ADOPTING NEXT-GENERATION ZERO TRUST

Rethinking Authentication, Access, and Integrity in a Zero-Trust World

Future of Cybersecurity Knowledge Community

December 2025

GLOBAL CYBERSECURITY FORUM | Site

Foreword

Dr. Hesham Altaleb
Chairman, Future of Cybersecurity
Knowledge Community
Saudi Information Technology
Company - SITE

Zero Trust has become a strategic imperative, yet a large number of organizations have not yet been able to implement it at scale. This white paper outlines the key challenges chief information security officers (CISOs) face in adopting Zero Trust and offers practical strategies to accelerate its implementation, align leadership and maximize impact. It also explores how AI is transforming Zero Trust in increasingly complex cyber environments by enabling continuous risk evaluation, context-aware decisions and intelligent enforcement.

Developed by the Future of Cybersecurity Knowledge Community, with the support of the Global Cybersecurity Forum, this report aims to equip security leaders with the clarity and guidance needed to drive Zero Trust transformation in complex, evolving environments.

We encourage leaders and professionals to engage with these insights and help shape the next generation of secure, resilient cyber systems.

About the Future of Cybersecurity Knowledge Community

The Future of Cybersecurity Knowledge Community is committed to exploring the potential opportunities and threats presented by ever-evolving Cyberspace. It also seeks to develop mechanisms that can maximize the benefits of this evolution and address the risks now looming on the horizon. It does this by bringing together a diverse array of expertise from a wide range of stakeholder groups.

The community welcomes leading technology companies, global cybersecurity organizations, cybersecurity research centers, reputable think tanks, academic institutions and other stakeholders with a vested interest in exploring and acting upon the future of cybersecurity.

Authors & Contributors

- **Dr Manar Alohaly** (SITE)
- **Heelah Alraqibah** (SITE)
- **Dr Faisal Sibai** (Accenture)
- **Dr Antonio Jara** (Libelium)
- **Ed Sleiman** (Microsoft)
- **Michael Mosaad** (Deloitte)
- **Qusai Al Rabei** (Schneider Electric)
- **Dr Stefan Deutscher** (BCG)
- **Shoaib Yousuf** (BCG)
- **Radu Balanescu** (BCG)
- **Alberto Pardo** (BCG)
- **Duna Alghamdi** (BCG)
- **Chaimae Haska** (BCG)
- **Dr Dan Bogdanov** (Cybernetica)

Contents

Table of figures

Abbreviations

Abbreviations	Definition
AI	artificial intelligence
API	application programming interface
BCG	Boston Consulting Group
CISO	Chief Information Security Officer
IAM	identity and access management
IT	information technology
NIST	National Institute of Standards and Technology
OT	operational technology
SEB	Scandinavian Private Bank (Skandinaviska Enskilda Banken)
SITE	Saudi Information Technology Company
SMPC	secure multi-party computation
TEE	trusted execution environment

Executive Summary

The era of static trust is over. As cyber ecosystems expand across cloud, remote work, artificial intelligence (AI)-driven threats and machine identities, traditional security models are under growing pressure. The urgency this creates is clear: organizations must not only embrace Zero Trust architectures - where every access request is considered untrusted until verified - but also accelerate their evolution in an adaptive, intelligence-driven direction.

This paper distills insights from a Future of Cybersecurity Knowledge Community study. Drawing on interviews with CISOs, practitioners and experts, it identifies three key challenges currently slowing Zero Trust adoption:

- **The Zero Trust promise is proven, but execution is fragile:** Many efforts stall due to fragmented leadership, cultural resistance and the challenge of re-engineering legacy systems. Zero Trust cannot succeed as an information technology (IT) project alone; it demands enterprise-wide alignment and sustained executive sponsorship.

- **Technical complexity remains the Achilles' heel:** Retrofitting heterogeneous environments, especially in operational technology (OT) and multi-cloud, often introduces risk. A fragmented vendor landscape compounds the challenge, forcing the deployment of a patchwork of tools, rather than a coherent strategy.

- **The external environment often raises the stakes:** Regulatory constraints and evolving adversary techniques pressure organizations to act decisively while navigating market fragmentation.

The opportunity presented by Zero Trust architecture, however, outweighs these obstacles. The next generation of Zero Trust can – and must – move beyond static controls to Adaptive Trust. This will be powered by real-time telemetry, AI-driven enforcement and dynamic identity governance. In this model, human and machine actors alike are verified, contextualized and governed at machine speed.

To enable this shift, we have introduced a new framework: EDGE. Standing for establish, deploy, govern and evolve, it is an actionable architecture that seeks to:

- **E**stablish alignment and executive buy-in
- **D**eploy Zero Trust incrementally, focusing on high-value areas first
- **G**overn through visibility, automation, and adaptive controls
- **E**volve continuously with shifting threats and priorities

Zero Trust is no longer a strategic aspiration, but the backbone of modern security. Organizations that embed intelligence, embrace adaptability and align security with business transformation will not only safeguard operations, but also unlock agility, trust and resilience in the future.

1. The evolution of trust: Why Zero Trust, why now?

Perimeter-based security is no longer viable. With cloud expansion, remote work, AI-driven threats and a surge in non-human identities, the idea of a trusted internal network has collapsed. In perimeter-based security, once the boundary is bypassed, implicit internal trust and flat controls allow lateral movement, making the breach difficult to contain. Zero Trust offers a modern alternative: verify every access request, segment tightly and adapt, based on risk.

This white paper outlines the key challenges CISOs face in adopting Zero Trust and offers practical strategies to accelerate implementation, align leadership and maximize impact. It also explores how AI is transforming Zero Trust, enabling real-time detection, dynamic access and scalable security for an increasingly complex cyber landscape.

1.1 What Is Zero Trust and why did it emerge?

Zero Trust is a cybersecurity model grounded on the principle "never trust, always verify". Unlike traditional perimeter defenses that rely on network location, Zero Trust treats every access request as untrusted until verified. The US National Institute of Standards and Technology (NIST) Special Publication 800-207 defines Zero Trust as "a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly, but must be continually evaluated".[1]

Zero Trust gained traction in response to cloud computing, mobile workforces and insider threats. These undermined the logic of static perimeters and created the need for new architectures that validate access per resource, assume breach conditions, and restrict trust to the narrowest necessary scope.

Moreover, traditional enterprise security resembled a medieval moat-and-castle: once a user crossed the firewall (the "moat"), they were considered trusted and often had broad internal access within the "castle".[2] This model fails to protect against insider threats or lateral movement after a breach. As shown in Figure 1, Zero Trust is better understood through a "hotel" metaphor: while users can enter the lobby, they need verified keycards for each room or resource they wish to access. This reflects how Zero Trust enforces continuous, per-resource authentication across the environment – even for users already "inside" the system.

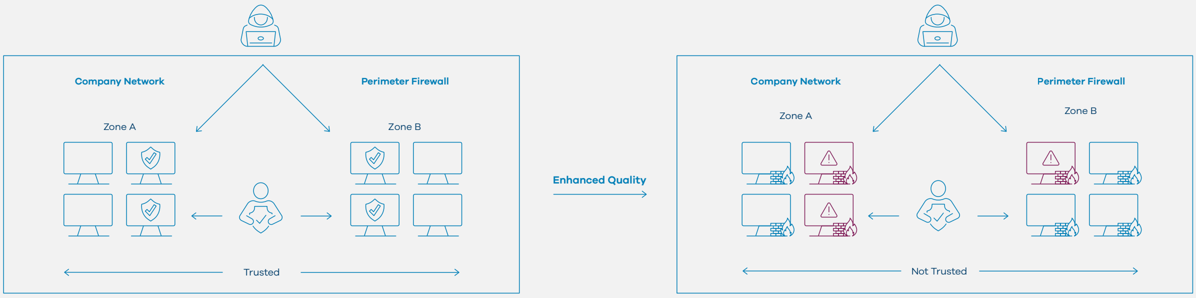
New paradigm rejects old security model of "inside means trusted" and "outside means untrusted"

Transformation from the castle

Intruder gains access to corporate network, and by default, has wide ranging access internally. Insiders already within the network have free reign.

...to the hotel

Intruders and insiders must continuously request access to each resource individually.



- High walls and a moat protect the castle
- An attacker looks for a single weak point
- Once violated all assets are potentially compromised
- Insiders given free reign

- The entrance of a hotel is less secure, but still protected
- Elevators and rooms are safe with keys and codes
- Objects are protected at multiple levels
- Insiders only given access to what is necessary for theirole

Figure 1: Zero Trust: moving from "moat-and-castle" to "hotel" security

Source: BCG: From Zero to Hero: Why Zero Trust Adoption is Struggling

Zero Trust implementation relies on several standard architectural practices:

- **Least-privilege access:** This principle limits every user or system to the minimum access rights needed to perform their function. The NIST stresses precise, least-privilege access to limit the impact of a compromised identity or device.[1]

- **Micro-segmentation:** The Zero Trust model breaks networks into smaller isolated zones, limiting lateral movement and internal threats.[3] Micro-segmentation is used to enforce tight access boundaries.[3]

- **Continuous authentication and verification:** Zero Trust replaces one-time checks with continuous verification using multi-factor authentication, identity checks and behavior monitoring.[3]

- **Encryption and context-aware controls:** Zero Trust systems rely on strong encryption to protect data both in transit and at rest. By implementing robust encryption techniques and effective key management, these systems ensure that sensitive information remains inaccessible to unauthorized users.[3]

As the Zero Trust model matures, its scope may begin to extend beyond access control into data processing itself. Cryptographic technologies – such as trusted execution environments (TEEs), secure multi-party computation (SMPC) and zero-knowledge proofs – make it possible to enforce security and privacy policies even while data is being computed. The innovations in these technologies reduce reliance on trusted internal processing environments, reinforcing Zero Trust's core principle: never assume trust – not even during computation. While still emerging, such capabilities are gaining traction across sectors like finance, healthcare and cloud infrastructure, and may shape future extensions of the Zero Trust principles.

1.2 Zero Trust: No longer just a strategic aspiration

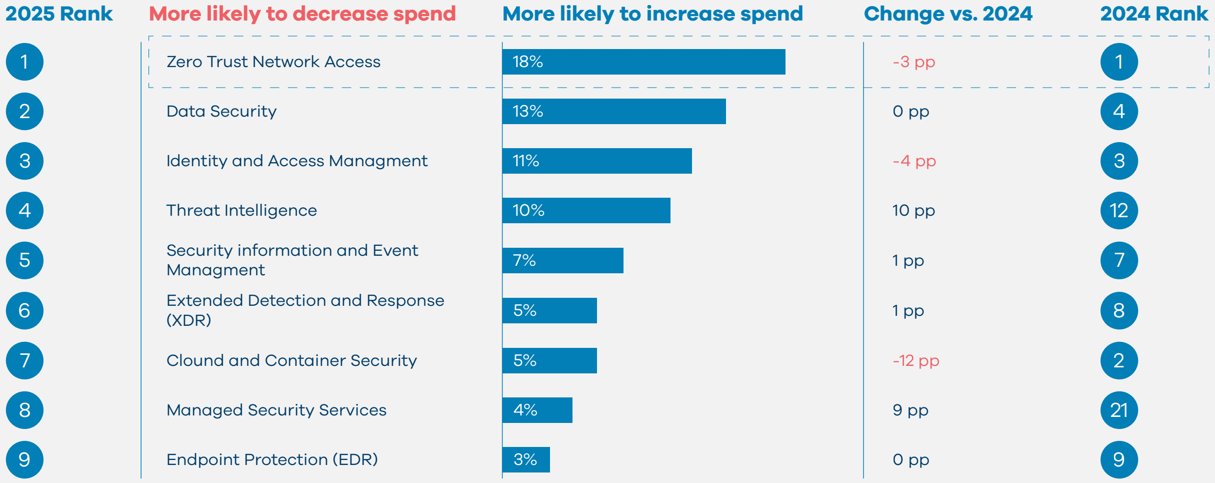
Across high-risk industries, Zero Trust has shifted from a cybersecurity concept to a strategic necessity. In manufacturing, it isolates legacy systems and verifies devices in order to counter billions of attacks. In finance, it protects digital channels and transaction flows, reinforcing trust in an environment of accelerating threats. Public sector and defense agencies rely on it to safeguard national data and remote operations, while energy providers use it to shield vulnerable supervisory control, data acquisition and OT networks. In healthcare, where ransomware threats loom large, Zero Trust now underpins efforts to protect patient data and prevent breach escalation. No matter the sector, the signal is the same: Zero Trust is no longer optional – it is mission-critical.

As shown in Figure 2, Zero Trust network access was the top-ranked category for expected spending growth among CISOs in both 2024 and 2025 – underscoring that Zero Trust continues to be the highest investment priority for security leaders.[4]

This sustained focus reflects more than a trend: it signals a fundamental shift in how organizations approach risk. With the rise of AI-driven attacks, hybrid work and ecosystem complexity, traditional perimeter defenses have become irrelevant. CISOs now see Zero Trust not as an enhancement, but as the architectural backbone of modern security.

Top product categories for expected spend growth

Q: Please select up to 3 product categories where you expect the largest spend increases or decreases over the next year (2025 vs. 2024). (N=300)



*pp: percentage point

Figure 2: BCG 2025 CISO survey: Top products for expected spend growth

Source: BCG: Annual Cybersecurity CISO Survey: AI Creates New Cyber Risks. It Can Help Resolve Them, Too

As Zero Trust shifts from aspiration to implementation, its organizational impact is becoming tangible. Yet cybersecurity leaders struggle to effectively communicate the benefits of zero-trust architecture to different organizational stakeholders.[5] Framing Zero Trust not just as a security architecture, but as a business enabler, is critical to securing alignment and sustaining investment.

Organizations that implement Zero Trust effectively can unlock measurable business benefits across three dimensions:[5]

- **Risk reduction and resilience:** Zero Trust minimizes the blast radius of breaches and operational errors by continuously verifying every user, device and connection. This containment not only reduces the likelihood of catastrophic incidents, but also lowers recovery costs and protects reputation – key metrics for boards and regulators alike. Zero Trust also supports regulatory compliance by providing granular visibility into who accessed what, when and under what conditions. This is critical for auditability and risk reporting, particularly in highly regulated industries like financial services.
- **Business enablement and agility:** By decoupling security from static perimeters, Zero Trust empowers organizations to embrace new business models with confidence. It supports secure digital transformation initiatives, enables merger and acquisition integrations, and facilitates rapid deployment of new services. In doing so, it enhances business agility, allowing teams to innovate without waiting for lengthy security redesigns. For a globally distributed workforce, Zero Trust

enables secure, real-time collaboration across geographies, devices and partners, reducing friction while maintaining control.

- **Operational flexibility and user experience:** Zero Trust removes reliance on fixed network boundaries and physical locations, enabling secure access from anywhere and on any device. This flexibility allows organizations to adopt hybrid and cloud-native environments without adding complexity, ensuring that security evolves in step with the business. When implemented effectively, Zero Trust also improves user experience by enabling seamless, context-aware access, eliminating unnecessary barriers while maintaining security posture.

2. Beyond the hype: Current factors holding Zero Trust back

Despite its promise, Zero Trust often stumbles in execution and in practice, leaving Zero Trust transformations falling short of their targets. Indeed, while the Zero Trust model offers undeniable security and business advantages, many organizations struggle to move beyond the conceptual into the operational, as what looks clear on paper becomes far more complex in practice. Implementation is not only technically demanding, but deeply dependent on organizational context. Zero Trust is not a plug-and-play solution – it is an adaptive architecture that must be tailored to each organization's risk profile, legacy systems, regulatory constraints and threat landscape.

As a result, Zero Trust journeys often diverge. Some achieve meaningful progress while others stall, fragment, or quietly fail. These mixed outcomes reveal a deeper truth: successful Zero Trust adoption requires more than the right tools or intentions. It also demands alignment across technology, governance, culture and execution.

The following section explores the key obstacles that hinder effective Zero Trust implementation. Drawing on insights from around a dozen in-depth interviews with cybersecurity leaders, industry practitioners and active members of the Future of Cybersecurity Knowledge Community, a set of recurring themes was isolated. These revealed three main dimensions preventing Zero Trust adoption and success: 1) a lack of organizational alignment; 2) technical and architectural complexity; and 3) constraints posed by regulatory and market fragmentation. The following subsections examine these three dimensions.

2.1 Lack of organizational alignment

Zero Trust cannot succeed in isolation. Yet in many organizations, core teams – such as security, risk, IT, governance and business – operate in silos, each with their own strategic priorities, operational tools and cultural language. This multi-layered misalignment slows decision-making, undermines shared accountability and introduces conflicting interpretations of what Zero Trust actually means.

A 2023 survey by Forrester[6] reported that when asked what the major obstacles to Zero Trust initiatives were, 47% of enterprise security leaders cited a lack of key personnel, while 46% noted conflicting priorities. This highlights how cross-functional alignment frequently stands in the way of progress.

A lack of leadership alignment also often compounds these organizational silos. Too often, Zero Trust is pitched as a technical upgrade, rather than a strategic transformation. As a result, initiatives struggle to secure executive buy-in and funding dries up before outcomes can materialize. Even when there is intent, the absence of a structured program – one complete with clear milestones, roles and cross-functional governance – leads to drift and stagnation.

Cultural resistance adds another layer of inertia. Without proper communication, Zero Trust is often perceived as disruptive, overly rigid or poorly defined. Longstanding habits and internal politics foster skepticism, while the absence of clear implementation goals leaves many teams disengaged.

Without unified leadership and shared accountability, Zero Trust initiatives risk becoming fragmented, underfunded and ultimately abandoned. This leaves organizations exposed, despite their earlier investment.

2.2 Technical and architectural complexity

Even with strong alignment, many organizations hit a wall when confronting the technical realities of Zero Trust. Legacy systems – those designed for perimeter-based models – lack the application programming interfaces (APIs), visibility, and policy enforcement capabilities required for granular access control. Retrofitting these environments is often both costly and operationally risky. According to a Deloitte poll conducted during the "Is Zero Trust the way?" webcast in 2023, 44.6% of C-suite and other executives reported that complexity and compatibility issues with legacy systems and environments were the greatest challenge to Zero Trust adoption.[7]

This is especially true in OT environments, where safety-critical systems dominate and any disruption can have serious consequences. In these cases, strict Zero Trust controls can introduce unacceptable risk, making rollout unlikely to go beyond controlled pilots.

Poor architectural visibility is another common issue. Many teams lack a clear understanding of the systems they are trying to protect – application dependencies, protocol behaviors, identity flows and access patterns. Without this baseline, Zero Trust policies become speculative, at best. Segmentation is similarly misunderstood and is often implemented as arbitrary isolation, rather than the creation of dynamic, risk-based trust zones that reflect real access needs.

Moreover, Zero Trust is not static. Fine-grained policies require continual tuning, context-aware enforcement and escalation paths when access is denied. Without automated ways to manage these processes – especially at scale – organizations risk operational bottlenecks and degraded user experiences.

Unless organizations overcome technical debt and architectural blind spots, Zero Trust will remain aspirational, trapped in pilot stages without delivering enterprise-wide impact.

2.3 Regulatory and market fragmentation constraints

Beyond internal barriers, organizations face significant friction from the broader ecosystem. Regulatory and legal constraints – particularly those related to monitoring user behavior and location – can clash with foundational Zero Trust principles, such as continuous verification and dynamic enforcement. These constraints vary across jurisdictions, making global adoption even more complex.

Complicating matters further is the fragmented state of the vendor landscape. The Zero Trust market is saturated with overlapping tools that target vastly different use cases. These may range from identity and endpoint management to network segmentation and machine identity. A 2025 StrongDM survey found that 52% of organizations struggle with managing multiple tools in Zero Trust deployments, while 49% cited inconsistent policies across multi-cloud environments.[8] This highlights how tool and vendor fragmentation remains a key adoption hurdle. Without a unified framework, teams are forced into inefficient point solution patchworks, undermining both performance and strategy.

Without clear frameworks and interoperable solutions, organizations will struggle to operationalize Zero Trust across borders. This hampers scalability, increases cost and erodes confidence in the model's viability.

The above findings highlight the most pressing technical, organizational, and cultural barriers that prevent Zero Trust from achieving its full potential. By distilling these shared challenges, this analysis can provide security leaders with a clearer view of where to focus effort, foster cross-functional alignment and unlock measurable progress.

In the next section, we examine how AI is rapidly becoming a transformative force for Zero Trust, helping organizations improve detection and move toward autonomous, adaptive security models.

3. Zero Trust next frontiers: Adaptive, intelligent and verifiable

While Zero Trust has laid the groundwork for modern cybersecurity, it is only really the beginning. As organizations scale cloud-native infrastructures, embrace microservices and leverage AI, the model is evolving into something far more dynamic: Adaptive Trust.

In today's ecosystems, trust cannot rest solely on credentials or static policies. Instead, non-person entities from devices and APIs, workloads and automation agents must be verified continuously. The NIST Special Publication 800 207 referred to above had already anticipated this shift, calling for trust decisions based on real-time context (device health, behavior and network activity), not just identity credentials.[1] It is now widely forecast that Zero Trust architectures will be increasingly augmented by AI to enable autonomous decision-making, adaptive controls and predictive capabilities.[9, 10]

As AI agents and autonomous systems become integral to modern operations, zero-trust architectures must evolve alongside them. The future of security depends not just on verifying human users, but also on managing an army of AI-driven identities acting at lightning speed. Gartner predicts that by 2028, at least 15% of day-to-day work decisions will be made autonomously by AI agents,[11] introducing new challenges around identity governance, behavioral accountability and real-time policy enforcement.

This report now highlights in more detail the key challenges these new developments reveal.

3.1 Future challenges: When synthetic identities think and act

- **Proliferation of non-human identities:** Enterprises now manage an average of 45 non-human identities for every human one – a number rapidly rising with the adoption of AI agents.[12] This explosion of machine-driven identities challenges existing identity and access management (IAM) frameworks and amplifies the risks of credential sprawl, policy drift and unauthorized access.

- **Increased velocity of access decisions:** Autonomous agents make decisions and take action at lightning speed – far faster than static policy frameworks can adapt. Legacy trust models struggle to keep up.

- **Opaque behavior and accountability:** As agents act independently, tracking and attributing behavior becomes much harder, especially when misconfigurations or attacks impersonate intelligent action.

- **Blurring of trust boundaries:** Autonomous systems often cross organizational or cloud boundaries. This erodes the traditional notion of a trusted internal network and exposes data to risk at all stages – whether at rest, in transit or, increasingly, in process. This, in turn, complicates compliance with existing frameworks.

Yet, while these challenges are significant, they also open the door to powerful opportunities – especially when Zero Trust is reimagined through the lens of AI-driven automation and intelligence.

The subsections below now highlight some of these potential benefits.

3.2 Emerging opportunities: Making trust smarter – powered by AI

- **Context-aware, autonomous enforcement:** When AI is embedded into Zero Trust, identities – both human and machine – can be continuously evaluated. Alerts, isolations or policy adjustments happen instantly, not after hours of manual triage. In fact, AI-powered Zero Trust implementations have reported reductions in average incident response times from 4.2 hours to just 12.3 minutes – a dramatic leap in operational efficiency.[13]

- **Behavioral telemetry at scale:** AI systems can analyze vast activity streams that range from identity behavior to traffic patterns. This enables real-time detection of anomalies that would overwhelm traditional defenses.

- **Just-in-time, risk-adaptive access:** By replacing static privileges with dynamic, context-aware access, AI enables systems that adapt in real time to changes in posture, identity use and risk.

- **Next-generation identity governance:** Intelligent identity graphs, lifecycle automation and privilege sprawl detection allow organizations to manage both human and machine identities with unprecedented visibility and control.

Looking ahead, Zero Trust must be identity-first, real-time and intelligence-embedded. Autonomous systems demand adaptive trust – models that learn, enforce and evolve at machine speed. Organizations that anticipate this shift will not only secure AI-driven operations, but will also enable them to thrive.

3.3 Emerging opportunities: Encrypted processing and cryptographic assurance

Zero Trust has traditionally focused on verifying access, but advances in cryptographic technologies are pushing the model further, extending Zero Trust principles into how data is processed, not just who accesses it. This evolution removes yet another layer of implicit trust: the assumption that internal processing environments are secure by default.

Until recently, technologies such as SMPC, TEEs, homomorphic encryption and zero-knowledge proofs were confined to academic research or highly specialized use cases. In the last few years, however, major cloud providers and industry consortia have made significant strides in commercializing and standardizing these capabilities, turning them into practical tools for mainstream enterprise use.

These advances allow organizations to cryptographically verify that data remains protected, even during computation, whether processed on internal systems, in the cloud or by external partners.

This marks a foundational shift in Zero Trust: from managing access to also governing usage and intent. It reinforces the model's core principle: never assume trust, not even inside the processor.

4. Next-generation Zero Trust adoption recommendations

The evolution of Zero Trust from theory to partial adoption has revealed two important realities. First, the model is conceptually sound, but challenging to implement at scale. Second, AI may soon reshape how trust is evaluated and enforced – possibly moving us from static Zero Trust toward a more adaptive, intelligence-driven model.

Looking ahead, successful Zero Trust transformations will require more than technology. Based on insights gathered from cybersecurity leaders, strategists and practitioners, the path forward depends on leadership clarity, strategic prioritization and cultural alignment.

To address Zero Trust adoption challenges, this whitepaper introduces the EDGE Framework – a practical model designed to guide organizations through a structured, outcome-driven, Zero Trust journey.

The EDGE Framework consist of four pillars: establish, deploy, govern, evolve. It is designed to help organizations overcome the three common pitfalls of Zero Trust adoption: fragmented leadership, technical complexity and market fragmentation. The EDGE Framework provides a structured, phased approach to move from strategic intent to operational reality.

Furthermore, as AI reshapes cybersecurity, the EDGE Framework helps organizations embed intelligence into each phase of Zero Trust, from strategy to operations. By enabling real-time decisions, automating enforcement and scaling adaptive trust, AI transforms Zero Trust from a static model into a living, learning architecture.

4.1 The EDGE Framework: Turning Zero Trust aspirations into security

As shown in Figure 3, the four pillars of the EDGE Framework provide a strategic pathway from initial alignment through implementation to sustained maturity.

Each phase is interdependent and essential. The subsections below provide more detail about each pillar, along with recommendations for its implementation.

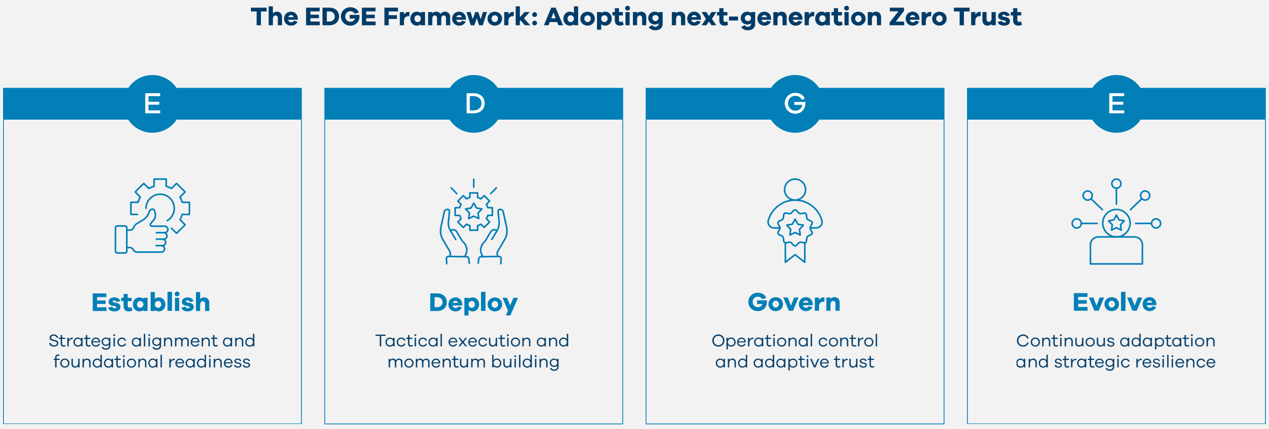

The EDGE Framework: Adopting next-generation Zero Trust
E
Establish
Strategic alignment and foundational readiness
D
Deploy
Tactical execution and momentum building
G
Govern
Operational control and adaptive trust
E
Evolve
Continuous adaptation and strategic resilience

Figure 3: The EDGE Framework for adopting next-generation Zero Trust

E – Establish: Strategic alignment and foundational readiness

Addresses: Lack of organizational alignment, leadership gaps and cultural resistance

The success of any Zero Trust initiative begins with shared understanding and executive alignment. Such an initiative must be treated not as a security upgrade, but as a business transformation. Without a strong strategic foundation, Zero Trust efforts often stall or become siloed.

Key recommendations:

- **Simplify the narrative:** Translate Zero Trust into business language, focusing on outcomes like risk reduction, compliance and business agility.
- **Set a shared vision:** Use a common reference architecture to align stakeholders and remove ambiguity. A lack of clarity around definitions and scope is a leading cause of failure.
- **Leadership education:** : Invest in structured training to help stakeholders understand that Zero Trust is a mindset shift – and one that affects people, process and policy.
- **Engage stakeholders early and build momentum:** Involve business, technical and security leaders from the outset. This is crucial in aligning expectations, securing executive sponsorship and identifying cross-functional champions who can co-own implementation goals and drive sustained governance across the organization.

D – Deploy: Tactical execution and momentum building

Addresses: Complexity of legacy systems, lack of clear roadmap and cultural inertia

With alignment in place, the next step is to translate strategy into action, quickly and deliberately. Instead of attempting a wholesale transformation, successful organizations prioritize initiatives that are high-impact, yet manageable.

Key recommendations:

- **Use case prioritization and phased rollouts:** Focus early efforts on high-risk, high-value areas. Demonstrating tangible risk-reduction builds credibility and supports further investment.

- **Phased adoption:** Use AI to prioritize Zero Trust investments based on risk telemetry, usage patterns or access anomalies.

- **Quick wins with automation:** Leverage AI-powered IAM, behavior analytics or anomaly detection to reduce manual overhead.

- **Empower security champions:** Identify advocates in business units or engineering teams (e.g., DevOps) who can lead by example and influence adoption from within.

G – Govern: Operational control and adaptive trust

Addresses: Lack of architectural visibility, policy drift and governance fragmentation

Zero Trust relies on decision making in real-time and continuous enforcement. Governance provides the structure for Zero Trust to scale sustainably. With AI, governance becomes more adaptive, shifting from static control to context-aware enforcement.

Key recommendations:

- **Establish intelligent visibility:** Deploy AI-powered telemetry and asset discovery to gain real-time visibility into users, devices, access flows and behavioral baselines. This visibility is foundational for risk-aware decision-making and policy design.

- **Automate behavioral governance:** Use machine learning to dynamically enforce just-in-time access, detect anomalous behavior and adjust trust zones in real time. AI can reduce manual overhead while enabling more precise, adaptive control.

- **Strengthen policy enforcement with safeguards:** AI-driven engines should be integrated for access approvals, risk scoring and incident escalation. At the same time, oversight mechanisms such as the "four-eyes" principle should be maintained to mitigate automation blind spots.

- **Ensure cross-functional accountability:** Define clear roles and escalation paths across security, IT and business functions. Use shared dashboards and automated reporting to track ownership, exceptions and policy adherence at scale.

E – Evolve: Continuous adaptation and strategic resilience

Zero Trust is not a destination – it is a living capability. As technologies, threats, and business models evolve, so too must the Zero Trust model. Organizations that treat it as static will quickly fall behind.

Addresses: Regulatory constraints, vendor/tool fragmentation and change fatigue

Key recommendations:

- **Treat Zero Trust as a journey:** Establish feedback loops and ongoing refinement processes. As threat models evolve, policies and controls must evolve in parallel.

- **Model validation:** regularly stress-test Zero Trust implementations with red teaming or AI-based simulation of adversarial behavior.

- **Vendor orchestration:** Use AI platforms to abstract complexity and normalize policy enforcement across fragmented tools and clouds.

- **Strategic re-alignment:** Re-engage stakeholders periodically to assess alignment with evolving business and regulatory goals.

In summation, the EDGE Framework is not only a roadmap for implementation – it is also a response to the organizational, technical and ecosystem-wide challenges that Zero Trust faces today. By embedding AI and fostering alignment at every phase, it can transform Zero Trust from a static ideal into a dynamic capability fit for the future.

Conclusion

Zero Trust has shifted from aspiration to necessity. Perimeter-based models can no longer secure a landscape defined by cloud, hybrid work and the surge of machine identities. Yet adoption remains uneven, hindered by technical complexity, fragmented tools and organizational silos.

The path forward, however, is clear: Zero Trust must evolve into an adaptive, intelligence-driven model where trust is dynamic, continuous and context-aware. AI will play a defining role in this shift, enabling real-time enforcement at the scale and speed modern enterprises demand.

This whitepaper introduced the EDGE Framework – establish, deploy, govern, evolve – as a practical guide to move from strategy to execution. By embedding adaptability and aligning security with business priorities, organizations can transform Zero Trust into a foundation for resilience and agility in the intelligent era.

Appendix: Methodology

This whitepaper employed a multi-stage, qualitative research approach designed to explore challenges in Zero Trust adoption and the evolving role of Zero Trust architecture across industries. The methodology consisted of three key phases: literature review, expert interviews and a synthesis of findings.

1. Literature Review: A comprehensive review of relevant publications, including industry reports, academic articles and white papers. This phase aimed to establish a foundational understanding of Zero Trust principles, historical context, implementation patterns and emerging trends.

2. Expert Interviews: Around a dozen of structured interviews were conducted with subject-matter experts, including experts from the Future of Cybersecurity Knowledge Community. The interviews focused on a number of key questions, including:

- What do you see as the key barriers to Zero Trust adoption in organizations today – and what practical steps can CISOs take to overcome these?
- What are your views on Zero Trust shifting towards Adaptive Trust? What indicators would tell us we are moving in that direction? In what ways can AI improve Zero Trust frameworks?
- In what ways can AI improve zero-trust frameworks?

These discussions provided a critical layer of qualitative insight, offering first-hand perspectives on the challenges and enablers of Zero Trust transformations.

3. Consolidation and Analysis: In the final phase, findings from the literature and interviews were analyzed thematically to identify recurring patterns, and points of alignment or divergence. The consolidated insights informed the structure of this report, shaping both the thematic chapters and the final recommendations.

Endnotes

1. NIST/US Department of Commerce (2020). NIST Special Publication 800-207: Zero Trust Architecture
2. BCG (2023). From Zero to Hero: Why Zero Trust Adoption is Struggling
3. International Research Journal of Engineering and Technology (2024). Zero Trust Security Model: Implementation Strategies and Effectiveness Analysis
4. BCG (2025). Annual Cybersecurity CISO Survey: AI Creates New Cyber Risks. It Can Help Resolve Them, Too
5. Gartner (2025). Guide to Communicating the Value of Zero Trust to Stakeholders
6. Forrester (2023). A Zero Trust Strategy Addresses Workloads and Applications
7. Deloitte (2023). Legacy Tech Poses a challenge to Zero Trust Adoption, While Risk Management Needs Continue to Drive its Adoption
8. StrongDM (2025). The State of Zero Trust Security in the Cloud Report
9. Hashim S. and M. Ikhlaq – self-published (2023). Zero Trust Meets AI: Redefining Security in the Age of Advanced Threats
10. International Journal of Science and Research Archive (2024). Zero Trust Architecture and AI: A Synergistic Approach
11. Gartner (2025). Gartner Predicts Over 40% of Agentic AI Projects Will Be Canceled by End of 2027
12. Cloud Security Alliance (2025). Securing Non-Human Identities in the Age of AI Agents | CSA Summit 2025 at RSAC
13. International Research Journal of Modernization in Engineering, Technology and Science (2025). AI integration in Zero Trust Security Architecture: A Technical Overview

GLOBAL
CYBERSECURITY
FORUM

Site