Nicholas Ferguson

Senior Platform Engineer

I build infrastructure as a product — from edge protection sensors and fleet management to developer platforms and build systems. Solo delivery, production quality, at velocity.

GitHub | LinkedIn | Download PDF

750K	9,775	172	11
Lines of Code	Test Cases	API Endpoints	Months
shipped to production	automated validation	designed & documented	4 security platforms, solo

SECURITY PLATFORMS

Built from Zero, Shipped to Production

Four security platforms delivered in 11 months as a solo engineer post-acquisition. Each built from scratch — architecture, implementation, testing, documentation, and deployment.

1 API Protection Platform SYNAPSE

Rebuilt from the ground up in Rust on Cloudflare's Pingora framework. Synapse is an edge protection sensor with on-board intelligence — all blocking decisions happen inside the reverse proxy process with zero network hops. Goes beyond traditional WAF rules with campaign correlation, full request and response body scanning, sensitive data detection (DLP), schema violation blocking, and behavioral anomaly detection.

80+ API endpoints **450µs** full-stack e2e **247µs** WAF + DLP **22+** DLP patterns **25MB** binary

72K RPS

Rust | Pingora

2 Edge Protection Hub SIGNAL HORIZON

Command plane for the Synapse sensor fleet. Centralized orchestration for deploying, configuring, and monitoring distributed edge protection infrastructure. Features data analytics, privacy-preserving collective defense across tenants, collaborative incident response, and threat hunting. Automated provisioning, health checks, and rolling updates across global fleet.

TypeScript | React | WebSockets | ClickHouse | PostgreSQL | Redis

Managed infrastructure serving $50M/year software

3 Security Testing Platform

Multi-tenant 8-tool integrated platform for attack simulation, rule validation, and security posture assessment. Includes rule studio, attack forge, orchestration engine, and knowledge exchange. Auto-provisions Synapse sensors and all infrastructure needed for 100K+ RPS distributed performance tests on AWS.

TypeScript | React | k6 | Docker | PostgreSQL | WebSockets | AWS

8 integrated tools, complete BAS capability

4 Linux Endpoint Agent

Lightweight agent for Linux systems that intercepts and routes traffic bound for AI model provider APIs to an AI firewall gateway for inspection. Kernel-level traffic interception with eBPF, minimal performance overhead, designed for transparent deployment in production environments.

Linux | systemd | eBPF | Rust

Kernel-level integration with minimal overhead

DEVELOPER PLATFORM

End-to-End Development Platform

Designed and built a complete internal developer platform for a multi-product organization — covering build, test, release, documentation, licensing, and infrastructure. Every component built to eliminate manual process and give engineers self-service access to the full development lifecycle.

Cross-Platform Build Engine

Custom DSL and framework that abstracted compile, package, version, and test operations for 3 flagship products and 20+ shared components across Windows, macOS, iOS, Android, Linux, and Embedded Linux. Self-bootstrapping with guaranteed reproducible builds. The engine itself was semantically versioned — infrastructure treated as a first-class product.

6 target platforms **3** flagship products **20+** shared components

PowerShell · C# · C++ · Docker · .NET · MSBuild · gcc · Yocto · LLVM · MSVC

CI/CD Automation

Built integrations that automatically updated and closed issues, notified QA with everything needing testing per release — saving hours of manual work by release managers. Built release branching tools for 3 products and 20+ components. Created the only GoCD PowerShell module with complete API surface coverage, plus a pipeline template diff/merge tool that reduced turnaround from 1+ hours to minutes.

GoCD · PowerShell · REST APIs

Static Analysis & Break Detection

Built a tool that analyzed nightly mainline builds to determine the breaking change and automatically notify the author. Zero false positives, 100% accuracy for compiler errors — no human triage needed for broken builds.

0 false positives **100%** accuracy

PowerShell · C# · C++

Documentation Platform

License Management Portal

Documentation-as-code platform with structured information architecture. Automated publishing pipeline, linting for style consistency, and topic-based authoring organized around the Diátaxis framework for tutorials, how-tos, reference, and explanation.

Antora · AsciiDoc · Vale · Diátaxis · JavaScript · Ruby

Self-service portal for managing legacy-format corporate licenses. Reduced turnaround from 3 days to instant for previously-approved licenses. Managed $2M total license value.

3 days → instant turnaround

$2M managed

C# · .NET · SQL Server

Hybrid Build Infrastructure

Designed and specced the hardware for a hybrid build infrastructure. AWS-hosted control plane with on-premises NAS and VMware cluster of compute nodes using SSD arrays for ephemeral build environments. Included custom artifact repository, release management platform, and a new telemetry system collecting metrics during builds. Resolved CPU WAIT times of 1–7 seconds that were bottlenecking the entire engineering organization.

AWS · VMware · InfluxDB · Grafana · C# · SQL Server · Linux · GoCD

OPEN SOURCE

Security Tools — Publicly Available

Open-source security tools built to validate real-world attack scenarios, test security infrastructure, and provide training environments. All publicly available on GitHub.

Apparatus Network Simulation Platform

AI-augmented network simulation supporting 13 protocols with fault injection, honeypot deployment, and traffic analysis. Built for security testing and network resilience validation.

13 protocol support · Fault injection · Honeypots

Python | Docker | React | 13 Protocols

Crucible Attack Simulation Framework

Comprehensive attack simulation framework with 119 pre-built scenarios covering OWASP Top 10, API abuse patterns, and advanced persistent threat chains.

119 attack scenarios · OWASP coverage · APT chains

Python | OWASP | REST APIs | Docker

Chimera Vulnerable Application Platform

Intentionally vulnerable API server spanning 450+ endpoints across 22 industry verticals. Purpose-built target environment for security tool validation and training.

450+ endpoints · 22 verticals · Training platform

Python Flask PostgreSQL Docker

TECH STACK

Production Experience

Full-stack production experience from kernel-level systems to cloud infrastructure to frontend applications.

LANGUAGES

Python | C# / .NET | TypeScript | SQL | Bash | C++ | Rust | PowerShell

INFRASTRUCTURE

Linux | KVM | RHEL | Ubuntu | SELinux | systemd | AWS | Serverless | Kubernetes / EKS | Docker | Terraform | Terragrunt | Ansible

DATA

PostgreSQL | SQL Server | MongoDB | InfluxDB | ClickHouse | Redis | Kafka (MSK) | Elasticsearch

SECURITY

WAF / API Security | OWASP | BAS | Threat Detection | DLP | Offensive Testing

PLATFORM

CI/CD Pipelines | Nginx | Fleet Management | Observability | Build Systems | Documentation-as-Code

METHODOLOGY

How I Build

AI-Augmented Engineering

The 750K lines in 11 months wasn't just long hours — it was a fundamentally different workflow. I treat AI coding tools (Cursor, Claude, Copilot) as force multipliers that let me operate at the architecture level while maintaining implementation velocity. The AI handles boilerplate and pattern execution; I handle system design, integration logic, edge cases, and validation.

This isn't "AI wrote my code." It's a deliberate engineering methodology — every line ships with tests, documentation, and review. The 9,775 test cases exist because AI-augmented velocity means there's no excuse to skip validation. The result is production-quality platforms delivered at a pace that typically requires a team of 4-6 engineers.

Infrastructure as Product

I don't build tools — I build platforms. Every internal system I create has API documentation, onboarding guides, and a developer experience designed for the engineers who come after me.

Documentation-First

Authored all published documentation at A10 Networks. Built docs-as-code platforms. I believe if it isn't documented, it doesn't exist.

Test-Driven Confidence

9,775 test cases across 4 platforms isn't an accident — it's the methodology. Comprehensive test coverage enables the velocity that AI-augmented development makes possible.

Solo to Scale

Built platforms that eliminated operational overhead for entire teams and automated routine work to create capacity for higher-value projects. One engineer's output, team-level impact.

$60K/mo

Identified and implemented infrastructure optimizations that reduced monthly AWS spend by $60,000 through right-sizing, reserved capacity planning, and architecture improvements.

This portfolio supplements a standard resume. All metrics are from production systems.

GitHub LinkedIn Download PDF