Deloitte.

Zero-Trust-in-a-Box

Never trust, always verify

Together, Deloitte and Zscaler unbox zero trust designed to secure enterprise and network infrastructure.

Transforming your security experience

Discover how we can help strengthen your organization's communications security—with a focus on optimizing both costs and operational efficiency.

Enhanced business agility and resilience through unified threat protection enabled by Deloitte and Zscaler's integrated Zero Trust framework.

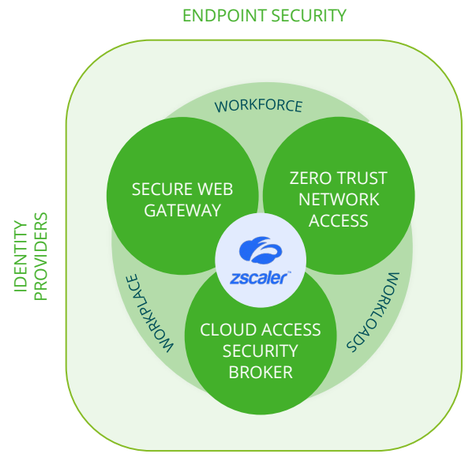
A customized roadmap and business case, jointly developed by Deloitte and Zscaler, to guide your Zero Trust transformation.

Rapid validation of your security use cases, maximizing value and minimizing disruption with Deloitte and Zscaler's combined capabilities.

What's in the box?

APPROACH

- Zero Trust (ZT) assessment
- Core Security Domains Addressed
- Tailored business case to support your transformation journey



OUTCOME

A tangible roadmap, a business case, and real-world proof of value—all laid out in a set time frame—setting the stage for broader zero trust transformation.

Our capabilities

Data Security

Safeguards your organization's cloud-based data from theft, misuse, or loss by continuously monitoring for potential misconfigurations, vulnerabilities, and permission issues that could create attack vectors.

This ongoing scanning helps ensure data remains secure and protected against emerging threats.

Zero Trust Branch

Deloitte leverages Zscaler's Zero Trust Exchange platform to help clients implement secure, simplified, and cost-effective Zero Trust branch architectures.

We offer a comprehensive approach to modernizing branch security, making it more agile, resilient, and better suited for a cloud-first environment.

GenAI/AI Guard

We provide a comprehensive framework for managing the risks associated with GenAI, allowing businesses to innovate safely.

Implements robust AI guardrails to enable the safe use of public AI, shield private AI environments from malicious attacks, and defend against AI-driven threats.

Data Loss Prevention (DLP)

Cloud-based DLP can prevent sensitive data leaks for on-premises and remote users.

Enables secure collaboration and web access from any location by continuously monitoring outbound traffic and applying real-time safeguards to block unauthorized data exposure.

Our success stories across industries

Life Sciences Biopharma

CLIENT CHALLENGES

- High-risk regions lacking security visibility/controls.
- “Cloud first” approach hampered by aging on-premise infrastructure.
- Network and application segmentation difficulties.
- Outdated security/network standards.
- Excess hardware at data centers causes cost/complexity.

WHAT WE DID

- Developed a Zero Trust reference architecture using SABSA framework.
- Inventoried/prioritized services for phased migration to cloud.
- Identified high-risk locations, apps, and sites.
- Coordinated with network, identity, and cloud teams for cohesion.
- Delivered a roadmap and segmentation to isolate threats and modernize security.

Chemical Manufacturing

CLIENT CHALLENGES

- Limited security oversight of remote users.
- No security controls/visibility for cloud workloads.
- Inability to isolate/segment network environments (risk of malware spread).
- Outdated network/security standards.
- Inefficient backhauling for remote user security enforcement.

WHAT WE DID

- Designed a comprehensive network security solution using Zscaler and NextGen firewalls.
- Established a standardized Network Security Standards document.
- Analyzed user personas, apps, and traffic flows for integrated design.
- Aligned stakeholders on security policies and access requirements.
- Enabled secure remote access and improved visibility for cloud and user traffic.

Health Care

CLIENT CHALLENGES

- Balancing security with generative AI usage.
- Rapid expansion of generative AI tools/websites.
- Data loss risks via generative AI sites.
- Lack of control over internal and external AI application access.
- No consistent policy enforcement for new AI-driven workflows.

WHAT WE DID

- Assessed generative AI usage and tool landscape.
- Identified all internal and external generative AI tools.
- Proposed CASB and URL filtering rules for safer gen AI enablement.
- Defined Web DLP policies to prevent sensitive data uploads via AI.
- Delivered a robust web DLP structure using Zscaler Internet Access (ZIA).

Potential Outcomes

Enhanced detection and prevention of data loss, cyberattacks, and unauthorized access, reducing risk across user, app, and network environments.

Provided secure, reliable connectivity for users—whether on-premises or remote—without sacrificing productivity or user experience.

Enabled transformation to cloud-first or zero trust models, eliminating legacy hardware dependence and improving scalability and flexibility.

Delivered comprehensive monitoring, centralized policy enforcement, and reporting to meet regulatory requirements and boost oversight.

Streamlined security and network operations, reduced manual interventions, and automated policy enforcement, driving cost and time savings.

Safe adoption of new technologies (like generative AI and cloud apps) and supported agile business processes through secure digital transformation.

LEARN MORE

If you’re ready to tap into Deloitte’s experience in digital transformation and cybersecurity, along with Zscaler’s leading Zero Trust Exchange platform, then let’s talk.

CONTACT US

Wayne Mattadeen
Alliance Leader
Deloitte Consulting LLP
wmattadeen@deloitte.com

Henry Li
Managing Director
Deloitte Consulting LLP
henli@deloitte.com

Lee-Lan Yip
Specialist Leader
Deloitte Consulting LLP
leyip@deloitte.com

Shanov Mudaliar
Alliance Manager
Deloitte Consulting LLP
shmudaliar@deloitte.com