Coforge

Secure the AI Era with Defense-in-Depth and Zero Trust

An AI Security Operating Model that's built on the principle of "Defense-in-Depth"

Powered by the Zscaler Zero Trust Exchange, Coforge helps simplify security complexity, manage evolving cyber risks, and strengthen enterprise resilience.

AI powered approach to provide security for workforce, workplace and workloads

Protect : Zero Trust - Eliminate implicit trust across users, devices, workloads, data, and AI agents

Detect: Zero Dwell – Unify telemetry across endpoint, identity, cloud, SaaS, OT, and AI workloads

Mitigate: Zero Delay - Rapid containment, recovery, and restoration at machine speed (autonomous workflow)

AI Era security imperatives from workloads to workforce

01

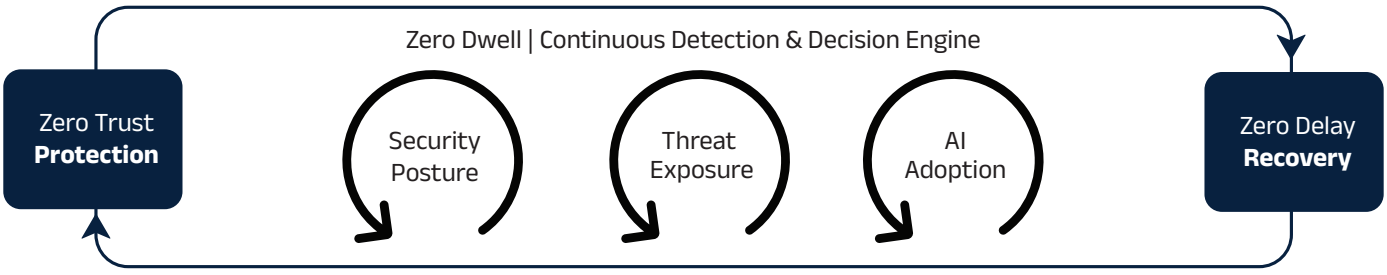
Never Trust, Always Verify
Identity-centric perimeter, continuous verification, least-privilege, micro-segmentation, AI/data guardrails

02

No blind spots
Identity-centric perimeter, continuous verification, least-privilege, micro-segmentation, AI/data guardrails (model access, prompt firewalls, RAG boundary controls)

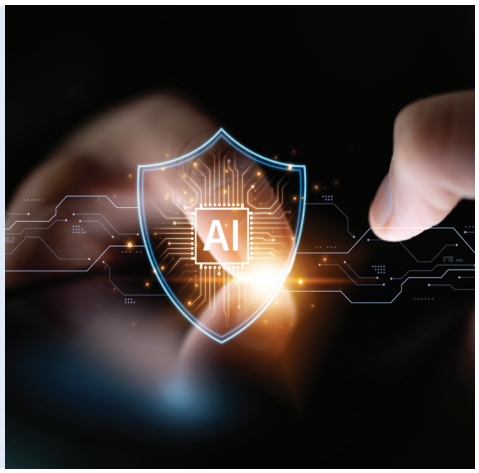
03

Recover Now
Human supervised, agentic response from auto-isolation to pre-rehearsed runbooks to self-healing infrastructure and business platforms



Key Features & Differentiators

- **Risk Based Vulnerability management** across Infrastructure and Applications
- Auto remediation & smart automation use cases
- Mature SOPs, Automation, Reporting & Metrics
- **Automation First Approach** with continuous innovation
- Talent pool of security SMEs with Gold standard Trainings and Certifications
- **2.6 Mn** Threats managed, and **100+** Threat Advisories published every month
- Automated Identity Mgmt. workflow to reduce manual intervention



Value Proposition

- **> 95%** User awareness effectiveness
- Global coverage with skilled cybersecurity professionals
- False Positive reduction by **80%**
- End-to-end security design with interoperability across IT, cloud and compliance teams
- Reduction in User Onboarding timelines by up to **85%**
- **98+%** Access Governance achievement rate
- Phishing simulation click rate: **< 5%** (in 6 months)
- Improved service metrics: MTTD (Avg. 15 Mins) and MTTR (Avg. 30 Mins)

Better Together, bringing the proven delivery model to Zscaler Platform

Zero Trust Platform Architectural North Star	**Mod Squad for Security** Workforce • Workplace • Workloads • B2B	**AI-Powered** Protect • Detect • Mitigate	**Measurable ROI** Cost • Risk • Experience
ENTERPRISE IT PRIORITY **Hybrid & Remote Workforce** Replace VPN, secure any-to-any access	**Z-Scaler Platform** **ZPA (Private Access) + ZIA (Internet Access) + Client Connector** ZTNA for private apps; SWG, FWaaS, DLP, Sandbox for internet & SaaS	**AI –Operating Model** Coforge	**Outcome Committed** **Eliminate VPN attack surface** Faster, safer user experience
Cloud & SaaS Adoption Secure M365, Salesforce, AWS, Azure	**ZIA + Data Protection (CASB / DLP) + Posture Control (CNAPP)** Inline CASB, SaaS posture, cloud workload & code-to-cloud security	Z - Deploy	**Safe cloud acceleration** Data loss prevented at every egress
Reduce Attack Surface & Ransomware Make apps & users invisible to the internet	**Zero Trust Exchange + Deception + ITDR + Breach Predictor (AI)** No inbound exposure, identity threat detection, AI-driven prediction	UnifiedSecurity.AI	**Lower breach probability** Measurable cyber risk reduction
Cost Takeout & Network Simplification Retire MPLS, firewalls, proxies, VPN concentrators	**Zscaler for Branch & Cloud Connector + ZDX** Direct-to-cloud, branch transformation, experience monitoring	SecOps.AI	**30–50% infra cost reduction** Architectural simplification
AI Adoption & Data Protection	**AI Guard + Data Protection + Risk360** GenAI app visibility, prompt/data controls, quantified risk posture	Mod Squad	**Safe enterprise AI rollout** Board-ready risk reporting

OUR ANSWER · 3-LAYER AI DEFENSE-IN-DEPTH

Detect | Protect | Mitigate

PROACTIVE SENSOR MESH
SecureEdge2Cloud
PROTECT

Zscaler Zero Trust Exchange

Z-Deploy

Eliminates the attack surface. Enforces Zero Trust at every user, device, workload, and data flow.

Telemetry feed →

PROACTIVE DECISION ENGINE
UnifiedSecurity.AI
DETECT

Continuous Detection & Decision Engine

Workplace | Workload
Workforce | AI Agent

Identity – Human, Non-Human and External (API)

Residual only →

AGENTIC TRIAGE AND RESOLUTION
SecOps.AI
MITIGATE

Agent + Human SecOps Delivery

Acts on the residue. Contains real incidents in minutes — not days. Triage · Containment · Forensics

80% **20%**

DETECT is the decision engine — PROTECT feeds it, MITIGATE acts on residue.

Solution Overview

INFRASTRUCTURE & CLOUD SECURITY

- Network & Workplace Security
- SASE
- Workload Security
  - Cloud Workload Protection Platform
  - Cloud Security Posture Management
  - Container and microservices security
- Messaging & Collaboration Security
- Cloud Native Security (AWS and Azure)

IDENTITY & ACCESS MANAGEMENT

- Identity Governance & Administration
- Access Management
- Privilege Identity & Access Management
- SSO/MFA services
- Consumer IAM
- Endpoint Privileged Management
- Secrets Management

MANAGED DETECTION & RESPONSE

- Security Event Monitoring and Analytics
- User and Entity Behavior Analytics
- Security Orchestration, Automation and Response
- SIEM/SOAR Platform management
- Threat Intelligence including Brand Monitoring
- Threat Modelling, Threat Hunting, Incident Response

SECURITY ASSURANCE

- Vulnerability Lifecycle Management
- Application Threat Modelling
- Application Security Testing
- Red Teaming Services, External Attack Service Management
- Penetration Testing

DATA SECURITY

- Data Discovery and Classification
- Encryption and Key Management
- Data Loss Prevention
- Data Security Posture Management
- Cloud Access Security Broker
- Database Security

GOVERNANCE, RISK & COMPLIANCE

- Compliance Readiness Services – NIST, CIS, PCI, HIPAA, GDPR
- ISO 27001 Implementations
- IT & Supplier Risk Assessments
- Cyber Resiliency/Maturity Assessments
- Phishing Simulation and Security Awareness

JOINT VALUE PROPOSITION

Coforge + Zscaler: one architectural answer for four problems

THE 5 TECHNICAL PROBLEMS

- Flat networks — east/west traffic unrestricted across EHR, PACS, AD
- Shared credentials — tap-and-go, locum accounts, MFA gaps on Citrix/VPN
- Un-inventoried devices — biomed/IoMT, unmanaged Windows, BYOD outside EDR
- Un-monitored SaaS — 200+ apps with no DLP, posture, or session control
- Un-monitored AI — clinical scribes and copilots adopted without guardrails

THE JOINT MOTION

ZSCALER
PROTECT

+

COFORGE
DETECT + MITIGATE

=

Zero Trust across user · device · workload · data — one architecture for all four problems.

OUTCOMES FOR THE CIO/CISO

- Lateral movement contained — segmentation enforced at the workload
- Identity-first access — ZTNA + MFA replace VPN for every persona
- Full asset discovery — IoMT and biomeds segmented and governed
- Inline data protection — PHI stays on the wire across SaaS
- AI usage governed — shadow AI killed; sanctioned copilots with guardrails

Platform + Mod Squad = Future of Delivery

(Outcomes in days & minutes)

zscaler	Coforge	One Unified
Platform Data Security Cloud Security AI Security	Mod Squad Agentic Fleet Human + Agent Operations	Cyber Security Operational Model For AI era

Zero Trust Platform
Architectural North Star

Mod Squad for Security
Workforce • Workplace • Workloads • B2B

AI-Powered
Protect • Detect • Mitigate

Measurable ROI
Cost • Risk • Experience

Coforge Security Practice – An Overview

60+ Customers	**500+** Trained professionals	**2.6Mn+** Threats managed daily	**250+** MITRE Use Cases
25+ Industry certification	**8** Security Frameworks	**ISO Certified** 9000, 20000, 27001	**SOC 2 Certified**

Security Engineering

Cloud Security
- Reimagine Zero Trust Architecture from Edge 2 Cloud
- Zero Trust Security
- Workload Security
- Workplace Security
- Network and Perimeter Security

Data Security
- Securing Data, Databases and Data pipelines
- Database Security
- Data Loss Prevention
- Encryption and Key Management
- Data Privacy & Compliance Governance

AI Security
- Establishing governance for both sovereign and Ai leveraging clients
- AI Model Security
- AI Runtime Security
- GenAI and LLM Security
- AI Governance

Security Ops

Security Assurance
- Build, modernize, and AI-enable the enterprise estate
- App Test (SAST/DAST/SCA)
- Vulnerability Assessment / Penetration testing
- Continuous Threat & Exposure Mgmt

Security Remediation
- Run autonomous, self-healing operations at scale
- Apps & Platform Resiliency
- Cyber Vault & IRE
- Patch Policies & Controls
- Cloud, Workplace and Workload Remediation

Secure Operations
- GPU-accelerated AI-ready infra with managed MLOps
- Managed Detection and Response
- Security Device Management
- Identity Access Mgmt & Governance
- Cyber Resiliency & Recovery

zscaler · Microsoft · paloalto NETWORKS · BURPSUITE · tenable · RAPID7 · servicenow · rubrik · CROWDSTRIKE · sonarqube · Qualys. · Checkmarx · ARCHER · okta · CYBERARK

About Coforge

Where AI engineering meets industry expertise

Coforge is an **AI-native engineering services leader**, where AI forms the foundation of how we design, build, and deliver intelligent solutions for global enterprises. We combine advanced AI capabilities with hyperspecialized industry expertise to engineer scalable, resilient, and autonomous enterprises. Our AI agents work alongside an AI-enabled workforce, including specialized Full-Stack Digital Engineers (FDEs) operating in hybrid, pod-based delivery models.

With a strong focus on trusted and responsible AI, Coforge delivers secure, governed, and enterprise-grade solutions across the full engineering and delivery lifecycle. Moving beyond AI experimentation, we are outcome-led by design - enabling clients to achieve measurable business outcomes such as reduced operating costs, accelerated cycle times, improved operational resilience, and sustained business growth.

Learn more: **www.coforge.com**