



TECHNICAL BRIEF

Asigra SaaSAssure Security Brief

Index

Asigra Security Mission	3
Protect from Data Loss – Anytime, Anywhere	4
Secure by Design	5
Shared Cloud Security	5
Data Resiliency and Storage Efficiency	6
Single-Sign-on for Simplified Access	6
Conclusion	6



Asigra Security Mission

At Asigra, security is paramount in all development initiatives. We have established a comprehensive enterprise security program meticulously designed to meet the rigorous security demands of our diverse customer base. Ensuring the safety of customer data remains our unwavering priority, encompassing every facet of product development, the entire development lifecycle, and the execution of backup operations. To that end, we use SonarCloud to scan all code for vulnerabilities before pushing it into the final stages of our DevOps pipeline.

Protect from Data Loss – Anytime, Anywhere



We realize businesses are tasked with shouldering the responsibility of guaranteeing data security, irrespective of the method or location of backup solutions utilized. From expanding the existing data center to embracing SaaS applications as part of a cloud-first strategy, data security remains our central concern. This commitment holds whether the business’s backup deployment occurs on-premises, in the cloud, or a hybrid model. Opting for cloud-based solutions doesn’t entail any compromise on security. With SaaSAssure powered by Asigra, data is fortified at rest and during transit, thanks to our robust security protocols and data governance tools.

In contrast to conventional approaches, the SaaSAssure platform is engineered to offer a rock-solid security foundation and is provided as-a-service. Our platform is designed to deliver inherent security advantages. This includes harnessing cloud-based infrastructure like AWS, which offers mature security features and global accessibility. Security remains perpetually vigilant at the infrastructure level, granting organizations the liberty to access their cloud data whenever and wherever they need it.

The protection of data from loss or compromise, regardless of its whereabouts, is of paramount importance. The proliferation of data stored in the cloud and increased mobile device access, is redefining traditional security boundaries. We employ adaptable backup and recovery solutions that serve as a shield against data

loss or compromise. Robust remote device encryption and sanitization capabilities to prevent data breaches. Geolocation features block high-risk regions. IP reputation lookups filter access from command-and-control botnets. Automated bot protections are in place to limit DOS attacks. We will offer antimalware scans and Content Disarm and Reconstruction (CDR) for file-based SaaS platforms to protect organizations relying on shared cloud-based file services.

Secure by Design

Ensuring data security during transit and at rest is a top priority for Asigra. We employ industry-standard Transport Layer Security (TLS) for secure data transmission to SaaSAssure. Once data reaches our platform, it undergoes immediate encryption using a unique AES 256-bit encryption key exclusively dedicated to the customer. At Asigra, we never allow direct employee access to backup data, ensuring logical separation and preventing data leaks in the cloud. Our customer encryption key is session-based, eliminating the need for complex key management solutions.

Asigra's pioneering technology fortifies security by breaking files down into individual blocks for unique blocks to be transmitted to SaaSAssure on a global scale. This approach conceals data, rendering it impossible to decrypt without authenticated customer credentials.

Shared Cloud Security

Security in the cloud is a shared responsibility. Asigra secures data across the entire spectrum, from infrastructure to application. While Cloud Service Providers (CSPs) safeguard infrastructure and platform layers, our software augments security within the hosted application. This includes layer 3 firewalling, advanced AI-based intrusion prevention systems, 20 months of logs for incident re-creation and a sophisticated SEIM set up to ensure security.

Data Resiliency and Storage Efficiency

Data resilience and storage efficiency are guaranteed through our utilization of AWS S3, a highly robust storage infrastructure. Amazon S3 ensures redundancy and conducts regular integrity checks to maintain data integrity. This includes regional data center redundancy.

Asigra relies on CSP certifications alone for security validation. At launch or shortly following, Asigra will hold SOC 2 type II, FIPS 140-3 compliance, and GDPR. We also use a third-party cybersecurity company for external and internal penetration testing and monitoring.

Single Sign-on for Simplified Access

Streamlining access management becomes essential as the number of applications proliferates, particularly with the advent of cloud-based applications. Asigra will support cloud-based Single Sign-On (SSO) solutions based on AWS Cognito. This includes Google, Microsoft AD, SAML, and OpenID. In addition to traditional multifactor authentication (MFA), we have also created an industry-leading multiperson approval (MPA) process. When MPA is enabled, multiple people must approve a potentially destructive action that may result in the loss of data.

To ensure audit readiness, Asigra offers real-time audit logging of security events for users and administrators. Role-based access control (RBAC) is implemented to curtail privileged user access and enforce privacy.

Conclusion

As the adoption of cloud-based SaaS applications continues its upward trajectory, the demand for robust security and information governance capabilities intensifies. Asigra is well-equipped with the tools and expertise to deliver security in virtual environments, consistently elevating the state of virtual security.

About SaaSAssure

Total control over data, or data sovereignty, solves many problems. However, backing up the fast-growing mountain of data from SaaS apps is a daunting task. Partial solutions only paper over the need for future work. What's needed is a way to close data gaps, keep up with data growth, and even make comprehensive backups stable and secure not just now but in the future. SaaSAssure helps businesses of all sizes accomplish that.

Find out more about our secure SaaS backup platform, [SaaSAssure](#).

SaaSAssure is ultimately
part of the broader picture
of data management.