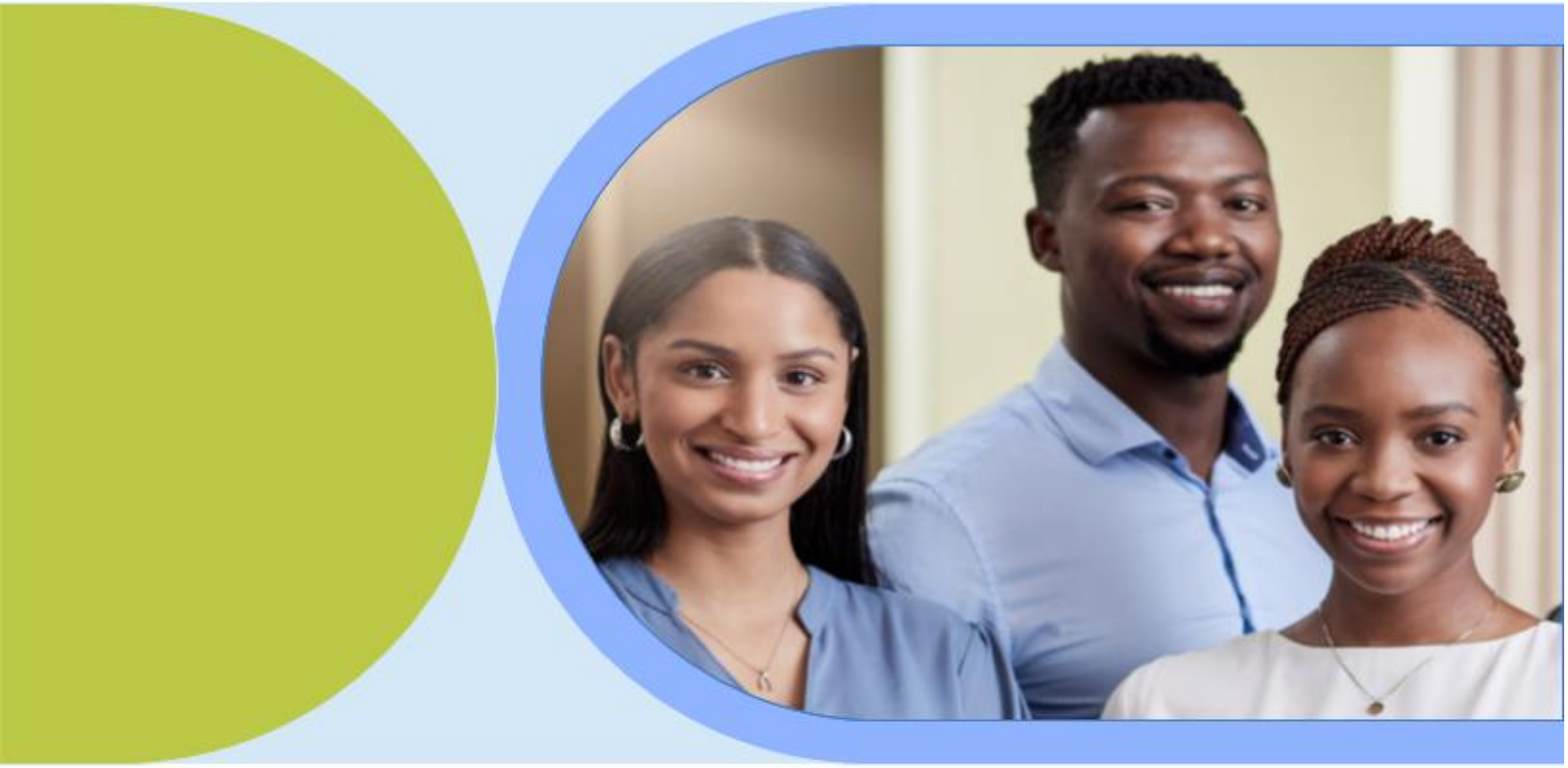
Crown Commercial Service

zensar



Zensar's Service Definition Document for Identity & Access Management (IAM)

January 2026

Table of Contents

1 Introduction

This document defines Zensar's Identity & Access Management (IAM) service, covering architecture, operating model and integrations.

Identity sits at the heart of Zero Trust, modern estates span hybrid cloud, SaaS and on-prem with users, partners, machines and APIs accessing critical data. IAM ensures the right identities get the right access at the right time with strong authentication, least privilege and continuous governance (e.g., access reviews), reflecting industry guidance from NIST Digital Identity Guidelines for authentication strength.

Zensar value proposition. We combine platform expertise (e.g., Microsoft Entra ID for identity governance, Conditional Access and PIM, SailPoint for IGA; CyberArk for PAM) with our delivery governance and integrations (ServiceNow/JML, SCIM).

Our aim: faster time-to-control, measurable risk reduction and audit-ready evidence.

---

2 Service Overview (What Zensar's IAM delivers)

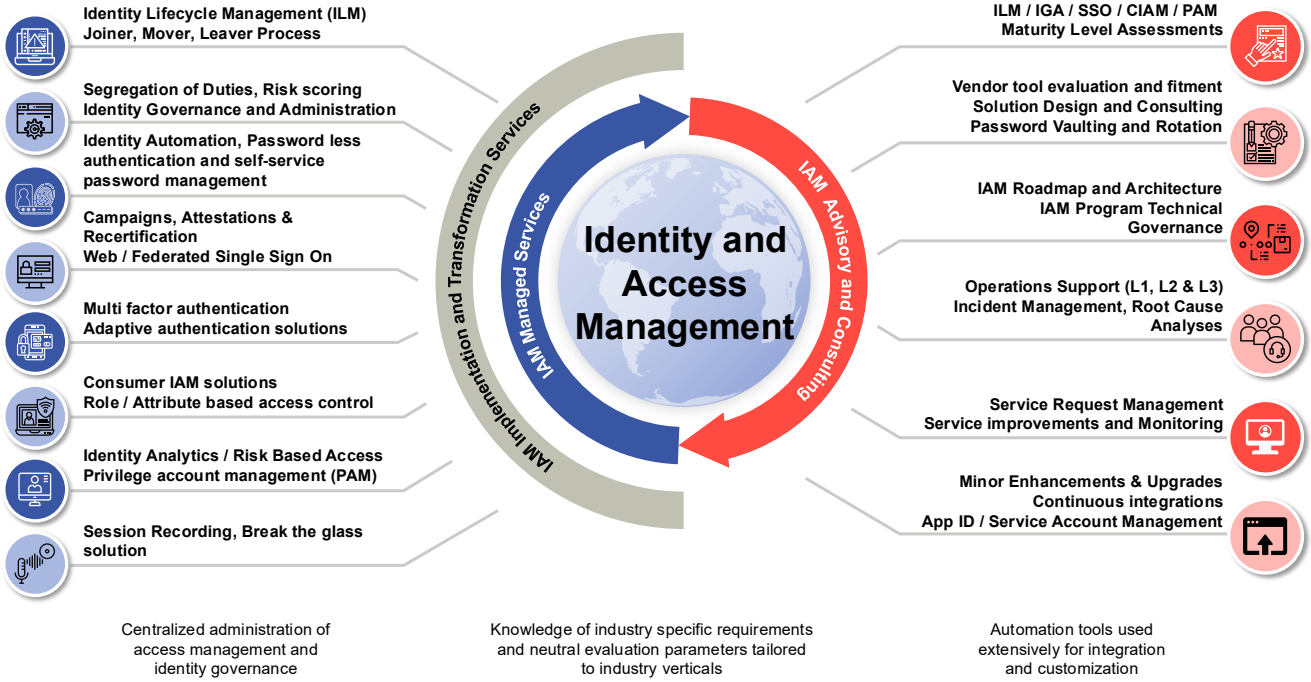
Zensar's IAM (ZenTrust IAM) is a managed, modular program comprising IGA (Identity Governance & Administration), Access Management (SSO/MFA/Conditional Access), PAM and Lifecycle Automation (JML), implemented and operated across hybrid environments (on-prem, cloud, SaaS) and aligned to Zero Trust principles (verify explicitly, least privilege, assume breach).

Core outcomes:

- Strong Authentication & Policy-based Access (MFA, phishing-resistant options, Conditional Access); aligns to Zero Trust identity guidance.
- Least Privilege & Just-in-Time (JIT) Privilege using Microsoft Entra PIM and/or PAM vaulting/session control for powerful roles
- Governance at Scale—access reviews, certifications, SoD policies and auditable trails with IGA platforms like SailPoint.
- Lifecycle Automation (JML)—HR-driven joiner/mover/leaver workflows and SCIM-based provisioning to SaaS and cloud.

ZenIAM Offerings

zensar



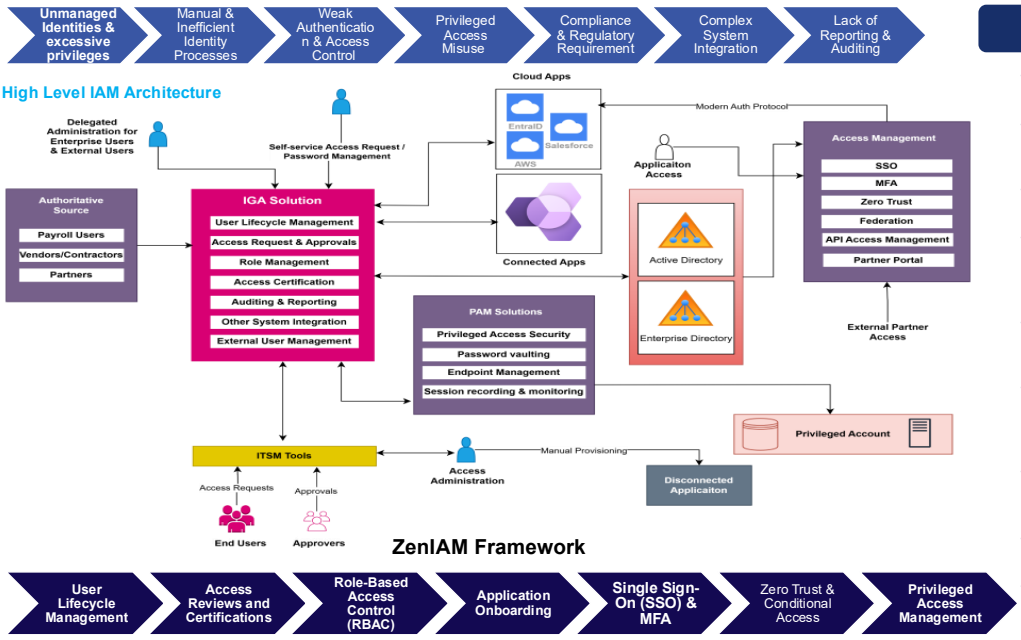
3 Reference Architecture & Components

Identity Plane (Core).

- Directory & Federation: Microsoft Entra ID (SSO/OIDC/SAML, Conditional Access, B2B), federating with on-prem AD where required.
- IGA Platform: SailPoint (IdentityIQ or Identity Security Cloud) for lifecycle events, certifications, SoD, role modeling and policy-based provisioning.
- PAM Platform: CyberArk for credential vaulting, rotation, JIT access, session brokering & recording (PSM/PSMP).
- Automation & Provisioning: SCIM 2.0 standards for interoperable provisioning to SaaS; HRMS as the authoritative source for JML.

Security & Compliance Threading. Controls map to NIST and ISO/IEC 27001 and other regulatory guidelines.

Customer Challenges



Benefits

- Ensure consistent enforcement of security policies across all components.
- Automating user provisioning, de-provisioning, and access requests through IGA reduces manual effort and human error.
- Ensures users only have access to the resources they need, reducing unnecessary permissions.
- Facilitates compliance with legal and regulatory frameworks such as GDPR, HIPAA, and ISO 27001 by providing detailed audit trails and access control policies.
- Simplifies reporting and access review processes, ensuring timely adherence to regulatory requirements.
- PAM's credential vaulting eliminates the need for users to manually manage or share passwords for sensitive accounts, reducing errors and increasing productivity.
- Zero Trust security framework by ensuring that access is granted only to verified users and accounts, minimizing the attack surface
- Integrates seamlessly with cloud, on-premises, and hybrid environments.
- Implements session monitoring and activity logging to detect and respond

4 Operating Model & Service Flow (Zensar-run)

4.1 Define – Scope & Strategy

- Identity sources (HR, partners), in-scope systems, trust boundaries, policy goals (MFA coverage, PIM rollout), maturity baseline vs Zero Trust identity objectives.

4.2 Design – Blueprint & Policy

- Conditional Access policy set (user, device, location, risk), passwordless options, SoD rules, role models, approval chains.

4.3 Build – Platforms & Connectors

- Entra ID tenant hardening, PIM configuration (eligibility, approvals), SailPoint connectors & policies, CyberArk vaults/PSM, SCIM endpoints for SaaS.

4.4 Run – Govern & Improve

- Access reviews, recertifications, outlier analysis, PAM session monitoring/forensics, KPI dashboards (MTTR for access revocation, review completion rates).

4.5 Integrate – ITSM & JML

- ServiceNow request catalogue & workflow orchestration; HR-driven JML (hire/transfer/terminate) integrated with IGA and SCIM provisioning.

5 Service Tasks & Deliverables

Zensar Tasks

- Discovery & Design (identity sources, app catalogue, SoD policy, role modelling).
- Platform Configuration (Entra CA/PIM; SailPoint policies/workflows; CyberArk vaults/PSM; SCIM connectors).
- Integration (ServiceNow request/approval, webhook/API for status updates, HR feed).
- Governance Operations (access reviews scheduling & evidence, PAM session audits, KPI dashboarding).
- Change & Release (CAB changes for policy updates, periodic control tuning).

Deliverables

- IAM Strategy & Blueprint (Zero Trust-aligned).
- Configuration Runbooks (CA policies, PIM settings, IGA workflows, PAM platforms).
- RACI & Operating Procedures (JML, access requests, break-glass handling).
- Reports & Evidence:
    - Access Reviews (completion, revocations),
    - PAM session logs/recordings (as per policy),
    - KPIs (provisioning SLA, review/recert SLA),
    - Compliance mappings (ISO/NIST/PCI).

6 Lifecycle Automation (JML) & Provisioning

JML Orchestration. HR triggers Joiner (create identity + baseline access), Mover (reconcile roles; remove old entitlements to avoid privilege creep), Leaver (disable + deprovision promptly). IGA automates approvals, SoD checks and SCIM pushes to apps; ServiceNow handles request tracking and exceptions.

Standards-based Provisioning. SCIM 2.0 for consistent CRUD of users/groups to SaaS; simplifies multi-app provisioning at scale.

7 Privileged Access Management (PAM) & Just-in-Time Access

Vaulting & Rotation. Centralise privileged credentials; rotate automatically; remove standing access.
Session Control & Recording. Launch, broker and record privileged sessions (PSM/PSMP), with searchable audit trails and policy-based retention.
JIT Privilege (PIM). For cloud and directory roles, Microsoft Entra PIM provides time-bound activation, approval/MFA and review—integrated into governance.

8 Reporting, Integrations & Automation

Executive & Audit Reporting. Access review outcomes, revocations, exception handling, PAM session summaries, KPI/OKR dashboards; evidence aligned to ISO 27001 and NIST,
ITSM (ServiceNow). API-based workflows for requests, approvals, break-glass and offboarding; integration guidance follows REST best practices and scoped roles.
CI/CD & API. Use platform APIs (Entra, SailPoint, CyberArk) for automation; SCIM for standardised app provisioning.

SECURITY ORGANIZATION

- 650+ Security professionals
- 100+ specialized resources in IAM
- Partnered with 30+ clients across the world.

ECOSYSTEM COLLABORATION

- Leverages a vendor-agnostic approach and the best partnerships and thinking
- Collaboration with local University and Zensar's Centre of Excellence to provide intensive cybersecurity training to upskill and reskill

INNOVATION CENTER

- Client showcases and workshops
- Alliances collaboration
- Innovation hub consisting of ZenLab collaboration with various team. Blue Teaming, Red Teaming and Purple Teaming

IAM EXPERIENCE

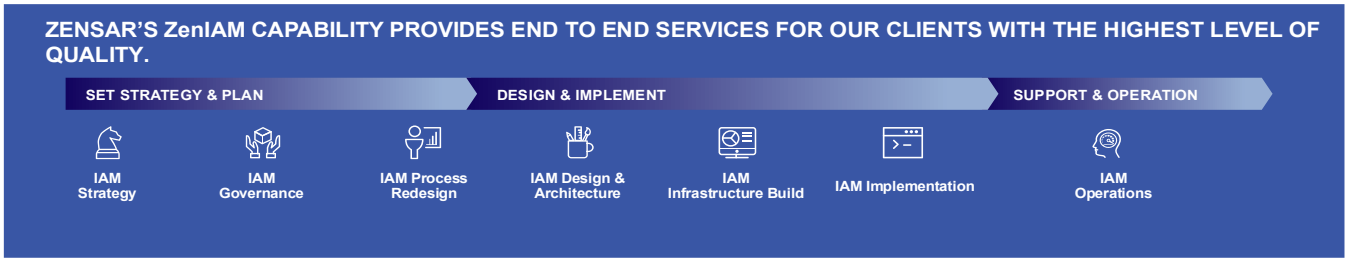
- Over 15 years of IAM experience
- IAM expertise from strategy through implementation to operations

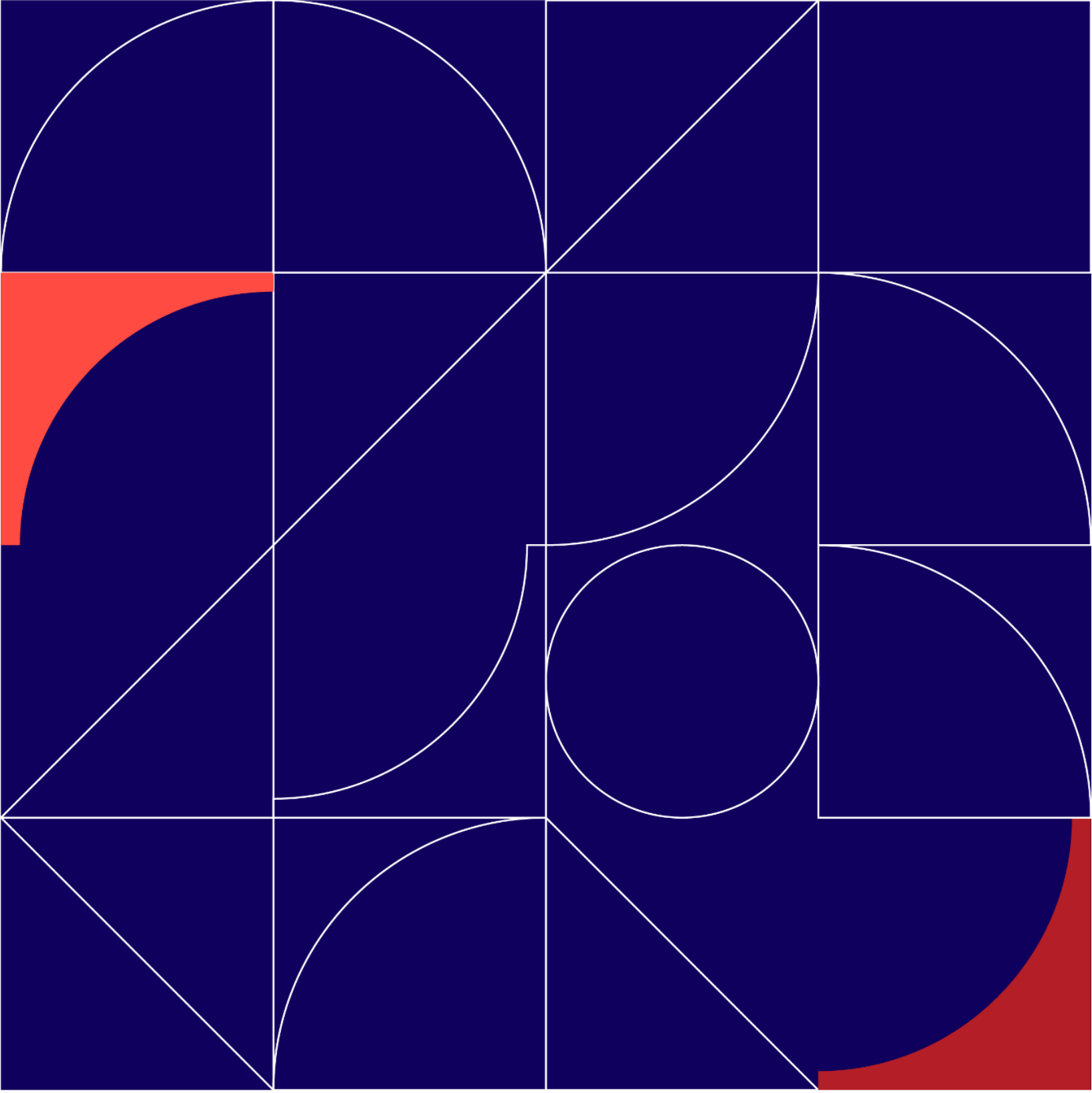
CULTURE OF NON-STOP INNOVATION

- Accelerates R&D and allows us to focus on innovating today, while anticipating tomorrow's threats and opportunities
- Asset development

ACCELERATORS AND FRAMEWORS

- Modular and scalable platforms to meet your cybersecurity objectives
- Customized change management with in-depth understanding of all components required to ensure successful deliveries of security projects





We conceptualize, build and manage digital products through experience design, data engineering and advanced analytics for over 130 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,000+ associates work across 33 locations, including San Jose, Seattle, Princeton, Cape Town, London, Singapore and Mexico City.

For more information please contact: **marketing@zensar.com** | **www.zensar.com**

An RPG Company