GEORGE ALBANESE

Endpoint Automation Engineer

917-657-0636 • George.Albanese@outlook.com • Remote (Norwalk, CT) • https://www.linkedin.com/in/george-albanese

PROFESSIONAL SUMMARY

Endpoint automation engineer with 10+ years of progressive IT experience, currently owning modern device management, identity governance, endpoint security, and production automation for a remote-first organization. Manage a **585-device environment** across Microsoft Intune (Windows/iOS/Android) and Jamf Pro (macOS) with **80 configuration profiles** spanning security baselines, ASR rules, Defender EDR, BitLocker, and cross-platform compliance. Designed and built the organization's entire **Conditional Access framework (20 policies)** and app protection policies across Android, iOS, and Windows. Build and operate production automation — HR-driven provisioning, termination workflows, CVE intake, and data-protection backups. Core stack: **PowerShell, Microsoft Graph API, Azure Automation, Intune, Entra ID, Conditional Access, Defender, Jira.**

CORE COMPETENCIES

Endpoint Mgmt	Microsoft Intune (Autopilot, Config Profiles, Compliance, Remediations, App Deployment) • Jamf Pro • LAPS • DFCI
Identity & Access	Entra ID / Azure AD • Conditional Access (architect, 20 policies) • SSO / MFA • Certificate-based Auth
Endpoint Security	ASR Rules • BitLocker • Defender for Endpoint (EDR) • Defender AV • Windows Firewall • SmartScreen
Automation	PowerShell • Microsoft Graph API • Azure Automation Runbooks • Azure Blob Storage • SQL
ITSM & Dev Tools	Jira • ServiceNow • Remedy • Git • Dayforce (HRIS Integration)
Platforms	Windows • macOS • iOS/Android • M365 • Teams • SharePoint • Google Workspace

PROFESSIONAL EXPERIENCE

Endpoint Automation Engineer — Revalize, Inc. *2022 – Present*

Owns modern endpoint platform, identity governance, endpoint security, production automation, and data protection for a fully distributed US workforce.

- Own the endpoint platform across **585 devices (543 Intune / 42 Jamf)** with **80 configuration profiles**, 7 compliance policies, and a 117-app deployment catalog spanning Windows, macOS, iOS, and Android.
- **Designed and implemented the organization's entire Conditional Access framework** — 20 policies covering per-platform compliance enforcement (Windows joined/BYOD, macOS, iOS, Android), tiered MFA (admins, all users, guests, Azure management), risk-based policies via Entra ID Protection (risky sign-ins, high-risk users), legacy auth blocking, BYOD containment, and W365 Cloud PC access controls.
- Own endpoint security stack: **Attack Surface Reduction rules** (Office child process blocking, PSExec/WMI blocking, LSASS credential theft protection, vulnerable driver blocking), **BitLocker** (silent deployment + non-TPM handling), **Defender for Endpoint/EDR** across Windows and macOS, Windows Firewall, and **LAPS** with version-aware pilots.
- Manage **app protection policies (MAM) across Android, iOS, and Windows** for BYOD data protection; maintain compliance policies differentiated by enrollment type (Azure AD Joined, Registered, W365, macOS) with Threat Defense connectors for iOS and SOC 2 controls for mobile.
- Operate **Windows Autopatch with staged deployment rings** (Test → Ring1 → Ring2 → Ring3 → Last) for Edge and M365 Apps updates; build and maintain proactive remediations including WinGet-based update workflows.
- Built HR-driven onboarding pipeline *(Dayforce → Azure Automation → SQL queue → provisioning dispatcher)* with idempotency, retry/backoff, kill switches, and structured logging — **saves ~10–15 minutes per new hire** and ensures consistent, auditable provisioning.
- Implemented termination automation tied to Jira tickets: date-gated execution, certificate-based Graph API auth, idempotent account disablement, automated Jira audit comments, and mailbox-to-shared-mailbox conversion — **saves ~5–10 minutes per offboard** and strengthens compliance posture.
- Built CVE intake automation *(Teams trigger → Defender TVM API enrichment → Jira ticket creation)*, standardizing vulnerability triage and removing a recurring manual step from the security review cycle.
- Own data protection workflows backing up **4–5 Google Workspace tenants and 5–10 SharePoint sites** to Azure Blob Storage with integrity validation and CSV-based change logging; coverage actively expanding.

- Built and standardized Jira Service Management intake forms and Virtual Service Agent flows; reorganized Confluence knowledge base to improve onboarding and operational documentation.

Technical Support Specialist I — Brookfield Properties *2019 – 2022*

- Delivered white-glove end-user and executive support (200+ employees) across M365, Cisco Jabber, WebEx, VPN/remote access, iOS devices, and new hardware; provided direct CEO-level support during critical incidents.
- Led 1:1 executive onboarding and training (VP/SVP level) on new hardware, conferencing platforms, and productivity workflows.
- Supported office transitions and expansions: documented current-state environments, assessed technology requirements, and coordinated deployment of temporary and permanent workspaces.
- Authored internal knowledge base articles; trained and mentored 3 deskside technicians on Remedy/ServiceNow, Intune concepts, Cisco tools, and conference room hardware.

System Analyst II — NYC Health + Hospitals (Bellevue) *2018 – 2019*

- Supported clinical applications and network operations in a fast-paced hospital environment, providing incident triage, troubleshooting, and escalation for Epic, Cerner, Quadramed, and eClinicalWorks.
- Managed a high-volume queue (40–60+ tickets/day), maintaining strong documentation, SLA adherence, and effective handoffs to Tier 2/engineering teams.

Analyst — ASI System Integration, Inc. *2017 – 2018*

- Managed a high-volume ticket queue (30–60 tickets/day; 100+ on peak days) providing remote technical support to field technicians and end users nationwide, ensuring timely escalation and SLA adherence.

Solutions Architect I — Network Access Corporation *2017*

- Monitored and supported multiple client networks in an MSP environment using PRTG, LabTech, ConnectWise, and FortiGate; maintained documentation covering vulnerabilities, inventories, firewall policies, routing, and DNS.

IT Specialist — Pittsburgh Technical College *2016*

- Provided frontline IT support to students, faculty, and staff; triaged and resolved technical issues while maintaining a strong service focus in a high-volume campus environment.

IT Helpdesk Intern — American Museum of Natural History *2014*

- Provided Tier 1 support (~15 requests/day) for museum staff; built, deployed, and re-imaged systems using Ghost. Assisted with a network technical audit under the Deputy CIO.

EDUCATION & CERTIFICATIONS

Associate degree, Information Technology — Pittsburgh Technical Institute *2015 – 2017*

Certifications: CompTIA Network+ • CompTIA Security+

In Progress: MD-102 (Endpoint Administrator) • SC-300 (Identity & Access Administrator) • AZ-104 (Azure Administrator)