Deloitte.

Reimagining the modern infrastructure security organization

Infrastructure security has been largely static for a decade, but advances in AI, evolving business needs, and stricter compliance requirements are now driving organizations to modernize and rethink their security functions.

Tools such as digital assistants, chatbots, and generative pre-trained transformer (GPT)-powered solutions now streamline requirement gathering, automate document creation, and accelerate system integration and compliance—resulting in faster, more efficient workflows with less manual effort. Unified platforms and Generative AI (GenAI) further enhance productivity by automating documents, speeding up audits, and enabling near real-time updates to operations. Additionally, advances in natural language processing (NLP) and agentic AI make it possible to automate complex, context-aware tasks that were previously beyond the reach of traditional automation.

While operational efficiency improves, organizations contend with new challenges introduced by AI-driven automation, including adversarial attack vulnerabilities, data manipulation, and unauthorized access to AI models. In response, infrastructure security capabilities must evolve.

The changing landscape

The artificial intelligence (AI) landscape is evolving, both in how organizations are adopting it and how attackers are leveraging it.

AI adoption trends

Exponential growth in AI/ML transactions — **536.5B**[1] transactions from AI/ML tools from Feb–Dec 2024

Exponential growth In AI/ML usage — **12x**[1] increase in transaction volumes from Feb–Dec 2024

High rate of blocked transactions — **59.9%**[1] of AI/ML transactions blocked due to security concerns

AI attack trends

25%[2] of enterprises experienced data exposure related to GenAI usage.

60%[2] of organizations cite data leakage as their primary GenAI security concern.

5[2] attack vectors will surge in coming years: AI-powered phishing, deepfakes, exploitation of AI builders, AI-driven malware, and automated social engineering.

1. Data sourced from ThreatLabz 2025 AI Security report. 2. Insights from Zscaler Secure GenAI Adoption document.

Securing AI adoption with infrastructure security

Edge					Network			Endpoint		
Distributed denial of service (DDoS) protection	Web application firewall (WAF)/ content delivery network (CDN)	Inline cloud access security broker (CASB)	Inline data loss prevention (DLP)	Secure web gateway (SWG)	Access control/firewalls Network intrusion prevention system (NIPS) Network detection and response (NDR) Application programming interface (API) gateway & security Domain name system (DNS) security Email security	Micro-segmentation	Network access control (NAC)	Privilege management	Vulnerability mitigation	Mobile security Endpoint security/endpoint detection and response (EDR)

User/remote access (zero trust network access/endpoint behavior)

CASB

Provides visibility and control over cloud-based AI applications and data flows.

DLP

Monitors and controls the movement of sensitive information, models, and intellectual property.

SWG

Discovers, controls, and filters internet access to AI tools and services, enforcing organizational policies.

AI firewall

Monitors and prevents threats to AI applications, large language models (LLMs), and AI agents.

Key capabilities

- Discovery of shadow AI usage across sanctioned and unsanctioned cloud services
- Policy enforcement for uploading, sharing, or downloading AI models and data sets
- Anomaly detection to detect unusual or malicious AI service usage

- Content inspection to detect and prevent unauthorized sharing of AI assets
- Automated alerts and blocking of risky data transfers via network or email
- Integration with AI firewalls, SWG, and CASB for unified policy enforcement

- Uniform Resource Locator (URL) filtering to block access to unsanctioned AI SaaS platforms (e.g., public GenAI tools)
- Secure Sockets Layer (SSL) inspection to monitor encrypted traffic for policy violations
- User and group-based access controls for sensitive AI resources

- Real-time detection of anomalous access to AI models or data sets
- Automated blocking of attacks to AI applications
- Integration with threat intelligence to recognize new AI-related attack vectors

Connect to accelerate

Contact our leaders to dive deeper into the blueprint and reimagine what's possible for your organization.

Mark Nicholson
Principal
Cyber AI GTM Leader
Deloitte & Touche LLP
manicholson@deloitte.com

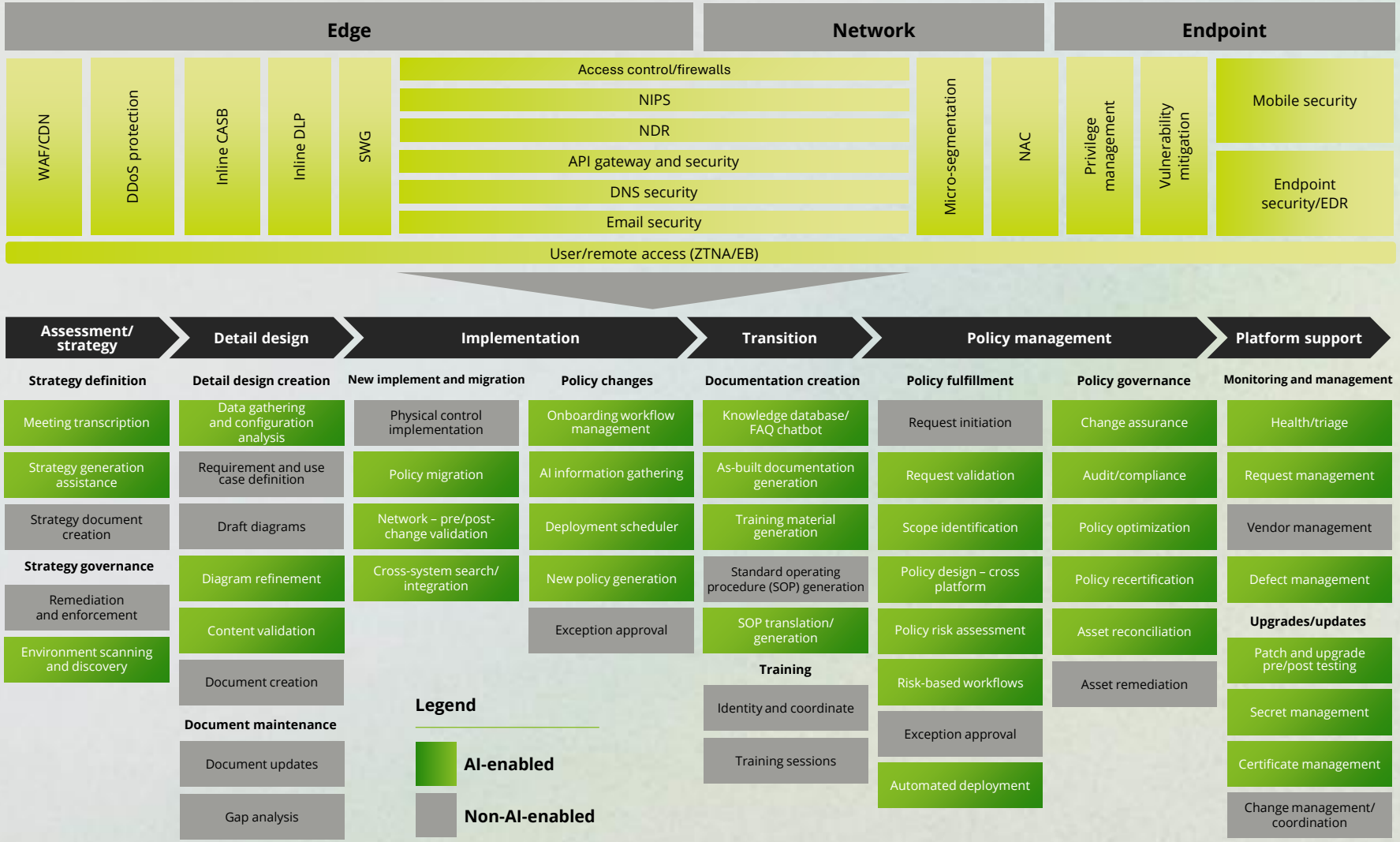
Naresh Persaud
Principal
AI Transformation Leader
Deloitte & Touche LLP
napersaud@deloitte.com

Henri Li
Managing Director
Infrastructure Security Leader
Deloitte & Touche LLP
henli@deloitte.com

Steve Ruzzini
Senior Manager
Cyber AI GTM Activation Lead
Deloitte & Touche LLP
sruzzini@deloitte.com

Embracing AI within infrastructure security

A blueprint for an AI-powered future: Infrastructure security spans multiple capabilities with associated vendor tools across edge, network, and endpoint. How those capabilities and vendor tools are managed from assessment through implementation, policy management, and support can be greatly uplifted through AI. The legend below identifies AI-enabled and non-AI-enabled services.



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Copyright © 2025 Deloitte Development LLC. All rights reserved.