SIEMENS
Ingenuity for life

Siemens

MindSphere security model

Version 1.0

Enabling customers to confidently operate in a secure cloud environment

Executive summary

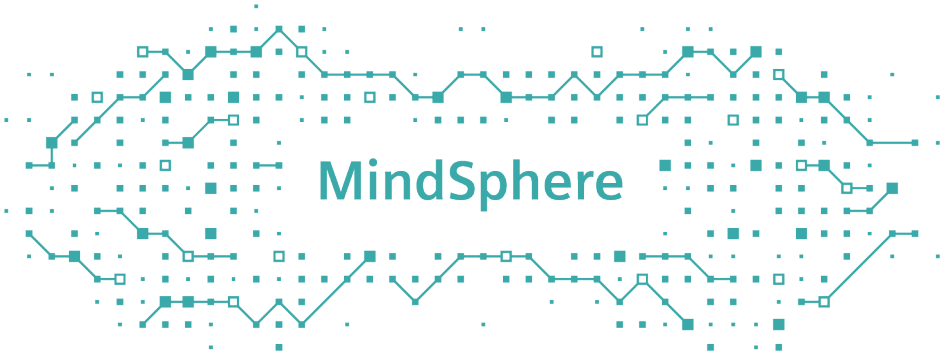
As an organization that leads in automation and connected devices, Siemens understands the importance of having in-depth, proactive cybersecurity policies. This knowledge is embedded in the foundation of the MindSphere security model. By working with cloud infrastructure providers and customers, Siemens can enforce consistent shared policies and practices for MindSphere. A multilayered security concept enables the guarding of sensitive data, applications, operating systems and infrastructures. As such, MindSphere approach integrates cybersecurity throughout the lifecycle of the Industrial Internet of Things (IIoT) platform.

Abstract

Digitalization is at the forefront of the next industrial revolution, Industry 4.0, enabling the IIoT. This IIoT revolution has given companies the capability to not only interconnect assets, products, value chains and business models, but also to collect large volumes of data and aggregate it in a centralized location for analysis. Although the IIoT offers significant opportunities for generating additional value, it also poses a new set of questions and needed controls for data and system security.

Industrial companies need to confidently expand digital service portfolios across global operations to drive greater value for customers, but security concerns can be a limiting factor. The connected device industry increases exposure points within value chains, threatening the security of data that impact business-critical functions. This makes it critical to select a proven IIoT solution, which has been developed by a trusted partner with strict security guidelines.

Security excellence is among the top priorities of Siemens for its MindSphere platform. Protecting data throughout its lifecycle, from connecting devices and data retention to decommissioning, is the sole mission of the dedicated MindSphere security team.



Governance, principles and guidelines

MindSphere architects implement security into the platform by design. The Siemens Information Security Policy establishes the basic principles for information security at Siemens, and by extension, MindSphere. It defines the mandatory high-level requirements and general rules for information security without being bound to specific technologies or platforms. This policy establishes blueprints for information system solutions to align with international standards. Security is embedded in the foundation of MindSphere with secure development lifecycle processes, design principles and guidance from Siemens' international security experts. These principles and guidelines drive all platform design decisions.

"Who protects my data?" This is often a key concern. Siemens' worldwide team of experts collaborate to protect the solution, assets and all customer data. They work on concerns that cut across the platform in cooperating with other areas of the MindSphere organization to maintain availability and resiliency.

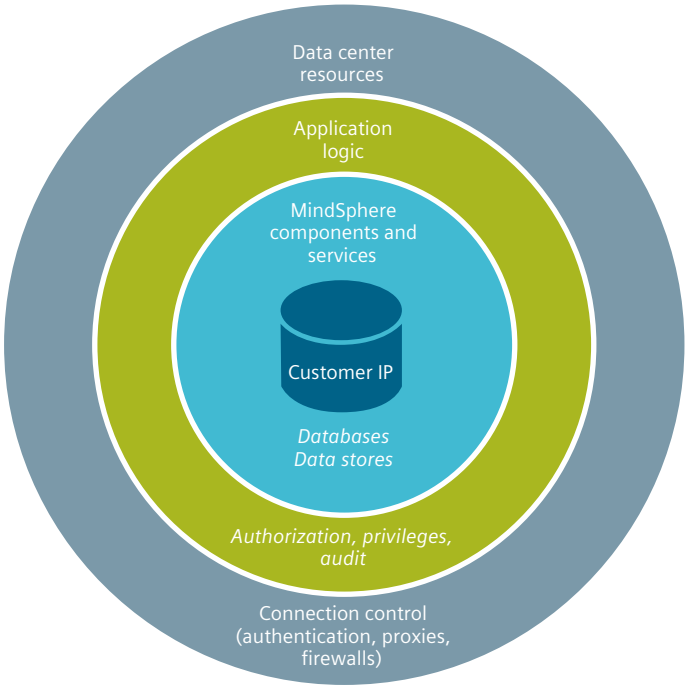


Figure 1: MindSphere multilayered security model.

Providing a secure environment

Industry standards and certifications

MindSphere follows industry standards for automation and control system environments designed to meet the highest level of security, such as the leading cybersecurity standard International Organization for Standardization (ISO) 27001 Information Security Management System Framework. This standard influences how MindSphere handles security at every level, from MindConnect device security to secure communications and throughout the data lifecycle. MindSphere is certified for International Electrotechnical Commission (IEC) 62443-4-1, secure development lifecycle (SDL). This standard defines requirements related to cybersecurity for products intended for use in the industrial automation and control systems environment.

MindSphere adheres to all local, national and international laws and regulations relating to the handling of data by a cloud platform provider in countries where it is offered. This includes, but is not limited to, the provisions of the General Data Protection Regulation (GDPR) addressing cloud platform providers. A compliant MindSphere solution increases the availability of the platform and the services offered on it.

MindSphere has a multilayered security model, so Siemens is partnering with cloud infrastructure providers that meet the highest levels of international certification. Working closely with internal security expert partners, guidelines were developed to deploy best practices across MindSphere.

Security architecture

A strong IIoT solution requires a detailed security driven system architecture that can effectively represent multilayered security within the solution. The MindSphere platform is designed to be a scalable, resilient and efficient infrastructure. Features such as strict access management, encryption, network security, tenant and environment separation, and filtered communication channels through the controlling MindSphere Gateway are fundamental to the MindSphere architecture. MindSphere security features are not only evident, but are crucial to the operation of the entire system. Figure 2 depicts the security highlights of the MindSphere architecture.

Identity management and access control

The MindSphere access policy and rights model is an aggregation of state-of-the-art, rule-based and role-based rights models. This model conforms to the standards recommendations of the National Institute of Standards and Technology (NIST).

The identity and access management domain model dictates how a customer can authorize users and administrators within MindSphere. Maintaining a clear procedure for authorizing and consistently authenticating users with appropriate permissions protects sensitive data from disclosure. As seen in figure 2, access management between accounts is always run through JSON Web Token (JWT) checks.

Authentication and authorization

Granting appropriate access to data is at the heart of identity management and access control (IAM). MindSphere supports multifactor authentication (MFA) to confirm the identities of users trying to access the system. The passwords used with MFA follow international industry standards for required strength. Authentication and coarse-grained authorization at the web application programming interfaces (APIs) and web applications level rely on authentication and authorization information provided by MindSphere IAM components. The fine-grained authorization of MindSphere

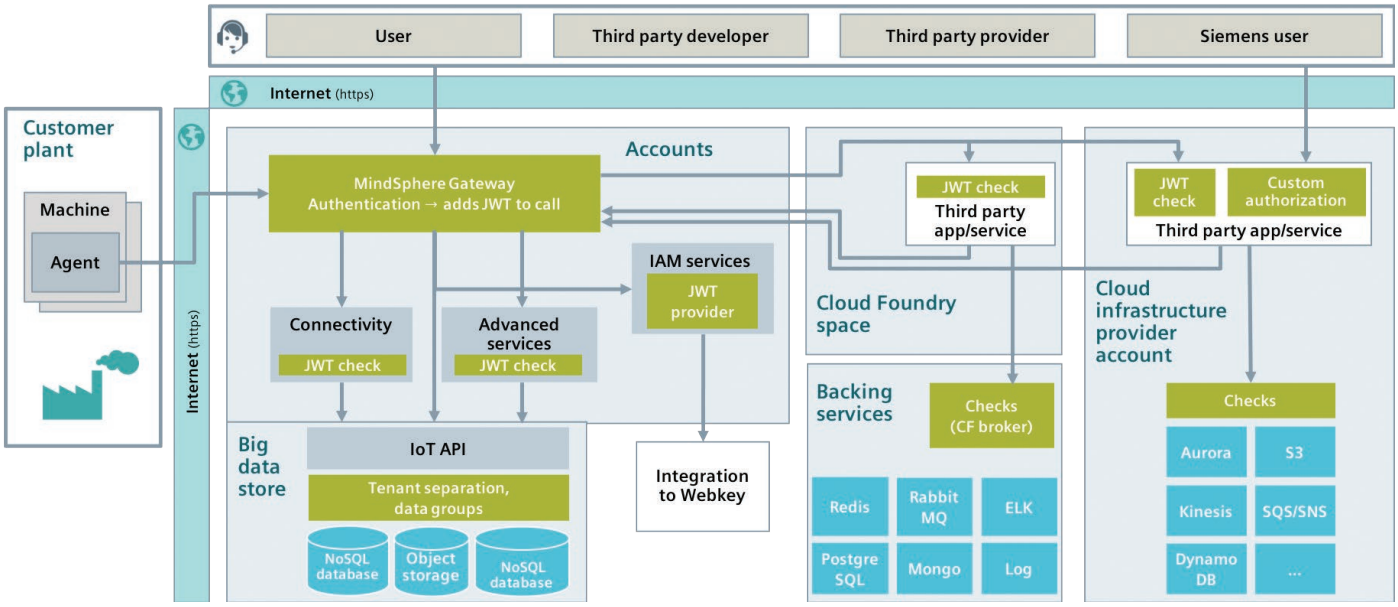


Figure 2: This diagram shows the MindSphere security architecture. All calls from users and devices go through the gateway.

comes from MindSphere APIs to validate authorized calls depending on the context of the application and the user permissions.

Secure communication

All communication from the client to MindSphere through public endpoints are secured through TLS v. 1.2, per industry best practices for communications. Reliable x509 certificates are used from the Siemens Trust Center, which are trusted by the European Telecommunications Standards Institute (ETSI) and the Certification Authority Browser Forum (CA/B Forum). MindSphere is using the state-of-the-art cipher suites with perfect forward secrecy (PFS) to avoid replay attacks.

Secure device connectivity

MindSphere supports software and hardware connectivity solutions that enable communication from customer equipment to MindSphere. But connecting both new and legacy machines comes with unique security challenges. Each customer needs differing connection solutions tailored to their needs, providing hackers the opportunity to exploit any new vectors in an IIoT environment if proper security measures are not in place. MindSphere defines how security is handled for both Siemens produced MindConnect hardware and MindConnect software-enabled devices. As can be seen in figure 3, MindConnect devices play a major role in the security system of MindSphere.

MindConnect device security

MindConnect devices provide secure, cost-efficient and easy connectivity from the field to the MindSphere platform. The devices come with strict rules for access control, onboarding and off boarding, network separation, data control and secure firmware updates.

Every MindConnect device has a unique identification number embedded in it. During onboarding, this number is used to register a particular MindConnect device for a particular customer. A device is onboarded only if it presents a valid unique ID and an onboarding security token, which is only issued to an authenticated and authorized user. This way, only valid MindConnect devices from Siemens are onboarded to MindSphere. The configuration files deployed in this manner are encrypted to provide for the confidentiality of the configuration files to be deployed on the device.

MindConnect devices employ security mechanisms to connect and send data only to the MindSphere platform. The devices only collect the data that is configured to be collected. Security relevant events that occur on these devices are logged, such as when someone-connects to MindSphere and installs firmware updates.

MindConnect devices adhere to specific standards to protect automation networks. Standards include separation of external and automation networks, supporting only outbound TLS v1.2 communication by the external network, read-only access to automation protocols, proxy support and off boarding.

Security patches and updates for potential software security vulnerabilities are made available for installation through online firmware updates. The device queries MindSphere regularly for a firmware update.

MindConnect Integration and MindConnect IoT Extension

MindConnect Integration and MindConnect IoT Extension are connectivity services that expand MindSphere connectivity to more protocols, business systems and devices. Securing these endpoints comes with a set of guidelines. The physical aspect of these elements rely on the standards of the infrastructure provider. To protect network aspects, limited ports and services come through the internet and all internal communication and data storage is encrypted for data confidentiality. Regular testing, logging, auditing and monitoring help to harden the application level to maintain industry standards according to ISO 27001. Coarse and fine-grained access controls use standard authentication and authorization processes based on realms, users, user groups and authorities.

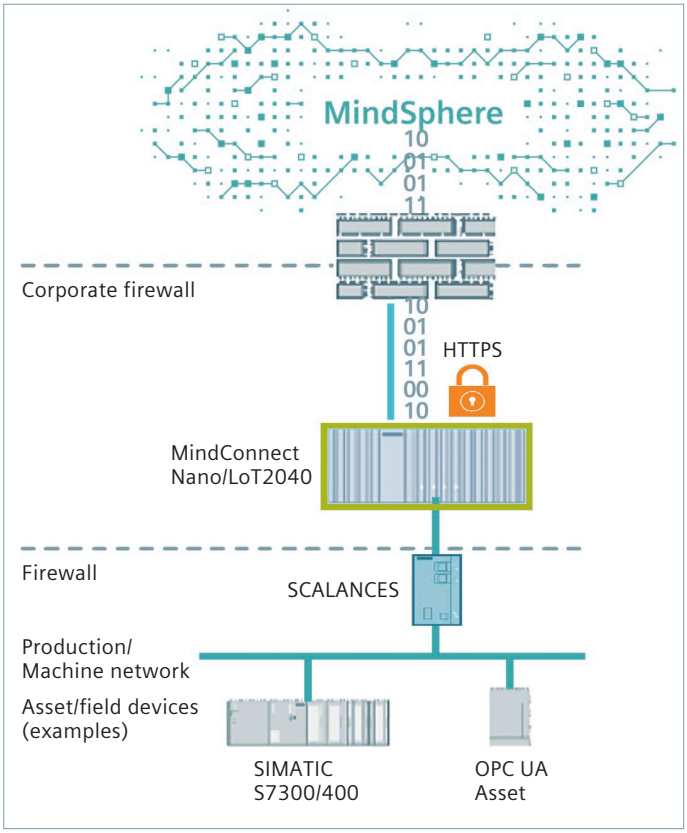


Figure 3: This diagram shows device security, connecting assets to the MindSphere IIoT platform.

Application and tenant management

Security at the web application layer protects MindSphere from vulnerabilities that account for the largest portion of attack vectors. Building a strategy for protecting applications and the tenants they are built on is important to the security framework as a whole. MindSphere employs strict tenant isolation and separation with API gateway support, validation checks and content security policies (CSP) to protect tenants and their applications. A web application firewall at the MindSphere Gateway filters external web application communication to prevent attacks.

The MindSphere CSP describes the type of resources the browser should load from which resources. It is a crucial step in creating a secure environment for applications. MindSphere customers, partners and internal developers are bound to the policy instructions and therefore offer additional security for applications interacting with sensitive data. Specific rules, policies and standards guide the CSP to increase security standards.

With MindSphere, Siemens is dedicated to making only quality solutions available to customers. Siemens reserves the right to check third-party applications before they go to production.

MindSphere digital offerings enable access across multiple environments through subtenancy, cross-tenancy and multi-tenancy. When exposing MindSphere to new users, securing the tenant is a primary concern of tenant owners expanding their digital services. Since the customer controls the data in MindSphere, they use the MindSphere IAM to employ granular access control for their data. That means tenant administrators assign and revoke roles and scopes to the appropriate users, viewers and editors to control visibility and the level of interaction that all customers have with their products, data and applications.

Protecting sensitive data

Availability controls

Data classification and encryption

Data classification methodologies categorize organizational data based on levels of sensitivity. Proper classification maps the controls, level of access and protection appropriate to the data. Although it is the responsibility of the data controller, Siemens works with its MindSphere customers and partners to help properly classify information levels, types and access. Within this model for classification, encryption standards, cryptographic keys and distribution protect information. Encryption masks sensitive information communication in a way that makes it unreadable without a protected key to decrypt the information back into a usable format.

All communications to MindSphere from an external network are done using HTTP over TLS v1.2. As shown in figure 2, all communications are secure when coming from external sources. The TLS configuration follows the latest security recommendations for strong encryption. Data-at-rest represents data that you persist for any duration, such as block storage, object storage, databases, archives and any other storage medium. By using authentication and authorization measures outlined in the identity and access management policies, MindSphere protects data-at-rest. If data is leaving the MindSphere internal network, then it is always encrypted in transit with the latest TLS algorithms as shown in figure 2. Unless otherwise determined by the customer, data is kept in the region where it was collected with no replication of data across regions. Integration with other systems is possible only via MindSphere IAM using the respective authorization mechanisms.

Datacenter protections

MindSphere collaborates with infrastructure providers that protect the physical storage of data and sensitive information at the server location. Infrastructure best practices are built to guarantee high scalability and availability. Through industry standards for physical equipment management, infrastructure providers maintain a multilayered approach to protect servers from hackers and unwanted users. Logging, monitoring, penetration testing and response teams make up the strategy for managing and limiting vulnerabilities onsite.

Backup and recovery plans

A comprehensive approach to data backup and recovery helps to mitigate the risk of data loss. Failing to appropriately plan for potential data loss can lead to disaster. MindSphere employs Siemens' Usage Transparency Service (UTS) to perform regular internal health checks and monitor systems that could potentially fail and compromise data. By following strict regulations, data is backed up daily and those backups are kept for 30 days. These data stores also employ strict tenant separation supported by MindSphere authorization mechanisms. Services protecting these stores also run redundantly in a minimum of two availability zones to maintain accessibility.

Security controls and monitoring

Detective controls help organizations understand the scope and potential impact of threats and security incidents. Identifying potential threats and security incidents before they occur and responding appropriately with incident management processes are a vital component of a secure response process. MindSphere security controls enable traceability – monitor, alert and audit actions. The operational teams responsible for vulnerability management focuses on identifying, assessing and mitigating commonly known vulnerabilities and configuration issues that might represent a potential risk to the security of systems or services. These same teams are able to detect and fix vulnerabilities autonomously as part of the continuous development activities.

Penetration testing

MindSphere penetration testing is done by Siemens security experts at regular intervals throughout the year to the extent permitted by law. Simulated malicious attackers attempt to break into the system and either steal data or carry out a denial-of-service (DoS) attack. Findings from the penetration tests are analyzed and followed up.

Logging, monitoring and audit logs

MindSphere monitors the security related events of cloud infrastructure configurations to maintain compliance with internal Siemens regulations. These are monitored with best practice checks based on the Siemens internal threat and risk analysis (TRA) process and the primary recognized industry standard for cybersecurity, the CIS Benchmark. If issues are found, notifications are sent to the appropriate MindSphere teams for correction.

Keeping a detailed record of activity throughout a solution allows security teams to practice forensic security activities. MindSphere collects cloud provider infrastructure logs using native services. These services keep track of who uses the infrastructure resources, how they use it, when they use it and where they use it. Internally, MindSphere logs cloud provider resource usage and IAM and access control platform events.

Audit logs track security events through a chronological record leading up to an incident or event. In addition to standard logging, audit logs provide the sequence of events important for incident resolution. Detailed actions and events are chronologically logged across the solution.

Summary

Data privacy

Compliance with data protection principles and laws is as important to Siemens as it is to our customers. An overview and summary of the MindSphere privacy architecture can be found in the "Siemens MindSphere Data Privacy White Paper."

Conclusion

Security is an important strategic pillar of MindSphere. Customer data must remain secure in the cloud. The Siemens MindSphere team is paving the way in IIoT security excellence, empowering its customers to confidently operate in a protected and secure environment. With the MindSphere multilayered security concept and architecture (figure 2), data is protected throughout the lifecycle, from connecting devices and data retention to decommissioning.

Security review

Multilayered approach for network, system and user-level security

Certifications and standards

- MindSphere follows the ISO 27001 Information Security Management System Framework
- MindSphere is certified to IEC 62443-4-1, secure development lifecycle

Architecture

- Identity management and access control
  - Role based access control (RBAC) model
  - Coarse grained authorization
  - Multifactor authentication
- Communications
  - TLS v. 1.2 for communication from client to MindSphere through public endpoints

Connectivity

- Hardware
  - Onboard only with valid, unique ID and security token
  - Separation of external and automation networks
  - Encrypted configuration files
  - Read-only access to automation protocols
  - Proxy support
  - Secure offboarding
- Software
  - Encrypted internal communication and data storage

Application and tenant management

- Tenant isolation and separation through API gateway support, validation checks and content security policies

Availability and security controls and monitoring

- Data classification and encryption
  - HTTP over TLS v1.2 to communicate to MindSphere from external network
  - MindSphere data is encrypted in transit with TLS algorithms
  - Data remains in region collected
- Backup and recovery
  - Siemens' Usage Transparency Service
  - Data backed up daily and kept for 30 days
  - Services protecting data stores run redundantly in a minimum of two availability zones
- Controls and monitoring
  - Penetration testing
  - Threat risk analysis process
  - Audit logs

Siemens

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

www.siemens.com/mindsphere

75966-A7 12/18 C