

Matt Olds

Seattle, WA | 415-318-9797 | mtolds@gmail.com | <https://www.linkedin.com/in/matt-olds/>

Security Leader Driving Enterprise & Cloud Security at Scale

Identity & Access MGMT
SaaS Security & Vendor Risk Assessment
Data Privacy & Retention Schedules
Cloud Technologies
Cost Optimization
Workforce Development
Business Collaboration
Process Creation & Improvement

Security and IT leader with 13+ years owning enterprise and cloud security in high-growth SaaS environments. Hands-on across identity, endpoint, cloud infra, and SaaS security posture.

Build programs from scratch and operate them at scale with small teams: vulnerability management, incident response, and in-house security training.

Lead investigations, containment, and post-mortems as incident response manager. Partner with Legal on DSAR, privacy automation, and data retention. Have stood up vendor risk assessments, SaaS security reviews, AI tool review, and formal risk registries.

CAREER HIGHLIGHTS

- Served as **Incident Response Manager** for all security events at TuneIn | Partnered with the legal team to create the formal process for all security incidents. Led investigations, coordinated containment and remediation, and standardized post-mortem documentation across the organization.
- Stood up **continuous vulnerability management and annual penetration testing**, integrating findings into Jira for developer triage and remediation tracking.
- Deployed **container-level security** across all production systems, strengthening detection and response capabilities.
- Deployed a **Twingate-based zero-trust module** for GitHub Actions self-hosted runners, enabling secure CI/CD access to internal infrastructure with enforced IP restrictions on source code.
- Partnered with Legal to deploy **Transcend** for automated data classification and DSAR compliance. Owned end-to-end privacy request workflow.
- Owned **SaaS security and vendor review** for all company services including security intake and vendor risk evaluation. Managed negotiations and renewals for all Engineering org tools (AWS, Snowflake, Mode Analytics, Datadog, etc.).
- Drove **\$1M in annual cost savings two years running** through cloud and SaaS optimization, while maintaining and improving security posture.

PROFESSIONAL EXPERIENCE

TuneIn | Seattle, WA (Remote)

Director of Security, CloudOps, and IT | 2024 – Present

- Own enterprise security program end-to-end: identity, endpoint, SaaS posture, vulnerability management, and incident response across the corporate and production environments.
- Rolled out **annual penetration testing and continuous vulnerability management**; integrated findings into Jira workflows for developer triage and remediation tracking.
- Deployed **container-level security** across production, strengthening detection and response across all production systems.
- Defined and executed disaster recovery plan, including migrating production DNS to **Infrastructure as Code** to eliminate single points of failure.
- Conduct **SaaS and vendor security reviews** for the entire company; manage intake, risk evaluation, and remediation tracking.

- Partnered with Legal and Finance to implement contract management software (SpotDraft), tightening oversight on security and privacy clauses across vendor agreements.
- Directed AWS infrastructure optimization in parallel, delivering **~\$750k in savings** since the start of 2024 with minimal developer time required.

Tuneln

Sr. Manager of CloudOps, Security, and IT | 2021 – 2023

- Served as **Incident Response Manager** for all security events: led investigations, coordinated remediation across engineering teams, and standardized post-mortem documentation in Confluence.
- Implemented **Transcend** in partnership with Legal and compliance, enabling automated data classification and end-to-end DSAR request handling.
- Designed and deployed **CI/CD pipelines on GitHub Actions** with self-hosted runners behind Twingate, enforcing source code IP restrictions and securing build infrastructure.
- Strengthened identity and access posture across enterprise SaaS: Okta administration, MFA enforcement, and access governance for high-risk services.
- Built observability and cost-reporting frameworks (AWS, New Relic, Cloudflare) that doubled as security telemetry, enabling faster anomaly detection alongside cost remediation.
- Expanded org scope to include CloudOps and Security without adding headcount, scaling coverage through automation and tooling.

Tuneln

Manager of Corp IT | 2017 – 2021

- Strengthened security posture by deploying **endpoint protection, centralized password management (1Password), and MFA** across high-risk services.
- Built scalable on/offboarding and access lifecycle processes adopted company-wide, reducing standing access and orphaned accounts.
- Hired, trained, and developed a 5-person team supporting 300+ employees across 3 offices and remote.
- Owned IT-Finance partnership, managing budgets for hardware/software and optimizing vendor spend.
- Developed multi-channel support system (chat, email, ticketing) with sub-5-minute response SLAs.

Tuneln

Team Lead – Corp IT | 2015 – 2017

- Directed company-wide software rollouts including WebEx, GitHub, Egnyte, and Zoom, with security and access controls baked into each deployment.
- Managed office expansions and relocations, coordinating buildouts, moves, and teardowns.
- Expanded Jira adoption beyond Engineering, building and managing projects for Product, Sales, Finance, Legal, and Content teams.

Tuneln

Systems Analyst | 2013 – 2015

- Owned provisioning and lifecycle management of all employee hardware and software assets.
- Standardized onboarding/offboarding, including hardware provisioning and account management.
- Created first formalized new-hire orientation program, improving employee ramp-up time and consistency.

Digital House AV | San Francisco, CA

Lead Installer | 2007 – 2012

- Led AV installation teams and managed client-facing service calls.