Hilti Fieldwire, Inc.

Type 2 SOC 3

2024

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

March 1, 2023 to February 29, 2024

Table of Contents

SECTION 1

ASSERTION OF HILTI FIELDWIRE, INC. MANAGEMENT

ASSERTION OF HILTI FIELDWIRE, INC. MANAGEMENT

March 8, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Hilti Fieldwire, Inc.’s (‘Fieldwire’ or ‘the Company’) Software as a Service (SaaS) Services System throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that Fieldwire’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in “Hilti Fieldwire, Inc.’s Description of Its SaaS Services System throughout the period March 1, 2023 to February 29, 2024” and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that Fieldwire’s service commitments and system requirements were achieved based on the trust services criteria. Fieldwire’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in “Hilti Fieldwire, Inc.’s Description of Its SaaS Services System throughout the period March 1, 2023 to February 29, 2024”.

Fieldwire uses Amazon Web Services, Inc. (‘AWS’ or ‘subservice organization’) to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fieldwire, to achieve Fieldwire’s service commitments and system requirements based on the applicable trust services criteria. The description presents Fieldwire’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fieldwire’s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Fieldwire’s service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Fieldwire’s controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that Fieldwire’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Fieldwire’s controls operated effectively throughout that period.

Eric DeFreitas

Eric DeFreitas
VP of Finance and Operations
Hilti Fieldwire, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Hilti Fieldwire, Inc.

Scope

We have examined Fieldwire's accompanying assertion titled "Assertion of Hilti Fieldwire, Inc. Management" (assertion) that the controls within Fieldwire's SaaS Services System were effective throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that Fieldwire's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Fieldwire uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fieldwire, to achieve Fieldwire's service commitments and system requirements based on the applicable trust services criteria. The description presents Fieldwire's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fieldwire's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fieldwire, to achieve Fieldwire's service commitments and system requirements based on the applicable trust services criteria. The description presents Fieldwire's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Fieldwire's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Fieldwire is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Fieldwire's service commitments and system requirements were achieved. Fieldwire has also provided the accompanying assertion (Fieldwire assertion) about the effectiveness of controls within the system. When preparing its assertion, Fieldwire is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Fieldwire's SaaS Services System were suitably designed and operating effectively throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that Fieldwire's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Fieldwire's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Fieldwire's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Fieldwire, user entities of Fieldwire's SaaS Services during some or all of the period March 1, 2023 to February 29, 2024, business partners of Fieldwire subject to risks arising from interactions with the SaaS Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
March 8, 2024

SECTION 3

HILTI FIELDWIRE, INC.’S DESCRIPTION OF ITS SAAS SERVICES SYSTEM THROUGHOUT THE PERIOD MARCH 1, 2023 TO FEBRUARY 29, 2024

OVERVIEW OF OPERATIONS

Company Background

Fieldwire was founded in January 2013 with the objective of optimizing field collaboration for the construction industry. The Fieldwire application connects the entire field team, from the project manager to each specialty contractor's foreman, on one construction management platform. Making it effortless for anyone to view their drawings, schedule work and track their punch list while they are in the field. The organization is based in San Francisco, California. In November 2021, Fieldwire was acquired by the Hilti Group, changing the name of the corporation to Hilti Fieldwire, Inc.

Description of Services Provided

Fieldwire provides full-service field construction management application for the construction industry.

Blueprint Viewer

Fieldwire’s construction management software provides projects with a fully featured blueprint management solution, making it easy for users in the field to view, edit and share drawings. The construction app makes it easy for clients to work off the latest plan information.

As-Built Drawing Software

Fieldwire captures as-built documentation with a full set of markup tools. At the end of a project, clients can export a comprehensive record drawing set. Fieldwire will automatically transfer the tasks and markups to the newest sheet version. That way, the client’s as-built drawings are always accurate and everyone on the project stays in sync.

Construction Management

The Fieldwire mobile and web-based construction management software allows you to easily assign work no matter where you are. You can set a priority, category, due date, and assignee to each chunk of work.

Building Inspection

Fieldwire allows the client to report issues directly from the construction site on their mobile device and document it with photos, annotations, and comments. Users are able to plan a full inspection containing hundreds of inspection items pre-loaded with building inspection checklists. As a building inspector, you can also share those checklist templates with the engineers and superintendents on the project to drive quality and consistency on the project.

Punch List

Fieldwire’s construction app allows clients to complete a walkthrough in minutes while attaching the pertinent details about each deficiency. Any contractor deficiency reported in Fieldwire can include photos, checklists, categories, hashtags, and due dates. Clients can create a template for common deficiencies with attached checklists and duplicate them across locations that need a Quality Assurance/Quality Control review.

Principal Service Commitments and System Requirements

Fieldwire has designed its processes and procedures to meet its objectives for its field construction management application. These objectives are established in order to incorporate the commitment to competence of the executive team throughout the organization.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offered provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the application are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role. Use of encryption technologies to protect customer data both at rest and in transit is in place.

Fieldwire establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Fieldwire's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System

Infrastructure

Primary infrastructure used to provide Fieldwire's SaaS Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	Heroku Dynos (Performance-M)	Runs Fieldwire web application through virtualized container-based infrastructure
Backend and Processing Servers	AWS EC2 (AWS-managed AMIs, Instance size varies)	Runs Fieldwire application programming interface (API) and background processing through virtualized container-based infrastructure
Databases	AWS RDS Aurora (Postgres)	Runs production Postgres database for Fieldwire API with daily and weekly backups
Databases	AWS Elasticache (Redis and Memcache)	Runs production Redis database for Fieldwire API background processing

Software

Primary software used to provide Fieldwire's SaaS Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
NewRelic	N/A	Monitoring application used to provide monitoring, alert, and notification services for the AWS production environment
Papertrail	N/A	Aggregate and store production server logs for the AWS production environment
Rollbar	N/A	Aggregate and alert around errors reported from AWS production environment

Primary Software		
Software	**Operating System**	**Purpose**
Sentry	N/A	Aggregate and alert around errors reported from AWS production environment
CloudWatch	N/A	Aggregate and store access logs for AWS and AWS production environment
Mixpanel	N/A	Aggregate and store engagement metrics from production web, iOS, and Android apps
Firebase	N/A	Aggregate and store engagement metrics, errors and crashes from production iOS and Android apps

People

The Fieldwire staff provides support for the above services in each of the following functional areas:

Security Committee - The Security Committee is comprised of the Quarterly Information Security meeting attendees. In addition to discussing existing risks, threats and vulnerabilities, the team identifies risks mitigated by controls already in place. Remaining residual risks are summarized and reported to Senior Management in a timely manner.

Senior Management - Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, will ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They will also assess and incorporate results of the risk assessment activity into the decision-making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

COO and CTO - The COO and CTO are responsible for the enterprise's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

System and Information Owners - The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. The system and information owners are responsible for reviewing, approving and when necessary, testing changes to their IT systems. Thus, they will sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware, etc.). The system and information owners will therefore understand their role in the risk management process and fully support this process.

System Users - The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, employee system and application users are provided with annual security awareness training, and customer users receive security guidance and documentation during onboarding and through support functions.

Data

Data is encrypted with AES 256. Customer personally identifiable information (PII) is specifically located and encrypted within the relevant data tables. Data uploaded by customers while using the application are also encrypted in transmission and when stored. Customer reporting is provided through the application and generated by customers directly.

Processes, Policies and Procedures

Fieldwire maintains a comprehensive Information Security Policy (ISP) that details the procedures that describe physical security, logical access, computer operations, change control, and data communication standards and expectations of employees. Employees are required to acknowledge their understanding and adherence to the comprehensive ISP upon hiring and re-acknowledge as significant changes are made.

Physical Security

The Fieldwire corporate headquarters in San Francisco, California require an authorized key fob to gain access to the office. The offices are monitored with video surveillance. The office remains locked after business hours.

Management performs annual access reviews to validate that persons with physical and logical access are active employees, and termination procedures applied ensure the timely retrieval of physical keys.

The customer-servicing production environment is housed within AWS who act as a sub-service organization to Fieldwire. AWS maintains the physical and environmental controls on which Fieldwire relies to protect its systems. No Fieldwire employees have physical access to the regional data centers currently.

To validate the continuing operating effectiveness of AWS' physical and environmental controls on which Fieldwire relies, Management obtains and reviews AWS' independent SOC 2 auditor's report on an annual basis for testing exceptions that would require further investigation and discussion with the service provider.

Logical Access

Fieldwire uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Employee access to the AWS environment is controlled, by role, via the AWS IAM (identity management) authentication tool. User, role-based, access is controlled in the application and authenticates to the database.

Assets, both production and corporate, are tracked and the inventory receives routine updating. Each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Passwords conform to defined, complex, password standards and are enforced through parameter settings in the AWS administrator dashboard and within the application.

Remote access into the production environment is tightly restricted to only authorized workers based on their role. Workers accessing the production and development systems remotely require an encrypted transport protocol to access and a second-factor authentication mechanism in the form of token, along with user ID and complex password.

On a quarterly basis, managers perform access reviews for workers with system access to assess the appropriateness of the access and permission levels and request modifications based on the principle of least-privilege, whenever necessary.

Computer Operations - Backups

Fieldwire performs full data backups nightly and weekly Applications deployed to the AWS platform are automatically backed up as part of the managed services process on secure, access controlled, and redundant storage.

Nightly and weekly backups are retained for specified intervals, and failure alerts are received by the VP of Engineering and his designees. Failed backups are investigated and resolved in a timely manner.

Fieldwire utilizes continuous monitoring tools with alerting enabled to assess system health and data throughput latency and errors which would signal if there were backup system issues. In addition, Management reviews the testing performed by independent auditors to validate the operating effectiveness of the AWS backup and recovery controls.

Computer Operations - Availability

Fieldwire monitors the capacity utilization of physical and computing infrastructure to ensure that service delivery matches SLAs by monitoring the AWS Dashboard, related metrics and alerts. Fieldwire evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Fieldwire utilizes the vendor alerts and AWS Dashboard for System Metrics health tool to monitor the application and database servers and infrastructure routers and switches. Packets per second and CPU Load are monitored within the production environment along with the servers' memory usage, RAM and disk space.

Additionally, multiple monitoring tools are deployed on the application and DevOps receives and reviews application/web server pre-defined error alerts. A proprietary script provides alerting that is reviewed on a daily basis for unauthorized or unexpected changes made to production servers, which could signal a security concern and ultimately impact availability, on the Production equipment.

Fieldwire has implemented an Incident Response policy and procedures to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Change Control

Fieldwire maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing results, whenever applicable, are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Infrastructure changes are performed by Fieldwire's infrastructure as a service provider, AWS, who houses the Fieldwire production environment within AWS data center locations. AWS is responsible for applying firmware and security patches; however, Fieldwire actively monitors vendor and security industry vulnerability notifications impacting its infrastructure servers, routers, databases, and operating systems to ensure timely patching by AWS personnel. In addition, Management reviews the testing performed by independent auditors, as documented in Section 4 of the AWS annual SOC 2 report, to validate the operating effectiveness of the AWS backup and recovery controls.

Data Communications

The Fieldwire infrastructure was architected with data encrypted communication channels between the application and database. Remote access is gained by a limited number of authorized administrators who provide a second-factor authentication mechanism, in the form of token, along with user ID, complex password, as well as the recognized IP address for each system being used to access remotely.

In addition, the Fieldwire production environment has undergone vulnerability and penetration testing to validate the security of the platform.

Boundaries of the System

The scope of this report includes the SaaS Services System performed in the San Francisco, California facilities.

This report does not include the cloud hosting services provided by AWS at the US West facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization’s last review.

Criteria Not Applicable to the System

All Common/Security and Confidentiality criteria were applicable to the Fieldwire SaaS Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at the US West facilities.

Subservice Description of Services

AWS is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

Complementary Subservice Organization Controls

Fieldwire’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for the trust services criteria related to Fieldwire’s services to be solely achieved by Fieldwire control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Fieldwire.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
	CC2.1, CC6.1, CC6.6, CC6.7, CC7.1, CC7.2	Network connections are routed through boundary protection mechanisms.
	CC6.8, CC7.2	Malware detection, virus detection, and alerting are enabled in the production environment.

Fieldwire management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet the relevant trust services criteria through contracts, such as SLAs. In addition, Fieldwire performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Fieldwire’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Fieldwire’s services to be solely achieved by Fieldwire control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Fieldwire’s.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Fieldwire.
2. User entities are responsible for notifying Fieldwire of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Fieldwire services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Fieldwire services.
6. User entities are responsible for providing Fieldwire with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Fieldwire of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.