REEKOH

Security Feature Highlights

Why we care about Security

Security is a core principle at the very centre of the Reekoh platform and product suite. It's importance to the acceptance and success of IoT cannot be understated, and Reekoh is committed to accelerating the widespread adoption of IoT.

As an enterprise-grade platform, our customers also expect us to have this commitment to security. For them, IoT represents not just business intelligence and operational efficiencies, but new business models. Our solutions power this revenue generation, so things need to work securely.

Reekoh takes is responsibility as a steward of sensitive data seriously. Secure management of this data, and prevention of data breaches, is paramount to building credibility for all parties in the market.

IoT solutions are like chains, linking numerous vendors and technologies together, and the weakest link is where vulnerabilities can be exploited. Our approach to security is to mitigate as many of these weak links as possible.

Our modular framework gives us the ability to rapidly develop and mature new features, including our security capabilities. We have compiled here a high-level overview of the key security elements of the Reekoh platform and product suite.

To speak with one of our IoT security experts, email security@reekoh.com

External cybersecurity auditing

Reekoh has worked with cybersecurity experts Entersoft as external security auditors, to test and validate our technical design and implementation of various security features.

Entersoft was deeply involved with Reekoh's engineering team, consulting on "security by design" principles, as well as providing ongoing vulnerability and bug testing.

Entersoft recognises Reekoh's efforts to reduce security threats and maintain rigorous security standards, and passed the Reekoh platform through its security testing process.

ENTERSOFT

OWASP
Open Web Application Security Project

Reekoh's Security Features

Device Identity

- Every device that publishes data needs to be known to the platform
- If a device is not known, Reekoh will simply reject the data
- Inventory Sync integrations are used to simplify synchronising of Reekoh device identities with other 3rd device registries or master records
- Flexible device identity field selection (on Gateway plugins)
- X.509 Client Certificates (optional)

Secure IoT Protocols

- Reekoh runs an internal CA which allows it to issue server certificates
- Use various security features of specific protocols
- Prioritise use of MQTT/S, HTTP/S and TCP over SSL/TLS
- Use DTLS for UDP, CoAP and LWM2M
- Bring your own PKI, enabled through the Gateway API

Cloud Security

Microsoft

- Reekoh's IPaaS runs on Microsoft Azure
- Azure provides massive scalability particularly with elastic scaling and management of containers
- Access to a Security Toolkit (Load Balancers, WAFs, etc)
- Get benefits of ISO x without cost
- Provides Blueprints for security
- Federation with Office 365

Secrets Management

HashiCorp Vault

A Tool for Managing Secrets

- We deal with a range of secrets - Passwords, API Tokens, Keys
- Use HashiCorp Vault with SSL Transport for storing secrets
- Use password fields in configurations (no over the shoulder data loss)
- Metadata is stored in Vault as well to secure any sensitive values

Container Isolation

- Reekoh is a leader amongst IoT products in its adoption and architecture of Kubernetes / Docker / Micro Services
- Containers give ability to isolate each component on a pipeline so each plugin only knows what it needs to
- No data contamination
- Kubernetes has market-leading features for configuration management
- Reduces human error

Role-Based Access Control for Users

- Granular pre-defined roles for users
- Users can build Custom Roles specific to their requirements
- Revoke User access
- API tokens inherit user roles
- Lock down data workflow pipelines to specific users to control access to various IoT use cases

---

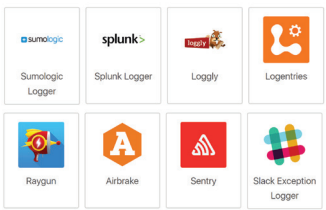
API Token Security

- JWT Web Tokens with Expiry
- APIs are protected via SSL
- Use of Auth Tokens (instead of username and password)
- Tokens are linked to Roles (RBAC for API)

HTTPS

- All of Reekoh's web services and interfaces are secured with SSL
- Reekoh follows best practice configurations (DH and Server)
- Implementation of HSTS, disable insecure ciphers
- Use of Public CAs to ensure websites are trusted

Platform-wide Logging



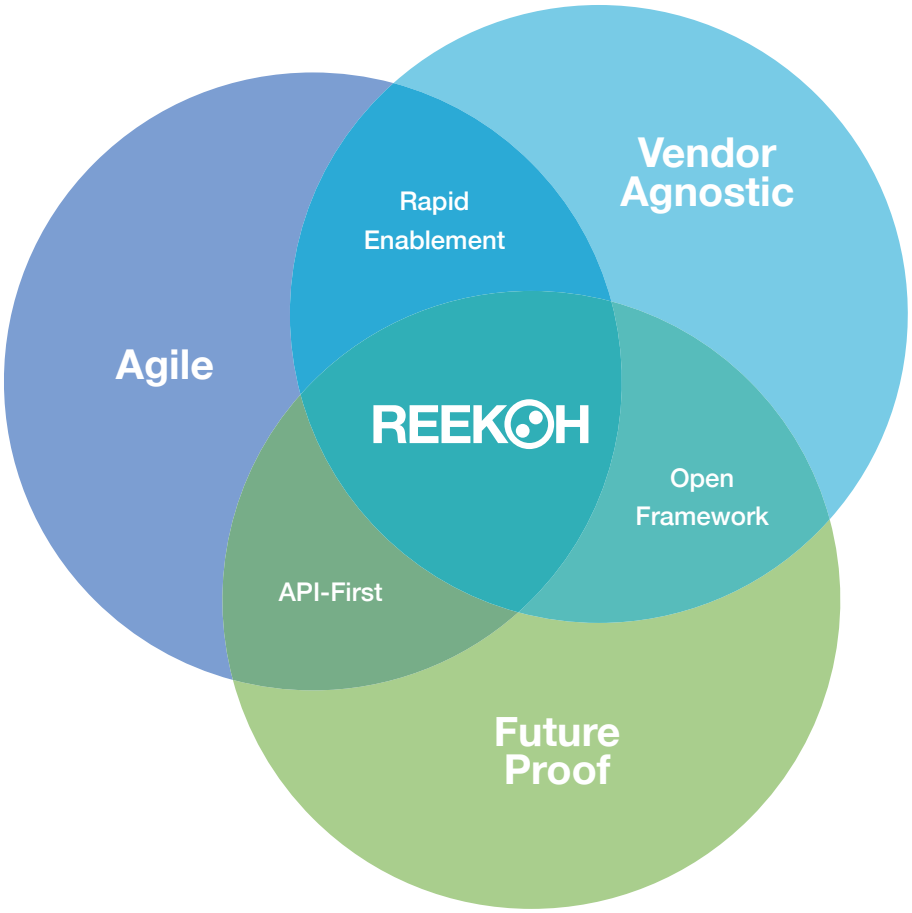
- Reekoh extensively logs everything that is happening throughout the platform across data management and user interaction
- Logs are available via API
- Logs can be forwarded to 3rd Party Systems (SIEM)
- Chose to forward Exceptions and Normal Logs
- Granular Logging within all categories of plugins

About Reekoh

Reekoh is the leading platform for IoT Data and API Management.

Our open frameworks and suite of tools including flow-based data integration design, security and rapid data visualisation, enables enterprise and government customers with an agile and scalable capability for delivering IoT solutions and strategies.

With offices in Australia and Manila, and global partnerships across the full range of IoT solution components, Reekoh is accelerating enterprise IoT adoption across all industries and verticals.



Gartner 2017 CoolVendor

sales@reekoh.com
reekoh.com

REEKOH
Things just became clearer™