

StylusAP Innovation Security FAQ



StylusAP Security: Frequently Asked Questions

1. Why use SaaS for document management?

According to an early August 2007 Gartner report, worldwide total software revenue for Software-as-a-Service (SaaS) within the enterprise software markets is projected to surpass \$5.1 billion in 2007, a 21 percent increase from 2006 revenue. “SaaS adoption is highest in applications that support simplified, common business processes or large, distributed virtual workforce teams,” Sharon Mertz, research director at Gartner, said. “Ease of use, rapid deployment, limited upfront investment in capital and staffing plus a reduction in software management responsibility all make SaaS a desirable alternative to many on-premises solutions, and they will continue to act as drivers of growth.”

2. How is StylusAP optimized for security?

SaaS enables StylusAP engineers to build additional security at points within our solution where typical on-premises enterprise content management (ECM) products cannot. The definition of SaaS — purpose-built Web technology — implies modularity. Because auditing and securing small modules is the cornerstone of many security architectures, our SaaS model provides customers with additional security benefits beyond the limits of most traditional applications.

Through the use of SaaS, the StylusAP solution is more agile and better prepared to respond to new security requirements, customer demands and changes. Our SaaS model is built upon industry-standard tools, protocols and frameworks — such as Microsoft .NET — that contain a wide variety of pre-existing security enhancements such as Secure Socket Layer (SSL), two-factor authentication and strong access control. We leverage, embrace and extend these existing security technologies to our customers, thereby dramatically increasing the overall security of our solution.

3. What else does StylusAP do to address security concerns?

Security is always a concern when handling confidential and proprietary documents. At StylusAP, we take your data’s security very seriously by investing a large amount of resources into a proactive security framework that ensures we always maintain the highest levels of security for your data.

StylusAP addresses security concerns using a method known as “defense in depth.” We look at each area of our solution, organization and people to see where security controls can reduce the risk of a potential data breach. To guarantee that we meet industry-standard best practices, we follow a structured security program modeled after ISO 27002 and Control Objectives for Information and Related Technology (CoBiT), two universal security frameworks.

More Information

www.stylusap.com

Phone 201.204.9079

sales@stylusap.com

Security Frequently Asked Questions (FAQ)

Our effective data security framework aids StylusAP in building and maintaining specific targeted security controls within our core solution, data centers and internal processes. Data availability, integrity and confidentiality are top priorities.

4. How is customer information controlled?

We use many controls to protect our customers' data. Specifically, StylusAP employs an advanced access control framework built into the core solution that enables secure authentication, records logs of user activity and allows administrators to control which users have access to highly sensitive documents.

Once your data resides in our secure data center, StylusAP has a documented disaster recovery plan that includes redundant and failover servers, routers and switches. Only select employees have access to the data center. Our internal security program contains comprehensive policies and procedures that ensure only those who need access to production systems are granted access for a limited period of time.

Limiting who has access to the system dramatically reduces the chance of an unauthorized party accessing confidential customer data. StylusAP's IT staff follows a best practices system-hardening process to strengthen our core systems and network devices from potential attacks.

5. Does StylusAP disclose the details of the controls?

We provide detailed information about our security policies and processes to customers who sign a non-disclosure agreement (NDA).

6. Can customers add additional controls like encryption or other authentication?

Customers cannot add additional controls to our servers, systems and equipment; however, additional services like encryption are available for a reasonable fee. We often assist customers as they search for additional controls to add to their own data networks.

Adding additional controls to customers' networks and systems will further reduce risk. We recommend that all of our customers implement an IT security program to protect their data once it leaves StylusAP.

7. What controls protect information downloaded from StylusAP?

We use an industry-standard authentication framework and SSL encryption to ensure that anyone downloading documents from StylusAP is properly authenticated and that the download cannot be intercepted during the transfer.

8. Does StylusAP mix customer information on the same systems?

Many SaaS architectures — StylusAP included — follow the multi-tenant data model that uses a common data store with virtual partitions of the data. Enhanced security controls ensure that customers' data never mixes.

During threat-modeling exercises, we ensure that one customer cannot access a different customer's data through a variety of detection controls as well as aggressive permission and access control lists installed and configured on our servers located in our secure data center. StylusAP developers follow similar guidelines when addressing areas of our solution in which customer data is accessed, presented or modified.

9. Does StylusAP provide the results of SAS 70 or other audits to customers?

Yes, any customer who has signed an NDA may request audit results. We currently use a third-party vendor to perform an annual penetration test to check the strength of our solution from an external attack.

10. Will StylusAP allow customers to conduct audits of your facilities?

Yes we will, depending upon the customer and type of audit. However, we always limit access to areas that contain confidential customer information.

Security Frequently Asked Questions (FAQ)

11. What internal control standards does StylusAP use?

We have adopted ISO 27002 and CoBiT as the two leading standards frameworks. We also use the IT Infrastructure Library (ITIL) to measure our effectiveness in meeting the objectives within each framework.

12. What contractual actions does StylusAP promise its customers regarding the security of their information?

We do not publicly disclose information regarding customer contracts.

13. What contractual remedies does StylusAP offer customers in case their information is compromised?

Even though we dedicate numerous resources to keeping customer data secure, security is performed at a best-effort level.

Contractually, we rarely enter into an agreement where StylusAP guarantees confidentiality or integrity of a customer's data; however, customers are welcome to request additional conditions to the StylusAP Security Board for consideration.

14. Does StylusAP offer customers levels of protection for confidentiality or availability?

Yes, we provide a service level agreement for the availability of customers' data. We invest heavily within our Information Technology Security programs to ensure the confidentiality and integrity of our customers' data, but we do not offer various levels of protection for different customers. All customers receive the highest level of confidentiality and data integrity protection we can offer.

15. What plans do you have in place for disaster recovery?

StylusAP provides various levels of disaster recovery options throughout our architecture and infrastructure components. Disaster recovery is provided seamlessly to

the customer from failover data center facilities to offsite backups.

16. Can customers view audit records?

Customers can review log-in and log-out times of their users in addition to users' activity history. These records provide customers with essential data for incident response or investigations when an unauthorized individual accesses a user's account.

17. Does StylusAP outsource work to other firms?

We do not outsource critical development and support to outside firms. External vendors perform audits.

18. How does StylusAP test its solution?

We perform an annual application assessment against our entire solution suite. We also use third-party security firms to educate our developers, IT staff and executives about upcoming security threats and trends.

Security Frequently Asked Questions (FAQ)

All development includes threat modeling and risk assessments for all areas of our solution that interact with customer accounts or data.

19. How can customers protect their information?

We have a solution paper that customers can view after signing an NDA. The solution paper covers the various processes and technologies they can deploy to help protect their information. We can also offer consulting services under a normal statement of work.

20. What happens with my data if I decide to leave StylusAP?

StylusAP provides a service to our customers who require backups of both the original customer documents as well as the metadata associated with those documents.

We can deliver a backup of your data as it is used in StylusAP to your location of choice in a variety of formats such as tape backup, optical storage or disk depending upon size of the data. This service is provided for a reasonable fee. Standard customer agreements are available.