Dev Bryant

Senior Endpoint Security Engineer | Identity and Automation

cv.bryant.dev root@bryant.dev linkedin.com/in/dev-bryant
Colorado Springs, CO github.com/quippy-dev

Summary

Senior endpoint security engineer with **10+ years** across security, systems administration, and Tier 3 operations. Lead the enterprise **ThreatLocker** deployment as primary engineer and point of contact for application control, rollout, recovery, and platform troubleshooting across **14,000+ Windows and macOS devices**. Engineer **CrowdStrike Falcon**, **macOS MDM (Jamf Pro)**, **Microsoft Intune**, **Entra ID**, and **Conditional Access** controls, and automate investigation, remediation, and difficult fleet recovery with **PowerShell**, Python, Microsoft Graph, and REST APIs. Lead the Delinea-to-**Bitwarden** migration, including policy, group-based onboarding, SCIM, and SSO. Previously led EDR engineering for **17,000+ endpoints** across **700+ MSP/MSSP tenants**.

Skills

EDR & Control	CrowdStrike Falcon (RTR, Fusion, PSFalcon), ThreatLocker (Ringfencing, application control), SentinelOne
Endpoint & MDM	macOS MDM (Jamf Pro), Intune, device compliance, security-tool deployment, configuration hardening
Identity	Microsoft Entra ID, SCIM/SSO, identity lifecycle, Azure app registrations, Exchange Online
Secure Access	Palo Alto Networks GlobalProtect, Strata Cloud Manager, Conditional Access, secure remote access
Automation	PowerShell, Python, Bash, Microsoft Graph and REST APIs, SOAR, AI-assisted engineering
Security Ops	Incident response, fleet remediation, endpoint telemetry, vulnerability assessment, Splunk, Cribl, NodeZero
Infrastructure	Windows, macOS, Linux, Windows Server, VPNs, VLANs, ACLs, enterprise firewalls

Experience

2026 | **Cybersecurity Engineer II, Ensemble Health Partners | Contract**

Endpoint security, identity, and automation for **14,000+ Windows and macOS endpoints**.

Endpoint Security Engineering

- Lead the enterprise **ThreatLocker** deployment as primary engineer and point of contact, owning policy design, Ringfencing, Secure Mode, application control, rollout decisions, agent recovery, and platform troubleshooting across the fleet.
- Build and maintain **CrowdStrike Falcon** policies plus **PSFalcon** and **RTR** workflows for investigation, containment, remediation, and recovery. Use Falcon RTR to repair broken security tooling, including failed ThreatLocker installations, when normal administration channels are unavailable.

Device Management & Identity

- Manage **macOS MDM (Jamf Pro)**, including system extensions, launchd services, security-tool deployment, and compliance remediation.
- Design **Microsoft Intune**, **Entra ID**, Conditional Access, and Exchange Online controls for device posture, identity, and application access.

Automation & Platform Rollouts

- Automate endpoint, identity, and Microsoft 365 administration with **PowerShell**, Python, Bash, Microsoft Graph, and REST APIs.
- Lead the migration from Delinea to **Bitwarden**, owning policy design, Entra ID onboarding groups, SCIM provisioning, SSO, use-case documentation, and the ServiceNow rollout plan.

Change Control & Documentation

- Write ServiceNow changes with implementation, validation, and rollback plans, plus technical documentation for security rollouts.

ThreatLocker | CrowdStrike Falcon / RTR | Jamf Pro | Intune | Entra ID / SCIM / SSO | GlobalProtect

2026 | **Cybersecurity Engineer (ThreatLocker Specialist), NDA | Contract**

ThreatLocker policy and remediation engagement. Additional details are covered by NDA.

ThreatLocker | Endpoint Security | Application Allowlisting

2025 | **Security Engineer, Visual Edge IT**

Led EDR engineering and automation for **17,000+ endpoints across 700+ MSP/MSSP tenants**. Served as Tier 3 escalation for endpoint investigations and difficult agent failures.

- Managed **SentinelOne** policies, STAR rules, exclusions, and indicator blocklists across the multi-tenant fleet.

Security Engineer, Visual Edge IT (continued)

- Designed configurable network quarantine policies in **SentinelOne**, using JSON allowlists for essential services (DNS/DHCP/DC) to avoid outages.
- Led **CrowdStrike Falcon** onboarding with Flight Control and parent/child CIDs. Wrote PowerShell scripts with **PSFalcon** to migrate policies across tenants.
- Built the **SentinelOne AIO Toolkit** (see Projects) to purge, install, roll back, and recover unhealthy agents at scale.
- Created **Falcon Fusion** workflows with Microsoft Teams for host-isolation approvals. Separately automated Azure app registrations through **Microsoft Graph**.
- Managed **ThreatLocker Ringfencing** and reviewed unknown binaries. Standardized **Horizon3.ai NodeZero** assessments and routed firewall telemetry through **Cribl** into **Splunk**.

SentinelOne | CrowdStrike Falcon | PowerShell / Automation | ThreatLocker | Splunk / Cribl

2024
2019

Linux System Administrator, HardenedVPN LLC

- Managed Debian and RHEL systems, including patching, SSH access, service reliability, and host firewall policy.
- Designed L3/L4 DDoS protection using **Cloudflare Magic Transit** and GRE tunnels for latency-sensitive services.
- Diagnosed production issues through logs, process inspection, and configuration review; applied ACLs and rate limits during incidents.

Linux Administration | Network Security | Cloudflare Magic Transit | VPN Infrastructure

2017
2014

Senior Technical Support Advisor III, Apple

- Handled Tier 3 AppleCare escalations for complex macOS and iOS issues involving account security, data integrity, device trust, crashes, and performance.
- Used logs and structured troubleshooting to isolate failures, coached advisors through escalations, and documented unusual defects for engineering and internal knowledge systems.

macOS / iOS | Tier 3 Escalation | Account Security | Technical Documentation

Projects

SentinelOne AIO Toolkit — 2025

Creator & Maintainer

Built and maintain a PowerShell toolkit used in production to purge, install, roll back, and recover SentinelOne agents across mixed Windows environments. Added API integration, package hash checks, execution timeouts, and service-tree cleanup to repair failed deployments safely at scale.

github.com/quippy-dev/SentinelOne-AIO-Toolkit

PowerShell | Automation | SentinelOne API

Home Lab Platform — Ongoing

Designer & Operator

Built and operate a home lab with MikroTik routing and switching, 10 GbE, multi-VLAN segmentation, UniFi gateway and access points, Rocky Linux and Windows Server hosts, more than 100 TB of storage, containers, and security tooling for automation and incident-response testing.

Rocky Linux | Windows Server | MikroTik | UniFi | 10 GbE

Certifications

CompTIA	Security Analytics Professional **(CSAP)**, Cybersecurity Analyst+ ce **(CySA+)**, Security+ ce **(Sec+)**
Microsoft	Azure Administrator Associate **(AZ-104)**, Security, Compliance, and Identity Fundamentals **(SC-900)**

Education

2023 **Cybersecurity Bootcamp**, Colorado State University / Fullstack Academy

- Completed **36 CEUs (360 hours)** of hands-on labs in network, endpoint, and application security.
- Placed **first in the cohort's Capture-the-Flag competitions**.