Connor Maddox

Information security architect

Security-first in any role.

Remote, US
deconfined@outlook.com maddox.sh LinkedIn GitHub

Information security architect with 15+ years securing regulated, global-scale environments across banking, enterprise, and the U.S. military. I design Zero Trust, network, and cloud security architectures across AWS, Azure, and hybrid environments, translating regulatory requirements into working controls: hardened baselines, Terraform guardrails, and security automation. My work connects threat modeling, hands-on engineering, and audit evidence to measurable reductions in risk, cost, and manual effort.

PROFESSIONAL EXPERIENCE

Lead Technology Engineer — Security Architecture & Migration Oversight · Valley National Bank

November 2024 – Present · Remote

- Own security architecture for an enterprise migration from on-premises infrastructure to AWS and Azure, embedding security by design as IT engineering replatforms 280+ applications.
- Package migration guardrails—trust boundaries, Zero Trust access, and hardened baselines—as reusable reference patterns, enabling teams to provision compliant workloads without per-application security review.
- Translate FFIEC and NIST CSF expectations into platform standards for logging, monitoring, identity, access, and configuration baselines, reducing security rework for individual workloads.
- Embed control validation and audit evidence collection in design reviews and CI/CD pipelines, reducing audit findings by approximately 20% across migration waves.

Cloud Security Architect · Valley National Bank

November 2021 – November 2024 · Remote

- Architected and validated cloud and on-premises controls against NIST CSF, CSA CCM, and FFIEC, establishing the baseline subsequently inherited by migrated workloads.
- Operationalized cloud security posture management with Wiz, identifying and reducing misconfigurations across AWS and Azure.
- Automated control validation and audit evidence collection in Python, reducing manual audit preparation by approximately 40% and improving consistency.
- Led architecture reviews for cloud adoption, digital banking, and payments, with hands-on guidance on WAF, firewall, identity integration, logging, and encryption.

Security Solutions Architect (Contract) · Santander Bank

June 2021 – November 2021 · Remote

- Designed and reviewed security architectures across business lines against NIST SP 800-53.
- Led security architecture for migrating credit card payment processing to a cloud platform, addressing application security, network segmentation, data protection, and PCI DSS scope.
- Delivered risk-based guidance balancing regulatory requirements with delivery timelines.

SVP, Managing Security Architect · Truist

April 2019 – June 2021 · Charlotte, NC

- Owned enterprise security architecture standards and review practices across 800+ applications, leading a team of nine architects.
- Led evaluation, selection, and deployment of a new endpoint security strategy, improving detection coverage while reducing cost by approximately 30%.
- Automated distribution of security guidance and reference patterns so a nine-person team could advise the entire $550 billion bank without becoming a delivery bottleneck.

Security Architect (Contract) · Credit Suisse

January 2019 – April 2019 · New York, NY

- Designed and deployed a global SOAR platform, automating triage and response and reducing SOC analyst workload by approximately 90%.
- Led market evaluation and integration of SIEM, endpoint, and gateway tooling aligned with NIST and ISO frameworks.

Security Solutions Architect · Dimension Data

November 2017 – January 2019 · Remote

- Designed global SD-WAN and Zero Trust network architecture for a worldwide consumer brand, bringing its global payment estate into PCI DSS scope.
- Led security solution design across 14 major global enterprise accounts, aligning architecture and controls with each client’s business and compliance objectives.

VP, Security Engineering & Architecture · Credit Suisse

February 2017 – November 2017 · New York, NY

- Redesigned enterprise vulnerability management, expanding coverage while reducing effort by approximately 30%.
- Realigned security products and processes with NIST CSF, establishing a stronger architecture baseline for program maturity.

Infrastructure & Security Solutions Architect (Progressive Roles) · Agio

November 2014 – February 2017 · New York, NY

- Designed an enterprise PKI migration with trust continuity, minimal downtime, and clear certificate lifecycle management.
- Led Tier 3 engineering and hands-on vulnerability assessment and remediation in client environments.
- Shifted client engagements to security-first delivery, identifying issues before deployment and reducing remediation cost by approximately 80%.

EARLIER EXPERIENCE

Senior Systems Administrator · Putnam City School District

2014

- Overhauled the network core, including switches and firewalls; selected and deployed a Fibre Channel three-tier SAN; and implemented defense in depth, saving approximately $145,000 per year.
- Rolled out a 1:1 student iPad program for digital textbooks and built an automated Minecraft for Education cluster with a custom web interface for teacher-deployed student instances.

Network Operations Supervisor / Systems Programmer · U.S. Air Force

2004 – 2011

- Served as a Staff Sergeant (E-5) in a second-level management role, leading first-line supervisors across multiple teams.
- Directed secure network operations and built mission-critical software, generating more than $1 million in combined annual savings.

TECHNICAL EXPERTISE

Cloud & hybrid security: AWS and Azure architecture (IaaS, PaaS, SaaS) · Secure workload design and migration governance · Hardened configuration baselines · Kubernetes and container security · CSPM / CNAPP (Wiz)

Zero Trust & network: Zero Trust architecture and SD-WAN · Segmentation, microsegmentation, and trust boundaries · Defense in depth, WAF, and NGFW · DDoS mitigation, DNS, and CDN security

Automation & infrastructure as code: Terraform and Python · CI/CD pipeline security (DevSecOps) · SOAR design and playbooks · REST / JSON APIs · Detection engineering requirements

Identity & access: SAML and single sign-on · Entra ID and Okta · Identity-centric segmentation · Privileged access boundaries

Threat & detection: Threat modeling (STRIDE) and MITRE ATT&CK · SIEM integration and SOAR automation · Endpoint strategy and vulnerability management · Data loss prevention and secure web gateways

Data protection & cryptography: PKI design and migration · Encryption gateways and tokenization · Hardware security modules · Certificate lifecycle management

Frameworks & compliance: NIST CSF and NIST SP 800-53 · FFIEC and PCI DSS · CSA Cloud Controls Matrix · ISO 27001

CERTIFICATIONS EARNED

CISSP (ISC2, earned 2016) · CNDA (EC-Council, earned 2017) · CEH (EC-Council, earned 2016)

EDUCATION

B.S., Information Technology Security · Western Governors University · 2017

A.A.S., Computer Science · Community College of the Air Force · 2010