

STEVE ROSS

Phoenix, AZ • hello@itsross.com • linkedin.com/in/steve-ross-b65774a5 • itsross.com

Digital workspace and infrastructure architect turned engineering leader. Twelve years in IT, the last decade running enterprise endpoint, identity, and EUC platforms at health-tech, investment-bank, and national e-commerce scale. VMware Certified Professional in Digital Workspace.

SUMMARY

- 12+ years in IT: a solo-IT foundation, then a decade of enterprise across Cerner (Oracle), VMware partner consulting, and The RealReal, as lead engineer, manager, and now staff architect.
- Led an 8-person infrastructure team (networks, identity, systems, endpoints) through a leadership transition and reduction in force. Ticket resolution improved 35%, downtime dropped, and backup resilience and monitoring shipped during the rebuild.
- Full digital workspace lifecycle in production: migrated 3,000 endpoints off on-prem Active Directory onto Entra ID, then off Workspace ONE onto Intune, with zero-touch provisioning across Windows, macOS, iOS, and Android. Today I own identity and both fleets: Okta, Google Workspace, Entra ID and Intune, and 2,600 Macs in Jamf.
- Engineering quality that shows up in dollars: one backup automation retired 5,000 enterprise archive licenses, roughly \$420K per year in recurring spend.
- Builds emerging tech into production: AI agent systems (FastMCP with Claude, GPT, and open-source LLMs) automate infrastructure operations and incident response today.

WORK EXPERIENCE

The RealReal, Inc.

Staff, Systems Engineer (Architect)

May 2024 – Present

- Architect and run production AI agent systems on FastMCP: multi-model pipelines (Claude, GPT, open-source LLMs) with RAG and structured output parsing that automate infrastructure operations, troubleshooting, and incident response across the team.
- Own the systems, identity, and endpoint estates end to end: Okta, Google Workspace, Entra ID and Intune, a 2,600-Mac Jamf fleet, and enterprise infrastructure spanning on-prem VMware (ESXi, vCenter) and multi-cloud (AWS, Azure, GCP) with 50+ servers; 3,500 users and 350 service accounts, under SOC 2 and SOX ITGC controls.
- Built joiner/mover/leaver onboarding and offboarding automation on Okta Workflows and Freshservice workflows, extended with Python and PowerShell against application APIs and keyed to Workday identity events.
- Eliminated monthly app repackaging across both MDM fleets with evergreen install scripts that pull the current vendor release at install time.
- Worked around per-user Microsoft licensing with Device Enrollment Manager enrollment, building device-to-user mapping at Autopilot OOB with dynamic device groups.
- Built international provisioning end to end: an approved Freshservice request adds the user to an Okta group that provisions an AWS Workspace in Sao Paulo, domain-joined, SSM-enrolled, EDR installed. Virtual desktops instead of hardware through customs.
- Maintain a national file-distribution pipeline on Nasuni, roughly 2TB per day between coasts, heavily automated in PowerShell with server-side copy and other optimizations.
- Wrote the backup automation that retired 5,000 enterprise archive licenses, eliminating roughly \$420K per year in recurring license spend.
- Run the on-premises Windows server estate alongside the cloud footprint, including WSUS patching, KMS activation, AD CS certificate services, and WDS imaging, the offline-capable stack that keeps an environment patched and activated without depending on vendor cloud services.
- Mentor six engineers, no title required, building the bench across both fleets.

Manager, IT Operations Engineering

May 2023 – May 2024

- Promoted from lead engineer to manager of the 8-person infrastructure team (two engineers each across networks, identity, systems, and endpoints) during a leadership transition and reduction in force. Kept every platform running while rebuilding the team.
- Improved ticket resolution 35% during the rebuild, alongside reduced downtime and new backup resilience and monitoring.
- Consolidated the service stack onto Freshservice, migrating the service desk off Zendesk and the IT asset management and change-control estate off ServiceNow, carrying ticket history and rebuilding workflows and automation on the new platform.
- Pioneered the change advisory board (CAB), standing up formal change management alongside the consolidation.
- Owned the full performance management lifecycle, hiring through exit, while backfilling a network engineer.
- Owned budget planning and financial oversight for a \$2M+ systems infrastructure and license budget; negotiated vendor contracts and cut recurring costs.

Lead, Endpoint Engineer

Jan 2021 – May 2022, Oct 2022 – May 2023

- Owned the full endpoint lifecycle for a 3,000-endpoint fleet across Windows, macOS, iOS, and Android. Led the MDM migration off Workspace ONE (OmniSSA) onto Intune with zero-touch provisioning (Windows Autopilot, Apple Business Manager/ADE, Knox Mobile Enrollment).
- Rebuilt the Active Directory Domain Services environment end to end, correcting a broken replication topology and the DNS timeouts and cascading failures it caused, then led the migration to Entra ID and federated Okta with Entra ID.

- Designed dozens of endpoint configuration baselines tuned for user experience as much as security.

Rebellion Defense, Inc.

Senior Solutions Architect

May 2022 – Oct 2022

- Tasked with designing MDM workflows and hardening endpoint security posture across Windows and macOS for a defense AI software company, including BYOD and mixed-ownership enrollment paths.
- Built zero-touch Apple ADE enrollment on VMware Workspace ONE.
- Brought managed identity to macOS with Jamf Connect, and modernized the application catalog using InstallApplications and Munki.

Entelligence LLC (VMware Partnership)

Senior Consultant

Jan 2019 – Jan 2021

- Professional services for VMware Workspace ONE: designed and implemented UEM/MDM solutions for enterprise clients managing 10K to 50K endpoints, with 95%+ deployment satisfaction.
- Ran operational support for a major US investment bank's entire on-prem Workspace ONE stack (vIDM, UAG, memcached, active-active MS SQL; 32 servers per stack, mirrored in DR, plus dev and UAT). Kept 100+ servers patched, monitored, and healthy in a SOC 2 banking environment.
- Ran Android device fleets numbering in the tens of thousands across hundreds of national bank branches, where the network link was available for update traffic only during defined windows, so configuration had to hold good state between sync opportunities rather than assume a reachable device.
- Led architecture and capacity planning engagements, performance-tuned UEM infrastructure at scale, and delivered training for client IT teams.

Cerner Corp (Oracle)

Systems Engineer

Jan 2017 – Jan 2019

- Administered core identity and directory services in a HIPAA environment, supporting 1,000+ endpoints across a diverse clinical fleet.
- Stood up and ran AirWatch MDM; facilitated large-scale software deployments and managed internal communication platforms.
- Built scripted automation for routine tasks and specialized lab equipment configuration.

Clean Adventures

IT Technician → IT Manager (sole IT)

2013 – 2016

- Foundation years, concurrent with the AAS: printer fleet service across a multi-site drug and alcohol rehabilitation company, grown into sole ownership of its networks, websites, and servers, plus a new office standup (phones, internet, web).

CERTIFICATIONS & EDUCATION

- VMware Certified Professional in Digital Workspace (VCP-DW)
- Jamf 200 (Jamf Certified Tech)
- Cisco CCNA
- AAS, Computer Networking

SKILLS & PLATFORMS

Digital workspace & endpoint: Intune, Windows Autopilot, Workspace ONE (OmniSSA/AirWatch), Jamf Pro, Google Workspace, MECM/SCCM, Apple Business Manager (ADE/DEP, VPP), Knox Mobile Enrollment, Microsoft Defender for Endpoint, Windows Update for Business, Azure Virtual Desktop, AWS/Azure WorkSpaces, across Windows, macOS, iOS, Android, and Linux fleets

Identity & access: Entra ID (Conditional Access, AD Connect), Okta (adaptive MFA, assurance policies, hundreds of app integrations), device trust across Windows, macOS, iOS, and Android (via Intune and Jamf), Google Workspace security (Vault, legal holds, DLP, Context-Aware Access), Active Directory Domain Services (AD DS: GPO, DNS, DHCP, ADFS, ADCS), PKI, email authentication (SPF/DKIM), SailPoint IdentityNow, BeyondTrust PAM, SAML/OAuth/OIDC, Kerberos, LDAP/S, RADIUS, MFA/SSO, zero-trust/ZTNA

Cloud & infrastructure: AWS (EC2, Lambda, CloudFormation, IAM, VPC, S3, Systems Manager), Azure (VMs, Functions, AVD), GCP, VMware (vSphere, ESXi, vCenter, vSAN, Aria), Hyper-V, Proxmox, Docker, SAN/NAS (Brocade Fabric OS, Fibre Channel, iSCSI), Veeam/Druva/NetApp, Nasuni

Hybrid & on-premises: Windows Server 2012 through 2025, WSUS, KMS, WDS, MECM/SCCM, MDT/WinPE/DISM, PXE boot, file and print services, Apache, IIS; offline and disconnected-capable patching, activation, and imaging

Observability & ITSM: Datadog, Splunk, Grafana, SolarWinds, PagerDuty, Statuspage; Zendesk, Freshservice, ServiceNow (ITAM, change control), Remedy, Slack administration and integrations; ticket and platform migrations

Security: CrowdStrike Falcon, Carbon Black, Jamf Protect, Wandera, Palo Alto (Panorama), Cisco Meraki, pfSense, Wireshark, VPN/IDS/IPS/WAF, data loss prevention; delivered in HIPAA, SOC 2, and SOX ITGC regulated environments

Automation & AI: PowerShell, Python, Bash, GAM, REST APIs, Okta Workflows, Freshservice workflows, Zapier, Tines; AI agent pipelines (FastMCP, Claude, GPT, open-source LLMs), RAG, structured output

Leadership: technical roadmaps, budget & vendor management, performance management, mentoring, DR/BCP, change management, stakeholder communication