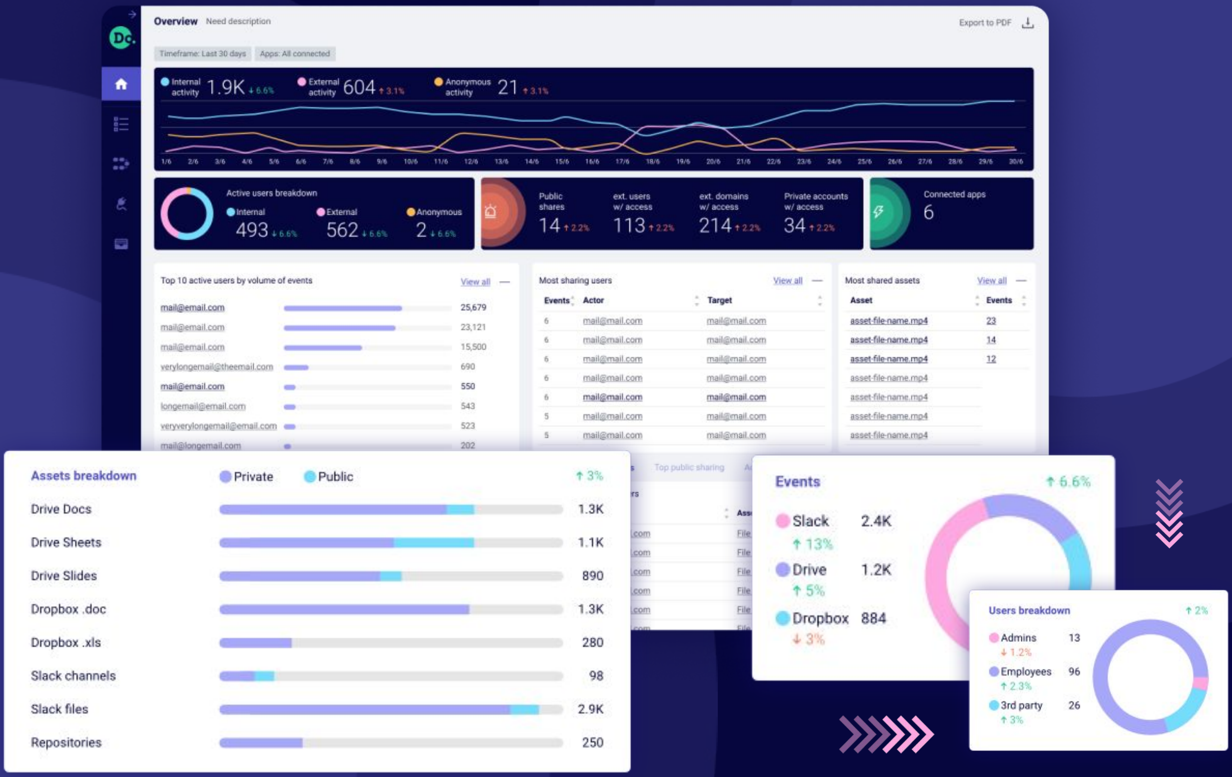
in docontrol.io

DoControl.

Security Whitepaper



DoControl is committed to earning and retaining customers' trust. Key aspect of this mission is designing a system with security capabilities embedded in all layers to protect customers' data at best practices. This documentation describes the security and privacy architecture, audits, certifications, processes, administration, and controls designed, implemented, and maintained to secure customers data on DoControl.

For questions or feedback, please contact our security team at security@docontrol.io.

V12.2020

Security Whitepaper

Table of Contents

Architecture and Segregation of Access

DoControl is operated in a multitenant architecture that is designed to segregate and restrict customer data access based on business requirements. The architecture provides a logical data separation for different customers through a customer-specific “Tenant ID”. It is generated automatically as part of an enterprise onboarding flow, and supports all users of the same enterprise. This implementation enables customer and user role-based access and privileges capabilities.

DoControl uses different environments for production, development, and testing ongoing product updates, providing an additional layer of data segregation.

Cloud-native Services

DoControl runs entirely on Amazon Web Services (AWS) and leverages several 3rd party products. As of 10/21/2020, DoControl uses the AWS managed services below. The list may change over time.

- Cognito
- Organizations
- KMS
- Certificate Manager
- GuardDuty
- Route53
- Systems Manager Parameter Store
- SQS
- Event bridge
- Lambda
- ECS Fargate
- CloudFormation
- DynamoDB
- Redshift
- S3
- Athena
- API Gateway
- IAM
- Glue
- Kinesis
- CloudWatch
- CloudTrail

Third-Party Functionality

Certain features of DoControl use functionality provided by third parties: Segment, Split.io, Intercom, and Google Analytics. DoControl does not collect PII in those services.

segment | split | Google Analytics | INTERCOM

Audits and Certifications

ISO 27001 certified since 10/20/2020. Certification is available upon request. As of 10/21/2020, DoControl has started the SOC2 certification process which planned to be completed by Q1 2021. CSA CAIQ Self-Assessment was published on 11/13/2020.

As DoControl runs entirely on AWS, certifications of AWS, including ISO 27001 certification and SOC reports, are available from the AWS Security and AWS Compliance websites.

Information Security Management ISO 27001 Certified | AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™ | CSA cloud security alliance®

Security Whitepaper

Security Policies and Procedures

DoControl operates in accordance with the following policies and procedures whose purpose is to enhance security:

- Create encryption keys using AWS KMS to encrypt customers' application OAuth/API tokens and then store in AWS Systems Manager.
- User activity logs are encrypted at rest, containing date, time, user ID, Tenant ID, the operation performed (created, updated, deleted), and source IP address.
- If inappropriate access is suspected, DoControl provides customers log entry records for use in forensic analyses as available.
- Specific administrative changes to DoControl (such as password changes and adding custom fields) are tracked in comprehensive audit trail logs and are available for viewing by customers. Customers may download and store this data locally.
- DoControl personnel does not define passwords for users. Passwords are reset at a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

Production Access

Access to DoControl's AWS production environment is restricted based on AWS Client VPN and Okta integration, enforcing the Separation of Roles and MFA requirements.

Security Whitepaper

Security Logs

All cloud-native services used in the provision of DoControl, including serverless lambdas, databases, and storage, log information to a centralized system to enable security reviews and analysis. All user management and authentication actions are audited via AWS Cloud Trail.

Incident Management

DoControl maintains security incident management policies and procedures. DoControl notifies impacted customers without undue delay of any unauthorized disclosure of their respective customer data.

Penetration Testing

DoControl's penetration tests are planned on a six months basis, in between annual compliance audits. Scope includes client-service communication, user authentication and authorization, multi-tenancy, and general cloud infrastructure setup.

Software Development

DoControl enforces code reviews and quality checks on each code commit in the software development process. DoControl leverages Github Dependabot to stay on top of every security vulnerability affecting Github repositories.

Security Whitepaper

User Authentication

Access to DoControl requires Multi-Factor Authentication. Password policies are enforced. DoControl plans to support multiple Identity Providers over time.

SaaS Authentication

Activating DoControl capabilities requires authentication to SaaS applications via OAuth or SAML-based login mechanisms. All secrets/tokens and sensitive authentication data are encrypted at rest using AWS KMS. Secrets/tokens are managed on AWS Systems Manager Parameter Store.

Physical Security

DoControl runs entirely on AWS and is subject to AWS data-center security as described in AWS Security and AWS Compliance websites.

Reliability and Backup

Our AWS infrastructure is designed to maximize reliability and stability. DoControl is based on AWS serverless Lambda functions supporting a Monthly Uptime Percentage of at least 99.95%, more details can be found at AWS Lambda Service Level Agreement. DoControl customers' data is backed up continuously. Backups are encrypted, stored in multiple locations, retained for 30 days, and can be restored at any time based on the customer's tenant ID. Customers may ask for backups deletion upon contract termination.

Security Whitepaper

Disaster Recovery and Business Continuity

As part of the GDPR effort, DoControl plans to support multi-region deployment to support data migration and DR implementation.

Data Encryption

DoControl uses AWS KMS to encrypt customer data at rest. DoControl uses AWS Certificate Manager to encrypt data in transit through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys.

Data access

DoControl's API is accessible via authenticated HTTPS calls powered by AWS Cognito. Secure and manual data access is restricted based on AWS IAM.

Audit Logs

DoControl achieves transparency with customers by generating three types of audit logs:

- Raw SaaS activity events - when users consume SaaS apps connected to DoControl, such activity events are pulled and consolidated.
- DoControl admin activity - when users onboard, configure, or consume DoControl's system, admin activity logs are generated.
- DoControl system activity - when DoControl acts on behalf of customers (i.e aggregate data, enforce policies, etc), system activity logs are generated.

Return of Customer Data - Right To Be Forgotten

Within 30 days of post-contract termination, DoControl customers may request the return of their respective data submitted to DoControl. DoControl shall provide such customer data via downloadable files in comma-separated value (.csv) format and attachments in their native format.

Sensitive Data

DoControl does not handle, stores, or process sensitive data, such as Social Security Number, personal data which reveals the racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

To provide the service to a business, we process personal information provided by SaaS apps used by our customers. This includes users' full name, email address, and account user name.

Generally, DoControl processes personal data regarding the usage behavior and usage patterns concerning the SaaS applications that the business's users use. This includes the end user's IP address and approximate location derived from the IP address.

DoControl.

docontrol.io | security@docontrol.io