SAGE® Security

Your data is one of the most valuable assets you own and one of our primary goals is to protect it with some of the most advanced secuirty systems available.

SAGE® Security by Armstrong®

Secure Hosting Environment

Partnerships

In order to provide advanced levels of infrastructure security, Armstrong® chose Amazon Web Services (AWS) to host SAGE®. Cloud security at AWS is the highest priority. You can read more about security at AWS here: https://aws.amazon.com/security/

AWS adheres to numerous global compliance programs, which can be viewed here: https://aws.amazon.com/compliance/programs/

In addition to AWS, Armstrong® also partners with Pivotal Web Services (PWS) and MongoDB Atlas. These providers build services on top of AWS. Further security information from these providers can be found here:

https://run.pivotal.io/policies/gdpr-and-data-security-faqs/

https://www.mongodb.com/cloud/trust

Physical Security

Physical & environmental security is provided by AWS data center physical buildings. Details of AWS physical & environmental security can be found here:

https://aws.amazon.com/compliance/data-center/controls/

https://aws.amazon.com/compliance/data-center/infrastructure-layer/

Virtualization Security

Industry best practices for virtualization security are observed for SAGE® hosting. Inherent in a virtualization solution is the ability to migrate servers and data stores in the live environment at any time. Additional resources can be allocated to the servers without the need to bring the system offline. The Hypervisor gives logical protected segmentation between virtual machines and between data stores. Private networks using secure private VLANs are configured for Armstrong®. In addition, virtual firewalls protect and limit data transmission between networks. Multiple firewalls and gateways monitor and protect traffic traversing the cloud infrastructure.

OS and Application Patching

System upgrades for application servers are handled regularly and automatically by PWS. Further information can be found here: https://community.pivotal.io/s/article/PWS-Upgrade-Frequency

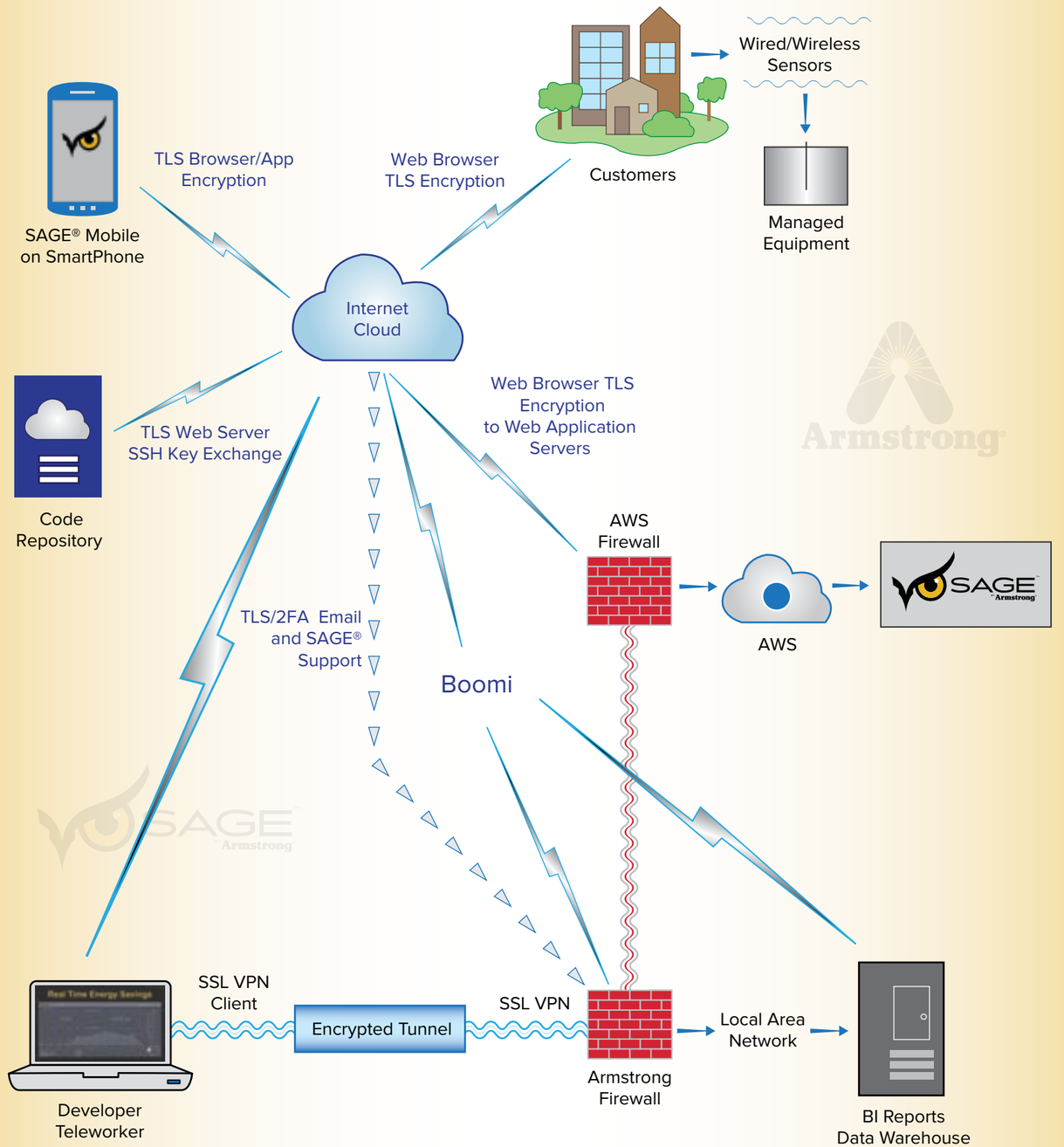
MongoDB Atlas regularly and automatically updates OS software and maintenance versions of database software. Armstrong® is notified when major/minor versions of the database software are available. The updates are applied and observed in the test environment. Once the functionality and security has been validated, the updates are applied to the production environment.

Remote Connectivity

Armstrong® developers do not access application and database servers directly. Updates and configuration changes are applied using tools provided by PWS or MongoDB Atlas. These tools are restricted to necessary personnel and are protected with strong passwords and 2FA. All communication is encrypted.

Database access is protected with strong passwords and encrypted.

With SAGE® you can be confident in the secure storage of your data and all data transactions.



With SAGE® you can be confident in the secure storage of your data and all data transactions.

Secure Hosting Environment

Best Coding Practices

SAGE® is a world-class utility system management software that is developed using best practices for application development security. The application is developed using simple and efficient code that reduces the likelihood for errors. Input validation is performed on data coming from trusted data sources; other input is dropped. Integral security is inherent in SAGE® software by developing using the principle of defense in depth.

SAGE® SDLC

The Armstrong® application development team creates software solutions using a mix of Waterfall and Agile programming practices as part of the Software Development Life Cycle. Periodic developer meetings during the design, coding, and testing phases ensure that security issues are identified and mitigated using the strength of the team. Iterative review of secure code and reported bugs ensures timely resolution of application vulnerabilities.

Coding Frameworks

Industry-tested common coding frameworks and libraries are used to enhance application reliability and integrity. The framework offers a comprehensive programming and configuration model. Development of SAGE® uses a security framework to integrate authentication and authorization.

Access Control

Access control for Armstrong® applications involves the use of least privilege to limit access to include only identified monitoring and management users. Each user has unique credentials for login to the SAGE® application. Secure application access is enforced using the access list configured in the authorization module.

Code Vault

Source code for custom applications must be protected from alteration. The patented SAGE® monitoring system retains source code for client-server and mobile applications in a secure source code repository. The cloud format allows for secure development collaboration and code storage utilizing SSH access and public-key asymmetric encryption technology.

Testing

The security framework protects against common web application attacks such as CSRF, XSS, and injection attacks. Developers are aware of secure coding practices which prevent back-door vulnerabilities and the ability to alter program characteristics.

Mobile Application Development

The mobile app uses the same authentication, authorization, and encryption mechanisms as the web application. iCloud Keychain is used to store SAGE® user login credentials.

With SAGE® you can be confident in the secure storage of your data and all data transactions.

Secure Operating Environment

Authentication

Centralized directory authentication is used to access the SAGE® environment. The authentication is integral to the security of the environment. Passwords are encrypted as data at rest within the directory.

Transport Security (Network)

Front-end web access of the SAGE® application relies on the security provided by SSL/TLS. The Public Key Encryption (PKI) algorithms provide 128-bits (or higher) of encryption. Authentication server traffic is encrypted using TLS-protected transactions.

Customer Data

Customer data created by energy management systems are not considered sensitive data. The live data consists of arbitrary data such as line pressures, temperatures, and acoustics. Stored data is comprised of aggregated equipment information. The power of the solution comes from calculations performed on the data and the cost savings that can be realized through analysis and trending.

Web and Application Security

Real-time transactions between the Proxy software and SAGE® are encrypted using SSL encryption. A username, password, unique token are required to send real-time readings to SAGE®. Furthermore, readings are validated upon receipt and dropped if they fail validation.

Web application security is provided between the customer browser and the SAGE® web servers. Developer management transactions to the SAGE® servers are likewise authenticated, authorized and encrypted using web browser security. Please see figure 1 for more information.

Malware

All SAGE® servers run Linux. Software is installed only from trusted and verified repositories, and kept up to date with security patches.

Security Audits

Logged entries are maintained regarding any system access and asset modification. Alerts of threats to the technology infrastructure are reviewed. Security analysis covers all logical technology layers to ensure defense in depth: physical security, applications, operating systems, network transmissions, data storage, and access control. Internal audits are validated by external third-party audits and penetration testing that meet the requirements of industry-standard security regulations- PCI and HIPAA.

With SAGE® you can be confident in the secure storage of your data and all data transactions.

Business Continuity and Disaster Recovery

Data Backups

The SAGE® database is continuously backed up. Snapshots are taken every six hours and retained for two days. Daily snapshots are retained for seven days. Weekly snapshots are retained for four weeks. Monthly snapshots are retained for 13 months.

Secondary Data Center

Although the primary data center for SAGE® is US East (N. Virginia), the servers and data could reside in other locations based on circumstances. Data may be replicated for redundancy, availability or performance reasons. A natural disaster or prolonged environmental failure could force a replication to secondary data center sites. The replication process is encrypted over a private network connecting the locations. Information about AWS regions and Availability Zones can be found at: https://aws.amazon.com/about-aws/global-infrastructure/

Connectivity

Water, power, telecommunications, and internet connectivity are designed with redundancy, so we can maintain continuous operations in an emergency. Electrical power systems are designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility. People and systems monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.

SAGE® Support

Installation

Installation of the SAGE® solution for monitoring steam and hot water components is the responsibility of the authorized representatives. Proxy installation could be required of either Armstrong® or our customers, depending upon the agreed deployment topology. Customers will have to configure the appropriate connectivity (NAT and access lists) on their firewalls and security appliances. Hosting of the SAGE® infrastructure is the privilege and responsibility of Armstrong®.

Application Support

Support for the SAGE® application is provided by Armstrong® developers and engineers. The first contact should be to SAGE® Support. Help can be provided through email and voice services. Contact information can be found at:
https://www.armstronginternational.com/products-systems/sage%E2%84%A2-armstrong.

Incident Response

Availability of servers and applications is monitored around-the-clock. Application availability alerts have been set up to contact Armstrong® personnel in case of operating system or application failure. Resources such as CPU, memory, network, and disk utilization are recorded and graphed for analysis and troubleshooting. Projected growth is implemented as resource upgrades to servers.

In the event of a security incident or data breach, Armstrong® will notify the customer immediately. Regular timely updates will be provided until a resolution is achieved. Any planned downtimes will be relayed to customers based on the list of organizational contacts that have been submitted to Armstrong®.

With SAGE® you can be confident in the secure storage of your data and all data transactions.

Armstrong International

INTELLIGENT SOLUTIONS IN STEAM, AIR AND HOT WATER

North America • Latin America • India • Europe / Middle East / Africa • China • Pacific Rim

armstronginternational.com