# David Cox

apply@davidjcox.com | davidjcox.com

## Summary

Versatile Enterprise Architect with 20 years of experience leading large-scale infrastructure transformations across on-premises, hybrid, and multi-cloud environments. Skilled in finding highly available, cost-effective, scalable, and secure solutions that add measurable value to the technical landscape of the enterprise.

## Skills

**Infrastructure:** Physical, Virtual, Hybrid, SAN, and Cloud Network Design, Migrations, DR/BCP, and IaC
**Platforms:** Azure Cloud, AWS, M365, Intune, Azure Virtual Desktop (AVD), VMWare, AI Foundry, and Ivanti
**Security & Identity Management:** AD, Entra ID, FortiNet, Tenable, Nessus, CrowdStrike, Duo, Defender

## Experience

**Principal Solutions Architect,** Resolve Tech Solutions – Remote January 2025 – Present

- Designed an enterprise scale Azure landing zone for a regulated financial firm to enable secure multi region workloads through management groups, policy driven compliance, identity separation and centralized network hubs which reduced architectural review findings by 60 percent within 6 months
- Architected an Azure Virtual WAN with dual region secure hubs, ExpressRoute circuits, BGP routing domains and firewall policy segregation that delivered deterministic traffic flows and decreased incident driven changes by 45 percent within 3 months
- Created a standardized Intake and Architecture Review process for business owned technology which improved FFIEC governance alignment by defining intake tiers, decision authorities and mandatory artifacts resulting in a sustained 2 quarter reduction in compliance exceptions
- Implemented a Privileged Identity strategy for cloud and on premises assets using Entra ID PIM role activation, local admin removal and break glass validation which reduced privileged access durations by 85 percent and eliminated persistent administrator sessions
- Developed conditional access designs combining device trust, user risk and MFA enforcement that eliminated legacy password only access paths for financial analysts and operations users and increased cloud authentication posture scores from 62 to 91 within 90 days
- Led a modernization of enterprise VDI by consolidating Citrix and RDS workloads into Azure Virtual Desktop with FSLogix, compute galleries and profile container tuning that improved login times by 34 percent and cut annual licensing costs by 28 percent
- 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
- Constructed a distributed routing architecture using Virtual WAN and Route Tables with explicit spoke isolation, Optimized routing intent and ExpressRoute prefer rules delivering predictable north south and east west flows and reducing change windows by 40 percent
- Integrated Azure Firewall with Rule Collection Groups and DNAT and FQDN filtering to protect financial workloads during cloud migration while decreasing rule count by 52 percent through object based policies and application grouping
- Created an end to end DR architecture using ASR, region failover patterns, CosmosDB replication models and storage account redundancy that cut RTO targets from 24 hours to 1 hour for high tier treasury workloads and enabled non disruptive quarterly failover tests
- Developed a cloud adoption platform blueprint with documented network controls, identity constructs, key management, backup expectations and data handling rules which reduced shadow cloud deployments by 80 percent within 2 quarters

- Implemented Azure Policy with deny and deploy if not exist assignments across subscriptions to enforce encryption at rest, TLS versions, diagnostic settings and resource tagging achieving 97 percent resource compliance within 90 days of deployment
- Automated network and governance deployments using Bicep modules for Virtual WAN, routing, firewalls, private DNS and policy sets reducing environment bring up time from 6 weeks to 10 days during the initial Everbank cloud program phase
- Produced a comprehensive network segmentation plan for a healthcare enterprise migrating away from a managed service provider which defined hub design, spoke boundaries, privileged paths and inspection points reducing VLAN related outages by 70 percent after cutover
- 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
- Created a structured ExpressRoute migration approach for a multisite healthcare network including LOA CSA coordination, BGP community planning, preferred path logic, dual provider failover and firewall hairpin avoidance which decreased maintenance windows by 50 percent
- Designed a remote branch edge rollout leveraging 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
- 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 percent
- Established a KQL driven analytics pipeline to monitor AVD, ExpressRoute, Firewall, Defender and Entra events centralizing operational intelligence and reducing duplicate monitoring tooling requests during the program intake phase by 90 percent
- Developed a tiered Operations Model for financial cloud workloads defining Level 1 through Level 3 responsibilities, escalation paths, monitoring obligations, release processes and risk acceptance rules improving operational readiness scores from 58 to 95 prior to go live
- 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 percent to 3 percent
- Authored a multi year cloud cybersecurity roadmap for a regional bank aligning patching, workload identity, application control, network inspection, data loss prevention and incident response objectives with regulatory examination cycles to reduce audit preparation gaps
- Mapped FFIEC and GLBA control expectations to landing zone components including identity boundary, encryption, privileged access, segmentation and DR ensuring exam evidence traceability and minimizing remediation cycles during quarterly compliance reviews
- Coordinated the offboarding of a large healthcare MSP provider by defining Active Directory Federation Services AD FS domain takeover order, credential transition, firewall policy extraction, DNS delegation, management tunnel migration, ACL and SID to SID History mapping which enabled cutover in under 90 days
- Drove adoption of Infrastructure as Code practices for network and identity layers standardizing modules, enabling code reviews and defining pipeline expectations that removed manual configuration drift and decreased unplanned changes by 41 percent
- Provided board and executive level briefings for a financial institution summarizing cloud risks, connectivity posture, operational maturity and compliance coverage which accelerated program approvals and shortened procurement cycles by 35 percent
- Defined storage, database, identity and network landing patterns for new workloads entering Azure establishing alignment between product teams and security and reducing architectural churn and rework by 55 percent
- 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 percent within 2 quarters

- 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
- Linked cloud governance with procurement and contract language by defining mandatory telemetry, access logging, DR commitments and secure traffic patterns for SaaS integrations reducing onboarding cycles for regulated workloads by 30 percent

**Senior Network Architect,** Sterling Bank & Trust – Southfield, MI December 2021 – Present

- Improved bank's FFIEC Consumer Compliance rating from 5 to 2 by creating an architecture review board to review 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.
- 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.
- Migrated 250 Citrix VDI users and 300 Remote Desktop Services users to AVD, improving uptime from 98.9% to 99.998% reducing latency by 25% and annual capital expenditures by 60% using hybrid architecture, Azure's Cloud Adoption Framework (CAF), landing zones, management groups, and Nerdio Manager (NME) for administration, redundant vWAN hubs, ExpressRoute, BGP and failover IPSEC VPN for hybrid connectivity, Azure compute gallery, FSLogix, App Attach and WinGIT for application and profile management with Azure Monitor, ControlUp, and Kusto Query Language (KQL) driven AVD Insights addressing COVID-era demands and supply chain constraints.
- 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 Business Continuity & Disaster Recovery (BCDR) plan reducing RTO from 24 hours to 1 hour and monthly downtime from 5 minutes to 6 seconds, saving $840,000 in annual data center fees using a hybrid multi-region architecture with Azure Site Recovery, CosmosDB, Azure Files, and synchronous SAN replication allowing remote workforce access via Azure Virtual Desktop VDI and eliminating on-site DR facilities.
- Replaced legacy 1GbE data center switch architecture and end-of-life SAN with a 100GbE spine and 10/25GbE leaf switch architecture, and NetApp AFF all-flash SAN achieving an 80x improvement in IOPS while reducing network-related incidents by 93% laying the groundwork for data center virtualization.
- Virtualized the entire datacenter using CIS hardened images and adopting Microsoft Cloud Security Benchmark, Azure's Cloud Adoption & Well-Architected Frameworks to reduce its footprint and power consumption by 60% and improve server uptime from 98% to 99.9% leveraging the new datacenter switch architecture, High Available (HA) VMWare, Azure Local Hyper-V and Azure cloud VMs deployed using Azure Resource Manager (ARM) Templates and Azure CLI.
- Segmented the data center, HQ, and 30 branch networks into VLANs, cutting network-related incidents by 93% by isolating ATM/VoIP traffic, establishing separate segments for servers, data, and out-of-band management, and integrating RADIUS/TACACS+ with Active Directory LDAP for centralized device control.
- Created comprehensive vulnerability assessment, risk management, threat detection and response strategy with Crowdstrike Falcon responding to threats in real-time and Tenable Vulnerability Management, Nessus, Defender and Intune to continuously identify, categorize and fix vulnerabilities, reducing the annual penetration test findings from 8 critical and 20 high in 2022 to 1 medium by 2024.
- Unified Identity and Access Management (IAM) providing a phishing resistant passwordless Single Sign-On experience using Entra as the SAML IdP for the FortiAuthenticator to streamline users access to physical infrastructure (FortiManager, FortiGate, FortiAnalyzer, FortiClient), IaaS (VMs & Storage) and issuing OIDC & OAuth tokens for SaaS (Adobe Creative Cloud, Office 365, Hubspot, Docusign) PaaS (AVD & Webflow) access with custom Role-Based Access Controls, Intune-issued client EAP-TLS certs and Conditional access policies resulting in 99% passwordless sign-ins.
- Implemented a Zero Trust Architecture (ZTA) in a hybrid environment, eliminating repeat unauthorized access incidents using VeloCloud SDWAN, FortiGate NGFW, Entra ID (MFA, Priviled Information Management, SSO,

JiT), Crowdstrike Falcon, Azure Policy, Bicep IaC, Splunk, CyberArk Privileged Access Management, Intune endpoint compliance, M365 E5, Defender for Cloud Apps, and Purview DLP.

- Developed bank-wide Intune MDM policies and deployed to 700+ endpoints with only 3 service desk escalations using a GPO to enroll devices in AD and Entra, and Intune configuration policies for BitLocker, LAPS, Nessus, CrowdStrike, PIM and Defender meeting baseline compliance without disrupting end users.

**Lead Systems Engineer** SMR Hosting – Livonia, MI December 2009 – August 2022

- Leader of engineering team responsible for $2M+ in revenue, 10 employees, and 80 managed clients by providing exceptional technical support and managed cloud infrastructure adhering to the CIS Benchmark and Microsoft Cloud Security Benchmark (MCSB) frameworks and enterprise-grade SLAs, monthly reporting and an Ansible / Jenkins automation framework to secure IT operations and host 450 Windows & Linux servers in 12 countries with 87% customer retention.
- Migrated SMB clients (200+ users) from on-prem AD to hybrid or cloud-based Azure AD, achieving 30–50% licensing savings, reducing footprint by 70%, and maintaining zero downtime through usage metrics from SolarWinds Observability, pilot migrations, and vCenter Converter, Azure Migrate, and AWS Migration Hub.
- Modernized Active Directory for 300+ users creating a new domain with PKI, DNS, DHCP, GMSA's and Azure AD Connect finishing the project 20 % ahead of schedule while achieving full SOX & GLBA compliance. Secured cloud traffic via site-to-site IPsec, NSGs, private endpoints, service endpoints, and automated naming and migration processes in collaboration with the CTO, CISO, and IT Steering Committee.
- Merged two AD domains (200 employees, 6 DCs) into a virtual environment during an 8-month M&A, streamlining access, enabling self-service password resets, and migrating Exchange to M365 via standardized naming conventions, custom Powershell automation, audit and migration scripts, and federated domain trusts.
- Replaced patch management software with Ivanti Security Controls, allowing local patch repositories to overcome 5- to 10-Mbps MPLS bottlenecks for 35 remote offices, bringing Windows and all third-party software up to date (previously a year behind) in one month.
- Replaced EOL IBM SANs with new modular NetApp NVME SAN, exponentially increasing data throughput, availability, resilience, and VM density using NVMe over TCP, SMB fileshares, and ONTAP SnapMirror to replicate source-volumes to an Azure Cloud Volume.

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

- Overhauled LiquidVPN's website and redesigned the user experiences across platforms (mobile, Windows, Mac), giving users a familiar experience regardless of platform while maintaining GDPR and PCI-DSS compliant and increasing quarterly sales by 35% by Implementing OAuth authentication, publishing website's REST API and integrating an in-app payment gateway for efficient sign-ups and account management.
- Automated infrastructure deployments with Terraform and Ansible, reducing setup time from hours to minutes by standardizing configurations and nearly eliminating human error.
- Achieved a 20% reduction in operating expenses and a 40% increase in availability, 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 market reach by 35% and cut vendor onboarding time by 50% measured by quarterly revenue reports and procurement SLAs by localizing web and mobile apps into six languages and implementing a vendor-management and DLP framework that streamlines oversight of international colocation partners.

**Lead Network Engineer** LiquidVPN – Southfield, MI January 2012 – February 2017

- Built and led a 10-person engineering team, reducing project delivery timelines by 20% and lowering churn from 18% to 3% by implementing feedback loops, bug bounties, and a CI/CD pipeline.
- Launched B2C SaaS VPN growing it to 300,000 users in 110 countries, driving 60% annual subscriber growth via multi-cloud architecture, secure encryption standards and media recognition in Wired and CNET.
- 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, vendor relationships, and financial accounts through phased migrations and domain trusts before taking on the IT Director role.

**Network Field Engineer** IBM Global Services – Warren, MI July 2005 – May 2010

- Built VMware ESX virtualization proof of concept (PoC) environments for IBM, Chrysler, and Ford, helping them to reduce their data center footprints by up to 40% and lowering energy costs by 25% through strategic server consolidation and virtualization.
- Implemented enterprise backup systems with IBM Tivoli, achieving 99.99% data recovery by adopting a dual-location tape strategy and 35%-cheaper media.
- Provided on-site 3rd level technical support for Windows and Linux servers for Fortune 500 clients' diagnosing Apache, IIS, SQL, NAT, DHCP, DNS, LDAP, Active Directory, Citrix Metaframe XP, Excel, and Exchange meeting strict SLAs and using meticulous troubleshooting to provide Root Cause Analysis (RCA).
- Pioneered a virtualization feasibility analysis, proposing a 40% footprint reduction to executives with cost estimates, risk assessments, and pilot proofs-of-concept.

## Education and Certificates

- **B.S. in Network and Information Technology** – Eastern Michigan University June 2001
- **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
- **CompTIA Network+, Security+, A+, and Microsoft MCSE** 2001–2005