

Bhavin Yadav

Santa Clara, CA 95050 | +15103860123 | bhavinyadav@gmail.com

Summary

Security-focused Product & Technical Marketing Leader with 14+ years driving AI-powered security solutions, cloud security platforms, and zero trust architectures at Cisco and HPE. Expert in translating complex security technologies into market-leading products and GTM strategies. Proven track record implementing enterprise security controls (ISO 27001, FIPS, GDPR), securing multi-cloud environments, and delivering AI-driven threat detection and data protection solutions. IBM Redbook author and certified security professional (CCSP, Security+, CC, TAISE) with deep expertise in network security, identity management, and compliance-driven security architectures.

Core Expertise

Cloud & Network Security

- Design and implementation of secure multi-cloud architectures (AWS, Azure) with zero-day protection, threat modeling, and penetration testing validation for cloud-native security services.
- Network security segmentation and policy enforcement across data center, campus, and branch environments using TrustSec, micro-segmentation, and distributed security controls.
- Identity and access management (IAM) controls, directory integrations, and RBAC implementation for secure cloud operations and AI-assisted policy workflows.

AI-Driven Security & Analytics

- Led AI/analytics-driven security insights on Cisco Nexus Dashboard, contributing ~10% incremental revenue (\$50M+) through threat detection, anomaly detection, and operational intelligence capabilities.
- Applied AI/ML and telemetry to optimize security operations, automated threat response, network segmentation policy, and compliance monitoring at enterprise scale.

Data Protection & Compliance

- Expert in data protection strategies against zero-day attacks, ransomware, and data exfiltration using encryption, secure snapshots, DLP, and endpoint security controls.
- Deep experience with security compliance frameworks (ISO 27001, FIPS 140-2, GDPR, RoHS) and audit-ready governance for enterprise security infrastructure.
- Maintained ISO 27001 compliance for 12,000+ network devices at Citigroup, managing vulnerability scanning, security patching, and incident response coordination.

Security Product Management

- 12+ years leading security-focused product strategy, roadmaps, and GTM execution for cloud security, network security, and data protection solutions.
- Created security whitepapers, competitive positioning, POC frameworks, and technical enablement content used globally by security teams, partners, and customers.
- Led security compliance initiatives, competitive take-outs, and customer security validations for mission-critical enterprise deployments.

Security Certifications & Leadership

Cloud & Cyber Security Certifications

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

Multi-Cloud & Networking

- Cloud Certifications: AWS, Oracle, Microsoft Azure, Aviatrix

Leadership

- Technology Leadership Management – Cornell University

Security Thought Leadership & Publications

- **IBM Redbook:** Fabric Resiliency and Security Best Practices for IBM c-type Products
- **Security Whitepapers:** Cisco TrustSec Fibre Channel Link Encryption, Non-disruptive Secure SAN Migration, Reliable and Highly Available Secure SAN Design
- **Industry Speaker:** HPE, Marvell/Cisco, and IBM security webinars and conferences on storage security, network security, and SAN security best practices
- **Security Blogs:** Published extensively on Cisco, HPE, and IBM community platforms covering data center security, cloud security, and network encryption

Professional Experience

HP Enterprise

Principal Product Manager, Hybrid Cloud Security & Storage Networking | 09/2023 – Present

- Lead security strategy and roadmap for HPE's hybrid cloud storage portfolio, implementing AI-driven security controls, zero-day protection, and compliance-driven architectures (ISO, FIPS, GDPR) across multi-cloud enterprise environments.
- Design secure cloud services on AWS and Azure with AI-based threat detection, implementing network security segmentation, secure multi-tenant architectures, and data protection for block storage and edge computing platforms.
- Develop comprehensive data protection strategies against zero-day attacks and ransomware, leveraging penetration tools, threat models, security validation, and countermeasures including storage snapshots, DLP, and endpoint security.
- Translate security and compliance requirements into technical value propositions, creating security-focused GTM content (whitepapers, threat assessments, security training) for global sales and partners.
- Partner with security, engineering, and compliance teams to ensure portfolio alignment with enterprise security standards, optimized security margins, and successful security lifecycle management.

Cisco Systems

Technical Leader / Manager, Cloud Security & Data Center | 2009 – 2023

- Led multi-cloud security architecture within Cisco's AI-driven Data Center Cloud Networking group, integrating secure cloud and on-prem environments with zero trust principles, TrustSec segmentation, and compliance controls.
- Managed team of security experts across DC cloud security, compliance validation, competitive security assessments, threat modeling, and secure Proof-of-Concepts for enterprise customers.
- Drove AI-driven security analytics innovation in Nexus Dashboard, delivering threat detection, anomaly detection, and security insights that contributed ~10% incremental revenue (\$50M+) to the platform.
- Designed and integrated identity and access management (IAM) controls, directory integrations (LDAP, AD), and RBAC frameworks to support secure cloud operations and AI-assisted security policy workflows.
- Created security enablement including TrustSec encryption whitepapers, security compliance guides, threat assessment frameworks, and competitive security positioning tools driving adoption and revenue.
- Managed secure cloud-based and on-prem POC labs demonstrating security capabilities for customers, SEs, and partners, including encryption, segmentation, and compliance validation scenarios.
- Engaged with Security, Engineering, Partners, and Customers to capture security requirements, shape security roadmap priorities, and deliver capabilities meeting compliance and threat protection standards.