

PATRICK BORGES

patrick.borges0514@gmail.com | 786-897-1651

SUMMARY

Systems and infrastructure administrator in managed services, currently supporting a municipal government and two police departments while managing and training junior technicians. Built a police department's CJIS security and compliance program across three sites. Strong in Active Directory and hybrid identity, Windows Server, Linux, network and firewall engineering, and infrastructure automation, with prior manufacturing and healthcare IT experience.

CORE COMPETENCIES

Systems & Infrastructure Administration | Deployment & Lifecycle Management | Vendor Coordination | Root Cause Analysis
IT Operations Management | Process Optimization | End-User Support Excellence | Incident, Problem & Change Management

TECHNICAL SKILLS

Directory, Identity & Endpoint: Active Directory Domain Services, domain controller deployment, OU design, Entra ID, Entra Connect, Microsoft 365 GCC, Microsoft Intune, Group Policy, AGDLP delegation, MFA (Duo, YubiKey), PowerShell

Networking: Cisco ASA/Firepower, pfSense, Ubiquiti UniFi, Cisco Meraki, VLANs & subnetting, site-to-site and client VPN (AnyConnect, WireGuard), dual-WAN failover, DNS (Pi-hole, Unbound, CoreDNS, DNSSEC), DHCP, NAT, nmap

Systems: Windows Server, Hyper-V, VirtualBox, Ubuntu, Debian, Fedora, apt/dnf package management, LVM/XFS, systemd, SSH

Security: Wazuh SIEM, Huntress, Microsoft Defender, Microsoft Purview, log retention & audit review, attack-surface reduction, least-privilege access design, network auditing & asset inventory (Snipe-IT)

Containers & Observability: Docker, Docker Compose, Portainer, Uptime Kuma, node_exporter

Tooling: Git/GitHub, SQL fundamentals, AI prompting for technical workflows (Claude Code)

PROFESSIONAL EXPERIENCE

Lansight Technology | Systems & Infrastructure Administrator | 2025 – Present

- Manage and train junior technicians, setting daily priorities, reviewing completed work, and developing their skills across Active Directory, endpoint management, and networking.
- Administer Active Directory and hybrid identity, network and firewall infrastructure, endpoint management, and public-safety systems for a municipal government and its police department.
- Serve as escalation point for complex infrastructure and security issues across the firm's other managed-services clients.
- Assessed a three-site, CJIS-regulated municipal police department against the FBI CJIS Security Policy and NIST 800-53 Moderate baseline for an FDLE audit, documenting control gaps with remediation roadmaps.
- Deployed the agency's first centralized SIEM and log-aggregation platform (Wazuh on Ubuntu Server), closing three documented audit control gaps and configuring CJIS-compliant retention (90-day indexed, 365-day archive) via automated index lifecycle policy and scheduled pruning; built and signed off the agency's first formal recurring audit-log review.
- Automated fleet-wide agent deployment through Group Policy using idempotent PowerShell staged in SYSVOL for zero-touch enrollment; integrated Microsoft Defender telemetry into the SIEM, validated the detection path end to end with controlled testing, and authored custom detection rules for alert tuning and false-positive suppression.
- Led the migration of the department's Computer-Aided Dispatch (CAD) system from CentralSquare to Mark43, coordinating vendors and stakeholders to maintain continuity of mission-critical public-safety operations.
- Built the department's remote-access VPN from scratch on Cisco Firepower, authenticating against Active Directory over LDAPS via a dedicated unprivileged service account, and deployed AnyConnect to give patrol officers secure field access.
- Engineered site-to-site VPNs linking remote sites to the main station (one new tunnel, one restored) and designed dual-WAN failover with a secondary carrier and segmented egress across a Cisco ASA/Firepower and pfSense fleet covering four VLANs.
- Replaced three failing access switches and a legacy hub in the main network closet with managed Ubiquiti UniFi PoE switches, modernizing the access layer and consolidating powered devices.
- Resolved UPN suffix rewriting and alternate-login-ID authentication failures in the agency's hybrid identity (on-premises Active Directory synced to Entra ID and Microsoft 365 GCC via Entra Connect) and made OU placement an enforceable policy control.
- Deployed a new Dell server, rolled out agency-wide MFA, configured patrol-unit GPS tracking, and owned user provisioning.
- Authored the agency's change-controlled CM-2 Baseline Configuration (network topology, asset inventory, control implementation record) and its Cybersecurity Incident Response Plan (CIRP).
- Performed FIPS 140-2/140-3 CMVP validation research across firewall, MFA, and mobile cryptographic modules, identifying firmware-to-certificate version mismatches that invalidated assumed compliance before audit submission.

Coke Florida | IT Analyst | 2024 – 2025

- Managed IT operations across 4 distribution centers supporting over 600 employees and 2,000+ devices.
- Administered Microsoft Intune and Active Directory, standardizing device compliance policy and streamlining onboarding.
- Deployed Meraki switches and wireless access points, strengthening network reliability across offices and warehouses.
- Implemented cabling and network-documentation SOPs, reducing repeat cabling faults and shortening fault isolation time.
- Supported enterprise A/V systems and Microsoft Teams meetings for executive operations.
- Reviewed change requests at the Change Advisory Board (CAB) for implementation risk and rollback readiness.

Health Choice Network | IT Field Help Desk | 2022 – 2024

- Supported over 500 endpoints and 300 staff members across multiple health centers.
- Optimized Microsoft Intune deployment workflows, tightening update compliance across the managed endpoint fleet.
- Administered on-premises Active Directory and Azure AD (now Entra ID), managing user accounts, groups, GPOs, and security permissions with zero access-related incidents.
- Installed and configured servers and networking equipment to improve clinic performance and reduce recurring ticket volume.
- Coordinated with vendors on infrastructure upgrades, improving uptime across clinic sites.

CERTIFICATIONS

- Microsoft SC-300 (Identity and Access Administrator) | CompTIA A+ | CompTIA Tech+ | ITIL 4 Foundation
- CJIS Security Awareness — Level 4 (IT/System Administrator)
- In Progress: LPI Linux Essentials (010-160) | CompTIA Network+ | Microsoft Azure Fundamentals (AZ-900)

EDUCATION

- Western Governors University (WGU) — B.S. Cloud & Network Engineering (Microsoft Azure) — In Progress
- Miami Dade College — IT Coursework