Kendis Security

We take our customer’s data security very seriously. We ensure the integrity of our customer’s data by using enterprise level security to perform audits on our application and networks.

Data center and network security

Kendis works very hard to ensure the integrity and confidentiality of your data. The data is hosted on AWS data centers that are certified as ISO 27001 and PCI/DSS Service Provider Level 1. Our Security Team is prompt to respond to security alerts and is available on call 24/7. Learn more

Application security

Safeguarding customer data is of the highest priority for us. We pride ourselves on taking effective measures and tests against security threats that can be made on our customer data. Penetration tests are done regularly.

Learn more

Product security features

Communications made with Kendis servers are all encrypted using industry-standard HTTPS. Our customers can easily manage their mode of access such as LDAP and Kendis authentication. Learn more

Best practices

At Kendis, we use the best security practices to make certain that your data is protected. Learn more

General Data Protection Regulation (GDPR)

You have complete control of your data at all times Learn more

Datacenter & network security

Physical security	
Facilities	All of your service data made in Kendis is hosted in AWS data centers. These are certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC II compliance. The AWS infrastructure is equipped with impeccable services that safeguard your data. These services include back-up power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data.

Physical security

On-site Security	To have the best on-site security, AWS has one of the best security measures that includes security guards, fencing, security feeds, and intrusion detection technology. Learn more about AWS physical security.
Monitoring	The staff at Kendis constantly monitors all Production Servers. While physical security, power, and internet connectivity are monitored by AWS.
Location	Kendis leverages AWS data centers in the United States. With Private Cloud hosting option customers can choose AWS location in the United States, Europe, and Asia.

Network security

Dedicated Security Team	Our Security Team is prompt to respond to security alerts and is available on call 24/7.
Protection	We use top of the line security for protecting our network. We also perform regular audits and utilize network intelligence technologies that watch for any attacks or malicious activity.
Architecture	For our network security architecture, we have divided it into various zones corresponding to their sensitivity, function and risk.
Network Vulnerability Scanning	Using proper Network security scanning, we are able to identify potentially vulnerable systems.
Third-Party Penetration Tests	At Kendis, we utilize the penetration testing services to perform tests on our Production Network.
Security Incident Event Management (SIEM)	This is critical in recording logs from key network devices and host systems. It also notifies the Security Team in case of any attack.

Network security

Intrusion Detection and Prevention	All services entry and exit points are closely monitored to detect any malicious activity. Alerts are generated.
Threat Intelligence Program	Our Threat Intelligence Program detects any threat that has been posted on threat intelligence networks. Quick action is taken against serious threats.
DDoS Mitigation	Kendis has architected a multi-layer approach to DDoS mitigation. We have designed a custom DDoS Component to prevent any sort of attack.
Logical Access	For accessing the Kendis Production Network, our employees have to use multiple factors of authentication.
Security Incident Response	If there is an alert, the teams providing network security are instantly notified and carry out the response.

Encryption

Encryption in Transit	All data transmissions are encrypted using industry best-practices HTTPS and Transport Layer Security (TLS) over public networks.
Encryption at Rest	Service Data is encrypted at rest in AWS using AES 256 key encryption.

Availability & continuity

Uptime	Kendis strives to maintain above 99% uptime. We rarely had downtime but in case it does, we assure you that we have our skilled engineers available 24/7 who would resolve this issue within minutes.

Availability & continuity

Disaster Recovery	In case of an event, we can easily recover from any disaster. Our strong technical environment, testing procedures and Disaster recovery plans ensure that.

Application security

Secure development (SDLC)

Security Training	We keep constant focus to train engineers on web application security covering OWASP Top 10 security risks and common attack vectors.
Java Spring Security Framework	We use Java Spring Security Framework for Kendis that are pertinent in reducing SQL Injection (SQLi), Cross Site Scripting (XSS) and Cross Site Forgery (CSRF).
QA	Our testing team ensures extensive and detailed testing.
Separate Environments	Production Environment is completely isolated from testing and staging activities. We make sure that all of our testing and staging activities are done in separate environments. We do not use any Service Data for testing or development.

Application vulnerabilities

Dynamic Vulnerability Scanning	With the help of Third Party security tools, we are able to scan and identify any security risks of the OWASP security risks, dynamically.
Static Code Analysis	We use static analysis tools to scan the source code.

Application vulnerabilities

Security Penetration Testing	Safeguarding customer data is of the highest priority for us. We pride ourselves on taking effective measures and tests against security threats that can be made on our customer data. Penetration tests are done regularly by Kendis.

Product security features

Authentication Security

Authentication Options	Our authentication options include Kendis secure sign-in, Okta single sign-on, and Active Directory for on-site deployments.
Secure Credential Storage	Kendis stores passwords which are not saved in human readable format hence enhancing its security.

Additional product security features

Role Based Access Controls	Kendis has different permission levels. Access to data is governed by role based access control (RBAC), and can be configured to define granular access privileges.
Transmission Security	All data transmissions with Kendis UI’s and API’s are encrypted using industry standard HTTPS/TLS over public networks.

Additional security methodologies

Security Awareness

Policies	Kendis has a very stringent set of security policies which are shared transparently with all the employees who have access.
Training	Our all employees have to attend an annual Security Awareness Training and all engineers receive annual Secure coding Training.

Employee vetting

Background Checks	All new employees are vetted carefully during the recruitment process.
Confidentiality Agreements	Newly hired employees have to sign a Non-Disclosure and Confidentiality agreement.