finch

Whitepaper

Security at Finch









Table of contents

Welcome to Finch, where security comes first 3

Security principles 4

Global data and security compliance 5

People security 6

Product security 8

Data security 10

Infrastructure security 11

Monitoring and responding to threats 12

Continuity and resilience 13

About Finch 14

Welcome to Finch, where security comes first

Since day one, security and transparency have always been priorities at Finch. We are committed to protecting the data of our customers, employers, and employees. With our enterprise-level security practices and third-party audits, you can be confident about how your data is being stored, shared, and protected.

As always, we encourage you to contact us for more information. You can request a copy of our compliance reports and additional documentation through our Trust Center, or reach out to us via email if you have any other questions.

Finch: the trusted unified employment API

With Finch's API, applications can access data and make changes across payroll, HR, ben admin, and recordkeeping systems through a single API. And because our API handles confidential employee data, security at Finch is paramount.

This paper details the security practices that govern our core platform, which gives B2B platforms secure, permissioned access to their customers' HR and payroll systems through one integration. The core platform consists of five products: Organization, Payroll, Deductions, Benefits, and Recordkeeper.

Security principles

Separation of duties

No single user or system should have too much authority.

Universal participation

We recognize strong security posture requires the cooperation of the entire workforce. Therefore, every Finch employee is responsible for the security of our product.

Defense in depth

Layered security mechanisms increase the security of the system as a whole. If one security system is circumvented, other systems should compensate to resist the attack.

Risk-based security

We acknowledge our security focus should be defined by the set of unique risks we face. Therefore, we continuously identify and manage emerging threats and significant risks.

Minimize surface area

Every feature adds a certain amount of risk to the overall security of an application. We aim to reduce overall risk by reducing the attack surface area.

Least-privilege

We aim to ensure users and systems have the minimum level of access necessary to successfully perform their functions.

Continuous monitoring and logging

We implement continuous monitoring and logging mechanisms to detect unauthorized use and to support incident investigations.

Global data and security compliance

Finch is SOC 2 Type II compliant and maintains compliance with HIPAA, CCPA, and GDPR. We have also self-certified under the EU-U.S. Data Privacy Framework (DPF). Our SOC 2 controls are audited annually by an independent third party, and we maintain strict internal protocols to ensure ongoing adherence to these standards.

A SOC 2 Type II report assesses how a service organization safeguards customer data. It involves collecting data over many months to confirm that Finch is following proper security procedures. Our most recent report is available through our Trust Center.

In addition, we are a member of the HR Open Standards Consortium (our co-founder and COO serves on its board), which includes payroll companies that Finch integrates with, such as ADP.

People security

People are the most important part of every company. At Finch, we are proud to employ a secure workforce comprised of people who take data security and privacy very seriously.

Onboarding and offboarding

Account permissions are established and reviewed at key milestones, including onboarding, internal transfers, and offboarding.

Leadership team

Security is a key priority for all members of the Finch senior leadership team. Company executives routinely review security protocols and standards to ensure that Finch continues to take appropriate security measures and our policies reflect our commitment to being at the forefront of data security.

Training

Finch maintains a strong security culture by ensuring all employees have the training, tools, and knowledge they need. All new hires receive security training that educates them on potential risks, best practices, and how Finch addresses security throughout the product development lifecycle. In addition, employees must complete annual security training and attest that they will follow our policies.

For employees with advanced security-related responsibilities, Finch provides additional technical training as needed. Finch also supports employees and contract personnel in securing their personal devices and home networks.

Policies and standards

All employees and contract personnel are bound by Finch's internal policies and standards regarding the confidentiality of our customer data and other security-related concerns. Employees and contract personnel have access to these guidelines and are responsible for understanding and following them. Employees review our security policies annually, and our Security team audits and updates them each year.

Background checks

As part of our interview and onboarding process, we take a number of steps to screen and verify employees and contractors. These steps include:

- Background checks in accordance with local laws
- Verification of education and previous work experience
- Reference checks
- Additional measures as allowed

Ongoing education

Security is not static. As new potential threats and risks appear, we continuously educate our workforce about additional security requirements and guidelines.

Levels of access

If you don’t belong in a room, you shouldn’t have a key to get in. We review employee permissions and access on a quarterly basis and remove access when it is no longer needed. Contract positions receive access that expires no later than the end of their contract.

Endpoint security

Laptops provided by Finch have a number of security measures, including disk encryption (which limits connections to external drives), anti-virus and anti-malware software, insider risk monitoring software, and endpoint detection and response (EDR) security. We use a dedicated data loss prevention (DLP) platform to detect sensitive data such as customer PII and block it from leaving Finch through unapproved channels, including personal email, unsanctioned AI tools, and removable media.

Vendor assessment

A key part of people security is ensuring that our vendors meet our security requirements. We review vendors and consider the level of access they require, both prior to partnering with them and on a periodic basis thereafter, with the frequency and depth of each review based on the vendor’s risk tier. A current list of our subprocessors, including the AI providers we use for support ticket triage, bug triage, and QA, is available in our Trust Center. Data shared with these AI providers is not used to train models.

Product security

Finch's products are secure by design. Security is engaged right at the start of the design process, following the Finch Secure Development Lifecycle, to ensure our products, policies, and practices follow industry standards.

Change management

When software needs to be changed or updated, we follow a thorough, proven process to ensure stability throughout our production environment.

- Every change to Finch software is tracked and approved through an auditable process in which we consider the benefit versus the risk of the proposed change.
- Changes must be reviewed by at least one member of our team before being applied.
- We test changes before, during, and after implementation.
- When a change impacts an internal unit at Finch, one of our partners, or one of our clients, we communicate with them and address any questions or concerns.
- We perform comprehensive security-focused reviews before any product launch.

Monitoring and protecting applications

Finch uses advanced systems that alert us to anomalies and other concerns.

- A Web Application Firewall (WAF) to identify and address attacks on our application that may affect availability, compromise security, or consume excessive resources.
- Application changes are safeguarded by CI/CD pipeline automated processes, including automated tests, container scanning, and static application security testing (SAST).
- Application dependencies are regularly scanned for vulnerabilities. Automated Pull Requests are created to upgrade dependencies to versions that resolve the issue.

Penetration testing

Finch engages leading independent organizations to perform application-level penetration testing annually. Any vulnerabilities are addressed quickly and thoroughly.

Explicit consent and permissioning

Finch prompts employers to review and grant consent to the specific data points an application requests access to.

That means when you enter your account credentials and establish a connection it is:

- **Secure** — Transfer of your information is encrypted end-to-end.
- **Private** — Employer credentials will never be made accessible to the developer you grant access to.
- **Permissioned** — Only what your users' grant via Finch's product scopes will be shared with your developer's application.
- **Scoped write access** — We only allow write access when your user grants permissions via Finch product scope.

By being deliberately explicit with permissions and building an employer-centric platform, we continue to build trust and confidence.

Data security

Finch utilizes encryption, limited access, and other industry best practices to protect your data within the Finch core platform.



Classification

We classify data in different tiers, which allows us to allocate the appropriate resources to keep it secure. These internal designations provide a general framework for security-related practices throughout Finch.

- **Highly restricted** — confidential data that could have a significant impact on Finch, our partners, our clients, and/or our end users if it were released
- **Confidential** — non-public data that is intended only for internal use but is not highly restricted
- **Public** — available to anyone and does not require any security measures



Data access

Finch aims to follow the principles of least privilege when designing applications and procedures. Users and systems should have the minimum level of access necessary to successfully perform their functions. Employee access is removed upon termination of employment. In addition, we review who has access to production environments on a quarterly basis and have systems in place to restrict storage on flash drives and other removable media devices.



Data encryption

Finch utilizes encryption protocols to protect data.

- Encryption at rest: All data in our datastores are encrypted using AES-256 with keys managed via AWS KMS.
- Encryption in transit: All data to or from the Finch infrastructure is encrypted in transit using TLS 1.2+.



Data segregation

Finch implements logical separation between customers by tagging all data with associated Client IDs to delineate ownership and allow for secure multi-tenancy. Our application uses these identifiers to enforce access controls and protect against data leaks.

Infrastructure security

Our infrastructure is designed to follow industry standards to keep your data and your customers' data safe.

Secure cloud infrastructure

Finch is hosted on industry-leading cloud infrastructure, leveraging years of safety enhancements to ensure maximum performance, resilience, and speed of deployment.

- Network segregation — our infrastructure implements a tiered network architecture to isolate web servers and data stores from direct internet connectivity.
- DDoS prevention — Specialized load balancers function as choke points for inbound public traffic. Load balancers isolate our application servers from resource-exhaustion style attacks (DDoS, Slowloris, etc).
- Intrusion detection — our intrusion detection systems (AWS GuardDuty) continuously monitor our infrastructure and workloads for malicious activity and deliver detailed security findings for visibility and remediation.
- Audit trail — we record all event history of our AWS account activity to enable security analysis, resource change tracking, troubleshooting, and detecting unusual activity.

Asset management

Every cloud asset that is a part of our infrastructure is inventoried and documented to ensure that it is secured appropriately.

Logging and monitoring

By keeping a watchful eye over the production environment and maintaining detailed logs, we can identify problems—and implement solutions—extremely quickly. We log all impactful changes, actions, and authentication attempts, and maintain an audit trail accessible to authorized employees.

Access to the production environment

Only authorized personnel can access the Finch production environment, which is principally hosted on AWS. All access is remote, requiring connection through a VPN that is restricted to a small subset of users through stringent access policies.

Penetration testing

Finch engages leading independent organizations to perform infrastructure-level penetration testing annually. Any vulnerabilities are addressed quickly and thoroughly.

Patching

Finch addresses vulnerabilities through security updates and patches provided by vendors. If we cannot perform a live patch, we use the most recently available base image and cycle assets to enable updates.

Monitoring and responding to threats

As part of our proactive approach to security, Finch takes a number of steps to recognize potential threats, mitigate them, and respond swiftly to incidents.

Continuous monitoring

We protect your data by continuously monitoring Finch's infrastructure using industry-leading intrusion detection systems. We want to know where threats are likely to come from, so we can respond and block them swiftly and effectively.

Finch utilizes a variety of proven AWS products and services, including:

- AWS Web Application Firewall to isolate our application servers from resource-exhaustion style attacks (DDoS, SlowLoris, etc)
- Amazon GuardDuty, an intelligent intrusion detection system (IDS) that continuously monitors for malicious activity and provides comprehensive recommendations for remediation
- AWS CloudTrail to record all event history of our AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services

Responding to incidents

Our 24/7 on-call team ensures all alerts are immediately acted on, so your data remains secure. All members of our team are highly qualified and have clear roles and responsibilities in the event of a security-related incident. These precautions are designed to enable us to triage security incidents, minimize their impact, and prevent future occurrences. Our Incident Response Plan is tested periodically through tabletop exercises, and we document lessons learned after every resolved incident to continually improve.

Responsible disclosure

We strive to ensure that any vulnerabilities are addressed quickly and efficiently. If we find vulnerabilities with our vendors, we notify them immediately. If someone finds a vulnerability with any Finch products or services, we encourage them to contact us immediately by emailing security@tryfinch.com.

Continuity and resilience

Finch works closely with AWS and other world-class organizations and services to ensure that we are prepared to handle security incidents quickly and with minimal impact.

Multiple data centers

Even if there is an outage at one center, our network infrastructure spans numerous availability zones, allowing us to continue serving our clients and end-users with minimal disruption.

Data backups

Finch performs regular daily backups of data across our data stores. All backups are encrypted. Backups are restored to a non-production environment at least annually to validate their integrity.

Data center security

We chose AWS for our production environment largely because of their commitment to security, including (but not limited to):

- Locations selected to mitigate extreme weather and other environmental risks
- Access granted based on least privilege
- Multi-factor authentication mechanisms for authorized staff
- Comprehensive inventory management system
- Continuous audit tools for electrical and mechanical systems

Disaster recovery

Finch's disaster recovery plan, which is reviewed and tested on a regular basis through tabletop exercises, helps ensure the security of key data and processes. In the event of an emergency, this plan will be our blueprint for restoring data and services.

Learn More

To get more information about our comprehensive, multi-layer approach to security, please visit our Trust Center (finch.secureframetrust.com) for compliance reports and documentation, reach out to us at security@tryfinch.com, or visit tryfinch.com.

About Finch

Finch is quickly becoming the API of choice for applications looking to expand their compatibility because we are:

Developer-friendly	We focus on developers, and empower them to create world-class solutions.
Reliable	Our infrastructure is built for scale, with 99.9% platform uptime and more than 16 million employee records synced to date.
Secure	We operate a secure, compliant data transfer process and adhere to SOC 2 Type II, HIPAA, CCPA, GDPR, and EU-U.S. Data Privacy Framework standards.
Efficient	Build on top of our API and connect with 250+ payroll, HR, and benefits providers through one platform.
Enterprise-ready	Our API is built for large-scale synchronization, having connected 100,000+ employers to date.

This report was last updated November 16, 2026.