360ADVANCED

CYBERSECURITY TRENDS IN THE DOCUMENT MANAGEMENT INDUSTRY

WHEN IT COMES TO CYBERSECURITY, DOCUMENT MANAGEMENT VENDORS FACE SEVERAL UNIQUE CHALLENGES.

They must prove to their customers that their platforms are secure – especially when it comes to integrating with other business platforms. Document management software can be used to store everything from customer data, such as names, addresses, and billing agreements, to proprietary business information, such as financial and accounting data. As a result, vendors must take appropriate steps to protect this information.

ON-PREM VS. SAAS

The SaaS market is growing by more than

20%

each year. [1]

This has led many document management vendors to move to a cloud-based delivery model. However, this shift also brings about a new set of security risks.

ON-PREM SECURITY CONCERNS

- Preventing unauthorized access to workstations with vendor software
- Limiting physical attacks
- Managing environmental concerns

SAAS SECURITY CONCERNS

- Selecting secure hosting facilities to store client data
- Implementing necessary security controls without degrading the customer experience
- Creating a disaster recovery plan that ensures continuous availability

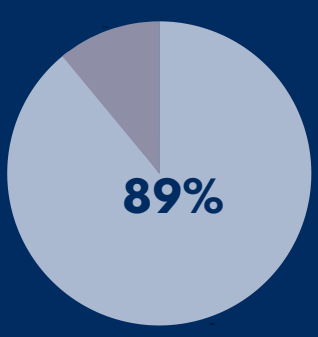
SHARED CONCERNS

- Segmenting applications outside of the corporate network
- Isolating production networks
- Encrypting data
- Continually testing for vulnerabilities
- Adopting SDLC best practices for secure coding and development

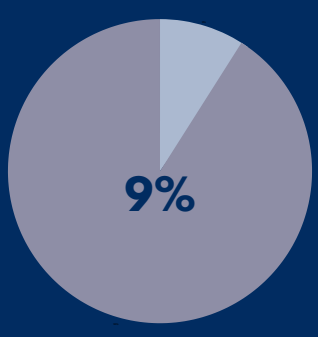
1: https://www.mckinsey.com/business-functions/risk/our-insights/securing-software-as-a-service

SECURITY AS A COMPETITIVE DIFFERENTIATOR

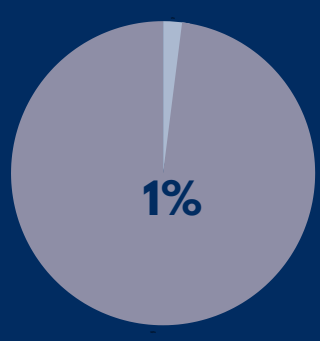
Whether on-prem or SaaS, document management vendors must assure customers that they have implemented appropriate security measures to earn their business – something the vast majority of software company executives rank as a top priority: [2]



HIGH PRIORITY



MEDIUM PRIORITY



LOW PRIORITY

2: https://reply.io/saas-report-2019

To acquire new customers in heavily regulated industries, such as law, healthcare, and finance, document management organizations must go above and beyond when it comes to protecting PHI. This is especially true at the enterprise level, where buying committees for new software platforms often include CISO and CTO personas.

SOFTWARE COMPANIES ARE ALSO INVESTING HEAVILY IN RESEARCH AND DEVELOPMENT - INCLUDING THE IMPLEMENTATION OF NEW SECURITY MEASURES.

A Reply.io study found that companies spent 67.5 percent of their annual revenue on R&D - more than they spent on either sales and marketing or general administrative expenses. [2]

67.5%

ONE INVESTMENT THAT CAN HELP DOCUMENT MANAGEMENT VENDORS STAND OUT IN A CROWDED MARKET:

COMPLIANCE AUDITS AND CERTIFICATIONS

Software vendors can easily claim that their platforms are secure – but without independent verification, customers may still be hesitant to implement their solutions.

Security assessments can provide valuable third-party assurance. The resulting reports and certifications allow vendors to easily communicate their compliance efforts and set themselves apart from competitors.

SOC EXAMINATIONS

SOC (Service and Organizational Controls) examinations help organizations establish credibility and trustworthiness. The resulting reports can be shared with prospective customers, reducing the need for repetitive security questionnaires.

HITRUST® VALIDATED ASSESSMENTS

Incorporating several industry-recognized standards, the HITRUST CSF provides a consolidated framework for risk management. Organizations that meet HITRUST's control requirements earn a certification that represents their efforts.

GDPR COMPLIANCE EXAMINATIONS

Document management vendors that serve international data subjects may be asked to prove their compliance with the EU's data protection regulation (GDPR). Proof of compliance helps convey appropriate privacy protections for consumer information.

PCI-DSS COMPLIANCE

Some users rely on document management systems to store or transmit payment card information. PCI-DSS compliance provides proof of secure handling controls.

ISO CERTIFICATIONS

Widely adopted throughout the software industry, ISO standards provide easy-to-understand frameworks for both cybersecurity (ISO 27001) and privacy (ISO 27701).

PENETRATION TESTING

Whether cloud-based or on-prem, document management vendors can test their systems to identify and address vulnerabilities before they can be exploited.

LEVERAGING COMPLIANCE TO PROMOTE GROWTH

A Ping Identity survey found that security concerns were one of the largest barriers for adoption, as reported by 37 percent of surveyed SaaS organizations.[3]

37%

3: https://www.pingidentity.com/en/company/press-releases-folder/2019/security-concerns-preventing-cloud-saas-adoption.html

HOWEVER, THE DOCUMENT MANAGEMENT INDUSTRY IS EXPECTED TO GROW AT A RATE OF MORE THAN 6.9 PERCENT THROUGH 2027, AND VENDORS THAT CAN SUCCESSFULLY ADDRESS THEIR CUSTOMERS' SECURITY CONCERNS ARE BEST-POSITIONED FOR GROWTH.[4]

4: https://www.marketwatch.com/press-release/document-management-services-market-to-register-69-cagr-by-2027-owing-to-increasing-adoption-of-technology-worldwide-states-fortune-business-insightstm-2020-06-02-101845546?tesla=y

As an experienced cybersecurity and compliance firm, 360 Advanced has helped document management vendors evaluate their security posture, become compliant with key regulations, and communicate their efforts to their customers. To find out how we can help you develop a reputation as a trusted provider of secure document management solutions, contact us today.

360ADVANCED

Making Better Businesses

www.360advanced.com

(866) 418-1708