DocuSign®

Security Brief

Security is an essential part of any software-based solution, but few business processes are as security sensitive as those involving electronic signatures.

When transactions contain highly sensitive information, like personally identifiable information, pricing details, proprietary business terms, intellectual property and more, you can't afford to take risks. That's why DocuSign emphasizes security and high availability in everything that we do. Protecting customers is DocuSign's number one priority, and our comprehensive approach addresses the security, privacy, compliance and validity of your DocuSign transactions.

It's a critical component of the DocuSign Agreement Cloud and a big reason why DocuSign is the most widely used e-signature solution in the world. DocuSign consistently meets the stringent security requirements of even the most security conscious organizations, including Fortune 500 companies, the world's largest financial institutions and other global companies.

In the following pages, we provide an overview of our security approach, which encompasses a number of key areas: our security assurance program, certifications and tests.

DocuSign security assurance program

Our dedication to deliver the highest level of security possible for our customers is centered on our security assurance program, which aligns our people, processes and platform to address the overall security, privacy and validity of your eSignature transactions.
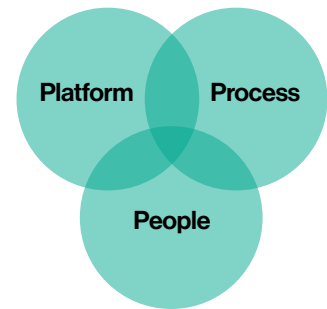
People

Security at DocuSign is everyone's job. We invest in training and awareness to ensure that security stays top of mind for all of our employees.

– A cross-functional team of experts that's 100% dedicated to security-related activities

– A security council that oversees risk management strategy and implementation across the organization

– Background checks for all prospective employees and suppliers

– A dedicated Chief Trust and Security Officer (CTSO) who manages security operations and continuously engages with the security community to ensure DocuSign stays ahead of emerging trends in the dynamic threat landscape

– Annual security and privacy training for all employees

– Training for engineers to ensure coding is done securely, with regular security audits of the code base

Process

DocuSign's business processes, including internal policies, software development and platform monitoring, take into consideration the security of our customer data.

– On-premise security policies, such as badge access, manned public entrances and physical access controls

– System access limited to a minimal number of personnel based on the least-privilege principle, with multiple layers of secured authentication required for all critical systems

– Active monitoring and alerting

– Security reviews within the DocuSign Software Development Life Cycle (SDLC), including the planning, design, implementation testing, shipping and response phases

– Formal code reviews and vulnerability mitigation by third parties for applications and access security

– Testing and validation of DocuSign's key management and encryption program by external auditors and documented in our SSAE 18 report

Platform

DocuSign's secure platform encompasses hardware and infrastructure, systems and operations, applications and access, and transmission and storage.

– Commercial-grade datacenters with diversity across vendors, so that critical customer documents remain available in the event of any business disruption

– World-class architecture featuring simultaneously active and redundant systems that allow the overall system to survive full-site outages and be "always on"

– Secure, near real-time data replication

– Physically and logically separated networks for systems and operations

– Malware protection

– Commercial-grade firewalls and border routers to resist/detect IP-based and denial-of-service attacks

– Multiple authentication options for signers

– Anti-tampering controls

– Digital certificate technology

– Two-factor encrypted VPN access

A holistic approach

DocuSign doesn't look at security in a vacuum. We consider all areas that keep your sensitive transactions protected, including privacy and compliance with laws and regulations globally. DocuSign's features ensure the enforceability and non-repudiation of our customers' documents.

– AES 256-bit encryption at the application level for customer documents to ensure confidentiality

– Access and transfer of data to/from DocuSign via HTTPS

– Use of Security Assertion Markup Language (SAML), giving users the latest capabilities for Web-based authentication and authorization, including single sign-on

– Ability for signers to authenticate when they sign, including multifactor and two-factor authentication

– A digital checksum (mathematical hash value) that validates documents haven't been tampered with outside of each signing event

– Certificates of completion after all parties have participated in the signing process

– Signature verification and unalterable capture of signing parties' names, emails, public IP addresses, signing events, timestamps, signing location (if provided) and completion status

– A digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action and timestamp

Security certifications and tests

DocuSign makes significant investments in enterprise security and operations, and we undergo rigorous scrutiny by third-party auditors to assess and validate the security measures we have in place.

– Consistently meets national and international security standards

– Continual leadership in defining industry best practices for third-party audits, certifications and onsite customer reviews

– Compliance with applicable laws, regulations and industry standards around the world, governing digital transactions and electronic signatures

– Dedicated chief legal officer and chief technology officer that ensure DocuSign and our products align with the latest legal and technology trends

– Ability to comply with specialized industry regulations, such as HIPAA, 21 CFR Part 11 and specified rules from the FTC, FHA, IRS and FINRA

ISO 27001:2013
The highest level of global information security assurance available today, ISO 27001 provides customers assurance that DocuSign meets stringent international standards on security.

Learn more about ISO 27001:2013 at **www.iso.org**.

SOC 1 Type 2 and SOC 2 Type 2
As a SOC 1 and SOC 2-certified organization, DocuSign complies with the reporting requirements stipulated by the American Institute of Certified Public Accountants (AICPA). We undergo yearly audits across our production operations, including our datacenter, and have sustained and surpassed requirements.

Further details may be found on the **AICPA website.**

PCI DSS

DocuSign maintains compliance with the current version of the PCI Data Security Standard (DSS) to ensure safe and secure handling of credit card holder information. As overseen by the Payment Card Industry Security Standards Council (PCI SSC), DocuSign places stringent controls around cardholder data as both a service provider and merchant. DocuSign is listed as a PCI Service Provider on the **Visa Global Registry of Services Providers.**

Additional information on PCI DSS may be found at **www.pcisecuritystandards.org.**

CSA STAR Program

DocuSign adheres to the requirements of the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program. The CSA STAR comprises key principles of transparency, rigorous auditing and harmonization of standards. Our Consensus Assessments Initiative Questionnaire (CAIQ) documents the rigor and strength of DocuSign's security posture and best practices and is publicly accessible for viewing and download from the CSA STAR registry for both **DocuSign** and **DocuSign Contract Lifecycle Management (FKA SpringCM)**.

Conclusion

We're committed to fiercely protecting the data our customers entrust to us. It's why we weave security into every aspect of our organization through the security assurance program, focusing on people, processes and platform. This is evidenced by our investment in meeting national and international security standards, including certification for ISO 27001:2013.

Our customers demand and expect thorough protection of their most sensitive transactions, and that's the stance we take in delivering exceptional document and data security. It's our priority, and it's at the core of the DocuSign Agreement Cloud and DocuSign eSignature — the world's number one way to sign electronically on practically any device, from almost anywhere, at any time.

Additional resources

The security we offer our customers extends beyond what's outlined in this document. A number of additional resources are available that further demonstrate DocuSign's industry-leading security strategy.

Follow the links below for more details on how we approach and deliver security.

Trust Center

DocuSign Partner Ecosystem Integrations

Policies:

Terms of Use

Privacy Policy

Use of Cookies