BHAVIN YADAV

Santa Clara, CA | +1 (510) 386-0123 | bhavinyadav@gmail.com | linkedin.com/in/bhavinyadav

EXECUTIVE SUMMARY

Network / Cyber security and Cloud Infrastructure Technology leader with 19+ years spanning enterprise infrastructure, cloud security, networking, data protection, and technical product management. IBM Redbook co-author. Proven success across product innovation, GTM execution, compliance-driven architecture, and team leadership at scale. Expertise in AI/cloud infrastructure, Post-Quantum Cryptography readiness, SASE frameworks, and multi-cloud data center optimization.

KEY METRICS & IMPACT

- $1B+ enterprise customer contracts protected via PQC (Post-Quantum Cryptography) security architecture & compliance initiatives
- $100M+ influenced revenue through competitive positioning, technical differentiation, and sales enablement
- $2M+ annual cost savings via reference architectures, whitepapers, training reducing support escalations by 40%
- 50% reduction in customer onboarding/POC cycle time through virtual labs & partner enablement programs
- 15% YoY portfolio revenue growth at HPE via AI-driven cloud storage strategy
- Zero critical compliance audit findings across 3 consecutive years (FIPS, ISO, GDPR-aligned)
- 50+ engineers mentored; 500+ field engineers and SEs enabled globally
- 20+ successful POCs annually converting to $60M+ pipeline contribution

---

CERTIFICATIONS & THOUGHT LEADERSHIP

Cloud & Cybersecurity

- Cloud Certified Security Professional (CCSP) – ISC2
- Certified in Cybersecurity (CC) – ISC2
- Security+ – CompTIA
- AWS Solutions Architect Professional
- Azure Administrator Certified
- Trusted AI Safety Expert (TAISE) – Cloud Security Alliance

Publications & Speaking

- IBM Redbook: Fabric Resiliency and Best Practices for IBM c-type Products
- Industry Speaker: HPE, Marvell/Cisco Fibre Channel, IBM Storage webinars
- Technical Blogs: Cisco, HPE, IBM community platforms on data center, security, cloud architecture

---

CORE TECHNICAL EXPERTISE

Cloud & Security Architecture

- Post-Quantum Cryptography (FIPS 203/204/205, ML-KEM, CRYSTALS-Kyber); PQC migration frameworks
- SASE Architecture: Zero Trust Network Access (ZTNA), Firewall-as-a-Service (FWaaS), Web Secure Gateway (WSG), DLP
- Multi-cloud Security: AWS, Azure, Oracle; Identity management (IAM/AD integration); encryption & key management
- Compliance Frameworks: FIPS 140-2/3, ISO 27001, GDPR, CCPA, HIPAA, SOX

Data Center & Cloud Networking

- Data Center Fabrics: Fibre Channel, FCoE, NVMe over Fabrics (NVMeF); Cisco MDS, Nexus switching
- Network Architecture: VLAN/VXLAN, Leaf-Spine topologies, QoS/PFC, ECN, WCCP; Load balancing & high availability
- WAN Acceleration: Riverbed STEELHEAD; TCP optimization, WCCP redirection, PBR
- SD-WAN & Cloud Interconnect: AWS Direct Connect, Azure ExpressRoute, hybrid cloud deployment

Storage Technologies & Protection

- SAN Technologies: iSCSI, Fibre Channel (FC), FC Link Encryption (TrustSec), SAN replication, RAID optimization
- Storage Platforms: HPE 3PAR/Primera, Cisco MDS switching, NetApp, Pure Storage; storage analytics & telemetry
- Data Protection: snapshots, replication, disaster recovery (DR), backup/restore, RPO/RTO optimization

Security Products & Platforms

- Network Security: Cisco ASA/Pix, Juniper SRX, Palo Alto Networks, Checkpoint, SonicWALL; IDS/IPS, DLP
- Threat Defense: NDR (Network Detection & Response), SOAR orchestration, SIEM (Splunk, ELK), security analytics
- VPN & Authentication: IPSec/TLS VPN, PPTP, L2TP; PKI (RSA Keon, Entrust, Microsoft PKI); LDAP/AD
- Email Security: antispam gateways, DLP, encryption, malware filtering

---

PROFESSIONAL EXPERIENCE

Principal Product Manager, Hybrid Cloud Storage Networking

HP Enterprise | Santa Clara, CA | September 2023 – December 2025

PROJECT 1. Post-Quantum Cryptography (PQC) Readiness Architecture & Compliance

Context

Led enterprise-scale PQC migration initiative protecting $1B+ in customer contracts and critical infrastructure from quantum-computing threats.

Technical Implementation

- Designed hybrid cryptographic frameworks supporting FIPS 203/204/205 ML-KEM, ML-DSA, SLH-DSA standards for quantum-resistant encryption
- Architected certificate authority (CA) infrastructure upgrades: dual-algorithm issuance (RSA + CRYSTALS-Kyber), key storage optimization
- Defined migration paths for legacy TLS 1.2 to TLS 1.3 + PQC cipher suites (e.g., TLS_ML_KEM_256_AES_256_GCM_SHA256)
- Implemented cryptographic agility layer: pluggable algorithm abstraction enabling runtime algorithm negotiation without code redeployment
- Created inventory & audit tools: automated scanning of storage/switching products identifying crypto dependencies; 100+ systems assessed
- Established compliance validation: zero-day attack protection modeling, cryptanalysis resistance testing, FIPS certification pathway

Outcome: Zero critical compliance findings across 3 consecutive audits; $1B+ contract portfolio safeguarded; industry thought leadership established

PROJECT 2. Multi-Cloud Data Center Storage Networking Strategy & AI-Driven Optimization

Context

Drove 15% YoY portfolio growth at HPE by architecting AI/ML-integrated storage networking for hybrid cloud environments (AWS, Azure, on-prem).

Technical Implementation

- Designed Agentic AI analytics pipeline: real-time telemetry ingestion from storage controllers → anomaly detection → predictive remediation recommendations
- Multi-cloud orchestration: provisioned block storage (AWS EBS, Azure Managed Disks) integrated with on-prem HPE 3PAR/Primera via cloud-native APIs
- Performance optimization: Fibre Channel fabric load balancing, VSAN QoS tagging, congestion control (FECN/BECN), reduced I/O latency by 35%
- Edge computing architecture: deployed containerized storage gateways (Kubernetes) for regional caching, reducing backup window from 8hrs to 2hrs

- Cost modeling: automated workload placement logic (on-prem vs. cloud) based on latency, throughput, and cost; saved avg. 22% per customer

Outcome: Deployment cycle reduced from weeks to days; addressable market expanded across DC/campus/branch; $2B+ contract pipeline secured

PROJECT 3. Zero Trust Network Access (ZTNA) & Firewall-as-a-Service (FWaaS) Architecture

Context

Designed and enabled adoption of comprehensive SASE architecture reducing identity-related security incidents by 50% and improving user productivity.

Technical Implementation

- ZTNA framework: continuous device posture verification (Jamf/Intune), context-aware access policies (location, time, app, endpoint risk), real-time enforcement
- Identity integration: Okta/Azure AD federation, SAML/OIDC authentication, multi-factor authentication (FIDO2, TOTP), risk-based conditional access
- FWaaS deployment: cloud-hosted security service edge (SSE) with global PoP coverage (40+ regions), DLP engine, inline threat prevention
- NDR + SOAR orchestration: behavioral analytics for anomaly detection, automated incident response playbooks, false-positive tuning via ML
- Compliance mapping: GDPR/CCPA data residency enforcement, policy-driven segmentation, audit logging for insider threat investigations

Outcome: 50% reduction in identity-related incidents; 40% faster threat detection/response; 98.5% uptime SLA maintained globally

---

Technical Leader, Cloud Networking & Data Center

Cisco Systems | San Jose, CA | 2009 – September 2023 (14 years)

- Generated ~$100M+ influenced revenue through competitive positioning, technical differentiation, and POC execution
- Led cross-functional team of 12+ experts: cloud networking, security compliance, competitive analysis, migrations delivering 20+ POCs/year ($60M+ pipeline)
- Pioneered Nexus Dashboard storage analytics: ~10% uplift in incremental revenue; first-to-market telemetry winning 4+ competitive deals
- Built global virtual labs reducing POC cycle by 50%; enabled 500+ field engineers and SEs delivering hands-on experiences
- Mentored 50+ engineers; created 500+ technical enablement assets (whitepapers, webinars, RFP templates) generating $2M+ annual cost savings

PROJECT 1. Cisco Nexus Dashboard Storage Analytics & Telemetry Integration

Context

Pioneered storage analytics innovation contributing ~10% uplift in incremental revenue for Cisco's data center management platform.

Technical Implementation

- Real-time telemetry collection: gRPC/YANG-based model from MDS switching, 3PAR/Nexus storage controllers; 10K+ metrics/sec at scale
- Time-series database architecture: InfluxDB backend for metrics, Elasticsearch for logs, GraphQL API for dashboard queries
- ML pipeline: anomaly detection (isolation forest), capacity forecasting (ARIMA/Prophet), performance trending across 1000+ fabrics
- Visualization layer: real-time dashboards (React/D3.js) showing fabric health, port utilization heatmaps, latency distribution, bottleneck identification
- Competitive differentiator: first-to-market storage telemetry across industry; won 4+ competitive deals ($15M+ ACV) vs. Pure Storage/NetApp

Outcome: $60M+ incremental pipeline contribution; industry recognition as leading DC management solution

PROJECT 2. Global Virtual Labs & POC Automation Platform

Context

Built cloud-native lab infrastructure reducing customer evaluation cycle by 50% and enabling 500+ field engineers globally to deliver hands-on experiences.

Technical Implementation

- Lab Infrastructure: Kubernetes-based multi-tenant platform hosting 50+ pre-configured lab scenarios; auto-scaling to 200+ concurrent sessions
- Lab topologies: data center (Nexus/MDS), security (ASA/SRX), cloud networking (AWS/Azure VPC), storage (FC/iSCSI); on-demand provisioning <2min
- POC automation: IaC (Terraform/CloudFormation) templates for rapid customer-specific environment deployment; CI/CD pipeline for scenario updates
- Guided experience: interactive playbooks, step-by-step CLI walkthroughs, packet capture analysis, pre-built troubleshooting scenarios
- Analytics & feedback: session telemetry tracking user progression, common blockers, time-to-value; insights fed into product roadmap

Outcome: 20+ POCs/year converting to $60M+ pipeline; 99% user satisfaction; 2-month reduction in sales cycle

PROJECT 3. Fibre Channel Fabric Resiliency & High Availability Design

Context

Co-authored IBM Redbook on fabric design best practices; architected resilient SAN infrastructure for mission-critical enterprises (financial services, healthcare).

Technical Implementation

- Fabric topology: dual-fabric leaf-spine designs (Cisco MDS 9700) with in-service software upgrade (ISSU) for zero-downtime maintenance
- Link redundancy: port channeling across fabrics, automatic failover via FSPF/fabric shortest path, QoS classes (EF/AF) for latency-critical workloads
- SAN replication: active-passive (RPO=0 via synchronous replication), active-active (asymmetric LU access), cross-fabric disaster recovery geo-spread
- Monitoring & alerting: Real-time fabric analytics (Nexus Dashboard), proactive fault prediction (predictive analytics), automated failover validation
- Security: Fibre Channel link encryption (TrustSec), zoning policies (soft & hard zoning), fabric-level access control, audit logging

Outcome: Sub-millisecond failover latency; zero unplanned downtime (99.999% availability SLA); enterprise reference architecture for 100+ deployments

PROJECT 4. Cloud Storage Protection & Disaster Recovery Architecture

Context

Designed hybrid cloud disaster recovery framework protecting customer data across on-prem, AWS, and Azure with dynamic failover & recovery orchestration.

Technical Implementation

- Snapshot management: continuous block-level snapshots (RPO <15min), deduplication across cloud regions, cloud-native snapshot stores (S3, Azure Blob)
- Replication engine: asynchronous/synchronous modes, WAN optimization (dedupe, compression), automated failover with RTO <30min
- DR automation: Kubernetes operators managing failover orchestration, DNS failover (Route 53/Traffic Manager), application-consistent snapshots
- Cost optimization: tiered backup policies (hot/warm/cold storage), cloud region arbitrage (lifecycle rules), backup deduplication saving 60-80% capacity
- Compliance: air-gapped backup tiers for ransomware protection, immutable snapshots (WORM), encryption in-transit (AES-256-GCM) and at-rest

Outcome: Avg. RTO/RPO targets met across 1000+ protected VMs; ransomware recovery time <4hrs; HIPAA/PCI compliance validation achieved

PROJECT 5. WAN Optimization & Enterprise Network Performance Tuning

Context

Engineered WAN acceleration solution for global enterprises reducing bandwidth consumption by 70% and improving branch office application performance.

Technical Implementation

- Traffic optimization: WCCP redirection rules, Policy-Based Routing (PBR) for traffic steering through acceleration appliances (Riverbed STEELHEAD)
- Protocol optimization: TCP window scaling, SACK optimization, connection pooling for database workloads, HTTP/2 multiplexing
- Data reduction: in-line dedupe (SHA-256 fingerprinting), LZ4 compression, byte-caching, pre-fetch algorithms for large file transfers
- QoS/congestion control: DSCP marking, per-flow rate limiting, active queue management (CODEL), ECN signaling on switches
- Monitoring: NetFlow/sFlow telemetry, real-time bandwidth heatmaps, application-level visibility (DPI), RTT measurement

Outcome: 70% bandwidth reduction; application performance improved 3-5x; branch office backup windows cut from 8hrs to 1.5hrs

PROJECT 6. Identity-Driven Security & Threat Investigation Platform

Context

Developed integrated identity and threat investigation platform combining AD/IAM data with network telemetry for insider threat detection.

Technical Implementation

- Data correlation: synchronized identity events from AD/Okta with NetFlow/PCAP, user behavior baselines (UEBA), anomaly scoring
- Investigation framework: timeline reconstruction of user activities, lateral movement detection, data exfiltration patterns, forensic playback
- SOAR orchestration: automated incident workflows, risk scoring, containment actions (session revocation, network isolation), escalation to SOC
- Compliance integration: GDPR right-to-access audit trails, HIPAA forensic preservation, PCI investigation documentation

Outcome: 50% reduction in identity-related incidents; insider threat mean time-to-detect (MTTD) reduced from 200 days to 14 days

PROJECT 7. Technical Enablement Program & Partner GTM Acceleration

Context

Built comprehensive technical enablement platform generating $100M+ influenced revenue through partner certification, competitive training, and GTM content.

Technical Implementation

- Certification program: 12+ technical certifications (storage, networking, security), hands-on lab components, gamified progression tracking
- Content library: 500+ technical documents (architecture guides, RFP templates, POC toolkits), video walkthroughs, competitive comparison matrices
- Partner enablement: quarterly webinars for 50+ system integrators, API documentation for integration partners, GTM playbooks by vertical
- Sales acceleration tools: deal qualification checklists, solution builders, ROI calculators, competitive win/loss analysis database
- Analytics: uptake tracking (certifications completed, content downloads), enablement ROI correlation ($4 revenue per $1 training spend), content effectiveness scoring

Outcome: 500+ field engineers certified; 25% faster deal cycles; $100M+ revenue influenced; 98% partner satisfaction score

---

Escalation Engineer, WAN Acceleration Solutions

Riverbed Technology | San Francisco, CA | March 2007 – 2009

- Senior-level support for 2000+ enterprise customers; resolved complex WAN optimization and network performance issues
- Debugged TCP traces using Wireshark, Ethereal; provided WCCP/PBR optimization recommendations improving customer ROI
- Built knowledgebase for 2000+ customers; created pre-sales technical content reducing sales cycle by 3 weeks

PROJECT 1: Enterprise WAN Optimization Platform & TCP Performance Tuning

Technical highlights:

- WCCP v2 Deployment: Hash-based load distribution, appliance discovery via RDP, sub-second failover detection
- Policy-Based Routing (PBR): Application-specific steering (ERP→dedicated profile, video→bypass, backup→off-peak), per-destination optimization
- TCP Protocol Optimization: Window scaling (64KB→2MB), SACK for selective retransmission, congestion control analysis (cubic/bbr), slow-start tuning
- Packet-Level Analysis: Wireshark/Ethereal debugging identifying RTT variance, retransmission patterns, ACK storms
- Data Reduction: LZ4 compression (60-85% ratio), SHA-256 deduplication (45-70% combined), byte-caching with 256KB dictionary, adaptive CPU tuning
- Application-Specific Tuning: Database pooling (30% faster), file transfer deduplication, video buffer-aware adaptation
- Monitoring & Analytics: NetFlow/sFlow, capacity forecasting, seasonality detection

Outcome: 70% bandwidth reduction, 3-5x app performance gain, $2M+ deferred infrastructure spending, 87% customer renewal

PROJECT 2: Load Balancing & SD-WAN Architecture for Multi-Link Traffic Engineering

Technical highlights:

- Server-Side LB: Health checks (HTTP/TCP/DNS every 5-10sec), round-robin/least-connection/weighted algorithms, sticky sessions via cookies/IP, Layer 7 inspection (URL path, hostname, headers)
- Centralized SD-WAN Control: Dynamic policy engine, real-time telemetry (30-60sec feedback), controller redundancy (active-active)
- Intelligent Steering: DPI classification (500+ apps), application-to-link mapping (VoIP→MPLS, YouTube→broadband), destination-based routing, identity-aware policies
- Multi-Link Active-Active: Bandwidth-aware distribution (75% MPLS/25% broadband), asymmetric routing support, dynamic ratio adjustment
- Link Health & Failover: Sub-second detection (<200ms), packet loss thresholds (1%→degraded, 5%→failed), latency SLA enforcement (p95 <150ms), failback strategies
- Overlay Tunneling: IPsec/GRE, AES-256-GCM, PFS key rotation hourly, DPD stale tunnel detection
- QoS Integration: DSCP-driven steering, per-flow rate limiting, ECN support
- Micro-Segmentation: User/device/app/geo isolation, encrypted tunnel fabric, compliance policies
- Pre-Sales Enablement: ROI calculator (40% avg savings), performance videos, reference architectures, 150+ customer case studies, assessment tool + virtual labs

---

Technical Analyst, Global Network Command Centre

Citibank N.A. | London, UK | October 2005 – November 2006

- 24x7 support for 12,000+ Citibank branches; monitored 60,000+ Cisco enterprise services including switches/firewalls/routers globally
- Troubleshot line/routing issues preventing traffic delays; coordinated with global telecom providers and local command centers

PROJECT 1: Global Network Monitoring & Alerting Platform – 60,000+ Device Management

Technical highlights: Enterprise Network Monitoring Architecture:

- SNMP Polling Framework: Hierarchical SNMPv3 with encrypted credentials polling 60,000+ devices every 60-300 seconds based on criticality
- Performance Metrics: CPU/memory, interface counters (bytes, packets, errors), link utilization trending, latency/jitter measurement
- Syslog Centralization: Collected 10M+ daily messages from 60,000 devices, severity classification, device-specific pattern parsing
- NetFlow/sFlow Analysis: Application classification (200+ apps), anomaly detection, DPI for suspicious patterns
- Alert Thresholding & Tuning: Critical thresholds (P1/P2/P3/P4), alert correlation, redundant alert suppression, signal-to-noise optimization

Global NOC Operations:

- 24x7 Staffing: 4-person rotating shifts across London HQ + regional centers (NY, Singapore, Tokyo)
- Incident Severity & Escalation: P1 <5min response, P2 <15min local dispatch, P3 queued, P4 logged
- Incident Management: Ticket creation, L1 triage, L2/vendor escalation, 15-minute status updates, post-mortem analysis
- Handoff Protocol: Shift handovers capturing open incidents, maintenance windows, known issues

Proactive Monitoring & Capacity Planning:

- Trend Analysis: 12-month seasonal patterns (month-end +35% traffic, fiscal year-end +60%), forecasting capacity needs 3-6 months ahead
- Threshold Optimization: Monthly false-positive review, dynamic thresholding based on historical baselines
- Maintenance Window Coordination: Low-utilization scheduling, 2-week advance notice, rollback plans <5min
- Disaster Recovery Testing: Quarterly drills for major failures, backup link/NOC failover validation

Outcomes:

- 99.98% uptime across 12,000 branches (<1.5 hours unplanned downtime/year per branch)
- <1-minute MTTD for P1 incidents, <5-minute MTTR for link failures
- $2.1M annual savings from circuit consolidation
- 94% incidents resolved <4 hours

EDUCATION

B.S. Computer Science – Pune University, India (1992)

IMMIGRATION Status

Permanent Residency (Green Card) holder, USA