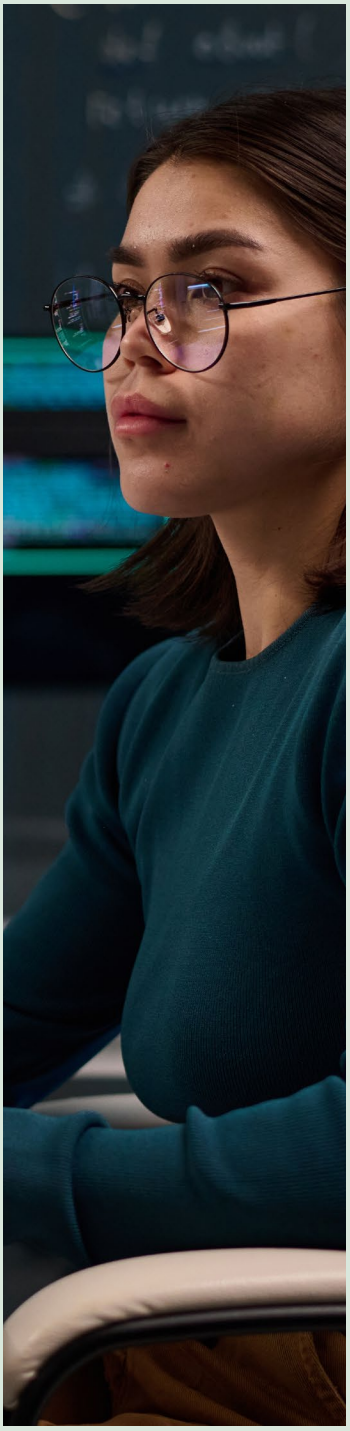
WHITE PAPER



ZERO TRUST FOR THE ENTERPRISE:

A STRATEGIC BLUEPRINT FOR MODERN SECURITY TRANSFORMATION

Abstract

In an era of escalating cyber threats and increasingly complex IT ecosystems, traditional perimeter-based security models are no longer sufficient to safeguard enterprise assets. Zero Trust has emerged as a transformative security paradigm that operates on the principle of "never trust, always verify," ensuring continuous authentication, authorisation, and validation of every user, device, and application. This paper presents a strategic blueprint for modern security transformation, guiding enterprises through the adoption of Zero Trust architecture as a foundational element of their cybersecurity posture.

Infosys
Navigate your next

Table of Contents

Executive Summary	03
Introduction	03
Understanding Zero Trust	04
Drivers for Zero Trust Adoption	05
Strategic Blueprint for Implementation	06
Challenges and Mitigation Strategies	07
Implementation Roadmap	08
Case Studies	08
Compliance Frameworks Mapping	09
CIS Benchmarks	10
Future Trends	11
Conclusion	11
Reference	12

External Document © 2026 Infosys Limited

Executive Summary

The rapid evolution of digital ecosystems, cloud adoption, and remote work has rendered traditional perimeter-based security models obsolete. Cyber threats are increasingly sophisticated, targeting identities, devices, and applications across distributed environments. To address these challenges, enterprises must embrace Zero Trust—a security paradigm built on the principle of "Never trust, always verify."

This strategic blueprint outlines a comprehensive approach to Zero Trust implementation, combining business priorities with technical rigour. It covers:

- Core Principles: Identity-centric security, least privilege access, and continuous verification
- Drivers for Adoption: Cloud migration, regulatory compliance, and advanced threat landscapes
- Implementation Roadmap: A phased plan with timelines and milestones — Assessment, Architecture Design, Pilot, Enterprise Rollout, and Continuous Optimisation
- Technology Enablers: MFA, SASE, EDR/XDR, SIEM, and automation for resilience
- Compliance Alignment: Mapping Zero Trust to NIST SP 800-207, ISO/IEC 27001, and CIS benchmarks
- Future Trends: AI-driven Zero Trust, IoT/OT security, and predictive analytics

By adopting Zero Trust, organisations can reduce risk, enhance compliance, and enable secure digital transformation. This is not a one-time project but a continuous journey towards adaptive, identity-driven security.

Introduction

The digital transformation of enterprises has fundamentally changed the way organisations operate, communicate, and deliver services. With the rise of cloud computing, remote workforces, and interconnected ecosystems, traditional perimeter-based security models have become ineffective. These legacy approaches assume trust within the network, leaving organisations vulnerable to sophisticated cyberattacks, insider threats, and lateral movement.

Zero Trust emerges as a modern security paradigm designed to address these challenges. Built on the principle of "Never trust, always verify," Zero Trust eliminates implicit trust and enforces continuous authentication and authorisation for every user, device, and application, regardless of location. This approach ensures that security is not tied to a physical network boundary but is embedded across all layers of the enterprise architecture.

In this strategic blueprint, Infosys explores why Zero Trust is essential for today's enterprises, outlines its core principles, and provides a detailed roadmap for implementation. By adopting Zero Trust, organisations can achieve stronger resilience against evolving threats, meet compliance requirements, and enable secure digital innovation.



External Document © 2026 Infosys Limited

Understanding Zero Trust

Zero Trust is a modern cybersecurity framework that eliminates implicit trust within enterprise networks. Unlike traditional perimeter-based security models — which assume that everything inside the network is trusted — Zero Trust enforces continuous verification for every user, device, and application, regardless of location.

Core Principles

1. **Identity-Centric Security**
   Every access request is authenticated and authorised based on user identity and context.
2. **Least Privilege Access**
   Users and devices are granted only the minimum permissions necessary to per-form their tasks.
3. **Continuous Verification**
   Security checks are ongoing, not one-time, ensuring that trust is never assumed.

Evolution of Security Models

1. **Perimeter Security:**
   Traditional model where trust is granted to everything in-side the network boundary
2. **Zero Trust Security:**
   Modern approach where no entity is trusted by default, and verification is enforced everywhere

Comparison of Security Models

Traditional	Zero Trust
Assumption Implicit trust within the network	Never trust, always verify
Network Perimeter Strong perimeter defenses	No implicit trust, verify everything
Access Control Broad access within the perimeter	Restricted, least privilege access
Verification One-time at login	Continuous



External Document © 2026 Infosys Limited

Drivers for Zero Trust Adoption

Key drivers include cloud migration, remote workforce expansion, sophisticated cyber threats, and compliance mandates. These factors necessitate a security model that is adaptive, resilient, and identity driven. Organisations adopting Zero Trust can achieve better risk management and regulatory compliance.

Below are few real-time numbers of attacks from 2020–2025, with the increase of AI adoption in all sectors by attackers.

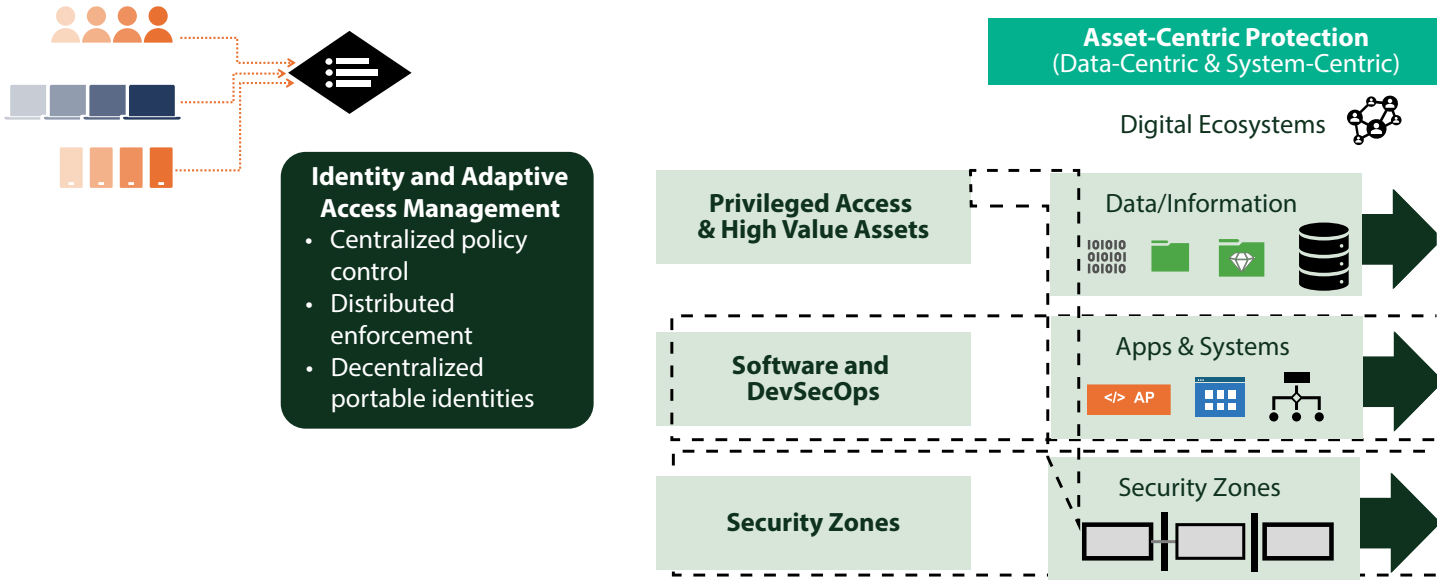
Key Observations

- While total attacks rise steadily, AI-powered attacks represent the fastest-growing segment, driven by automation, generative AI, and adaptive malware.
- By 2025, AI-driven threats accounted for over 50% of the projected attack growth, making Zero Trust and AI-aware defences critical.

Zero Trust Components

Risk Controls - establish overall security framework based on organizational risk

Secure Asset Management – enables you to identify, classify, secure, and maintain assets



Asset-Centric Security Operations – rapid and complete detection, response, and recovery from attacks

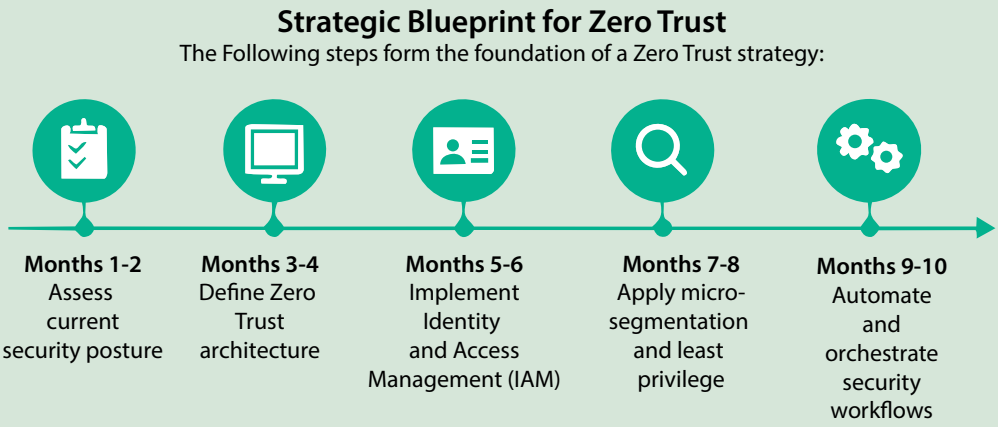
Posture Management – continuous improvement of attack prevention measures

Strategy, Integration, & Governance (SIG) – continuous management of risk, integration, & compliance

External Document © 2026 Infosys Limited

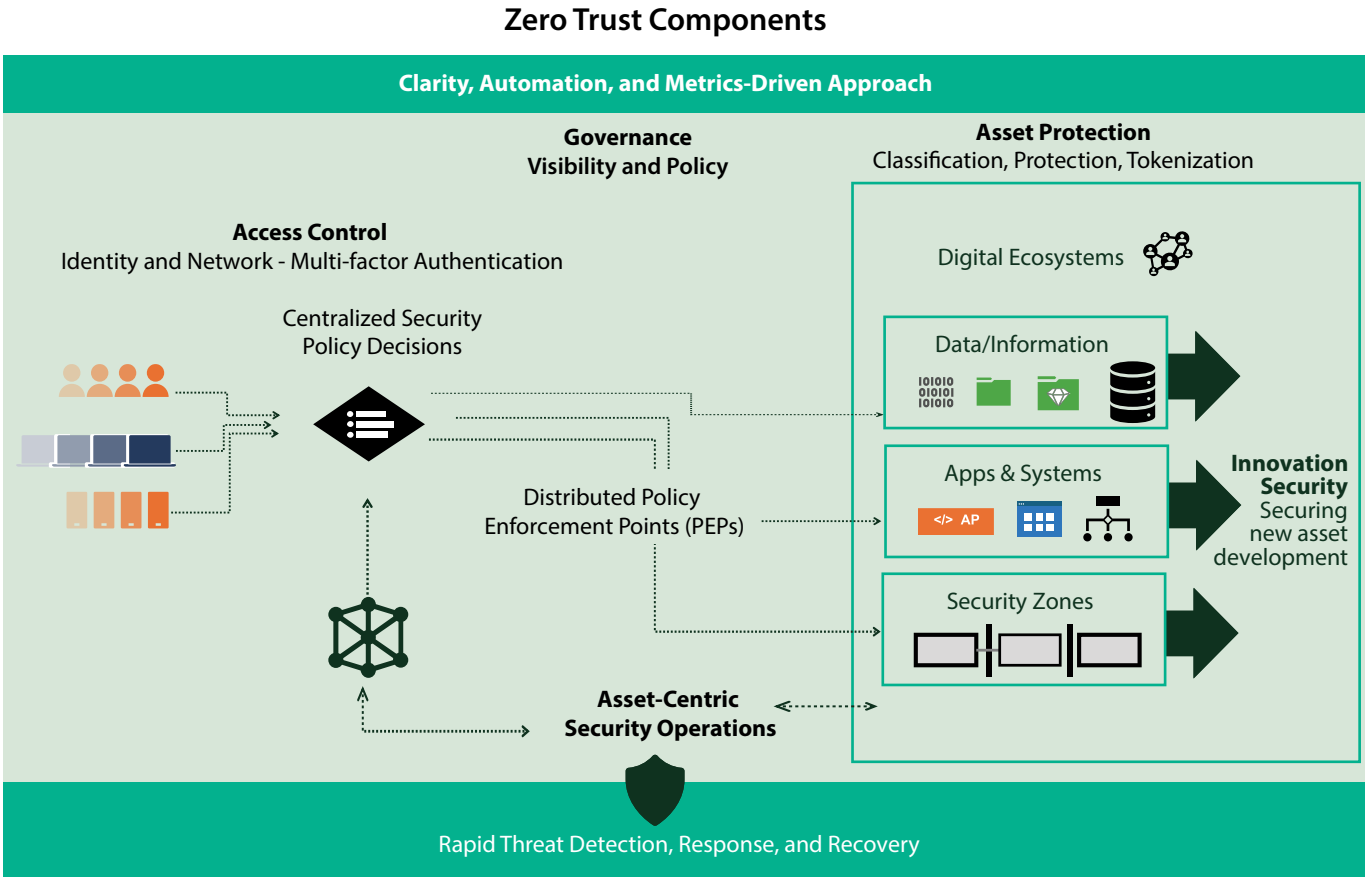
Strategic Blueprint for Implementation

The following timeline and infographic represent the foundation of a Zero Trust strategy along with the timeline it takes:



Technology Enablers

Key technologies include Multi-Factor Authentication (MFA), Secure Access Service Edge (SASE), Endpoint Detection and Response (EDR/XDR), and Security Information and Event Management (SIEM). Integration with existing infrastructure is critical for success.



External Document © 2026 Infosys Limited

Challenges and Mitigation Strategies

01

Cultural Resistance

- **Issue:** Employees and even IT teams may resist changes in access policies, fearing reduced productivity or complexity.
- **Impact:** Lack of buy-in can slow adoption and lead to policy circumvention
- **Example:** Pushback against MFA or strict access controls

02

Legacy Systems

- **Issue:** Older applications and infrastructure often lack support for modern authentication or segmentation.
- **Impact:** Integration complexity and potential security gaps
- **Example:** Mainframe systems or legacy ERP platforms without API-based identity integration

03

Cost and Complexity

- **Issue:** Implementing Zero Trust requires investment in new tools, skilled personnel, and process redesign.
- **Impact:** Budget constraints and resource limitations can delay rollout
- **Example:** High cost of advanced IAM solutions and network segmentation tools

Mitigation Strategies

01

Phased Implementation

- Start with high-risk areas (e.g., remote access, privileged accounts)
- Gradually expand to cover all users, devices, and applications
- Use pilot projects to demonstrate quick wins and build confidence

Executive Sponsorship

- Secure leadership support to align Zero Trust with business objectives
- Communicate benefits such as reduced risk, compliance, and secure digital transformation
- Provide change management programmes to ease cultural resistance

02

03

Leverage Automation

- Automate identity verification, policy enforcement, and threat detection
- Use orchestration tools to reduce manual overhead and improve efficiency
- Example: Automated provisioning/ de-provisioning of user access



External Document © 2026 Infosys Limited

Implementation Roadmap

The roadmap below includes phases, milestones, and suggested timelines:

Strategic Blueprint for Zero Trust

The Following steps form the foundation of a Zero Trust strategy:



Months 1-2
Assess current security posture

Months 3-4
Define Zero Trust architecture

Months 5-6
Implement Identity and Access Management (IAM)

Months 7-8
Apply micro-segmentation and least privilege

Months 9-10
Automate and orchestrate security workflows

Case Studies

Case Study: Leading Mining Company

A leading Australian mining, logistics and transportation company faced challenges with remote workforce security and regulatory compliance. By adopting Zero Trust principles, the institution implemented strong ZTNA architecture, micro-segmentation, and continuous monitoring. Results included a major reduction in security incidents and improved compliance with improved user experience.

Success Story

SASE implementation for mining company in Australia

Challenges

- Centralized Security stack at DC
- No Scalability in pace with Rapid Digital Transtormation
- No Cloud adaption, No flexibility to adapt new emerging Services
- Performance/User experience - Application de-centralization- Hair pinning of traffic at DC
- Management complexty - Multi Vendor Security Stack
- High operating Costs - Network links, Licenses

Solution

- Implemented 4 Service Connections (IPSec tunnels) from data center to Prisma Access for apps access from data center
- Connected 118 remote sites using IPSec connectivity with high availability using active-passive failover
- Onboarded all mobile users and deployed Global Protect agent on end points



Value delivered

- App based security policies, with granular access control (moved away from port-based security)
- Improve security posture by implementing granular access control for apps
- Moved from on-prem to cloud delivered security
- Highly scalable security Infrastructure with consistent security posture for all users and remote sites
- High availability for security infrastructure
- User experience improvement



Case Study: Leading Singapore Telecom Business

The client is a leading telecom company. Their requirement was to build a strong platform with best-of-breed agile services leveraging digital technologies to revolutionise customer experience. They were looking for a vendor who could support their digital transformation journey.

External Document © 2026 Infosys Limited

Solution Brief:

- Infosys built a zero-trust security framework with the key design principles — Defence in Depth and Secure by Design — which entails layered security controls
- Provided enterprise-grade security and enhanced it further for cloud environments by following industry standards (E.g. CIS benchmarks, NIST cybersecurity framework)
- Leveraged existing licences for security tools to enable the security controls at each layer, thereby optimising cost
- Implemented network, data and endpoint security along with identity and access management solutions as part of the digital transformation journey
- Implemented tenable security tools for vulnerability assessment lifecycle for the platforms and assets
- Zero Trust adoption enabled secure access for 10,000 employees in APAC, leveraging MFA, device compliance checks, and automated threat response.

Outcome: Enhanced resilience against current AI driven attacks and optimised cost and efforts with a unified cloud solution.

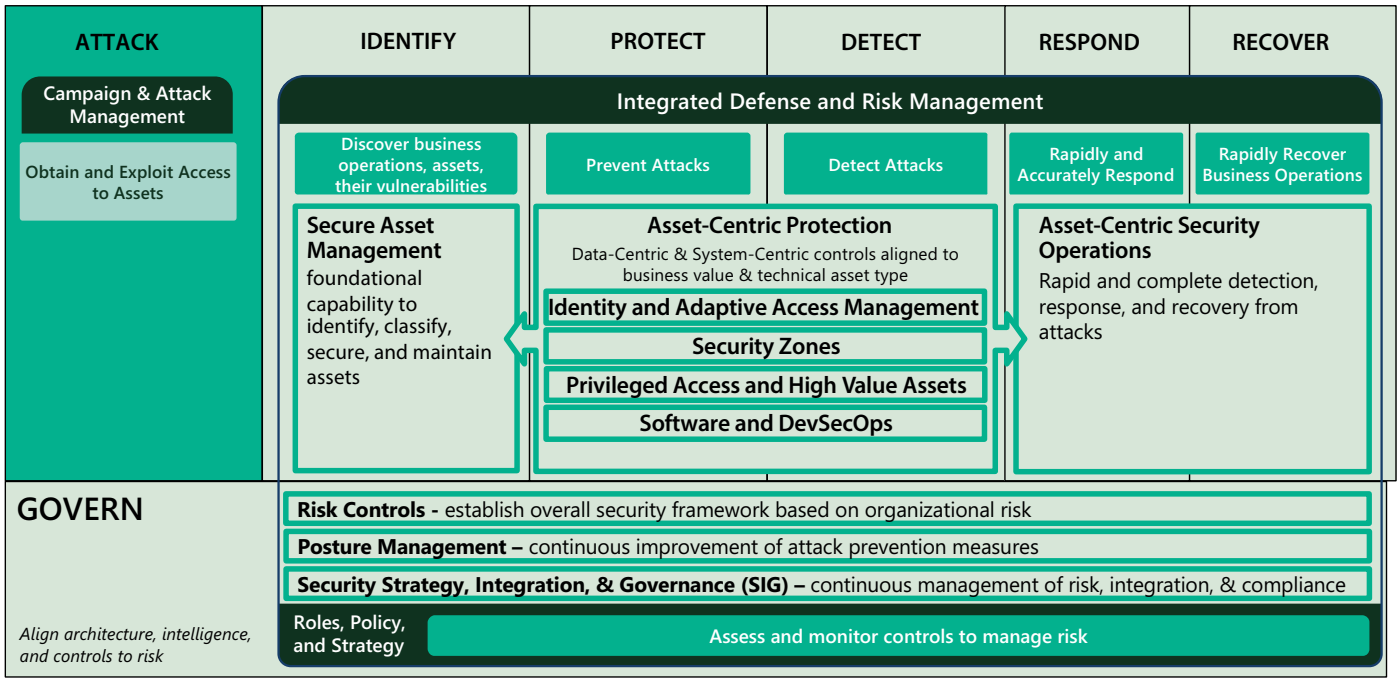
Compliance Frameworks Mapping

NIST SP 800-207 (Zero Trust Architecture)

- Aligns with Zero Trust principles: identity-centric security, continuous verification, and least privilege access.
- Provides guidelines for implementing Zero Trust across enterprise systems

Zero Trust Capabilities

Durable business outcomes for security (mapped to NIST Cybersecurity Framework)



ISO/IEC 27001 (Information Security Management)

- Zero Trust supports ISO 27001 controls for access management, risk assessment, and incident response
- Enhances compliance through strong authentication and network segmentation

External Document © 2026 Infosys Limited

COMPLIANCE MAPPING

Zero Trust Capabilities	ISO/IEC 27001 Controls
Access Control	✓
Cryptography	✓
Operations Security	✓
Communications Security	✓
Supplier Relationships	✓
Information Security Incident Management	✓

CIS Benchmarks

- Zero Trust complements CIS benchmarks by enforcing secure configurations and continuous monitoring
- Helps organisations meet best practices for endpoint and network security

Zero Trust Capabilities	NIST SP 800-207	CIS Benchmarks
Access Control	✓	✓
Cryptography	✓	✓
Operations Security	✓	✓
Communications Security	—	✓
Supplier Relationships	—	✓
Information Security Incident Management	—	✓



External Document © 2026 Infosys Limited

Future Trends

Emerging trends include AI-driven Zero Trust, Zero Trust for IoT and OT environments, and predictive analytics for proactive threat mitigation.

As cyber threats evolve and digital ecosystems expand, Zero Trust will continue to adapt and integrate with emerging technologies. Key trends shaping the future include:

1. AI-Driven Zero Trust

- What's Changing: Artificial Intelligence (AI) and Machine Learning (ML) will enhance Zero Trust by enabling predictive analytics for threat detection.
- Impact: Real-time anomaly detection and automated policy adjustments based on behavioural patterns

2. Zero Trust for IoT and OT

- Why It Matters: Internet of Things (IoT) and Operational Technology (OT) devices often lack robust security controls.
- Trend: Applying Zero Trust principles to secure IoT endpoints and industrial systems, ensuring device identity verification and micro-segmentation

3. Integration with SASE and XDR

- Development: Secure Access Service Edge (SASE) and Extended Detection and Response (XDR) will converge with Zero Trust to provide unified security across cloud and edge environments.
- Benefit: Simplified architecture and improved visibility across distributed networks

4. Identity as the New Perimeter

- Shift: Identity will become the primary control point for security, with advanced Identity and Access Management (IAM) and adaptive authentication.
- Future: Password-less authentication and continuous risk-based access decisions

5. Compliance Automation

- Trend: Automated compliance mapping and reporting integrated into Zero Trust platforms.
- Outcome: Easier adherence to frameworks like ISO/IEC 27001, NIST SP 800-207, and CIS Benchmarks.

6. Quantum-Resistant Security

- Emerging Need: Preparing for quantum computing threats by adopting quantum-safe cryptography within Zero Trust architectures

Conclusion

Zero Trust is no longer an optional security model—it is a strategic necessity for modern enterprises facing dynamic threats, cloud adoption, and remote work challenges. By eliminating implicit trust and enforcing continuous verification, Zero Trust significantly reduces attack surfaces and strengthens compliance with global standards such as ISO/IEC 27001, NIST SP 800-207, and CIS Benchmarks.

Implementing Zero Trust is not a one-time project but a continuous journey. Success requires:

- A phased roadmap with clear milestones
- Strong executive sponsorship and cultural alignment
- Integration of advanced technologies like IAM, MFA, SASE, and automation

Organisations that embrace Zero Trust will achieve:

- Enhanced security resilience against sophisticated cyber threats
- Improved compliance posture for regulatory frameworks
- Secure digital transformation, enabling innovation without compromising trust

Zero Trust is the foundation for the future of cybersecurity — adaptive, identity-driven, and built for a world without boundaries.

External Document © 2026 Infosys Limited

References:

White Papers & Guides

1. The Open Group Zero Trust work and Microsoft Reference Architecture 2025
   General Information - https://www.opengroup.org/forum/security/Zerotrust
   Zero Trust Commandments - https://pubs.opengroup.org/security/zero-trust-commandments/
   Zero Trust Reference Model - https://publications.opengroup.org/s232
2. EPAM Systems. (n.d.). Guide to zero trust cybersecurity for modern enterprises. https://www.epam.com/content/dam/epam/free_library/whitepapers/Zero_Trust_Whitepaper_06_23.pdf
   Includes NIST definitions, core principles such as "never trust, always verify," and practical transition guidelines for enterprises adopting Zero Trust.
   Read here [epam.com]
3. Juniper Networks. (n.d.). The rise of zero trust. https://www.juniper.net/content/dam/www/assets/white-papers/us/en/security/the-rise-of-zero-trust.pdf
   Debunks common industry myths about Zero Trust and explains practical implementation strategies for deploying Zero Trust networks.
   View PDF [juniper.net]

Government & Standards

- U.S. Department of Defense, Office of the Chief Information Officer. (2022). DoD zero trust strategy. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
  Provides a comprehensive roadmap for Zero Trust adoption across large, complex enterprises, with defined execution goals and target timelines.
- Cybersecurity and Infrastructure Security Agency. (2023, April 11). Zero trust maturity model (Version 2.0). U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
  Offers a maturity model and phased implementation guidance to help agencies and organisations progress toward Zero Trust.

About the Author



Rajesh Kumar Mohapatra is a Cyber Security leader with over 14 years of experience in security architecture, cloud security, infrastructure security, governance, risk management, and operational resilience. He specializes in securing hybrid enterprise environments across Azure Cloud Security and on-premises platforms, with expertise in Firewalls, Proxies, Cisco ISE, EDR/XDR, Email Security, Identity Security, and Data Security.

With a growing focus on AI-driven security and Responsible AI, Rajesh helps organizations address emerging risks associated with AI adoption through secure design, governance, and compliance frameworks. Currently serving as Principal Consultant – Infrastructure Management and Technology Manager (Cyber Security), he partners with business and technology leaders to drive secure digital transformation, strengthen cyber resilience, and align security strategies with organizational goals.

For more information, contact askus@infosys.com

Infosys
Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.