David Cox

Principal Cloud Architect

LinkedIn | davidjcox.com | Canton, MI - Open to Remote

Summary

Cloud Architect designing and delivering enterprise cloud platforms across Azure (primary), AWS, and multi-cloud for regulated financial-services and healthcare organizations. Specializes in Cloud Adoption Framework landing zones, hub-spoke and Virtual WAN / ExpressRoute network design, identity and Zero Trust governance, and reusable Bicep automation - pairing hands-on infrastructure-as-code with architecture governance through Azure Policy guardrails, design-review boards, and standardized intake. Proven at scale across a 440-VM data-center exit, a 27,336-user production migration, multi-region BCDR designs with sub-5-minute failover, and governed Azure AI Foundry platforms, while sustaining FFIEC, SOX, and HIPAA compliance.

Skills

Cloud Platform & Networking: Azure, AWS, Cloud Adoption Framework, Well-Architected, Landing Zones, Hub-Spoke, vWAN, ExpressRoute, BGP, Azure Firewall / NGFW, Private Endpoints / DNS, AVD, Cloud Migration & Modernization, Hybrid & Multi-Cloud
Infrastructure as Code & DevOps: Bicep, Deployment Stacks, .NET, C#, PowerShell, Python, Azure DevOps, Git, CI/CD, Container Apps, OpenShift (ARO)
Data & AI: Azure AI Foundry, Azure OpenAI, RAG / Vector Search, AI Landing Zones, API Management, Managed Identity, Private Endpoints
Architecture, Security & Governance: Architecture Governance, ITIL Service Management, Design Reviews, Reusable IP, Azure Policy, RBAC, PIM, Zero Trust, DR / BCDR, FFIEC, SOX, HIPAA, CIS Benchmarks, NIST CSF

Experience

Principal Solutions Architect, Resolve Tech Solutions - Remote April 2024 - Present
Projects: PAM Health (National Post-Acute Healthcare Network), EverBank (Financial Services)

- Cut new Azure landing zone provisioning from 3-14 days of drift-prone ClickOps to within 1-2 hours with zero drift by engineering 65 reusable, Policy-governed landing zones from hundreds of Bicep modules - the backbone of RTS's managed services, now spanning several hundred subscriptions at 14 enterprise clients.
- Architected Rackspace-to-Azure migration for a national healthcare network encompassing 440 VMs, 13 SQL clusters, and multi-region ExpressRoute connectivity with 4-week single cutover supporting 27,336 users, delivering approximately $2.4M annual MSP cost savings.
- Designed secure hub-and-spoke Azure Virtual WAN connectivity with Palo Alto Cloud NGFW, dual ExpressRoute circuits per hub, and routing-intent traffic inspection, cutting over 8 live production spokes after-hours with no business interruption.
- Built a 3-tier Azure AI Foundry platform (Light / Standard / Confidential) with private-endpoint-only isolation, egress lockdown, data classification, and customer-managed keys, enabling enterprise AI adoption under strict banking and data-residency rules.
- Raised landing zone compliance to 95% by implementing enterprise governance via 7 management-group-scoped Azure Policy initiatives (tagging, region, SKU, RBAC guardrails) on an audit-first, soak, then Deny-enforce cadence.
- Architected 27,336 user AD forest migration over 9 months replacing ADFS federation with Entra ID Password Hash Sync via net-new hybrid forest design, achieving zero-downtime domain cutover using native ADMT 3.2 and Password Export Server, without incumbent cooperation.
- Reduced standing privileged accounts from 165 to 2 break-glass by architecting a PIM and PIM for Groups strategy with CISO-level approval gates, tiered role activations (4-10 hours), group-based assignments, and Splunk audit logging.

- Cut Azure sandbox provisioning from roughly 3 months and multiple tickets to under an hour by building a self-service, Git-PR platform that auto-provisions and auto-deletes environments; adoption grew organically from 3 to 33 teams across 4 organizations.
- Raised telemetry coverage to 95% and cut MTTD/MTTR 25% with centralized Well-Architected Azure observability and FinOps - SIEM-first Log Analytics streaming security logs to Splunk via Event Hub, diagnostic settings covering 140 resource types, and per-subscription budgets.
- Cut architecture decision-cycle time 60% and contributor onboarding from 6 weeks to an 8-12 business-day ramp by architecting a GitHub Enterprise docs-as-code repository (CODEOWNERS governance, 60 ADRs, reference architecture catalog spanning identity, networking, security, and AI) adopted across 18 engineering and delivery teams.
- Cut expected recovery time 60% for high-tier treasury workloads by designing an end-to-end DR architecture using ASR, region failover patterns, CosmosDB replication models, and storage-account redundancy, enabling non-disruptive quarterly failover tests.
- Designed API Management gateway architecture for AI workloads with App Gateway (WAF) to internal APIM to private backends handling ~3M API calls/month via JWT validation, token budgets, rate limiting, managed identity authentication.
- Designed Azure Arc hybrid identity model enabling on-prem C# applications to authenticate to Azure AI Foundry using managed identities instead of client secrets, establishing secretless patterns for regulated AI workloads.
- Designed Private Link architecture connecting 10+ Azure VNets to 3 Snowflake accounts with Private DNS Resolver integration and centralized DNS zone linking across hub-spoke topology, eliminating public data platform exposure.
- Conducted architectural assessments for regulated clients against HIPAA, GLBA, and FFIEC frameworks, producing gap matrices and modernization plans that accelerated board approval for cloud programs by 2 quarters.
- Consolidated 40 Conditional Access policies to 26, eliminating legacy authentication bypasses and overlapping rules, achieving 100% MFA enforcement across 15+ critical SaaS applications for a regulated financial services organization.
- Remediated 40+ legacy Conditional Access policies by deploying Maester automated testing (1,632+ test cases) across CISA and CIS benchmarks with user impact analysis covering 2,273 accounts at a regulated financial services organization.
- Created a structured approach to third party access using Entra B2B, Conditional Access, limited egress, private endpoints and user risk evaluation lowering vendor assessment findings and strengthening SOC reporting positions for financial audit.
- Redesigned Technology Impact Assessment from binary change-detection to risk-routing decision engine with tier-aware pattern attestation, projecting 60-70% reduction in Architecture review overhead.
- Cut client-estate operational cost 25-35% and improved session reliability from 98% to 99.95% by designing AVD landing patterns replacing legacy Citrix and RDS - standardizing host pools, identity, FSLogix, imaging, and networking to turn multi-week custom builds into a repeatable 7-10 day delivery model.
- Cut workload approval time from weeks to 3-5 days by developing a cloud adoption platform blueprint with documented network controls, identity constructs, key management, backup expectations, and data handling rules, sharply reducing shadow cloud deployments.
- Cut SLA escalation disputes 76% and lifted monthly service-reporting coverage from 61% to 98% across 14 managed-service contracts by creating customer-facing service-tier models delineating Microsoft-platform, MSP-controlled, carrier, and customer-owned responsibilities with explicit SLOs, XLAs, and exclusions.
- Sustained 99.97% hybrid-connectivity availability across 18 ExpressRoute circuits and 7 data centers estate-wide by engineering dual circuits, active-active BGP, and BFD, cutting failover convergence from 7 minutes to 42 seconds and passing 24 consecutive failover tests without customer impact.
- Reduced congestion-related performance incidents 63% and cut RDP TCP fallback from 21% to 5% across nearly 400 sites and 124 SD-WAN edges by implementing QoS traffic classes prioritizing real-time AVD, Teams media, and interactive AI inference over bulk background traffic, holding p95 AVD RTT under 115 ms at peak.

- Built a pre production validation framework using synthetic transactions across AVD login, private endpoint reachability, app layer health and ExpressRoute routing confirming changes before release and reducing post change rollbacks from 22% to 3%.
- Built C#/.NET 8 diagnostic CLI automating 5 troubleshooting checks for Global Secure Access BYOD enrollment, using Microsoft Graph to classify root causes across Conditional Access, Defender, and DNS layers for a regulated financial services organization.
- Designed a remote branch edge rollout using FortiGate SDWAN, IPsec failover, and centralized logging with operational runbooks enabling legacy MSP offboarding and decreasing mean time to recover WAN incidents from 4 hours to 1 hour.
- Designed Azure DNS migration strategy for 47+ public zones with zero-downtime cutover via 24-48 hour TTL pre-staging and 100% zone validation protocols.
- Built a capacity and availability model for AVD session hosts using Azure Monitor, host pool utilization metrics and Log Analytics queries that projected weekly scale requirements and reduced concurrency related escalations from 17 per month to 2 per month.
- Performed a full Public IP rationalization for a healthcare cloud migration identifying and mapping cloud egress, inbound DDoS protected ranges, SNAT pools and firewall tiering which eliminated overlapping CIDRs and reduced security exception reviews by 65%.
- Published support playbooks for AVD, ExpressRoute, Firewall, Virtual WAN, Defender and Azure AD enabling infrastructure teams to close incidents without architectural intervention lowering L3 dependency by 70% within 2 quarters.
- Built a hardened access model for healthcare AVD workloads using Entra ID risk signals, Defender for Endpoint device checks, Intune compliance rules and outbound internet restrictions that reduced malware ingress events to zero during the first 120 days.
- Architected HSM-backed 2-tier PKI (offline root CA, Azure issuing CA, RSA 4096-bit) enabling certificate-based authentication across 49+ domains and issuing 50,000+ certificates in month one during forest migration.
- Built PamVpn, a full-stack .NET 10 service and portal (14.5K lines of C#, 4 projects, 28 Bicep files) automating the client-certificate lifecycle for an Azure vWAN Point-to-Site VPN - AD CS enrollment, Entra ID auth, MFA via Application Proxy, and instant revoke-to-audit offboarding.

Senior Network Architect, Sterling Bank & Trust - Southfield, MI December 2019 - April 2024
Reported to the CIO, owning enterprise architecture and IT strategy for a publicly traded regional bank (30 branches, 200+ employees) in a highly regulated environment; drove infrastructure modernization, cloud adoption, and security governance.

- Migrated 250 users from Citrix to AVD, improving uptime to 99.998% (from 98.9%), reducing latency 25% and capex 60% via hybrid architecture, CAF, vWAN hubs, BGP, IPSEC, FSLogix, App Attach, WinGIT, KQL, and ExpressRoute for COVID-era resilience.
- Designed BCDR strategy achieving sub-5-minute AVD failover via Azure Site Recovery with encrypted multi-region replication and automated failover, risk-assessing the solution and all SaaS, infrastructure, and cloud vendors against FedRAMP standards.
- Cut the severity-weighted confirmed incident rate 27% over 12 months (versus the prior 24-month baseline) by designing a Zero Trust Architecture spanning VeloCloud SDWAN, FortiGate NGFW, Entra ID (MFA/PIM/SSO/JIT), CrowdStrike, Azure Policy, CyberArk PAM, Intune, M365 E5, Defender for Cloud Apps, and Purview DLP.
- Improved bank's FFIEC Consumer Compliance rating from 5 to 2 by creating an architecture review board to confirm each proposed purchase or architecture meets corporate objectives prior to deployment and to validate the solution meets data governance, risk management, and regulatory compliance standards after deployment.
- Deployed unified endpoint security across 700+ endpoints using Intune MDM and CrowdStrike EDR, reducing penetration test findings from 28 to 1 medium by 2024.
- Enrolled 746 of 750 endpoints (99.5%) at 98.7% sustained policy compliance and cut zero-touch provisioning to under 30 minutes from unboxing to production-ready access by designing a 9-phase Intune MDM framework

(326 configuration files) spanning device compliance, Windows Update rings, Windows Hello, and multi-platform app deployment across Win32, iOS, and MDM.

- Eliminated user passwords with an Entra Authentication Methods policy reducing phishing and spray-attack surface by 80% using FIDO2 or Windows Hello for Business (WHfB), ADCS certificates, Cloud Kerberos trust, user and sign-in risk based conditional access policies to streamline user flows and raise security scores.
- Created a chatbot for intranet portal using Azure Files & AI Foundry, Container Apps, Cognitive Search, Python and Log Analytics, reducing ticket volume by 61% and saving $120K annually by handling 400 daily queries, auto-generating Freshservice tickets for escalations, and eliminating the need to staff service desk after hours.
- Replaced legacy 1GbE switches and end-of-life SAN with 100GbE spine/10-25GbE leaf and NetApp AFF, achieving 80x IOPS improvement and cutting network-related incidents 93%.
- Cut circuit failover from minutes to sub-15 seconds by enabling BGP BFD across hybrid ExpressRoute and SD-WAN connectivity with Azure Firewall Threat Intel, achieving clean routing-intent separation for on-prem and cloud domains.

Director of Information Technology LiquidVPN - San Juan, PR February 2017 - January 2020

- Overhauled LiquidVPN's website and redesigned user experiences across platforms (mobile, Windows, Mac), maintaining GDPR and PCI-DSS compliance while increasing quarterly sales by 35% via OAuth authentication, REST API publishing, and in-app payment gateway for efficient sign-ups.
- Cut infrastructure setup time from hours to minutes by automating deployments with Terraform and Ansible, standardizing configurations and nearly eliminating human error.
- Achieved a 20% reduction in operating expenses and improved service availability to over 99.9%, as measured by monthly OpEx reports and uptime dashboards, by migrating on-prem Active Directory to a multicloud, cloud-native architecture spanning AWS (EC2, RDS, S3, Route 53), Azure (Azure AD, RBAC, Front Door, Files, DNS, App Services, Cosmos DB), Google Cloud (Compute Engine, Cloud VPN, Docker), and Alibaba Cloud (ECS).
- Expanded global reach 35% and cut vendor onboarding 50% by localizing web/mobile into six languages and implementing vendor-management and DLP framework.

Lead Network Engineer and Founder LiquidVPN - Southfield, MI January 2012 - February 2017

Founded LiquidVPN as a startup and led all engineering and operations from inception through rapid growth and eventual acquisition. Managed product development, network infrastructure, and a global team for this consumer VPN SaaS provider.

- Launched B2C SaaS VPN to 300K users across 110 countries with 60% YoY growth via multi-cloud architecture, encryption, and Wired/CNET recognition.
- Built and led a 10-person engineering team, reducing project delivery timelines by 20% and lowering customer churn from 18% to 3% by implementing feedback loops, bug bounties, and a CI/CD pipeline.
- Achieved 99.99% uptime by devising a geo-redundant RADIUS solution replicated across four Azure regions, ensuring seamless load balancing and authentication for worldwide customers.
- Facilitated LiquidVPN acquisition, consolidating directory services, vendors, and accounts via phased migrations and domain trusts.

Education and Certificates

- **Microsoft Certified: Azure Network Engineer Associate** - AZ-700 January 2026
- **Microsoft Certified: Azure Virtual Desktop Specialty** - AZ-140 February 2025
- **Microsoft Certified: Azure Administrator Associate** - AZ-104 October 2024
- **Microsoft Certified: Azure AI Fundamentals** - AI-900 September 2024
- **Microsoft Certified: Azure Fundamentals** - AZ-900 September 2024
- **B.S. in Network and Information Technology** - Eastern Michigan University