FUJITSU

Solution Brief
Insight+ a New Way of Seeing

Security Aspects of the Insight+ Platform

Our comprehensive security strategy includes these components:

- Product security
- Operational security
- Physical and environmental security
- Business continuity management
- Organizational security

Introduction

Insight+ simplifies the health and performance management of complex technology infrastructures, while keeping customer systems and data confidential. This document describes the protections established by Fujitsu to ensure that our customers' data is fully protected, as well as describe the controls implemented to ensure the integrity and availability of the Insight+ platform.

Product Security

The Insight+ platform offers a range of security features that ensure complete privacy and security for customer data. The security stance of Fujitsu as well as its partners comprises a multi-layered strategy providing controls across all aspects of the platform encompassing the design and implementation stages; the transmission, storage, and access of customer data; and the ongoing operation of our technical infrastructure.

Data Classification and Handling

Fujitsu classifies customer data according to its sensitivity. Data classified as non-sensitive includes device identification information such as hostname and IP address, as well as the health and performance data associated with each device. Sensitive data includes device metadata (including operating system versions, SNMP community strings, and API passwords) as well as device configuration files, NetFlow data, and any personal identification for account holders.

The Insight+ platform encrypts confidential customer data upon receipt using industrial-strength AES encryption with the strongest possible key size (256 bits). Encryption keys are unique to each customer and generated in memory such that they are never stored to disk. This design ensures that it is virtually impossible for even the most sophisticated attacker to decrypt sensitive data.

Network Transport Protections

The Insight+ platform is accessed exclusively over HTTPS using Transport Layer Security (TLS) encryption via a browser, an API, or the Collector. TLS is a cryptographic protocol that protects against eavesdropping, tampering, and message forgery. The platform uses the most up-to-date version of the protocol (TLS 1.2), long encryption keys (2048-bit), and strong ciphers.

End-User Authentication

Insight+ user accounts are authenticated using a built-in authentication system, or via integration with a customer-configured identity provider via Security Assertion Markup Language (SAML). When using standard one-factor authentication, passwords are never stored directly but instead maintained in salted one-way hashes according to industry best-practice. In addition to minimum strength requirements, the hashing algorithm employs native resistance to brute-force attacks. Together these ensure that customer's passwords are safe even in a worst-case scenario. Two-factor authentication is also available to increase account security, either on a per-account or per-role basis.

Alternately, customers can elect to authenticate their end-users via their own SAML Identity Provider. Using SAML, our customers sign-in using existing credentials stored within their own in-house systems. As a result, authentication management policies such as password strength, password aging, or the use of multi-factor or biometric systems are directly controlled by the customer's existing systems.

Data flow overview

Role-Based Authorization

Once authenticated, end-user access is controlled by a sophisticated role-based access control (RBAC) system. Using RBAC, access can be limited to any area of the Insight+ platform via custom roles. For example, roles might be created to separate access on a device level, so that a network team and server team can't view one another's devices. Alternately, roles can be deployed to limit individuals' access to modify a monitoring collector's configurations. Roles can also control access to an individual account and its associated API tokens.

Network Whitelisting

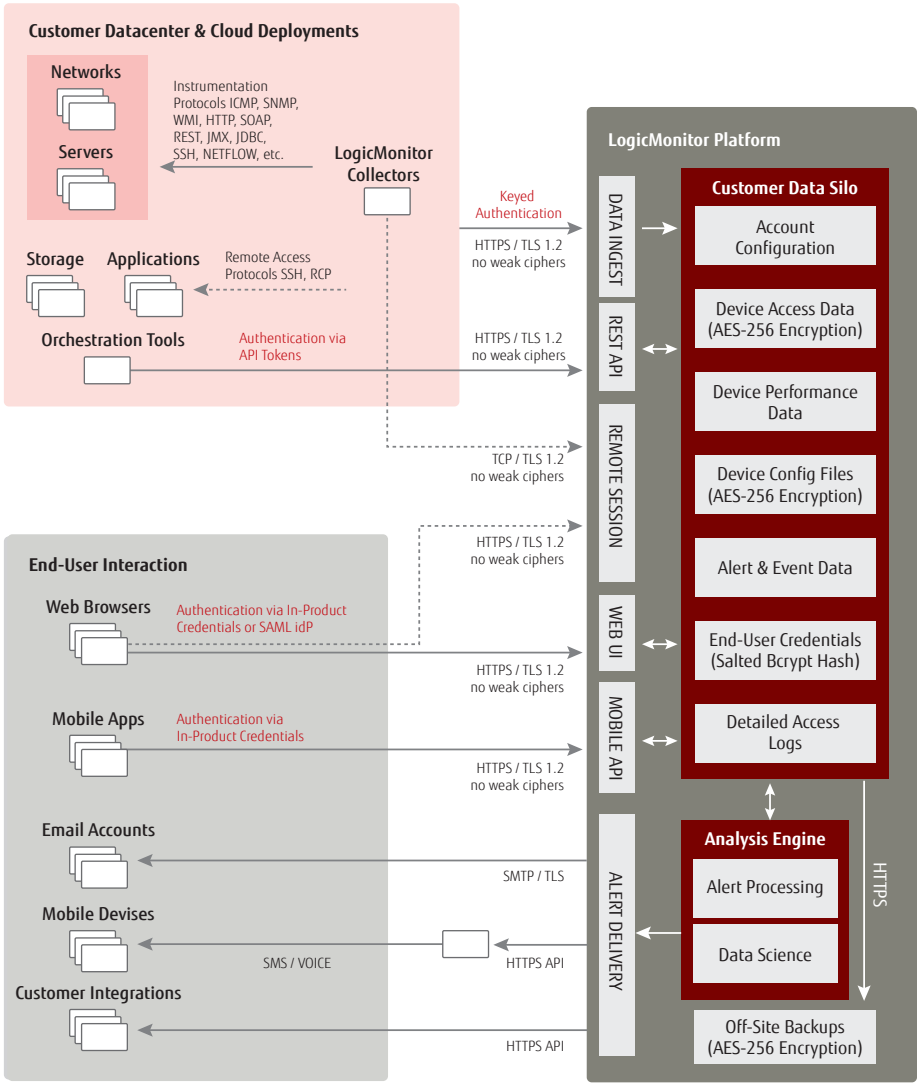
In addition to authentication controls, Fujitsu allows for the creation of a "Network Whitelist." This feature allows our Insight+ customers to provide a list of IP network blocks from which their account may be accessed. Any attempt to sign in from unspecified networks is blocked.

Collector Security

The collector has been carefully designed and developed with high security in mind. All communications made by the collector are outbound: either within your LAN to the devices it's assigned to monitor, or outbound to the monitoring platform. This design is specifically intended to limit the collector's attack surface.

Communication between the collector and the monitoring platform uses HTTPS/TLS with publicly-signed certificates to prevent man-in-the-middle attacks between itself and the platform. Each collector is cryptographically keyed to the platform via a strong credential which undergoes regular rotation. All sensitive device data handled by the collector is stored in-memory and never written to disk.

Figure 1: Insight+ Platform – Data Flow Overview



Keep customer systems and data confidential

Device Least Privilege

Best practices dictate that the Collector should have the lowest possible privileges to gather instrumentation for any given device; typically, read-only rights are sufficient. Access configuration for each device is entirely within our customers' control, and our support documentation provides details on how to configure the minimum required rights.

Secure Alert Transmission

Fujitsu supports the transmission of alerts via email, SMS, voice message, and API/webhook. Email alerts are delivered using Simple Mail Transfer Protocol (SMTP), with TLS encrypting alert message content. SMS and voice alerts are delivered to using authenticated APIs secured by TLS encryption. Any custom alerts configured via webhook can employ any security mechanisms the service endpoint supports.

Access Logging

The Insight+ platform maintains comprehensive, searchable audit logs which record actions taken within your account by end-users and API calls. Audit log retention is based on the selected pricing package (three months, one year, and two years). Offline storage of access logs via automatic report generation is possible through the platform's reporting features.

Penetration Testing

The platform is regularly validated via third-party penetration testing. Professional security teams are provided with the platform source code as well as full product access to validate the defensive security measures taken within the software development lifecycle.

In addition to third-party testing, a security defect testing regimen includes automated static code analysis (SAST), manual source code analysis, dynamic application security testing (DAST), along with manual testing for defects conducted from within the platform and collector environment. Any security defects discovered are escalated for immediate, highest-priority remediation.

Personally Identifiable Information

The monitoring platform is not intended to store personal data. Incidental collection of personal information is required for the purposes of user authentication, alert delivery, and auditing, but the scope of such data stored within the platform includes only the names, login credentials, email addresses, and (optionally) mobile device numbers of account-holders. These elements are considered confidential to our customers and handled accordingly.

The nominal personal information collected is only used in the context of service operation. This data is owned and controlled solely by the customer and is never shared with other organizations. Monitoring is performed in compliance with the European Union General Data Protection Regulation (GDPR) and offer a Data Protection Addendum (DPA).

Shared Security Responsibilities

The Insight+ platform provides a depth of security controls designed to be managed by account administrators. But customers must use these features consistently and effectively to ensure the security and integrity of their systems.

Specifically, end-user authentication, either using our stock authentication or SAML, should be configured such that each individual uses a unique account. Two-factor authentication is strongly recommended, either as provided in-product, or via a SAML identity provider. Appropriate roles should be created and assigned to user accounts based on the principle of least- privilege, restricting administrator access to as few individuals as possible.

Operational Security

The operational infrastructure on which the platform runs has been designed with high security as a primary consideration using a defense-in-depth approach to ensure comprehensive threat protection.

Platform Architecture

Fundamental to the security of the platform's operational infrastructure is the design of a multi-tenancy architecture, under which each customer account is created as a completely independent entity. Each customer account is logically and/or physically separated from every other, effectively isolating each customer from one another. This ensures that in the unlikely event of a security breach involving one account, other customer accounts remain protected.

Network and Operating System Security

The platform operates out of three geographically-distributed datacenters. Each operational footprint is secured by modern firewall systems employing intelligent packet inspection, traffic classification and filtering, and malware identification/blocking. The platform routes traffic through delivery controllers providing additional protections before sending the traffic to application servers. Production servers run non-virtualized Linux and are hardened according to defense-grade standards.

Network and operating system security

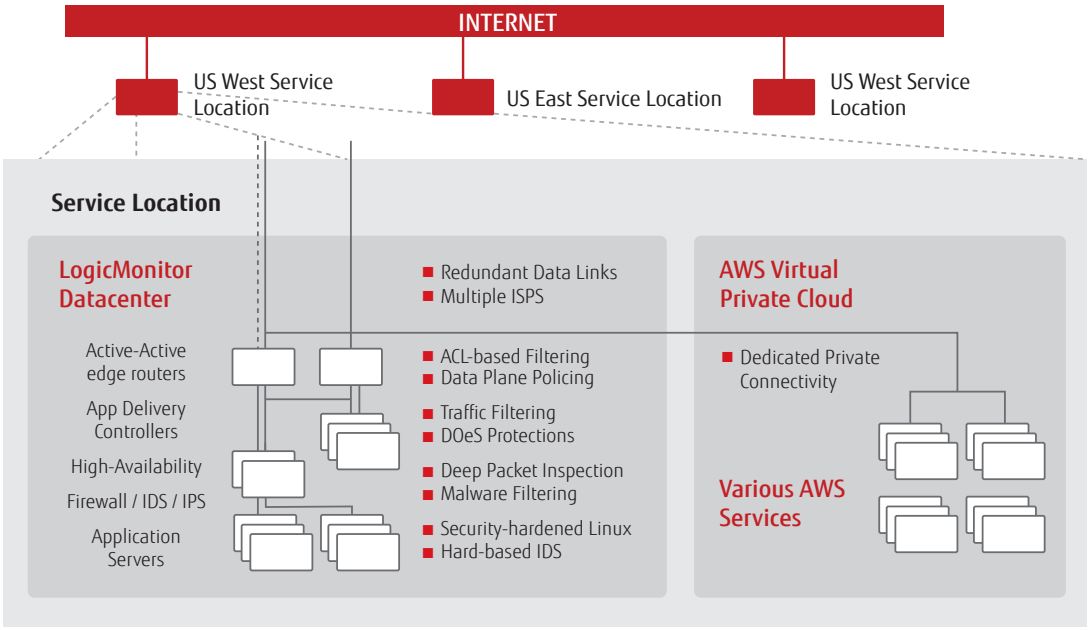


Figure 2: Network and Operating System Security

Vulnerability Management

Each application server runs intrusion detection software scanning for system vulnerabilities from within the production network. Vulnerability scans from both an internal and external perspective are conducted on an ongoing basis using commercial tools. This outside-in approach ensures that any possible issue is discovered. Once identified, the vulnerability is evaluated for risk, then prioritized and scheduled for remediation.

Incident Management

Insight+ has a formal incident management process for security events that may threaten the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. When an information security incident occurs, information security staff respond by logging and prioritizing the incident according to its severity. Events that directly affect customers are treated with the highest priority. Following remediation, incidents undergo post-mortem investigations as necessary to determine the root cause for single events, identify trends spanning multiple events over time, and develop new strategies to help prevent recurrence of similar incidents.

Physical and Environmental Security

The platform is operated as a hybrid deployment across colocated datacenters and Amazon Web Services (AWS) resources. To mitigate the risks from natural disasters and ensure continuity, service center locations are geographically distributed. Both data center sub-service providers and AWS maintain stringent controls around the physical and environmental security of each site. In the data center facilities, a five-step process is required to gain physical access to the servers, including a 24/7/365-manned security check, electronic keycards, and successive biometric scanning at each point of access. High-resolution video surveillance is also maintained throughout the facilities.

Environmental controls include:

- N+1 redundancy in generator-backed uninterruptable power
- N+2 redundancy in cooling capacity
- Very Early Smoke Detection Apparatus (VESDA)-based fire suppression
- Flood control
- Earthquake resiliency

Each facility is certified as compliant either with SOC 2 Type 2 or ISO 27001 standards, with their compliance reports reviewed annually to ensure ongoing maintenance of sufficient security controls.

Business Continuity Management

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, Disaster Recovery (DR) principles are integrated into the foundation of our service operation. The DR program includes multiple components aimed at minimizing the risk of any single point of failure.

Redundancy & Resiliency

In addition to maintaining operations across geographically-distributed service centers, a sufficient amount of redundant "warm-spare" hardware capacity is maintained in each location to absorb the failure of any other service location. Network equipment is deployed in N+1 high-availability pairs to provide for immediate failover. All devices

Multi-layered security strategy

employ redundant power supplies, each connected to independent generator-backed power circuits. Internet connectivity is fully redundant at each location, with WAN links to multiple ISPs maintained across physically disparate routing hardware.

Backup and Recovery

Backups of customer data are conducted via customer data "snapshots" every four hours. Upon generation, each snapshot is encrypted with a customer-specific key and transmitted to Amazon Web Services (AWS). Once in AWS, each snapshot package is replicated across at least two AWS geographic regions. A rotation schedule is maintained for each snapshot package, with a maximum retention period of one year.

The restoration of customer data from a snapshot is an automated process that can be actuated only by technical operations staff. The backup/restore processes undergo scheduled testing once per quarter.

Organizational Security

Personnel Security

Fujitsu personnel as well as that of our partner, are required to conduct themselves in a manner consistent with Fujitsu's guidelines regarding confidentiality, business ethics, and professional standards. Before hiring, Fujitsu and partner verify each individual's previous employment, conducts reference checks, and performs background checks where permitted by local labor laws and regulations. Upon acceptance of employment, all employees are required to execute a confidentiality agreement and must acknowledge receipt of and compliance with policies in our Employee Handbook. As part of the new-hire orientation, all employees receive baseline security training, with additional training provided based on an individual's role.

Access Control

Authentication

Fujitsu and our partner require a unique User ID for each of our employees, which each person must use to their activity on our corporate network. All business systems are configured such that they are only accessible by this unique account.

Access to any system that contains customer data requires authentication via a centrally-managed Single Sign-On (SSO) service. The SSO system enforces strong password policies, including password expiration, restrictions on password reuse, and minimum password strength.

On their first day of employment, each new employee is assigned an account and granted the minimum privileges required by their role as described below. At the end of an individual's employment, a policy-based workflow ensures that the associated account access is disabled.

Authorization

Access rights and levels are based on an employee's job function and role. Fujitsu uses the concepts of least privilege and need-to-know to match access privileges to defined responsibilities. Employees are granted only a limited set of default permissions to access common corporate resources. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives. Approvals are managed by workflow tools that maintain auditable records of all changes.

Accounting

Fujitsu's and our partner's policy is to log each authentication transaction and sign on request to each individual business system. These logs are maintained offsite in an immutable format and are reviewable on an as-needed basis.

Third-Party Auditing & Compliance

Fujitsu's partner has undergone multiple third-party audits of their information security program. The operation has been certified to the exceptionally high standards defined by the International Standards Organization, and is certified to the ISO/IEC 27001:2013 standard for security program management as well as the ISO/IEC 27017:2015 standard for the secure operation of cloud services. They maintain an audit program against the AICPA's Service Organization Controls (SOC) Trust Services Principles. Their processes around service infrastructure, software, people, procedures, and data handling are compliant with SSAE 18 criteria, and maintain a SOC 2 Type 2 report as certification.

Conclusion

Fujitsu is committed to keeping customer data safe and secure. The entire organization embraces each component of the multi-layered security strategy. Currently, thousands of customers trust Fujitsu and our partner to assist with the management of their technology infrastructure and we invest in that trust every day. Our customers can rest assured that Fujitsu and our partner value the confidentiality, integrity, and availability of their data.

Fujitsu Network Communications, Inc.

2801 Telecom Parkway, Richardson, TX 75082
Tel: 888.362.7763

us.fujitsu.com/telecom

1.0/12.20