Ayush Pandey

Cloud Solutions Architect and Team Lead | Azure, Microsoft 365, Security, Data, DevOps and AI

Bengaluru, India | zeroday3301@outlook.com | linkedin.com/in/ayush-pandey-zeroday

PROFESSIONAL SUMMARY

Cloud Solutions Architect with 5+ years designing, automating and securing Azure, Microsoft 365, AWS and Google Cloud environments for US banks, financial firms, healthcare providers, law firms and hospitality customers, across 300+ customer projects. I take engagements from the first technical call through scoping, SOW, costing and architecture to delivery and handover, and lead teams of engineers on projects. Reusable designs for AKS platforms, lakehouse data platforms, landing zones, migration with disaster recovery, Zero Trust identity, Purview data protection and AI security, mapped to HIPAA, SOC 2, ISO 27001, GDPR and NIST AI RMF, have served 5+ customers. Planned cloud architecture for 80+ customers and onboarded 50+ through Azure Lighthouse, GDAP and standard landing zones. Cut deployment time by 60% with infrastructure as code, onboarding and admin effort by about 30%, and customer cloud and licensing cost by about 40%.

CORE COMPETENCIES

Azure architecture and landing zones | AKS and containers | Data platforms | Migration and disaster recovery | Hybrid and multi-cloud networking | Zero Trust and identity security | Microsoft 365 and Purview | Sentinel and Defender | Infrastructure as code and DevOps | SRE and FinOps | AI agents and AI security | HIPAA, SOC 2, ISO 27001, GDPR | Team leadership and client delivery

PROFESSIONAL EXPERIENCE

Cloud Solutions Architect and Team Lead | Forte Technologies (formerly CloudScale365) | Delaware, USA | Jan 2024 to Present

Managed services provider for US clients in banking, financial services, healthcare, legal and hospitality. Remote from Bengaluru.

- Lead teams of engineers on projects: work allocation, peer review, escalations, client communication and coordination with networking, security and application teams.
- Own client engagements end to end: technical discovery, scoping, SOW, cost and engineering-hour estimates, roadmaps, target architecture, build, review and handover. Produced high-level designs, low-level designs and architecture decision records.
- Planned cloud architecture for 80+ customers and onboarded 50+ onto one managed platform with Azure Lighthouse, GDAP, landing zones, identity and network design, security baselines and monitoring. Cut deployment time by 60% and onboarding and admin effort by about 30%.
- Built reusable infrastructure as code with Terraform, Bicep and ARM and Azure DevOps pipelines, including policy checks on pull requests and drift detection. Automated tenant onboarding, GDAP consent and daily identity and device change reporting with PowerShell, Microsoft Graph, Logic Apps and Azure Automation.
- Designed and run AKS platforms: private clusters in hub and spoke with Azure Firewall egress and private endpoints, separate dev, test and prod environments, namespace isolation per customer with Entra group RBAC, Helm, ingress, autoscaling, workload identity, Key Vault secrets, Defender for Containers, Prometheus and Grafana monitoring and planned upgrades.
- Built lakehouse data platforms for finance and healthcare customers: ADLS Gen2 bronze, silver and gold zones with Databricks, Azure Data Factory pipelines from on-premises SQL, files and SaaS sources, private endpoints, RBAC and ACLs, Purview classification, and Synapse and SQL serving Power BI.
- Planned and ran wave-based migrations with dependency mapping, Site Recovery cutovers, tested rollback and disaster recovery runbooks with RTO and RPO targets. Migrated domain controllers to Windows Server 2022 and 2025 and databases from SQL Server 2014 to 2022.
- Architected the network foundation: hub and spoke, inspected egress through Azure Firewall, Front Door with WAF, Virtual WAN, Private Link, ExpressRoute and DDoS Protection. Deployed and tuned Palo Alto, Fortinet, Check Point and Azure Firewall and rolled out Zero Trust network access.
- Redesigned identity for 100+ users on Zero Trust principles: Conditional Access for admins, employees, guests and unmanaged devices, PIM and workload identity, released in report-only mode first with break-glass accounts excluded. Built joiner, mover and leaver processes with entitlement management and access reviews, and onboarded applications with SAML, OIDC and SCIM.
- Rolled out Microsoft Purview DLP, retention, sensitivity labels and auto-labeling for banking, financial-services and hospitality customers across Exchange, SharePoint, OneDrive and Teams, with PII and PHI discovery and eDiscovery.
- Led a HIPAA-compliant Microsoft 365 Copilot rollout for a cardiology practice with custom sensitive information types, a restricted PHI label, DLP, Conditional Access for unmanaged devices and extended audit and retention.
- Built detections in Microsoft Sentinel with KQL, MITRE ATT&CK mapping and Logic Apps playbooks, and cut incident response time by 40% through SIEM tuning. Ran vulnerability management with Tenable and Wiz, Defender for Cloud

posture reviews and SOC 2, ISO 27001 and HIPAA control mappings.
- Ran a cost and FinOps program (right-sizing, tagging, budgets, reservations and reporting) that cut customer cloud and licensing cost by about 40%, and built a CI/CD and SRE platform with SLOs, on-call and post-incident RCAs.
- Led Claude Enterprise and Microsoft 365 Copilot adoption inside the company aligned to NIST AI RMF, delivered AI security training, and built Azure OpenAI, AI Foundry, RAG and agent applications.
- Secured Google Cloud environments with least-privilege IAM, VPC segmentation, Security Command Center, Cloud Armor and VPC Service Controls, with workloads on GKE and Cloud Run.

Senior Cloud Engineer | Forte Technologies (CloudScale365) | Delaware, USA | May 2023 to Dec 2023

- Migrated domain controllers from Windows Server 2008 and 2012 to 2022 without losing authentication service, moving FSMO roles, DNS, DHCP and Group Policy.
- Deployed Azure Virtual Desktop to production for 100+ users on FSLogix and Azure Files, managed with Intune and Conditional Access.
- Rolled out OneDrive Known Folder Redirection through Group Policy, planned Azure subscription migrations and implemented Purview DLP for credit-card data for a financial-services client.

Senior Cloud Engineer (Project Lead) | IFI Techsolutions | India | Apr 2022 to Apr 2023

Microsoft partner serving technology, manufacturing, financial services, education, healthcare and construction clients in India and the UAE.

- Led projects through scope, cost estimation, architecture, implementation and closeout, and mentored junior engineers.
- Redesigned landing zones for a technology services enterprise and an investment firm with Azure Policy initiatives mapped to ISO 27001, HIPAA, GDPR and SOC 2. Designed a new ExpressRoute circuit, moved tape data with Azure Data Box and replaced Azure Firewall with Check Point.
- Built an AWS replica of a software company's Azure environment as its disaster recovery site with Terraform, and extended ExpressRoute to AWS Direct Connect and Google Cloud Interconnect with BGP route policy and tested failover.
- Orchestrated containerised workloads on AKS with Helm, ingress and Azure Container Registry through Azure DevOps release pipelines, and delivered a Data Factory, Databricks and Data Lake Gen2 platform for an investment firm.
- Led incident response for an educational institute after a breach: isolation, evidence preservation, restore from backup, Defender for Cloud, WAF log analysis and a Zero Trust rebuild.
- Delivered SAP migration to Azure with AVD for Tally and SAP disaster recovery, a China-region App Service behind Application Gateway with WAF, and file server replacement with Azure File Sync.

Cloud Engineer | IFI Techsolutions | India | Mar 2021 to Mar 2022

- Assessed and migrated workloads from on-premises, AWS, Google Cloud and private cloud to Azure across four client projects with VPN connectivity.
- Automated Azure deployments with Terraform, Bicep and ARM templates, cutting deployment time by 60%, and built disaster recovery plans with Azure Site Recovery.

KEY PROJECTS

- **Multi-tenant onboarding with Azure Lighthouse (Forte).** Architecture planned for 80+ customers and 50+ onboarded on one repeatable pattern with delegated access, security baselines, automated GDAP consent and daily identity and device reporting.
- **Secure Azure landing zones (IFI and Forte).** Management groups, hub and spoke, central logging, Azure Policy initiatives mapped to ISO 27001, HIPAA, GDPR and SOC 2, Key Vault, Defender for Cloud and Azure Arc, reused as the onboarding standard.
- **AKS platform for customer workloads (IFI and Forte).** Private AKS in hub and spoke with Azure Firewall egress, dev, test and prod separation, per-customer namespaces with Entra RBAC, Helm and GitOps delivery, Prometheus and Grafana. Reused across 5+ customers.
- **Lakehouse data platform (IFI and Forte).** ADLS Gen2 medallion zones with Databricks, ADF pipelines, private endpoints, Purview, and Synapse and SQL serving Power BI. Deployed as code and reused across 5+ customers.
- **Migration and disaster recovery programme (IFI and Forte).** Assessment, wave planning and Site Recovery cutovers from on-premises, AWS, Google Cloud and private cloud, with rollback, RTO and RPO targets, runbooks and tested failovers.
- **Multi-cloud hybrid networking (IFI).** ExpressRoute extended to AWS Direct Connect with Transit Gateway and to Google Cloud Interconnect, with BGP route policy, firewall zones, central logging and tested failover.
- **Infrastructure as code automation (IFI and Forte).** Reusable Terraform, Bicep and ARM with pipelines and policy checks on pull requests that block insecure changes and flag drift. Deployment time fell by 60%.
- **CI/CD and SRE platform (IFI and Forte).** Pipeline templates with approvals, branch policies, SLIs and SLOs, alerting, on-call, RCAs and SAST, dependency and container scanning.
- **Cost and FinOps programme (Forte).** Right-sizing, tagging, budgets and alerts, reservations and cost reporting across customers, cutting spend by about 40%.
- **Zero Trust identity architecture and Conditional Access (Forte).** Conditional Access, PIM, workload identity and segmentation designed as one model, staged in report-only mode, enforced without admin lockouts.
- **Identity lifecycle, SSO and governance (IFI and Forte).** Joiner, mover and leaver design, access reviews, SAML and OIDC onboarding, SCIM, B2B guest governance and ADFS migration to Entra ID.
- **Identity attack detection and response (Forte).** KQL detections and playbooks for password spray, suspicious OAuth

consent, privilege escalation and account compromise, with analyst approval before disruptive actions.

- **Purview DLP, retention and oversharing reduction (Forte).** DLP and retention in production across banking, financial services and hospitality, with PII and PHI discovery and eDiscovery.
- **HIPAA-compliant Microsoft 365 Copilot rollout (Forte).** Custom sensitive information types, restricted PHI label, auto-labeling, DLP and Conditional Access. Copilot enabled with PHI protected and blocked from unmanaged devices.
- **Microsoft Sentinel detection engineering and SOAR (IFI and Forte).** KQL hunting, analytics rules mapped to MITRE ATT&CK, Logic Apps playbooks and alert tuning to cut false positives.
- **End-to-end security incident response (IFI and Forte).** Account compromise, malware, ransomware and business email compromise handled from first alert to closure, each closed with a new Conditional Access or detection rule and a client report.
- **ExpressRoute and multi-vendor firewalls (IFI and Forte).** Firewalls with forced routing over ExpressRoute, circuit and bandwidth upgrade, Azure Firewall policy with IDPS and TLS inspection and NSG flow log analysis.
- **AI governance and agent threat modeling (Forte).** Claude Enterprise and Copilot adoption aligned to NIST AI RMF, with threat models for Copilot Studio and internal agents covering prompt injection, excessive permissions and unsafe tool calls.
- **Azure OpenAI, AI Foundry and RAG applications (IFI and Forte).** Vector search, prompt evaluation, Azure AI Content Safety, and agent actions through Semantic Kernel and Power Automate.
- **CrushBank enterprise AI agent with MCP (Forte, team contributor).** Ticketing, documentation, chat and source control behind one MCP search with source permissions enforced at query time.
- **Legacy platform modernisation (Forte).** SQL Server 2014 to 2022 migration with ODBC and SFTP restored, file servers moved to Azure Files, and an Azure workload moved to a private cloud with tested rollback.

TECHNICAL SKILLS

Cloud and architecture: Azure landing zones, Cloud Adoption Framework, Well-Architected reviews, hub and spoke, Azure Policy, Azure Lighthouse, GDAP, Azure Arc, Azure Virtual Desktop, Site Recovery, FinOps, AWS (EC2, S3, VPC, IAM, Direct Connect, Transit Gateway), Google Cloud (VPC, IAM, Security Command Center, Cloud Armor, GKE, Cloud Run, Cloud Interconnect)

Containers and data: AKS, Helm, GitOps, Azure Container Registry, Docker, Data Factory, Databricks, Data Lake Gen2, Synapse, Azure SQL, SQL Managed Instance, Power BI

DevOps and automation: Terraform, Bicep, ARM, Azure DevOps, GitHub, PowerShell, Python, Microsoft Graph, Azure Automation, Logic Apps, policy as code, SLIs and SLOs, RCA

Networking: ExpressRoute, VPN Gateway, Virtual WAN, BGP, Azure Firewall, Front Door, Application Gateway, WAF, DDoS Protection, Private Link, Palo Alto, Fortinet, Check Point, Cisco, Zscaler, Cloudflare Zero Trust

Identity and access: Entra ID, Conditional Access, MFA, PIM, access reviews, entitlement management, Entra ID Protection, B2B, Entra Connect, ADFS migration, SAML, OIDC, SCIM, Active Directory, Group Policy

Microsoft 365 and data protection: Exchange Online, SharePoint, Teams, Intune, Autopilot, Microsoft Purview (DLP, sensitivity labels, auto-labeling, retention, Insider Risk Management, eDiscovery, DSPM for AI), Microsoft 365 Copilot administration, HIPAA, GLBA, SOC 2, ISO 27001, NIST CSF, NIST AI RMF, GDPR

Security operations: Microsoft Sentinel, KQL, Defender for Cloud, Defender for Endpoint, Defender XDR, Tenable, Wiz, SentinelOne, Huntress, threat hunting, MITRE ATT&CK, SIEM and SOAR, incident response

AI engineering and security: Azure OpenAI, AI Foundry, AI Search, Copilot Studio, Semantic Kernel, LangChain, Model Context Protocol, RAG, prompt injection testing, agent threat modeling, responsible AI

CERTIFICATIONS

- **Microsoft:** Azure Solutions Architect Expert (AZ-305), Azure Administrator (AZ-104), Azure Network Engineer (AZ-700), Cloud and AI Security Engineer (SC-500), Identity and Access Administrator (SC-300), Azure Virtual Desktop Specialty (AZ-140), AI Services Administrator (AB-650), AI Transformation Leader (AB-731), Copilot and Agent Administration (AB-900), Microsoft Certified Trainer, and the Azure, Azure Data, Microsoft 365, and Security, Compliance and Identity Fundamentals certifications.
- **Other:** ICSI Certified Network Security Specialist (CNSS), Oracle Agentic AI Foundations Associate (1Z0-1157), Google Cloud Business Professional Accreditation, Managing Security in Google Cloud Platform, Essential Google Cloud Infrastructure, Google Cloud Platform Fundamentals, IBM Cloud, Introduction to Cybersecurity (Cisco), Cyber Security in M&A and Cloud and Disaster Recovery (EC-Council).

EDUCATION

MCA, IIIT Ranchi in collaboration with IIT Patna, 2026 to 2028 (in progress)

BCA, Devi Ahilya Vishwavidyalaya, Indore, 2017 to 2020