



SATYA TECHNOLOGIES
We Believe In Solutions

CAPABILITY PORTFOLIO · 2026 EDITION

One Partner for Cloud, Code & Cyber Resilience

A consolidated capability portfolio spanning Cloud Platform Engineering, Full-stack Software delivery, DevOps, on-premise Infrastructure, and Cybersecurity assurance built to give one accountable team the full mandate, end to end.

PREPARED FOR

Satya Technologies

DATE

22 June 2026

VERSION

1.0

Kolkata, India ♦ +91 89815 39687 ♦ info@satyatechnologies.in ♦ satyatechnologies.in

CONTENTS

What's Inside This Portfolio

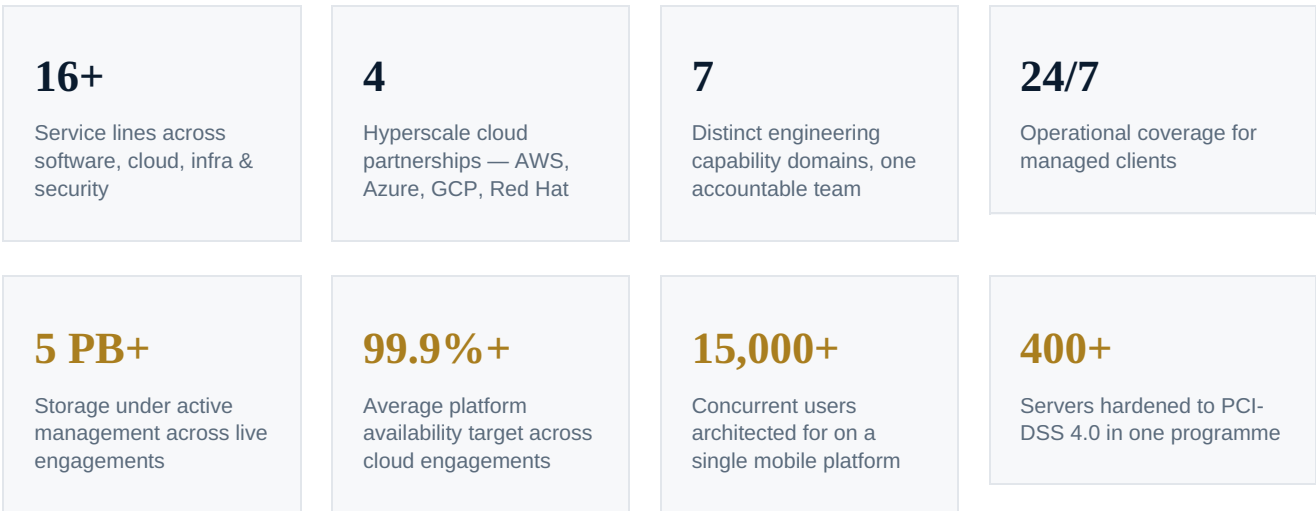
	01 About Satya Technologies Who we are, and the numbers behind the work	03
	02 Why Partner With Us Four commitments, and what else sets us apart	04
	03 Capability Map Software, cloud, DevOps, infrastructure, security & managed ops	05–06
	04 Technology & Partner Ecosystem Platforms and vendors we build and certify on	07
	05 Proven Engagements Case studies across finance, healthcare, media, SaaS & manufacturing	08–09
	06 Results That Speak Outcome metrics drawn from recent delivery	10
	07 How We Deliver Our six-phase engagement model	11
	08 Security, Compliance & Governance Frameworks we test against and help you reach	12
	09 Ways to Engage Commercial models suited to different needs	13
	10 Next Steps & Agreement How we kick off, and where to confirm	14

Built to Carry Full-Stack Responsibility



Satya Technologies designs, builds, and operates the technology stack modern enterprises run on — from custom software and mobile applications to multi-cloud platforms, on-premise data centres, and the security programmes that protect all of it. Rather than handing a project between specialist vendors, one accountable team carries it from architecture through to 24/7 operations. That continuity is why organisations in financial services, healthcare, manufacturing, media, and e-commerce keep extending our mandate, engagement after engagement.

BY THE NUMBERS DELIVERY FOOTPRINT



Figures are sourced from the engagements detailed in *Proven Engagements* (pages 08–09) and our active service portfolios.

"We believe in solutions, not silos fostering a culture of continuous learning, collaboration, and innovation so our clients get one team that can be trusted with the whole stack."

Four Commitments, One Standard



Innovation

We track emerging platforms — generative AI, bare-metal Kubernetes, Zero Trust — adopting them once they're production-ready, not just press-ready.

Deep Expertise

Every engagement is led by practitioners who have carried similar systems through production, not just through a proof of concept.

Client-Centric Delivery

Architecture decisions are recorded, justified, and reviewed with your team on a shared cadence — never a black box.

Quality Assured

Automated testing, solution checkers, and staged environments gate every release before it reaches production.

What Else Sets Us Apart

- ◆ **Security-first by default** — every cloud, infrastructure, and application engagement ships with least-privilege access, encryption at rest, and audit trails built in, not bolted on after a finding.
- ◆ **Automation over headcount** — Infrastructure-as-Code, GitOps, and policy-as-code reduce manual toil and the human error that comes with it, so quality doesn't depend on who's on call.
- ◆ **Vendor-neutral infrastructure options** — AWS, Azure, GCP, or fully on-premise bare-metal: we architect for your constraints and budget, not our preferred stack.
- ◆ **Transparent engineering** — architecture decision records, risk registers, and sprint velocity are shared, living artifacts your team can review at any time, not internal-only documents.
- ◆ **One throat to choke** — a single commercial and technical point of accountability across cloud, application, and security workstreams, so nothing falls into the gap between vendors.
- ◆ **24/7 follow-through** — delivery doesn't stop at go-live; managed operations, FinOps, and SRE coverage keep the platform healthy after launch.

Software, Cloud Platforms & DevOps



DOMAIN 01

Software & Product Engineering

- ◆ **Full-stack web applications** — React/TypeScript front-ends over .NET Core or Node.js APIs, with Azure Cognitive Services and OpenAI integrated for search, recommendations, and conversational features.
- ◆ **Native & cross-platform mobile** — Android architecture in Kotlin/Jetpack Compose built for 15,000+ concurrent users, plus cross-platform delivery via Flutter and React Native.
- ◆ **Enterprise applications** — Dynamics 365 (Sales, Field Service, Customer Service) and Power Platform (Power Apps, Power Automate, Power BI, Power Pages) on a governed Dataverse model with ERP integration patterns.

DOMAIN 02

Cloud Platform Engineering

- ◆ **AWS administration** across seven domains — compute, identity & federation, serverless and container hosting (EKS/Lambda/API Gateway), storage, and VPC networking — governed to the Well-Architected Framework.
- ◆ **Azure administration** across six domains — VM/App Service infrastructure, Entra ID & Conditional Access, AKS, Azure Monitor/Log Analytics, and Site Recovery-based DR.
- ◆ **Multi-cloud & migration advisory** — cloud-native modernisation, multi-cloud workload placement, and migrations executed with minimal downtime.

DOMAIN 03

DevOps & Site Reliability Engineering

- ◆ **CI/CD pipeline engineering** — Jenkins, GitHub Actions, Azure DevOps, and ArgoCD across Dev → SI/UAT → Production with automated quality gates.
- ◆ **Infrastructure-as-Code** — Terraform, Ansible, AWS CDK, and Bicep for reproducible, drift-detected environments.
- ◆ **Container & platform operations** — Kubernetes, OpenShift, and EKS/AKS cluster lifecycle management with GitOps delivery and policy enforcement (OPA/Gatekeeper, Kyverno).
- ◆ **Observability engineering** — Datadog, Prometheus/Grafana, CloudWatch, and Azure Monitor, tuned for signal over noise.

Infrastructure, Security & Managed Operations



DOMAIN 04

On-Premise & Bare-Metal Infrastructure

- ◆ **Hyperconverged private cloud** — Proxmox VE and Ceph storage fabrics delivering cloud economics on owned hardware, with 5 PB+ currently under active management.
- ◆ **Bare-metal Kubernetes** — kubeadm and Talos Linux clusters with Calico/Cilium networking, MetalLB, and Rook-Ceph persistent storage.
- ◆ **Enterprise self-hosted services** — Keycloak IAM, Kafka/RabbitMQ messaging, and HA PostgreSQL/MySQL/MongoDB for teams with data-residency or vendor-independence requirements.

DOMAIN 05

Cybersecurity & Assurance

- ◆ **Vulnerability Assessment & Penetration Testing** — network, web application, API, and cloud-configuration testing mapped to OWASP Top 10/WSTG, CVSS v3.1, and MITRE ATT&CK.
- ◆ **Privilege-escalation-focused application testing** — black-box testing of authentication, authorisation, session management, and business-logic abuse, with proof-of-concept evidence for every finding.
- ◆ **Security operations support** — Defender XDR triage, Vectra AI network detection, phishing response, and a three-horizon roadmap from immediate remediation to ISO 27001-aligned maturity.

DOMAIN 06

Cloud Operations & FinOps

- ◆ 24/7 production support across AWS, Azure, Linux & Windows estates.
- ◆ FinOps cost governance — rightsizing, Reserved Instances, zombie-resource clean-up.
- ◆ Patch & backup lifecycle ownership with RTO/RPO drills.

DOMAIN 07

Managed IT & Security Ops

- ◆ Entra ID, Conditional Access, Defender XDR & DLP management.
- ◆ Endpoint management — Intune/MEM enrolment and EDR strategy.
- ◆ Helpdesk & network operations with SLA-driven resolution.

ECOSYSTEM

Certified Across the Stack We Recommend



HYPERSCALE CLOUD PARTNERS

Amazon Web Services	Microsoft Azure	Google Cloud Platform	Red Hat
---------------------	-----------------	-----------------------	---------

SECURITY & NETWORKING PARTNERS

Cisco	Fortinet	Sophos	Palo Alto Networks	Check Point	CrowdStrike
Vectra AI					

INFRASTRUCTURE & BACKUP PARTNERS

HPE	Lenovo	Dell	Commvault	Veeam	Proxmox
-----	--------	------	-----------	-------	---------

DATA, MESSAGING & AI

OpenAI	Azure AI	Apache Kafka	RabbitMQ	PostgreSQL	MongoDB
--------	----------	--------------	----------	------------	---------

Core Technology Stack

FRONTEND	BACKEND	MOBILE	DATA	PLATFORM
React	.NET Core	Kotlin	PostgreSQL	Kubernetes
Angular	Node.js	Swift	MySQL	Docker
Vue.js	Python / Django	Flutter	MongoDB	Terraform
TypeScript	Java / Spring	React Native	Redis	GitHub Actions

Partnership status and certification levels are reviewed annually; current standing for any named partner above is confirmed on request as part of the discovery call.



Work That Speaks for Itself

FINTECH · TAX SERVICES

NRTAX — U.S. NRI Tax Platform

Greenfield, secure-by-design AWS platform with strict account-level data isolation and internal load balancing between the public tier and business logic.

Auto-scaled through peak tax season with zero manual intervention

HEALTHCARE · CLINICAL PLATFORM

Full-Rebuild Cloud Migration

Migrated a large clinical platform from a regional cloud to AWS, with Terraform-managed infrastructure, CDN delivery, and HIPAA-aligned malware scanning on every upload.

Zero data-loss migration · Real-time SLA monitoring via Grafana

EDTECH · E-LEARNING

Cloud-Native Microservices Platform

OpenShift-on-AWS-EKS platform serving thousands of concurrent learners, with a self-hosted Harbor registry enforcing image signing and vulnerability scanning.

4-stage promotion pipeline · Centralised log-to-incident workflow

LIFE SCIENCES · ENTERPRISE

Lift-and-Shift Platform Migration

Migrated an enterprise property-management solution from on-premises OpenShift to AWS EKS using continuous database replication, under formal change control.

Zero unplanned downtime · Fully reproducible IaC build

FINTECH · PRIVATE CLOUD

Hyperconverged Proxmox Cluster

Replaced an ageing VMware estate with a 6-node Proxmox VE + Ceph cluster, migrating 120+ production VMs with zero data loss via custom Ansible playbooks.

Material licensing-cost reduction · Real-time Grafana/Ceph observability

WHY IT MATTERS

Breadth Without Hand-Offs

Across these engagements, the same team that designed the architecture stayed accountable through migration, hardening, and steady-state operations — no re-briefing a second vendor, no gaps in ownership.



Infrastructure, Security & Scale

MEDIA & BROADCASTING

Multi-Site Ceph Storage Fabric

Geo-distributed, stretch-mode Ceph cluster across three data centres serving as a unified S3-compatible media repository, replacing SAN arrays and siloed NAS.

65% SAN/NAS cost reduction · <90s cross-site failover · 11-nines durability

SAAS · DEVOPS PLATFORM

Bare-Metal Kubernetes Platform

GitOps-driven, 30-node Talos Linux Kubernetes platform on Proxmox, giving engineering teams self-service provisioning with policy-as-code guardrails.

30+ deploys/day · <4-min provisioning · 40% lower cost than equivalent cloud

PAYMENTS · COMPLIANCE

PCI-DSS Hardening Programme

Remediated a 400-server Ubuntu/RHEL estate to PCI-DSS 4.0, automating CIS Level-2 baselines and continuous compliance drift detection.

0 critical audit findings · MTTD cut from 4 hours to 8 minutes

MANUFACTURING · ENTERPRISE APPS

CRM & Field Service Transformation

Dynamics 365 + Power Platform programme unifying sales, field service, and warranty on a SAP-integrated Dataverse model, with a 180-partner dealer portal.

Built toward an 80%+ field-service SLA-breach reduction target

Additional engagements on file span high-concurrency mobile architecture (15,000+ concurrent users), e-commerce disaster-recovery transformation (RTO cut from 8+ hours to 12 minutes), and web/network penetration testing for organisations preparing for ISO 27001 or PCI-DSS audits — references and detailed write-ups available on request.



Outcomes, Not Just Activity

65%

Storage infrastructure cost reduction following a Ceph fabric migration

97%

Faster mean-time-to-detect: 4 hours down to 8 minutes

12 min

Disaster-recovery RTO, down from over 8 hours on tape backup

0

Critical PCI-DSS audit findings across 400+ hardened servers

40%

Lower infrastructure cost vs. equivalent public cloud on bare-metal K8s

99.9%+

Average availability target maintained across cloud engagements

30+

Deployments shipped per day on GitOps-driven platforms

11 nines

Object-storage durability on a petabyte-scale Ceph fabric

How We Get There

- ◆ Every engagement starts with a measurable target — an SLA, a cost ceiling, a recovery time — agreed before the first sprint, not discovered at the end.
- ◆ Infrastructure-as-Code and automated testing remove the variability that turns a good architecture into an inconsistent one.
- ◆ Observability is built in from day one, so a metric like MTTD or SLA compliance is something we can show you live, not just report quarterly.



A Six-Phase Engagement Model

PHASE 01

Discovery

Requirements gathering, existing-system audit, and current-state analysis — so the plan reflects your environment, not a generic template.

TYPICAL DURATION: 1–2 WEEKS

PHASE 02

Architecture & Planning

Solution design, technology selection, and an architecture blueprint reviewed and signed off with your team before any build begins.

TYPICAL DURATION: 2–3 WEEKS

PHASE 03

Foundation & Build

Shared libraries, security framework, CI/CD pipeline, and core environments stood up — the scaffolding everything else is built on.

TYPICAL DURATION: 3–4 WEEKS

PHASE 04

Integration & Test

Feature delivery, integration testing, and security validation run continuously, with automated gates between every environment.

TYPICAL DURATION: ONGOING, SPRINT-BASED

PHASE 05

Deploy & Go-Live

Performance testing, load testing, and hardening ahead of a controlled production cut-over with a documented rollback plan.

TYPICAL DURATION: 1–2 WEEKS

PHASE 06

Hypercare & Optimise

Elevated monitoring immediately after launch, followed by knowledge transfer and a transition into ongoing managed operations.

TYPICAL DURATION: 2 WEEKS, THEN STEADY STATE

Held to Frameworks, Not Just Promises

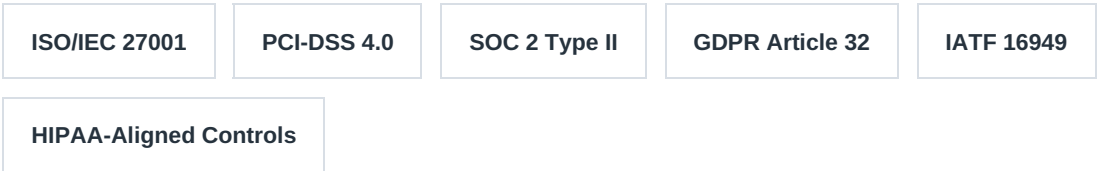


Security is not a separate line item we add at the end — it's the default condition of every engagement. Our testing methodology and operating model are mapped to the same frameworks your auditors and regulators will use to judge the outcome.

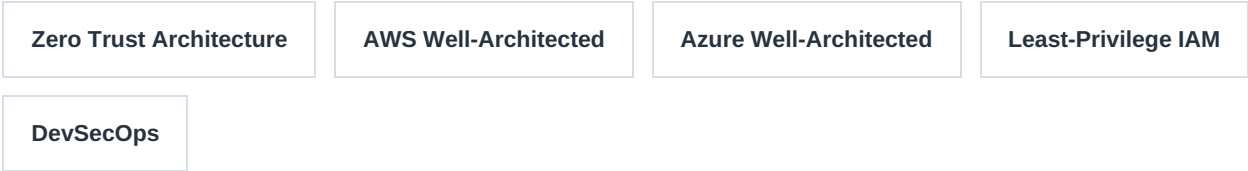
TESTING & ASSESSMENT STANDARDS



COMPLIANCE & CERTIFICATION TARGETS



ARCHITECTURE & OPERATING PRINCIPLES



What This Looks Like in Practice

- ◆ Every finding from a security assessment is delivered with a CVSS score, proof of concept, and remediation guidance — never a raw scanner export.
- ◆ Managed solutions, audit trails, and column-level security are standard on enterprise application builds, not optional add-ons.
- ◆ A three-horizon remediation roadmap — immediate, hardening, transformation — turns assessment findings into a budget-ready plan your board can approve.

A Commercial Model That Fits the Need



OPTION 01

Project-Based Delivery

Fixed-scope build with milestone billing — ideal for a defined platform, migration, or application build with a clear finish line.

OPTION 02

Managed Services Retainer

24/7 operate-and-optimize coverage across cloud, infrastructure, or security — billed monthly, scoped to your SLA.

OPTION 03

Dedicated Engineering Pod

A staff-augmented team embedded in your sprint cadence for ongoing product development, reporting into your roadmap.

OPTION 04

Security Assessment Sprint

A scoped 2–4 week VAPT or compliance-readiness engagement, ending in a board-ready report and remediation roadmap.

Most clients start with one option and expand into others as trust builds — a Security Assessment Sprint, for example, often becomes the entry point to a longer Managed Services relationship once findings are remediated.

Three Steps to Kick-Off



1

Discovery call

45–60 minutes to align on scope, constraints, and success metrics.

2

Tailored proposal & SOW

Scope, pricing, timeline, and team composition delivered within 5 business days.

3

Kick-off

Phase 1 Discovery begins within two weeks of signature.

This portfolio forms the basis for a tailored Statement of Work. To proceed, confirm your interest below or contact us directly to schedule your discovery call — whichever is easier for your team.

READY WHEN YOU ARE

Get in touch to schedule your discovery call

+91 89815 39687 | +91 79800 13007 · info@satyatechnologies.in · satyatechnologies.in

This document is commercially sensitive and prepared for the named recipient. It does not constitute a binding offer; a binding Statement of Work follows discovery.



Thank you for the opportunity to be considered as your engineering partner. We're ready when you are.

3/4, 75C, Park Street, 3rd Floor, Kamdhenu Building, Kolkata – 700016
+91 89815 39687 | +91 79800 13007 | info@satyatechnologies.in
satyatechnologies.in | linkedin.com/company/satya-technologies-cyber-security