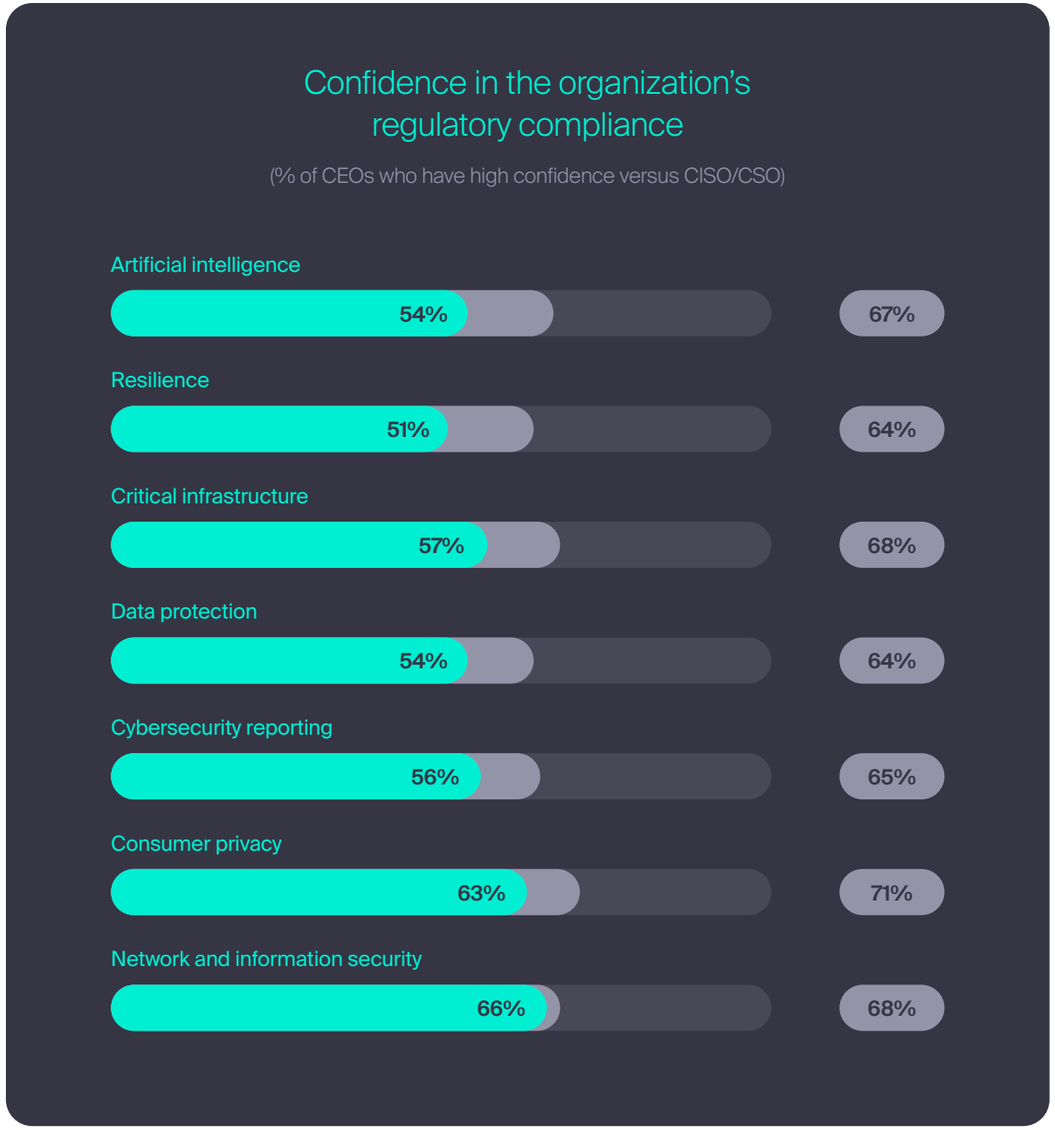
Regulatory pressure exposes the limits of traditional cybersecurity execution models

Regulation has become one of the main catalysts of the new cybersecurity paradigm, forcing organizations to integrate security, resilience, and accountability into corporate governance and decision-making mechanisms. **The new regulatory frameworks not only require technical controls**, but real capability to operate under risk, business continuity, third-party management, and executive accountability.

In this regard, regulation is pushing organizations in the right direction: increasing discipline, reducing systemic risk, and strengthening trust. Data confirms that **a large majority of organizations recognize that regulation effectively contributes to reducing cyber risk**. However, this same momentum has revealed a structural tension that connects directly with the central message of the report.

Compliance is advancing faster than real execution capability. The proliferation of regulations, their fragmentation across jurisdictions, and the growing complexity of requirements are exceeding the capacity of many organizations to absorb them and translate them into effective risk control.

Nearly seven out of ten organizations acknowledge difficulties in implementing existing regulations, not due to lack of awareness or investment, but because of the operational complexity they introduce: volume of requirements, dependence on third parties, verification across the supply chain, and lack of internal capabilities. Added to this is a perception gap within organizations themselves, where security teams are systematically less optimistic than the rest of leadership regarding the real level of compliance, especially in critical areas such as artificial intelligence, resilience, and critical infrastructure.



Sources: Ercom | Cisco | World Economic Forum

This misalignment is symptomatic of a deeper issue

Traditional cybersecurity models were not designed to operate under continuous regulatory pressure, interdependent risk, and highly dynamic environments. Compliance assesses the existence of controls; the adversary exploits their operational inefficiency. When security is managed as a compliance exercise, the organization may comply and still remain exposed.

In this way, regulation ceases to be a risk reduction mechanism and becomes an amplifier of complexity. Not because it is poorly designed, but because it exposes the limitations of a model that no longer scales. **The difficulty is not complying with more regulations, but doing so with a security model capable of absorbing that demand without fragmenting**.

69%

of respondents consider that **regulations are too complex or too numerous**, or that it is difficult to verify whether external providers comply with them

Sources: Ercom | Cisco | World Economic Forum

Cyber exposure and regulatory demands are outpacing organizations' operational preparedness

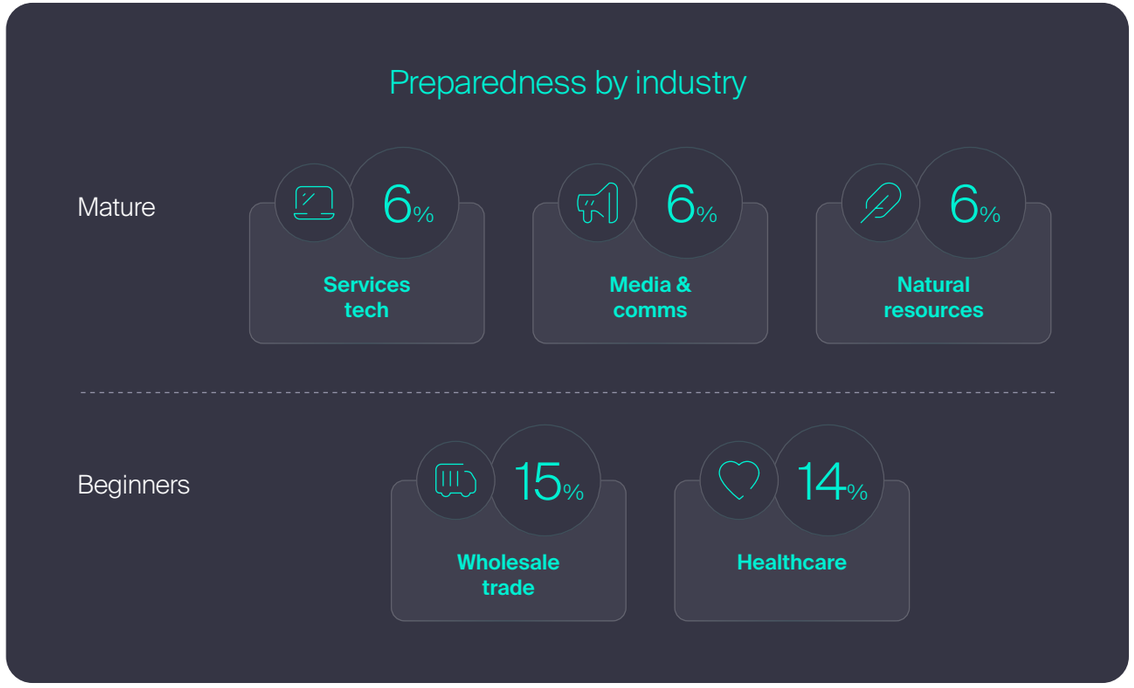
While a significant proportion of companies identify the lack of capabilities as one of the main barriers to resilience, only a minority are confident they currently have the necessary talent to meet their cybersecurity goals. This gap makes **the reliance on human intervention creates a critical bottleneck precisely when the environment demands operating at greater speed and scale**.

The combined effect is an increasingly visible gap between exposure, demands, and preparedness. **Even organizations with high investment levels and perceived maturity face growing difficulties in defending themselves effectively**, especially in regulated sectors and regions where regulatory pressure and operational complexity intensify.

Regulation, as observed, acts as an amplifier of a preexisting structural weakness, making it clear that the traditional cybersecurity model doesn't scale when exposure grows, **obligations increase, and human capacity remains limited**.

This mismatch reinforces that **the gap between actual exposure and preparedness cannot be closed solely with more people, more controls, or more compliance**. In an environment where risk is continuous, interdependent, and accelerated by AI, the ability to operate and defend systems can no longer depend on a human resource-intensive model.

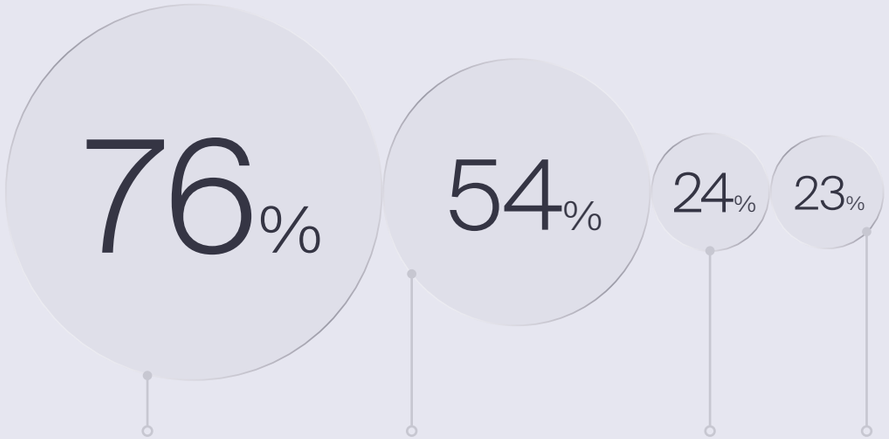
Regulatory pressure and growing exposure only confirm that **a model change is needed—one capable of absorbing complexity without fully transferring it to operations**.



Sources: Cisco | World Economic Forum

More talent does not equal more resilience: **the gap between human effort and systemic preparedness**

How organizations are responding



Internal upskilling
They train and reskill their current employees

Hiring
They hire cybersecurity professionals with experience

Self-training
They expect the development of autonomous skills

Apprenticeships
They promote apprenticeship or dual training programs

Non-traditional profiles
They recruit profiles outside traditional degrees

Where it truly translates to preparedness

As organizations ramp up upskilling and hiring to compensate for skill shortages, **confidence in resilience during critical incidents remains markedly uneven** across countries and regions.

Economies with greater institutional maturity and systemic capacity absorb this effort more effectively, while less-prepared ones remain trapped in a people-intensive model that doesn't scale.

Sources: Cisco | World Economic Forum

AI opens a new era of threat anticipation and stronger defense capabilities

What changes in cybersecurity when businesses and attackers use AI

The reality is that the rapid development of artificial intelligence is redefining multiple domains, and cybersecurity is no exception. When properly implemented, AI can enhance defensive capabilities, support human teams, and improve threat detection, response, and risk management. However, that is not the primary challenge organizations face today.

The real turning point is that **AI introduces systemic risks** when deployed haphazardly, inadequately governed, or used offensively by malicious actors.

Indeed, it has become—according to a broad majority of leaders—the primary driver of change in cybersecurity in the short term. Not because it replaces existing technologies, but because it **simultaneously alters three key dimensions of the security ecosystem**, creating a new asymmetry between offense and defense.

First, the **widespread adoption of AI systems** in enterprise environments **introduces an expanded attack surface**. Models, data, autonomous agents, and automated workflows become part of the business core, creating new dependencies and vulnerabilities that traditional controls weren't designed to manage.

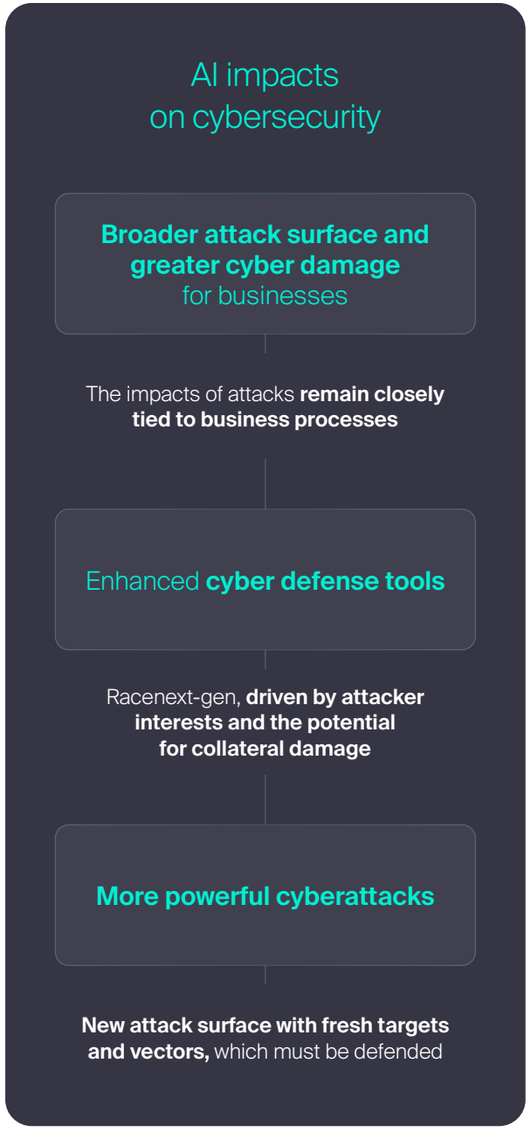
Secondly, **defenders are beginning to use AI to strengthen their capabilities**. Automating analytical tasks, enhancing detection, and accelerating response alleviates pressure on overburdened human teams and enables operations at otherwise unmanageable data scales.

The greatest impact, however, is occurring **on the adversary's side**. Threat actors are leveraging AI **as a multiplier of scale, speed, and sophistication, automating recognition, exploitation, and targeted social engineering**. The attack shifts from being sequential to an industrialized process, capable of real-time adaptation and continuous operation.

AI **reduces the marginal cost of attacks, increases their precision, and removes many of the technical barriers** that previously limited their reach.

These three dynamics illustrate the dual nature of AI in cybersecurity. But far from balancing out, their combination is **shifting the conflict toward an AI-driven arms race**, where the advantage tends to concentrate on those operating with higher automation and less dependence on human intervention.

Without robust governance and disciplined integration, AI doesn't reduce risk, it redistributes it and, in many cases, amplifies it. Acknowledging this reality is essential to understanding why organizations today start from a position of misalignment with the new cyber reality.



The adaptation race: organizations are falling behind

This misaligned acceleration isn't theoretical: it's reflected in how AI is governed, operated, and scaled on each side. While adversaries integrate it as a frictionless central engine with full automation at machine speed, many organizations adopt it in fragmented ways, dependent on human cycles. The result is a **set of structural asymmetries in AI usage** that put defense at a disadvantage.

The following four asymmetries explain **why today's AI-driven acceleration favors the adversary**:

AI usage asymmetries

	Defenders	Adversaries	Consequence
AI governance	Organizations adopt AI in a **distributed, partially governed manner with inconsistent controls** across business, IT, and security	Adversaries leverage AI **without restrictions, through continuous experimentation and with no operational friction** throughout the entire attack lifecycle	The exposure surface is growing faster than the real capacity for control and oversight
AI usage model	AI is used to **support analysis, keeping humans as the central point of decision-making** and validation	**AI automates end-to-end reconnaissance,** exploitation, and attack adaptation	**Human cycles fall outside the response window** against automated and persistent attacks
Adaptation speed	Detection, decision-making, and response **rely on sequential processes and manual validations**	The adversary **learns and adjusts its behavior in real time** during the attack itself	**The defense reacts too late** while the attack continuously evolves
Operational scalability	Defensive operations **scales with limited personnel, ongoing training, and constrained operational capacity**	The offensive operation scales **automatically, persistently, and without human fatigue**	The attack increases in volume and pressure until **overwhelming defensive capacity**

The next leap in cybersecurity is turning investment into effective protection

Exposure grows faster than organizations' ability to maintain control

Organizations now operate in an environment where the attack surface is structurally expanding, while defensive capabilities fail to evolve at the same pace. Companies clearly identify the threats that concern them most, yet the issue isn't a lack of awareness—it's a far more uncomfortable reality: **The threats that generate the greatest concern are consistently those for which organizations feel least prepared**.

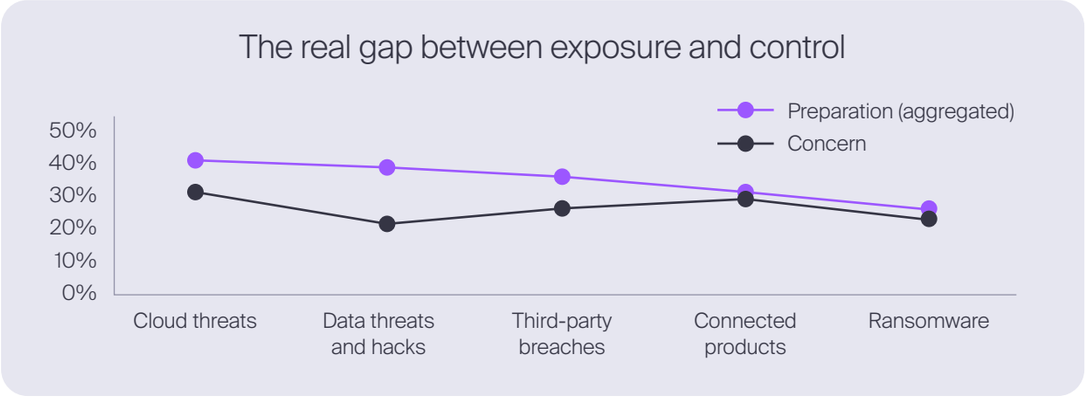
This mismatch highlights an underlying issue, **the preparedness is not aligned with the nature of the risk**. While exposure is distributed and interconnected, control remains fragmented across functions, technologies, and responsibilities. The result is a persistent sense of vulnerability, even in organizations that have invested significantly in security.

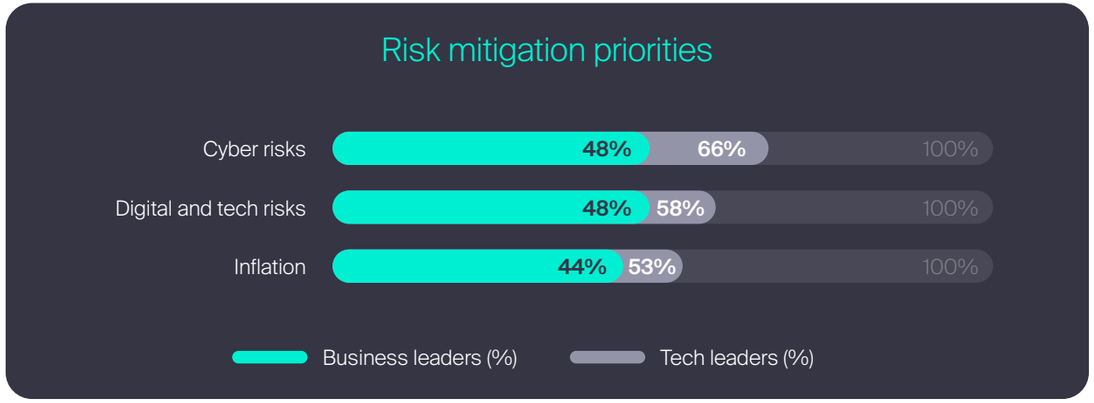
Compounding this gap is an **internal misalignment in priority perception**. Security leaders often identify threats like ransomware among the most critical risks of the organization, whereas this vision is not always shared by the rest of the executive committee.

This lack of cross-functional alignment **hinders the establishment of common priorities and reinforces the need for a shared language** between security and business.

There is also a **broad consensus on the importance of measuring cyber risk** to prioritize investments and allocate resources. However, this consensus rarely translates into effective practice. Only a minority of organizations quantify risk in a meaningful way, and when they do, they typically rely on partial assessments focused on individual controls, which provide a limited view of residual risk.

The barriers preventing this are determined by the **quality and availability of data, uncertainty about scope, legal concerns, and, especially, lack of confidence in the reliability of the results**. Added to this is the gap between what senior management needs in order to make decisions and what the security function is able to provide in terms of economic and operational impact.





Sources: Cisco | Huntress | Crowdstrike

The consequence is a fragile starting point

Despite growing concern, most organizations acknowledge difficulties in consistently implementing basic cyber resilience practices and, without cross-functional resilience, the business remains exposed to threats capable of compromising operations as a whole.

Organizations are not starting from a lack of awareness, but from a structural inability to transform that awareness into effective control, in an environment of continuous, interdependent risk amplified by AI.

Cyber risk quantification as an enabler

88% of executives recognize that it enables **prioritizing investments and communicating risk** in terms aligned with the business's risk tolerance, while 87% consider it key to allocating resources where the potential impact is greatest.

Quantifying risk **transforms cybersecurity into a strategic, demonstrable, and comparable capability**, anchoring decisions in consistent economic criteria rather than fragmented perceptions.

Sources: Cisco | Huntress | Crowdstrike

Surprisingly, higher investment is not translating into operational readiness

Given increasing exposure and growing risk awareness, one might expect sustained cybersecurity investment to yield equivalent improvements in actual protection capabilities. Yet in practice, this isn't happening. **Organizations invest more than ever in technology, services, and compliance, yet still struggle to operate effectively in a continuous-attack environment**.

The issue isn't lack of resources, but rather **the disconnect between investment and operational models**. Investment strengthens system components (tools, controls, or processes) but doesn't always build actual capabilities to detect, respond, and maintain business continuity under pressure. This gap consistently manifests across four key dimensions.

Although the **77% of organizations increased their cybersecurity budget in 2025**, most of the growth is concentrated in **tactical increases of 10% or less**. This pattern reveals defensive investment, designed to maintain the status quo rather than transform operational capability.

30% has increased its budget by 6-10%

8% has increased its budget by over 15%

Sources: Cisco | Huntress | Crowdstrike

Dimensions of disruption

1

Perceived readiness vs. Operational readiness

Organizations confuse preparedness with controls, audits, and frameworks. However, this perception does not translate into real improvements in detection, response, or resilience.

Effective preparedness is measured by the ability to operate under attack, not by compliance or the volume of controls.

2

Regulatory compliance vs. Real execution capability

Regulation has driven investment and raised the minimum level of security, but compliance does not equate to being prepared. Compliance assesses the existence of controls, not their effectiveness against real attacks.

This creates a false sense of security without improving operational capability.

3

The quantification of cyber risk as an unfulfilled promise

Few organizations succeed in translating their measurements into actionable economic impact. Quantification relies on partial metrics that fail to guide priorities or business decisions.

Without reliable risk measurement, there is no sustained action.

4

Capability gap: the limits of the human-dependent model

Investment remains focused on people and manual processes, a model that does not scale against AI-driven automated attacks. Defense depends on human cycles while the attack operates at machine speed.

Without automation and orchestration, investment increases complexity, not resilience.

The misalignment between real exposure and effective control capacity isn't the result of isolated decisions or individual shortcomings. It's the direct consequence of operating with a cybersecurity model designed for an environment that no longer exists. **Attempting to close this gap by increasing investment, adding controls, or reinforcing compliance only optimizes a structurally insufficient approach.**

Sources: Cisco | Huntress | Crowdstrike

A more secure organization starts with how it thinks, decides, and operates

Moving beyond reactive security through four foundational capabilities

The transformation required by today's cybersecurity is not, above all, technological. **Organizations are not failing because they lack solutions, but because they continue operating with a mindset conceived for an environment that is now obsolete**. The times when cybersecurity was considered something perimeter-based and focused on deploying controls, managing exceptions, and responding to incidents as isolated events no longer exist for corporations.

In this context, reinforcing controls or increasing investment without changing the way risk and operations are understood only optimizes a model that no longer scales. Cybersecurity ceases to be a technical function and **becomes an operational capability of the entire organization, impacting architecture, governance, operations, and business continuity**.

Therefore, **change cannot be partial or limited to a specific area; it must be global and comprehensive**, because risk is transversal and materializes wherever people, processes, technology, and third parties converge. Adopting new tools without transforming the corporate mindset creates a false sense of progress and reinforces the model's fragility.

To achieve this shift in mindset, **new concrete pathways are needed to materialize it within the organization**. Applying them consistently makes it possible to move from a reactive protection logic to a resilient operation under continuous attack.

Not adopting them implies accepting, implicitly, a progressive loss of control in the face of a reality that does not wait.

Pathways of transformation

1. **Zero trust and continuous identity**
   In a distributed environment, identity is the new perimeter, and **trusting once is equivalent to losing control throughout the entire access lifecycle**

2. **Defensive automation and machine-speed operations**
   Human cycles are no longer compatible with automated attacks, and **without automation, defense remains structurally outside the response window**

3. **Resilience by design and the capability to operate under disruption**
   Attack is not an exception, but a permanent condition, and **control is measured by the ability to absorb impact and continue operating**

4. **Cryptography and protection prepared for a post-quantum environment**
   Confidentiality and **long-term integrity cannot depend on cryptographic assumptions that are already in the process of being broken**

Zero trust and continuous identity, the basis of the new control model

The first essential transformation in reinvented cybersecurity is to definitively abandon implicit trust. The traditional model was built on the premise that it was possible to define a perimeter and that, once inside, users and systems could be considered trustworthy. This could work in closed and relatively stable environments, but it **breaks down irreversibly in cloud, hybrid, and remote ecosystems, where identities interact constantly and in a distributed manner**.

Most breaches today occur through the abuse of legitimate credentials. In fact, **in 2025, 1.8 billion credentials were stolen from 5.8 million devices**, consolidating the abuse of legitimate identities as the dominant vector. In an accelerated environment driven by artificial intelligence, where impersonation, advanced phishing, and automation drastically reduce barriers to entry.

Zero trust introduces a radical shift, where **it is assumed that a breach is possible as well as probable and that, therefore, every access must be verified continuously, contextually, and dynamically**. Identity is no longer validated at the time of login but is instead evaluated in real time, incorporating signals such as behavior, location, device status, or risk level.

This approach allows **permissions to be adjusted adaptively, limiting the impact of compromised credentials and significantly reducing account takeover**, even when the attacker has already bypassed initial controls.

89%

of breaches in 2025 **originate from credential theft**

Sources: Orange | Segurilatam | Ciber Safety | Avatier | Vectra

This pathway materializes in identity-first architectures

Humans, machines, and services are governed under principles of continuous verification and least privilege. It does not merely seek to strengthen access, but to regain control in environments where the perimeter has disappeared.

In SaaS, cloud, and BYOD ecosystems, identity is the only persistent point of control and everything else is transient. **Without a dynamic evaluation of access based on context and risk, the organization loses visibility and containment capability** at the very moment an attacker obtains valid credentials.

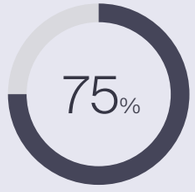
The criticality of this change is immediate. In a landscape where most attacks no longer attempt to break in but instead operate as legitimate users, continuing to treat identity as a point-in-time control leaves the organization structurally exposed.

The combination of stolen credentials, excessive privileges, and persistent access turns any initial compromise into a **systemic problem, difficult to detect and even more difficult to contain**.

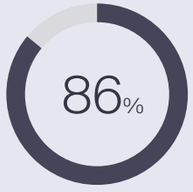
Not adopting this mindset allows the attacker to leverage the inherited trust of the previous model without the need to exploit complex technical vulnerabilities. Once inside, lateral movement, exfiltration, and impact escalation occur without friction and, in many cases, without generating significant alerts.

Zero trust with continuous identity is not, therefore, an incremental improvement or an advanced recommendation. **It is the minimum threshold from which cybersecurity becomes operable again in the new reality**. Without it, any other pillar rests on an unstable foundation, and control is lost not abruptly, but silently and progressively.

What impact is having this transformation practice

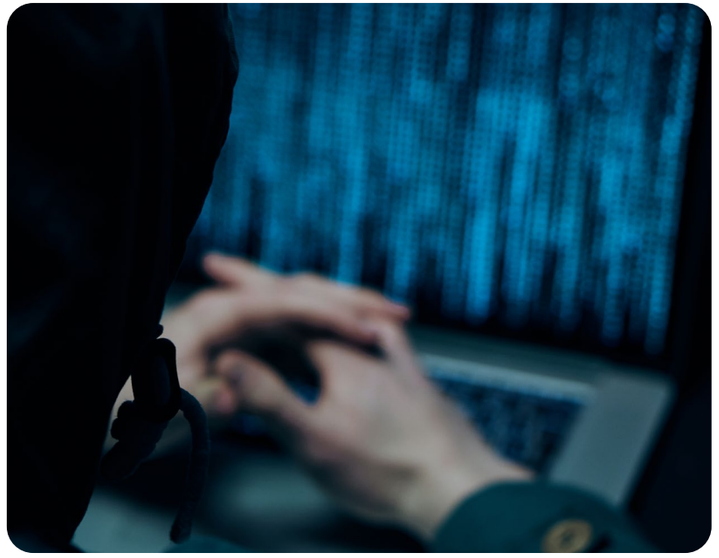


fewer account takeover incidents in organizations that implement continuous authentication compared to traditional models



of users **report a more positive authentication experience** after implementing continuous identity verification

up to a 40% reduction in support tickets related to access, significantly decreasing the time dedicated to reviews and lockouts

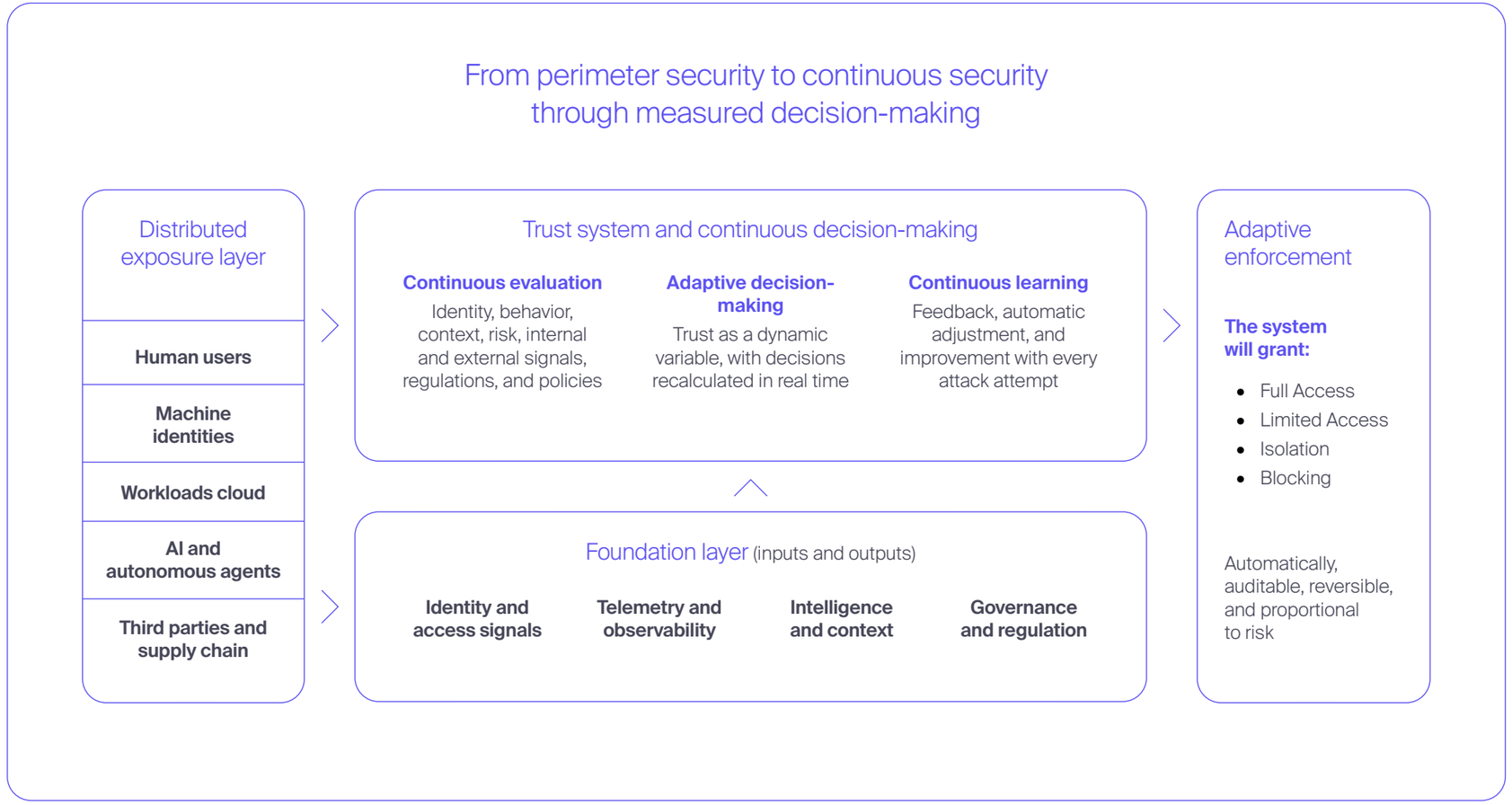


Sources: Orange | Segurilatam | Ciber Safety | Avatier | Vectra

1 Zero trust and continuous identity

For zero trust to be operable, it must translate into an architecture capable of evaluating, deciding, and applying access policies dynamically and in a distributed manner. Instead of concentrating security within a static perimeter, **control shifts to every interaction between users, systems, and resources, regardless of where they are located**. This requires clearly separating access decision-making, policy definition, and real-time enforcement, supported by multiple context, risk, and behavior signals.

This is achieved through the **Zero Trust architecture in which this approach materializes**, a model where no access is assumed to be trustworthy, all requests are continuously evaluated, and control is exercised where the interaction occurs, not where the network ends.



Defensive automation and machine-speed operation, control without human latency

Correctly defining who can access what is not enough if the organization cannot enforce that control at the required speed. The traditional cybersecurity model assumed that **human cycles — detection, analysis, decision and response — were compatible with the dynamics of the attack**, but that assumption has now been definitively broken.

Today, adversaries operate in an automated manner, supported by AI, completing attack cycles in minutes while human detection still occurs, on average, days later. **Time has therefore become another vector of risk**.

This new mindset requires accepting that people can no longer remain at the center of defensive execution. Their role must shift from reacting alert by alert to **designing, training and supervising systems capable of detecting and responding autonomously**. Seen this way, **defensive automation is not an operational optimization nor an incremental improvement of the Security Operations Center (SOC)**; it is the only way to keep pace with adversaries that already operate at machine speed.

This vision is embodied in **distributed and automated security models**, where detection, correlation and response are orchestrated in real time through platforms capable of processing millions of events per day without human intervention.

Automation enables isolating endpoints, blocking access, containing lateral movement or initiating recovery processes in seconds, drastically reducing the impact of an incident and minimizing human error, which is responsible for most breaches. At the same time, it frees security teams from operational fatigue, allowing them to focus on strategic analysis and continuous improvement.

The need for **distributed security** reinforces this shift in mindset. In hybrid, multi-cloud environments with IoT, OT and remote work, control must be applied where the interaction occurs.

Distributed agents, SASE architectures and enforcement at the edge make it possible to apply contextual policies at every access point, **limiting propagation even when the adversary has already obtained legitimate credentials**.

Without automation and machine-speed operations, the organization becomes permanently obsolete, as it will detect and respond late and will act when the impact can no longer be contained.

In an environment where **AI reduces the barriers to entry, accelerates phishing, enables impersonation and automates exploitation**, continuing to operate with manual defenses is equivalent to accepting a structural loss of control.

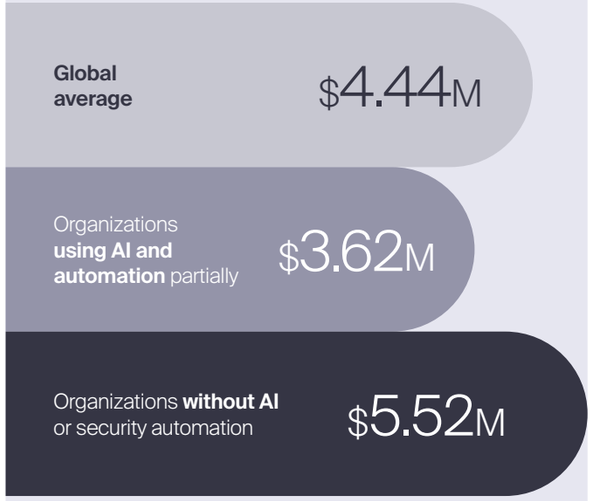
Defensive security automation is a basic condition for cybersecurity to become operational again in the new reality.

95%

human error still accounts for up **to 95% of breaches**

Impact of AI and automation on loss reduction

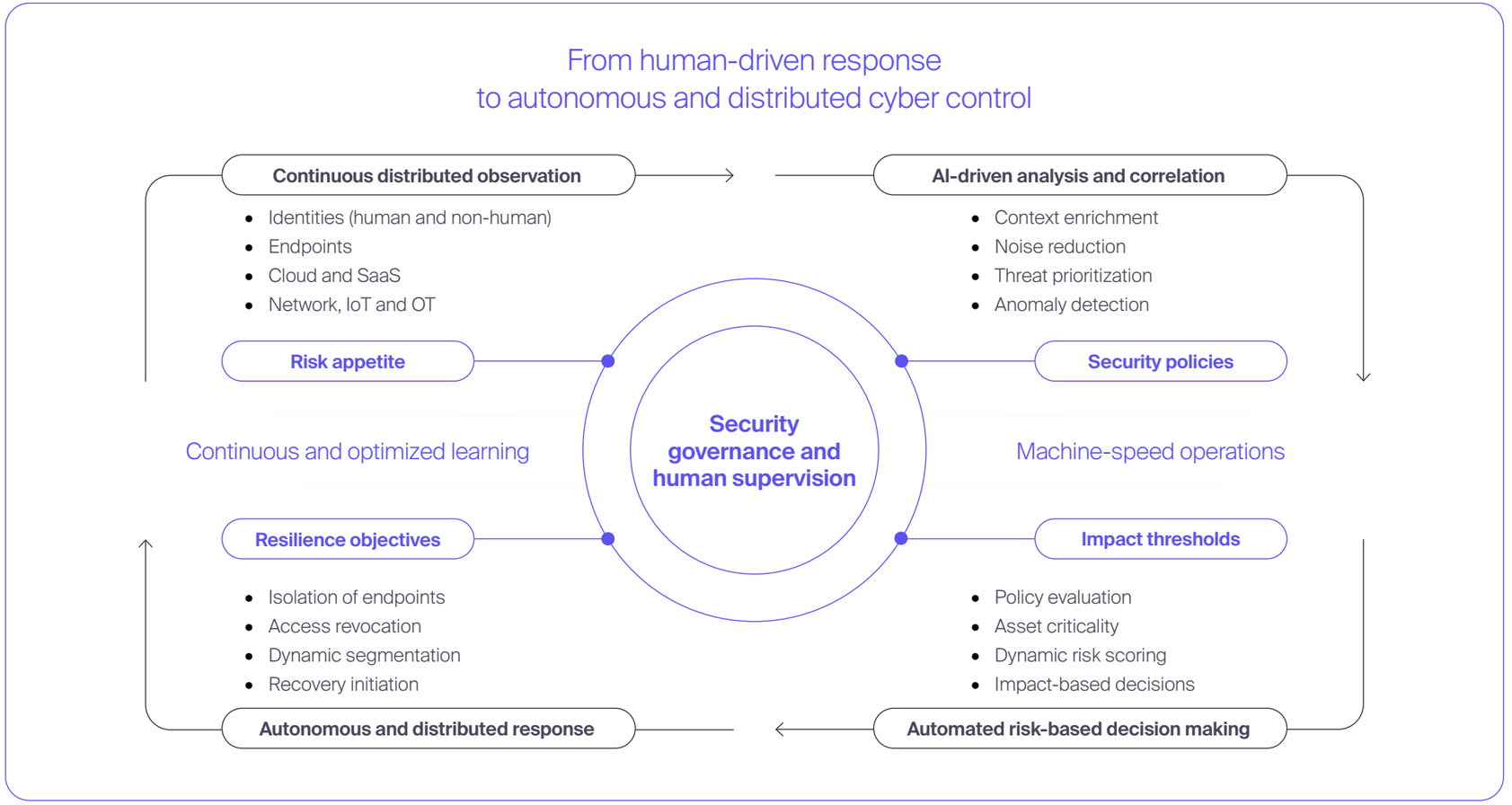
Effective adoption of AI and defensive automation **reduces response times by up to 80 days and materially decreases the economic impact of breaches (1.9 million dollars)**.



Sources: Fortinet | Orange | IBM | II

2 Defensive automation at machine speed

People define policies, risk thresholds and containment objectives, while automated platforms continuously execute detection, correlation and response. **Control stops being reactive and becomes permanent, distributed and orchestrated**, capable of acting in seconds wherever the threat occurs.



Resilience by design and the ability to operate under disruption

Even with continuous identity and defensive automation, assuming incidents can always be prevented is an illusion. The current model is fragile in an environment where most attacks no longer rely on technical flaws, but rather on the abuse of legitimate credentials and internal access that are difficult to distinguish from normal behavior. **In a reality accelerated by AI and cloud, a breach ceases to be an anomaly and becomes a plausible and recurring scenario**.

Resilience introduces a shift in mindset: **it must be accepted that compromise is the starting point and organizations must be designed to keep operating even when an attack occurs**, not only to try to prevent it. This means assuming partial failures, limiting impact from the origin and prioritizing critical services instead of applying a homogeneous protection logic. The objective is to integrate resilience from architecture design, processes and decision-making.

Operational resilience in cybersecurity has been translated into **architectures designed to absorb impact and recover in a controlled way**: microsegmentation that prevents lateral propagation, immutable backups that block extortion, automated failover mechanisms or orchestrated recovery that reduce downtime from days to hours.

Security stops being an added layer and becomes **an intrinsic attribute of the system**. In this model, **recovery capability is as important as detection capability**, and both are designed to operate under pressure.

The relevance of this approach is no longer only technical or strategic; it is increasingly regulatory and structural. **Frameworks such as DORA and NIS2 reflect a profound change in how cybersecurity is understood by regulators**. It is no longer enough to demonstrate preventive controls, policies or certifications; organizations must prove they can continue operating under disruption conditions. Resilience stops being assessed on paper and begins to be measured in practice.

These regulations introduce an explicit requirement for end-to-end operational resilience, covering anticipation, impact absorption, recovery and continuous adaptation. It is not only about having documented continuity plans, but about subjecting the organization to periodic testing, simulations of adverse scenarios and validation of real recovery capabilities.

Operating without resilience by design may already represent potential non-compliance, with direct implications in sanctions, reinforced supervision and accountability at the executive level.

Financial stability, service continuity and customer protection become explicit objectives of cybersecurity, directly aligning technological risk with business risk.

In non-resilient organizations, **every incident becomes a systemic crisis where prolonged interruptions, uncontrolled escalation of impact, significant economic losses and growing regulatory exposure converge**. The lack of capability to demonstrate effective recovery erodes the confidence of clients, partners and supervisors, amplifying the damage beyond the initial incident.

Conversely, **organizations designed to operate under disruption do not only limit technical impact**; they turn resilience into a competitive advantage. They recover faster, maintain service when others fail and reinforce their credibility with regulators and the market. In the new cyber reality, the difference is no longer between suffering incidents or not, but between being able to absorb them and continue operating — or seeing the viability of the business compromised.

Resilience enforced through sanctions

50%

of ransomware attacks in 2025 targeted **critical and essential sectors**

Essential

Fines of up to **10 million euros or 2% of global annual turnover**

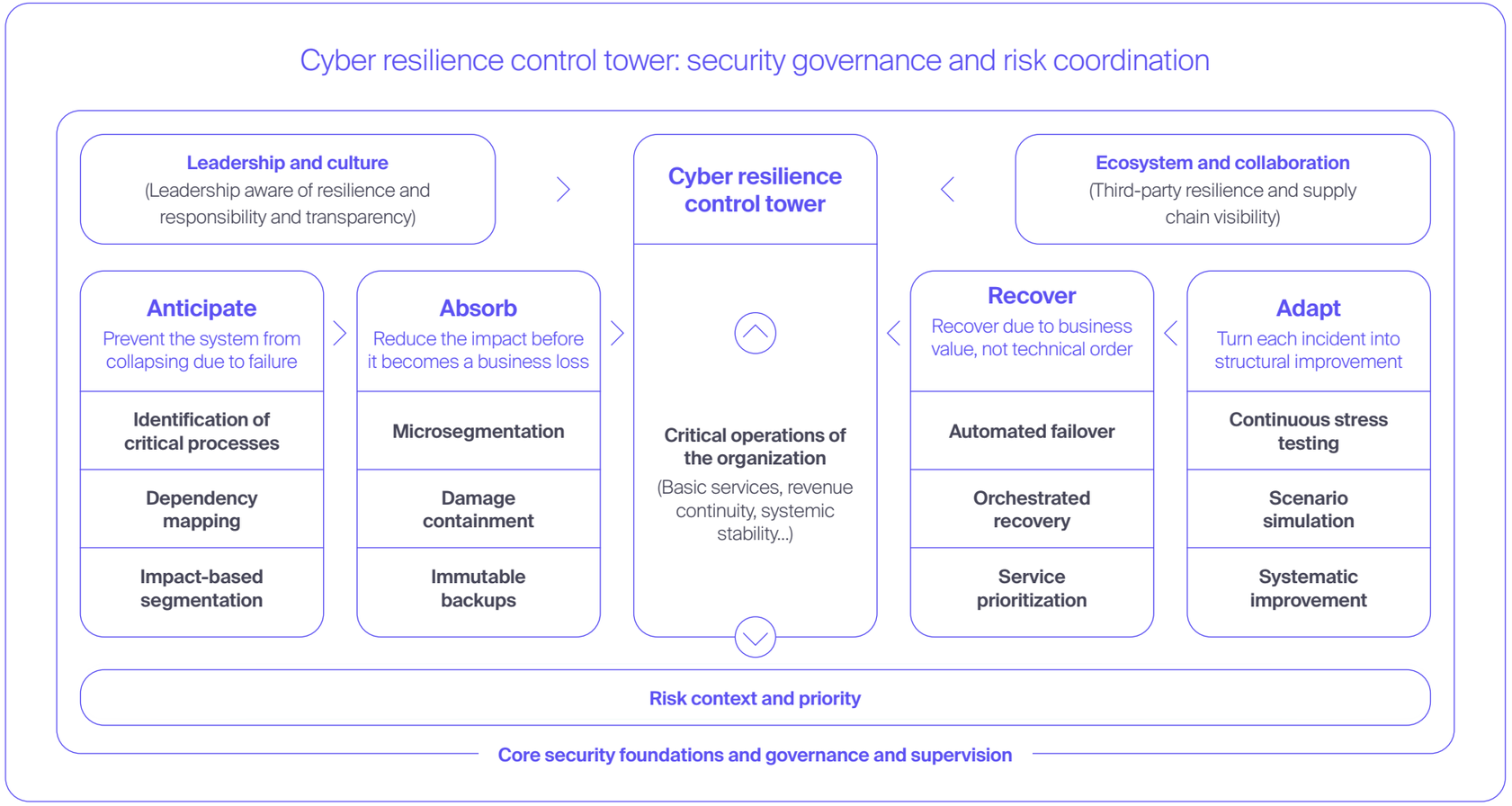
Important

Fines of up to **7 million euros or 1.4% of global annual turnover**

Sources: World Economic Forum | National Cyber Security Center | Google | AO Data Cloud | AENOR

3 Cyber resilience by design

Resilience must materialize both in operations (how the organization anticipates, absorbs, recovers and learns) and in the layers that enable it: leadership, governance, risk prioritization and ecosystem coordination. **This approach abandons fragmented visions and translates resilience into a coherent system, where the ability to operate at high speed is sustained by organizational decisions, governance frameworks and security foundations aligned with the business.**



Post-quantum cryptography and long-term protection: control that must stand the test of time

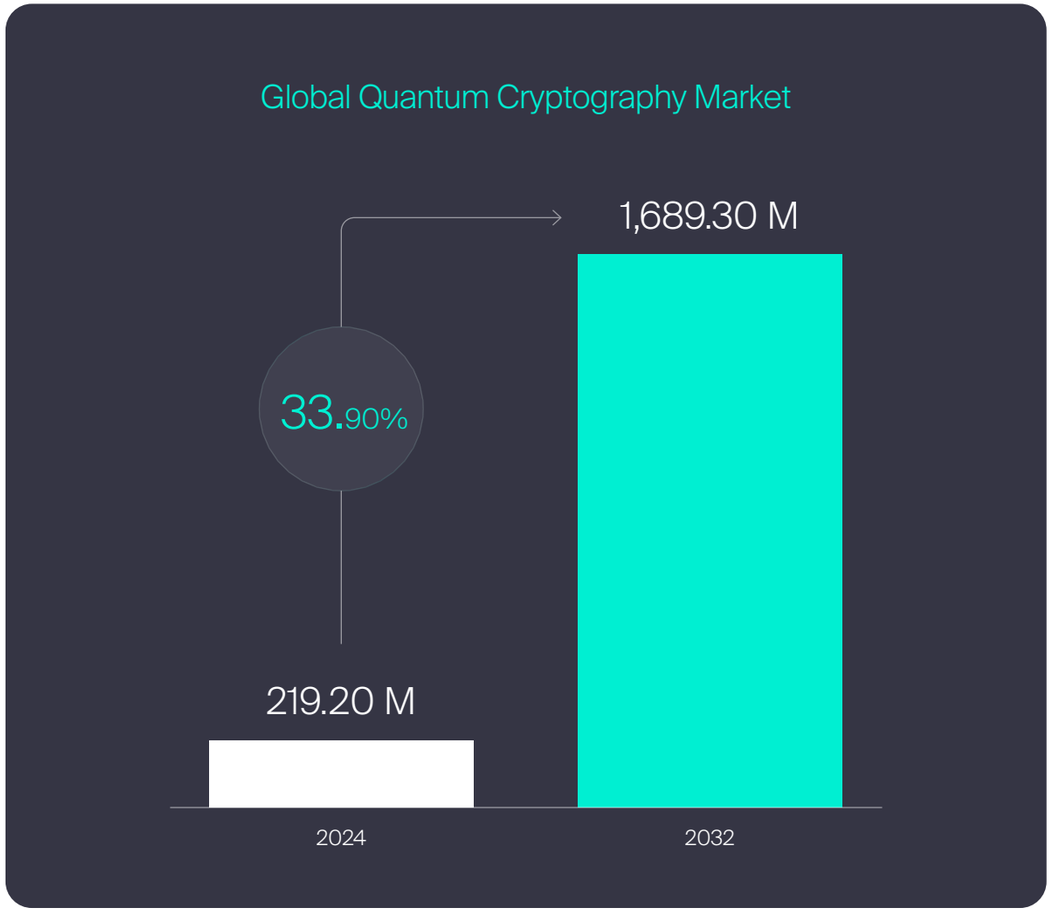
The fourth and final pillar introduces a dimension that the traditional cybersecurity model has tended to ignore: the durability of trust over time. For decades, cryptography has been the invisible foundation on which identities, communications, transactions and data protection are built. The inherited model assumed these foundations were stable and that protecting the present was sufficient.

The threat does not lie in a gradual failure of current algorithms, but in their abrupt obsolescence. Widely used algorithms such as RSA or ECC, currently considered secure, **could be efficiently broken by quantum algorithms**. The development of quantum computers with sufficient capabilities in the coming decade could turn this threat into a matter of when, not if. In such a scenario, keys that today would require millions of years of classical computation to break could be deciphered in hours or even minutes.

This shift challenges one of the deepest assumptions of the previous model: that encryption protects information throughout its entire life cycle. In reality, many critical assets (such as healthcare data, long-term contracts, intellectual property or root certificates) have lifespans measured in decades.

The strategy known as **harvest now, decrypt later** (collect now, decrypt later) allows advanced adversaries to collect and store large volumes of encrypted information with the objective of decrypting it once quantum capability permits. When that moment arrives, the **loss of trust would be retroactive and irreversible**.

Post-quantum cryptography introduces a new force: the need to anticipate the disruption before it becomes real. It is not about an immediate migration or a full replacement of algorithms, but about building **crypto-agility as a structural capability**. This implies knowing where and how cryptography is used, evaluating the exposure of assets over the long term and designing progressive transitions toward quantum-resistant algorithms while maintaining operational compatibility.



Sources: McKinsey | II | DMR | Fortinet | II | Data Bridge Market

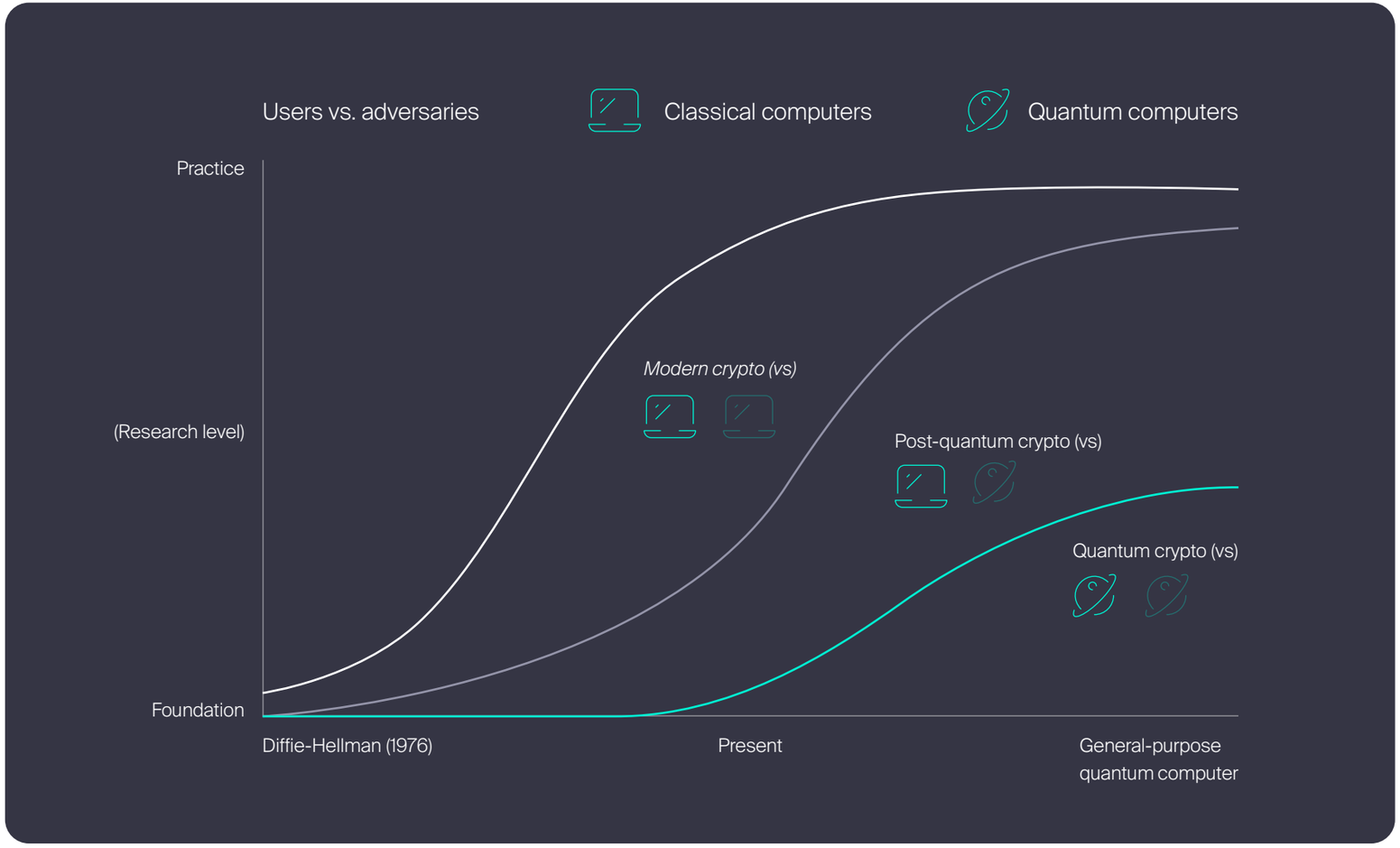
The signals supporting this trend are already tangible

In 2024, NIST finalized the first post-quantum cryptography standards (Kyber, Dilithium, Falcon and SPHINCS+), marking the formal start of the transition.

Certificates issued today, with life cycles of five or even ten years, may remain exposed if their migration is not planned now. At the same time, **major technology providers are already deploying hybrid schemes (classical + PQC)** in protocols such as TLS 1.3, anticipating a scenario where cryptographic agility will be a requirement for interoperability rather than an option.

Both in the United States and in Europe, **regulatory frameworks are beginning to explicitly require crypto-agility capabilities as part of digital resilience**. The progressive deprecation of classical algorithms, the obligation to audit cryptographic inventories and the protection of critical infrastructures are turning post-quantum preparation into an executive responsibility.

Not adopting this vision already carries a singular risk: **it does not manifest as an immediate incident, but as a deferred and systemic loss of trust**. When cryptographic assumptions collapse, **not only future security is compromised, but also the existing one**. Historical data, active contracts and regulatory evidence could become exposed simultaneously.



Sources: McKinsey | II | DMR | Fortinet | II | Data Bridge Market

4 Post-quantum protection

In the practical implementation of this strategy, it is not enough for information to be encrypted today — it must remain encrypted tomorrow. **The real problem lies in its ability to withstand a technological shift that is already underway**. When the lifespan of data exceeds that of the algorithm protecting it, security stops being binary and becomes temporal.

From traditional security to long-term protection

Traditional cryptography

Traditional cryptography protects information in the present, assuming that current algorithms will remain secure over time.

However, as the lifespan of data increases, this approach exposes organizations to **deferred risk**.

PQC

Post-quantum cryptography shifts the focus toward long-term confidentiality by incorporating **quantum-resistant algorithms and hybrid models**.

This enables anticipation of cryptographic disruption and protection of the value of information beyond the current technological horizon.

Enterprise execution

Effective adoption requires **visibility, prioritization and governance**.

Organizations must identify where cryptography resides, prioritize long-lifecycle data protection and progressively integrate hybrid capabilities across different areas.

Future anticipation

When integrated by design, security becomes a durable capability.

The organization preserves confidentiality throughout technological cycles, aligns with future regulations and ensures that digital trust survives quantum disruption.

Only **security designed to survive technological change**, capable of adapting, evolving and anticipating disruption, can sustainably preserve the trust of customers, regulators and digital ecosystems.

The future of cybersecurity is measured by the ability to keep business moving forward

From vision to execution: how organizations will operate

The four pillars define the minimum conditions for cybersecurity to become operational again in a reality of continuous attack, technological acceleration and increasing regulatory pressure. **Together, they address the structural limits of the previous model and establish a new mental framework: control is based on continuous identity, automation, operational resilience and long-term protection**.

However, recognizing the need for this new model is not equivalent to having adopted it. The main challenge for most organizations is execution. **The gap between understanding what must change and being able to implement it coherently remains wide**. Isolated initiatives, partial adoptions or purely technological approaches only delay transformation, reinforcing the false sense of progress that characterized the previous model.

The next step is to **put these pillars into practice and integrate them into day-to-day work**, deciding where to start based on each organization's risks, readiness, and circumstances.

How to build the new model without breaking operations

Restore basic control

- Continuous identity and operational Zero Trust
- Elimination of implicit trust
- Minimum control of access, privileges and exposure

Design for disruption

- Real continuity capability
- Segmentation, recovery, testing
- Alignment with DORA / NIS2

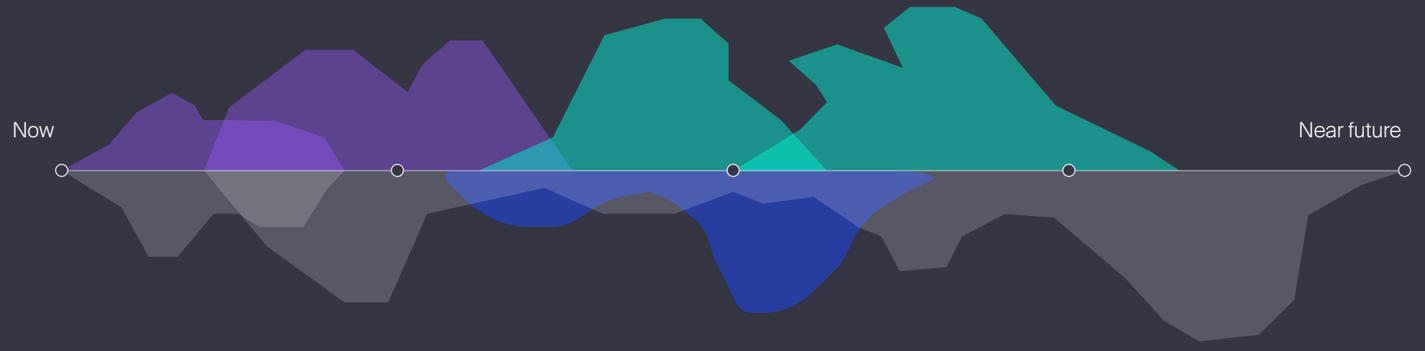
Close the time gap

- Defensive automation
- Distributed security
- Reduction of detection and containment times

Protect the future

- Crypto-agility
- Post-quantum readiness
- Protection of long-lifecycle data

In an environment of continuous risk, the cybersecurity roadmap must prioritize those capabilities that tangibly increase effective control, reduce asymmetry with adversaries and prevent irreversible risks, and must be governed as a transversal operating model with metrics oriented to impact, time and business continuity — **assuming that reinvented cybersecurity is a living system, not a final state**.



Softtek®

softtek.com