Cheyenne Bounds

/in/cheyennebounds/
contact@cheyennebounds.com

EXPERIENCE

T-Mobile | Seattle, WA | 2021 – Present

CYBERSECURITY ENGINEER, ZTNA (2/2025 – Present)

Develop, implement, and maintain secure network infrastructure solutions utilizing Zero Trust Network Access (ZTNA) and Virtual Private Network (VPN) technologies. Assess existing network security architectures and document findings and recommendations aligned with industry best practices. Monitor network security protocols and best practices related to ZTNA and provide guidance on improvements or updates. Respond to and manage cyber security incidents. Act as a leader and mentor to junior technical personnel. Collaborate with internal teams to develop and improve processes related to network security. Analyze data and trends to understand network security threats and vulnerabilities. Create and maintain technical documentation related to network security. Research and recommend new products and technologies to improve network security. Perform hands-on implementations and configurations of network security technologies. Ensure all security operations and maintenance activities are fully documented and up to date.

Key contributions:

- Supported identity- and policy-based access control implementations using Zscaler, integrating SCIM provisioning and Microsoft Entra ID to enforce Zero Trust access across legacy and data center–hosted environments.
- Integrated AI / LLM tooling into Tier 1-3 incident and service-task triage by building a custom knowledge MCP server (~19,000 indexed documentation chunks) and a suite of triage skills that encode team decision trees for internet-access, private-access, and endpoint-client requests.
- Automated 42% of previously manual security and access management tasks, increasing operational efficiency and reducing engineer workload.
- Built a DLP rule-builder CLI that detects sensitive (CPNI) data in carrier bills and proposes validated DLP dictionary/engine/policy configurations, and analyzed ~15,500 incidents and service tasks to surface recurring patterns and automation opportunities.
- Participated in control effectiveness testing and remediation efforts that resulted in 100% compliance with SOX, PCI, and CPNI requirements.
- Developed standardized documentation and repeatable evidence templates to improve audit readiness and support ongoing compliance cycles.
- Partnered with threat, engineering, and compliance teams to identify internal vulnerabilities, strengthen the control environment, and reduce insider risk in alignment with security best practices.

PROFESSIONAL PROFILE

Proven track record of innovation and leadership in the development and implementation of secure network infrastructure solutions by leveraging in-depth understanding of Zero Trust Network Access (ZTNA) concepts and application-level segmentation. Passion for maintaining the security of networks with a deep understanding of the security protocols and best practices associated with ZTNA, as well as experience in cyber security incident management and response. Ability to work independently and as part of a team, with excellent communication and problem-solving skills. Now integrating AI / LLM tooling (custom MCP servers and triage skills) into Tier 1-3 incident and service-task triage.

CORE COMPETENCIES

Enterprise Networking

Security Management

Project Management

Risk Assessment and Mitigation

Zero Trust Architecture

Security Operations

Vulnerability Management

Firewall & Endpoint Protection

SIEM Monitoring

DLP & Compliance Tooling

Security Documentation & Audits

Incident Response

Regulatory Compliance (SOX, PCI, CPNI)

Access Reviews

Cloud Security Principles (AWS/Azure)

Identity & Access Management (IAM)

EDUCATION

Master of Science (MS), Information Technology - Cybersecurity,
Purdue University Global

Bachelor of Science (BS), Computer Science,
Colorado State University Global

TECHNOLOGIES

Zero Trust Network Access (ZTNA): Zscaler, Axis, Prisma Access

(ZIA & ZPA)

IAM & SSO Integration

SIEM/SOAR Tools

Firewall (Palo Alto, Checkpoint)

SaaS Security

Cloud Migration

Configuration Auditing

AI / LLM Tooling (Claude, ChatGPT, Cursor) & Automation

Python

Splunk

ServiceNow

Jira

Agile/Scrum

Compliance Frameworks (SOX, PCI, NIST, CIS)

Email Protection: Proofpoint, Barracuda, SpamTitan, Mimecast

Data Loss Prevention (DLP): Microsoft Purview, Conditional Access, CASB solutions

Public Cloud Security: AWS, Azure, or Google Cloud Platform

DDoS / WAF: Cloudflare, Silverline, Cloud Armor

Firewalls / IDS / NDR tools

EXPERIENCE (cont'd)

T-Mobile Cont'd | Seattle, WA | 2021 – Present

ENGINEER, SYSTEMS ARCHITECTURE (4/2024 – 2/2025)

Oversaw total life cycle focus for the program from requirements development and architecture creation with a focus on complex system designs through architect definition. Partnered closely with internal teams, SMEs, program management, and Systems Engineering leadership to drive the technical solution across the program. Ensure the requirements and architecture focused on "building the right thing." Developed architectures, defining the physical architecture, allocating requirements to architecture elements, deriving requirements to drive details into the model, creating and refining modeling standards and design patterns, and distributing and merging model elements back into the baseline.

Key contributions:

- Designed and deployed hybrid-cloud infrastructure aligned with Zero Trust and On-Prem Cloud principles.
- Integrated advanced security protocols and hardening techniques to proactively reduce vulnerabilities and improve system resilience.
- Automated network operations, improving response times by 20% and reducing manual intervention.
- Led capacity planning initiatives to support traffic growth without degrading network performance.
- Developed and enforced policies to ensure high availability and compliance with SOX, PCI, and CPNI regulations.
- Collaborated with engineering and security teams to deliver secure, business-aligned network solutions.
- Mentored junior and senior engineers in troubleshooting, infrastructure best practices, and security-first design.

ASSOCIATE ENGINEER, SYSTEMS ARCHITECTURE (9/2021 – 4/2024)

Designed and developed system architectures, and defined key capabilities and performance requirements. Defined total systems design and technology maturity constraints in accordance with mission requirements. Developed system element architecture and design and interface definitions. Defined system implementation approach and operational concept. Developed models and architectural guidelines for current and future system development.

Key contributions:

- Led firewall and perimeter security operations, supporting high-priority applications and audits for SOX/PCI compliance.
- Managed escalations and high-pressure project requests with efficiency and consistent delivery under tight deadlines.
- Streamlined approval and validation workflows, reducing firewall rule turnaround times by 25%.
- Identified operational risks and implemented proactive measures to strengthen compliance readiness.
- Facilitated application migrations (e.g., PCF and TKE) while ensuring policy integrity and secure access during transition.
- Delivered technical documentation and collaborated with security, payment, and ops teams for infrastructure-aligned change control.
- Streamlined workflows and advocated for enhancements to operational tools to reduce friction and improve system performance.

Previous position as Launch Engineer Intern at Firefly Aerospace (built a Lua-based launchpad state warning system to USAF SSCMAN 91-710 range-safety standards) and Technical Support Specialist at Wave Broadband.