netdocuments®

Are Your Vendors Covering Your SaaS?

Information is the oxygen of today's business environment. It must be free flowing, without fear of being compromised from the numerous threats facing cybersecurity. According to an ALM study, 75% of companies listed third-party mistakes as one of their top fears for data security.

Ultimately, it is your responsiblity to test and challenge your vendor's security credentials, and understanding industry best practices for cybersecurity will help you do that more effectively. We have compiled a list of best practices you can adopt. In the end, you will have a guide that is easily understood, easily applied, and gives you the peace of mind that your data is safe.

We highly recommend SaaS vendors meet these standards:

Platform Services Architecture

SaaS platforms should be designed for comprehensive and continuous updates in security, evolving fluidly in the advent of new security threats.

Multi-level encryption

Hardware encryption alone is insufficient. SaaS vendors must have several points of encryption on both hardware and software.

Hardware Security Module (HSM)

The keys to your data encryptions are just as vulnerable as the data itself. If your keys are compromised, your encryptions are exposed. HSMs are vaults, created from a combination of hardware and software, that guard the keys to your encryptions.

Independent audits and certifications

Entrusting your data to a SaaS provider is a big commitment. It is critical to verify your SaaS provider in a number of third-party audits and certifications to ensure they are truly providing the security they claim to offer. These audits and certifications should be updated and renewed regularly to ensure maximum security.

Virus, malware, and ransomware protection

It is insufficient to simply detect threats like viruses and malware. Data isolation has proven to be much safer in most cases. SaaS providers should be keeping your data separated from their other clients as much as possible. This mitigates the damage done by viruses/malware in the event that security is compromised. If not separated correctly, a virus infiltrating one of your vendor's clients can infect you as well.

Federated Identity

This system links your identity in one system, such as your company identification system, to another (in this case, to your SaaS product). This makes your login and access more secure. Your company can customize its own login security. This same level of security is applied to the SaaS platform, as the SaaS login bounces back to your company identification system in order to enter.

Learn how NetDocuments meets each of these standards at netdocuments.com/security