CASE STUDY

Cybersecurity SOC 2 Compliance Within The Solution

athenaworks

Index

Project Overview

Career Equity is a workforce development platform designed to centralize and streamline the training-to-hiring process. It connects employers, training providers, job seekers, workforce development organizations, funders, universities, and support services organizations through a single, integrated solution that manages ATS functionality, training workflows, candidate tracking, and program analytics.

At Athenaworks Canwill, we also invest in solving industry-wide challenges through our own product innovation. Career Equity is one such initiative. Recognizing a critical gap in workforce development systems; fragmented platforms that separated training, candidate management, and hiring; we built Career Equity to unify the full talent journey. This is a Athenaworks Canwill-owned platform, purpose-built to modernize and scale equitable employment pathways across sectors.

Focus: Security & Compliance

As the platform handles sensitive data across public-private partnerships, education institutions, and clean energy initiatives, robust cybersecurity and compliance practices are critical.

The following sections detail the security innovations, governance measures, and compliance milestones that enable Career Equity to protect user data, support enterprise-grade availability, and meet regulatory expectations.

Platform Security Architecture

AWS Serverless + VPC: The Career Equity platform is built on AWS Serverless architecture with AWS Virtual Private Cloud (VPC). All services and APIs operate within the boundaries of the VPC, ensuring complete network segmentation and secure service execution. This architecture enforces strict access pathways, effectively acting as a built-in firewall and perimeter control mechanism.

AWS-Native Services: Career Equity leverages AWS IAM for access management, AWS CodePipeline and CodeCommit for secure CI/CD, and AWS Secret Manager for encryption of sensitive credentials. While Shield and WAF were not explicitly stated, firewall protections (deny-by-default rules) were confirmed, consistent with AWS defaults.

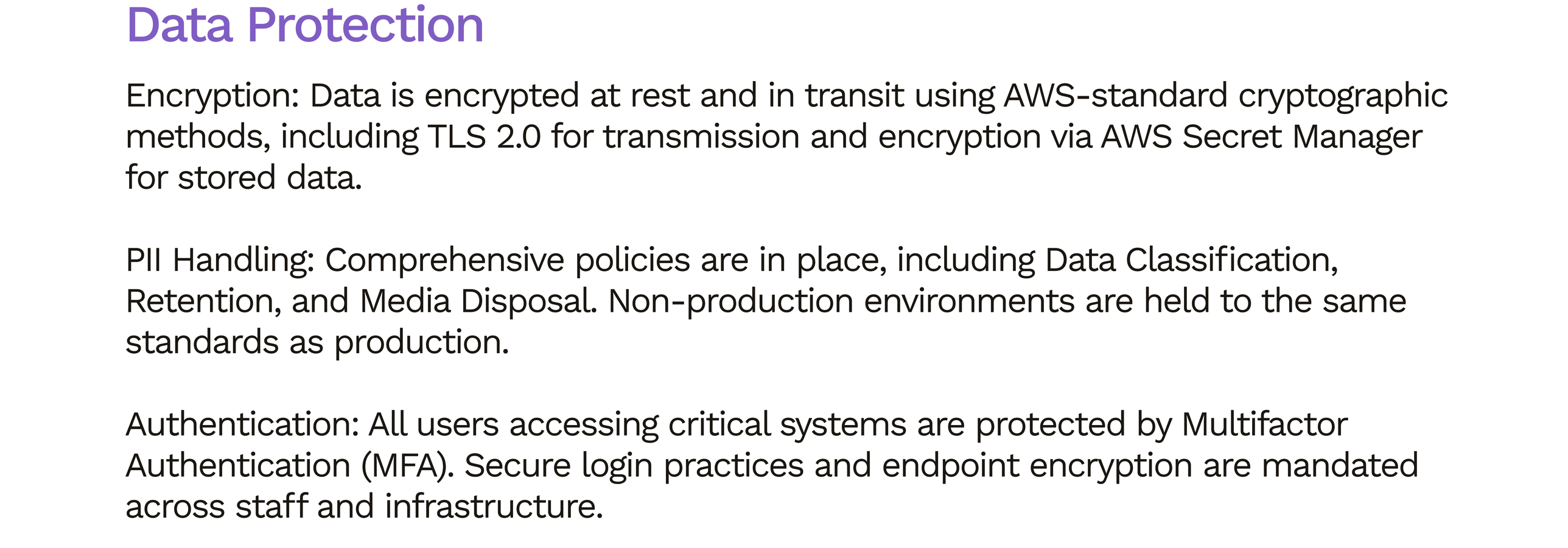
Data Isolation: The platform uses infrastructure-level network isolation within the VPC, ensuring that all development, testing, and production environments are logically segmented. Role-based access control (RBAC) and least-privilege principles are enforced.

Data Protection

Encryption: Data is encrypted at rest and in transit using AWS-standard cryptographic methods, including TLS 2.0 for transmission and encryption via AWS Secret Manager for stored data.

PII Handling: Comprehensive policies are in place, including Data Classification, Retention, and Media Disposal. Non-production environments are held to the same standards as production.

Authentication: All users accessing critical systems are protected by Multifactor Authentication (MFA). Secure login practices and endpoint encryption are mandated across staff and infrastructure.



Compliance and Certifications

SOC 2 Type II (2024-2025): Career Equity has been audited and certified by a third-party assessor. The audit confirms effective implementation of controls aligned with the Trust Services Criteria: Security, Availability, and Confidentiality. The following areas were reviewed and passed with no exceptions:

- Infrastructure and logical access
- Incident response and vulnerability management
- Risk assessments
- Vendor and subservice evaluations
- Policy enforcement and internal audit

Other Frameworks: While SOC 2 is the primary framework in use, encryption, access, and retention practices appear consistent with GDPR-aligned expectations. No mention of HIPAA or FedRAMP tracking.

AI Integration Security

External Service (Textkernel): Career Equity currently integrates Textkernel for resume parsing. Textkernel is believed to be SOC 2 compliant and handles sensitive data according to its own data privacy agreements. Career Equity ensures API integrations are secured and monitored.

In-House Parsing: A proprietary engine exists but is not yet live. Plans to replace Textkernel will involve formal internal compliance review.

Threat Monitoring & Incident Response

Threat Detection: Infrastructure is configured to generate and analyze audit logs and trigger alerts for suspicious or anomalous behavior. Sprinto is used for continuous compliance monitoring.

Incident Response: Documented procedures include roles, severity classification (S1–S4), and time-bound SLAs. Events are logged, reviewed, and resolved within defined timelines.

Penetration Testing: Annual penetration testing is conducted by a certified third-party vendor.

DevSecOps & Code Management

CI/CD: AWS CodePipeline and CodeCommit are used for deployments, governed by IAM-based access controls.

Secrets Management: AWS Secret Manager ensures that sensitive credentials are
Remaining tests are executed manually

- Jira is used for defect tracking and QA case management

Future Roadmap

Planned Enhancements:

- Migration to newer database and front-end frameworks (React upgrades)
- Gradual deployment of in-house resume parsing engine
- Continued updates to endpoint policies, audit logging, and IAM refinements

Governance:

- Although no rigid six-month cycle exists for security upgrades, ongoing quality and security controls (e.g., password rotations, policy refreshes) are enforced per SOC 2 standards.encrypted and restricted by policy.

Testing Tools:

- 40% of test cases are automated using custom scripts

Contact Us

athenaworks.com

athenaworks