prezent™

Securing the Prezent platform

An overview of the Prezent security program

Table of Contents

1. Introduction

Prezent delivers sophisticated business storytelling capabilities–audience empathy, structured storylines, high-end designed templates, expert guides, and contextual learning modules–at employees' fingertips to help them bring ideas to life through presentations and slides tailored to their audiences' preferences.

Prezent enables any organization and any team to automate the creation, standardization, and distribution of business presentations.

Prezent provides a software as a solution (SaaS) platform that uses enterprise-grade cloud architecture. Prezent instances are unique per customer ensuring high availability and no coalescence of customer data. Prezent operations use standardized infrastructure, processes, and tools regulated by globally revered governance and compliance frameworks to extend the highest level of security to our customers.

This document describes Prezent's security across several key administrative and logical security domains. These include architecture, information lifecycle, security operations, disaster recovery/business continuity, privacy, compliance, and software development. These domains are represented from the context of Prezent as a software vendor.

Prezent is an AI-powered presentation productivity platform that supercharges business communication by combining audience preferences, business storyline and brand approved designs.

2. Definitions

Prezent

Prezent enables customers to link real-time data with activities, tasks, and processes to achieve better work outcomes. Prezent provides a SaaS UI that includes, but is not limited to:

1. Personalized presentation fingerprints
2. Customer-specific slide templates and presentations
3. Presentation builder
4. Real-time sharing, collaboration, and learning
5. AI-based search

Instance

Prezent runs in the AWS Cloud using compute, storage, and database services.

- Each instance (production, customer test, quality assurance "QA") is contained within a separate AWS cloud project. The project infrastructure provides granular access control to all aspects of the infrastructure. Access from external locations is controlled through configuration and firewall rules. Access to internal components of the platform is only possible via Multi-factor Authentication "MFA" controlled access using Secure Shell ("SSH") protocol. Access is granted on a project and component within each project (i.e., pods, storage, and database) basis.
- Data is persisted in AWS Storage, DynamoDB, and Postgres Services using Advanced Encryption Standard ("AES") 256 encrypted disks for all data stored at rest. Customer data is never coalesced in the Prezent storage.

3. Security responsibilities

Data roles and responsibilities

As the "data controller," customers always retain ownership of their data and are therefore responsible for meeting the requirements of privacy legislation in the jurisdictions in which they operate and from which they collect personal data. If an individual requests information directly from Prezent regarding data that may be stored about them on Prezent, Prezent will refer that individual to the customer.

Prezent fulfills the role of "data processor" and complies with the associated obligations it entails. Prezent does not store any customer proprietary data. We store only presentation templates that are created using Prezent. Therefore, have no visibility of the conditions under which the data was collected by the customer, whether appropriate permission was obtained, or if data is being used in accordance with those conditions.

Regardless of how customers classify data that is stored in their instance, Prezent's single operating and security model ensures that data is protected.

Prezent fulfills the role of "data processor" and complies with the associated obligations it entails.

The shared security model

Prezent focuses on the security, compliance, and reliability of the platform, the system it runs on, and the environment in which it is hosted. When using Prezent, the customer is responsible for ensuring that their organization is using our products in a compliant way. Overall, security is a shared responsibility between customers, Prezent, and its data center providers. The areas of responsibility are shown in the table below.

Responsibility	Customer	Prezent	Data center providers
Data management and classification	●		
Media disposal and destruction		●	
Backup and restoration		●	
Authentication and authorization	●		
Data encryption at rest and in transit		●	
Encryption key management	●	●	
Security logging and monitoring		●	
Vulnerability management		●	
Business continuity and disaster recovery		●	
Secure SDLC processes		●	
Penetration testing		●	
Privacy	●	●	
Regulatory and legal compliance	●	●	●
Infrastructure management		●	
Security management		●	
Personnel security	●	●	●
Environment controls		●	●
Physical security			●

4. Information security governance and risk management

Security frameworks

ISO 27001 (formally known as ISO/IEC 27001:2013) is a standard for Information Security Management System (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk management processes with the aim of keeping information secure.

Prezent holds an ISO 27001 certification, which demonstrates a high level of integration between the ISO 27001 code of practice and Prezent ISMS.

Furthermore, data is hosted and processed within Amazon Web Services, which holds SOC and ISO 27001 certifications.

Security management and policies at Prezent

Prezent Information System Security Manager, Chief Product Officer, and Vice President of Engineering all report to the Chief Executive Officer. This simple organizational structure provides executive visibility and oversight regarding security and risk management.

During normal operations, the organization is supported by several domain specialist teams. These include security engineering; security operations and threat response; application development and security; and audit, risk, and compliance. There are also specific teams responsible for liaising with customers on security matters, shaping employee behavior, creating documentation, and other resources.

Prezent has clearly defined roles and responsibilities for individuals within the teams and has taken steps to ensure standard information security best practices in its security processes are achieved.

Prezent security program is described in its information security management system (ISMS) and associated security policies and standards. These are reflected in an extensive list of security policies and other relevant documentation.

Examples of Prezent security policies include:

- Access Control Policy
- Asset Management Policy (AMP)
- Business Continuity and Disaster Recovery Plan
- Bring Your Own Device (BYOD) Policy
- Change Management Policy
- Code of Conduct
- Cryptography Policy
- Data Management Policy
- Employee Personal Data Protection Policy
- Human Resource Security Policy
- Incident Response Plan
- Information Security Policy
- Information Security Roles and Responsibilities
- Operations Security Policy
- Risk Management Policy
- Secure Development Policy
- Third-party Management Policy
- Vulnerability Management Policy

These documents are assessed and updated annually and when significant changes occur.

Risk management

Prezent has defined processes and procedures for managing and assessing strategic and operational security risks. Risk assessments are performed regularly to identify and assess the likelihood and impact relating to risks. These can include technical, reputational, contractual, financial, regulatory, or fraud risks. Risks are categorized in accordance with their impact and likelihood in a formally documented procedure.

Key security, risk, and compliance stakeholders meet regularly to discuss security and risk items, and any identified risk is quickly and efficiently managed in a timely manner to safeguard the confidentiality, integrity, and accessibility of Prezent and Prezent customer data. Prezent executive management is regularly briefed on current and new security risks, and any potential threats that could impact Prezent and its customers.

Access reviews

All Prezent team members have unique credentials as well as established authorization to access Prezent information assets. Access to systems and information is restricted based on the responsibilities of the individual and their role.

Access rights reviews of user, administrator, and service accounts are performed quarterly to verify that user access is limited to systems that are required for the job function.

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time for access termination is 24 business hours.

5. Compliance

Regulatory and industry compliance

Prezent has a full-time dedicated Information System Security Manager and Information System Security Officer who are responsible for management of information security, including governance and compliance programs throughout the organization. This requires engagement across multiple functional areas within Prezent, including product, operations, legal, finance, and procurement. Prezent engages an external legal counsel to understand the company's obligations to existing and new laws and statutory regulations within the jurisdictions in which it operates. The finance and accounts department are responsible for ensuring Prezent's compliance with relevant financial regulations, including Sarbanes Oxley (SOX), a requirement for all US public companies.

Prezent itself is not subject directly to vertical-specific regulation, such as HIPAA or PCI; however, it does have many customers who are. And through the features in the Prezent and organizational transparency, it can support those regulated customers in meeting their obligations. The table below summarizes Prezent's security-related certifications.

Certification or attestation	Description	Geography	Industry
ISO/IEC 27001:2013	ISO/IEC 27001:2013 specifies information security management best practices and controls	International	All
SSAE 18 SOC 1 and SOC 2 Reports	SOC 1 Type 2 focuses on protecting the confidentiality and privacy of information in the cloud that affects the financial reports of customers. SOC 2 Type 2 focuses on controls that are relevant to security, availability, processing integrity, confidentiality, or privacy.	International	All
GDPR	GDPR is a law on data protection and privacy for EU citizens.	European Union	All
CCPA	CCPA protects the data subject rights of natural persons who are California residents.	California, United States	All

6. Physical and logical architecture

Overview of physical architecture

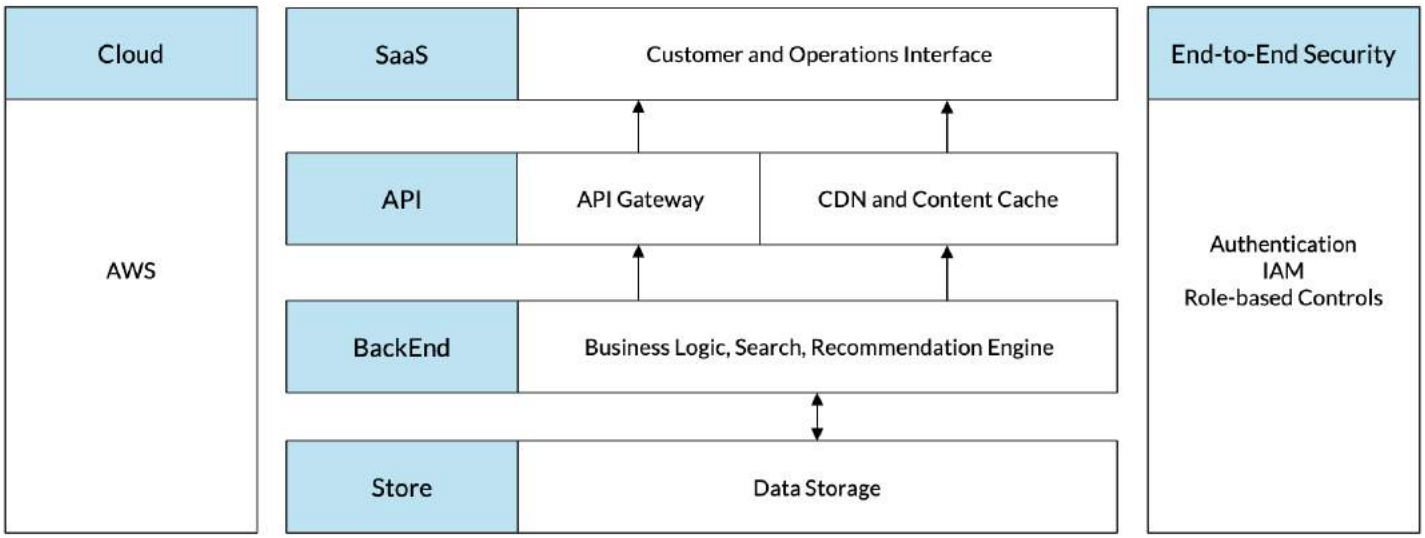
Prezent is a fully remote company with no centralized headquarters or physical network. Prezent is built on AWS cloud. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Data center physical security

Prezent uses AWS, Google, Atlassian, and GitHub as a subservice organization for data center colocation services. These operators provide Prezent with a secure and reliable space to operate in. The data centers are highly secure facilities with 24/7 monitoring by closed-circuit cameras and security personnel, and they have strict procedures for physical security.

The details of individual data centers may vary slightly; however, all facilities have similar operating characteristics. In all cases, contractually, the data center providers must be either ISO/IEC 27001:2013 accredited and/or conduct regular SSAE 18 SOC 2 Type 2 audits.

Overview of logical architecture



Architecture, scalability, security

The cloud environment supports elasticity allowing for significant economies of scale and operational agility. The security risks in a highly homogenous service are often more predictable and easier to manage than in highly diverse environments typical of many enterprises. Prezent is focused on securing data processed within its application boundaries.

Customers and web services connect to Prezent over HTTPS using TLS for communication. All interactive end-user activities are performed using a standard web browser. There is no requirement for customers to install any client software on any desktop, laptop, tablet, or smartphone to access Prezent. User access is controlled using a secure role-based IAM module.

Requests are received by the API gateway and processed through application logic before passing to the relevant database service. Database servers are installed in a discrete, non-internet routable network segment. Requests from end users cannot be made directly to the database and are only issued from a customer's Prezent instance.

Automation

Many activities in the Prezent infrastructure are conducted entirely using automation with minimal to zero human interaction. For example, our search and recommendation engines use machine learning.

7. Availability

Failover

A failover of an instance typically occurs when availability of a customer instance cannot be maintained. This could be due to a local component failure, or an event such as a major environmental incident or resource outage.

In the case of a local component failure, a failover to a snapshot will be attempted first. When a database issue/outage is identified, all current active production instances in the impacted data center will be rolled over to the backup database instance. In this circumstance, a recovery time objective (RTO) of two hours and a recovery point objective (RPO) of one hour is targeted. Actual times are usually significantly shorter than the stated RTO/RPO.

Data backup and recovery

Prezent uses redundant RDS, NoSQL instances to ensure full backup recovery of its databases. For local files of employee workstations, Prezent has a shared google drive which acts as a backup. Access to Prezent databases is heavily restricted using role-based authorization controls.

Business continuity and disaster recovery

Prezent's Business Continuity and Disaster Recovery Plan details our key business processes and critical services.

A disaster affecting the corporate environment could occur with little or no impact on the ability for the AWS data centers within the cloud to continue to operate. In both cases, the business continuity and disaster recovery procedures are supported by a series of tested processes, automations, and supporting documentation, allowing Prezent to quickly and effectively act when availability of its cloud or critical supporting services are affected.

8. Secure software development

Prezent uses a formal change control procedure to control the changes to systems within the software development lifecycle. As a requirement of this process, any significant changes must be reviewed and approved by the Tech Lead prior to merging into the production branch.

Application security teams

Prezent has dedicated teams of security engineers (i.e., development team, product team, and QA team) who are deeply integrated into the overall software development program. The teams perform several functions, including but not limited to:

- Managing the various internal and external testing program
- Performing architectural reviews in respect to new security features
- Performing assessments of Prezent services and organization instances used for running its business
- Curating educational security materials, including those for customers

Software developers are expected to adhere to Prezent's coding standards throughout the development cycle, including standards for quality, commenting, and security.

Prezent follows Open Web Application Security Project (OWASP) standards to make sure that OWASP Top 10 vulnerabilities are not introduced into its products.

Testing during development

During development, code for Prezent is subject to continuous ongoing testing of security functionality. No code shall be deployed to Prezent production systems without documented, successful test results. Peer reviews at the code level are also performed. Acceptance testing programs and related criteria are established for new information systems, upgrades, and new versions.

Any validated security issue found is also checked for and, if necessary, remediated in supported versions of the Prezent application. This remediation is provided either in the next patch for that release or as a hotfix, subject to criticality.

Application penetration testing

After internal testing, external application penetration testing is carried out, providing independent review and transparency around Prezent's secure development practices. A third-party organization is given an extended period of time and access to the resources necessary to review and test the next release of Prezent before it is made available to customers.

On completion of a first round of testing, any confirmed issues are entered into the Prezent vulnerability remediation process that is centrally managed. Remediation activities are taken one at a time to safeguard Prezent's IT systems and data. Once the remediation is complete, a second round of testing is conducted again by the same third-party organization. This is to confirm the provided remediation or mitigation functions as expected. Results of the third-party testing are consolidated into a sanitized penetration test report accessible to customers by request.

9. Information lifecycle and data management

Information classification

Prezent applies relevant data classification levels to all customer data it hosts. Prezent does not inspect or monitor its customers' data and has no ability to understand how any data may have been classified by individual customers. For Prezent, the overriding requirement towards customer data is that it remains hosted solely in the private cloud and is treated and handled according to its policies for all customer data.

Customers remain the data controller (i.e., data owner) for all data they store in their Prezent instance and should therefore apply access controls according to their data classification policies.

On completion of internal testing, external application penetration testing is carried out, providing independent review and transparency of Prezent's secure development practices.

Data retention

Customers decide what information is to be stored, how it is to be used, and how long it is retained. Prezent does not delete or modify customer data and only processes data in accordance with its contractual obligations.

Data that is deleted from a customer instance will remain backed up for 180 days before it is permanently deleted.

Data return, destruction, and media disposal

Throughout the lifetime of the subscription, some user data can be exported by Prezent's Product and Operations Teams through the back office Internal Operator Console.

Upon contract expiration or exit, or where requested, Prezent will supply a customer's data in an Excel / PDF format. Exiting customers have 180 days to request their data to be returned, after which all hosted and backed-up data is automatically deleted and overwritten.

10. Prezent security operations

Infrastructure vulnerability management

Prezent maintains an ongoing security monitoring capability and uses AWS documentation on best practices to inform the alerting and logging measures we take. Prezent also uses a third-party commercial tool for automated and continual infrastructure vulnerability management at scale.

Identified vulnerabilities feed into the overarching vulnerability monitoring and remediation program. Patching of affected systems, services, or applications is undertaken promptly and as necessary, in accordance with Prezent criteria and processes.

Operating system security

Prezent builds and maintains standard network device, appliance, and operating system build configurations. New devices and servers are deployed with automatic configurations relating to their function.

Controls relating to the monitoring of sensitive operating system files are in place. Anti-malware measures with regular updates are made to all servers as well as all corporate IT systems and endpoints.

Cloud infrastructure vulnerability management

Findings reported from the continuous scanning of its Cloud infrastructure by AWS vulnerability management tools are automatically logged within that instance. These are first reviewed by Prezent personnel to determine that the appropriate level of priority is assigned, taking into factors such as relevant mitigating controls and exposure. Those issues identified at the highest risk classification level will be targeted for remediation as quickly as possible.

Once it is determined that a patch needs to be deployed, this effort enters the change management process. During this process, the assets, risk, and potential impact to the relevant environment are identified along with the testing required, back-out plan, and timeline for deployment. Where no clear remediation is available virtual patching is implemented.

Prezent implements continuous vulnerability and risk management programs using in-house and external tools to identify, measure, and mitigate vulnerabilities.

11. Accessing data

Customer access to data

As the data controller, the customer determines who has access rights to their instance and the data stored in it. As the data processor, Prezent provides the tools for customers to secure and audit their instance according to their requirements. In general, Prezent does not access customer data, but it is sometimes necessary while resolving customer support tickets.

Prezent access to customer data

Occasionally, authorized Prezent operators may be required to access a customer's instance to provide support. Access to customer data is only for justifiable business use cases, such as debugging failures or other operational issues. This is done on an incidental, per-event basis, and not every customer support event will require access to customer data.

Only members of the Prezent support team who have been specifically assigned to an active incident can be granted access, and that access is granted on a just-in-time basis. Additionally, customers may specify that their explicit authorization is also required when that access is requested.

12. Authentication and authorization

Authentication

Prezent provides customers with two authentication options

Prezent instance provides customers with multiple authentication options that can be implemented simultaneously within an instance.

Security Assertion Markup Language (SAML) for Single Sign-On (SSO)

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML exchanges security information between an identity provider (a producer of assertions, commonly abbreviated to IdP), and a service provider (a consumer of assertions).

Prezent SAML 2.0 integration enables single sign-on by exchanging XML tokens with an external IdP. The identity provider authenticates the user and passes email and name attributes to the Prezent instance. If the instance finds a user with a matching attribute, the instance logs that user in.

The Prezent SAML plugin supports SSO-based authentication via a variety of SAML-compliant identity providers. This includes Active Directory Federation Services (ADFS), as well as third-party identity providers such as Ping, SecureAuth, SailPoint, Okta, or any that are compliant to the SAML 2.0 standard. Customers who implement their own SAML compliant IdP or opt for a third-party service can then also leverage this with other cloud services. When customers elect to use the SAML plugin, their password and credential policies are governed by their own IdPs.

Built-in “native” authentication & authorization

In the case of native authentication, passwords are managed solely by customers. When using native Prezent authentication, properties such as the length, complexity, rotation, and uniqueness of passwords are customizable by a customer.

Authorization

Customers have full control of entitlements granted to each of their users within Prezent. This includes a built-in role-based access control (RBAC) mechanism providing user groups. These can be used by customers to assign access to applications and data within their instances.

Customer access management

Prezent customers are responsible for the management of user identities within their instances. This includes the creation of individual identities (credentials) for each of their users, both internal and external, the methods used to authenticate those users, password policies (for built-in authentication), and the entitlements and access levels granted to those users.

13. Security logging and monitoring

Overview of logging and monitoring

Prezent takes a dual approach to continuous monitoring using both internal monitoring and third parties.

Internal monitoring

Prezent has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through direct conference calls. Within departments, code reviews and Prezent's quality assurance program help ensure internal controls are being followed and implemented.

Third-party monitoring

Prezent contracts a third party to perform annual penetration tests and uses the compliance automation client to monitor for new vulnerabilities. The compliance automation client is also used for tracking and logging of known vulnerabilities. The process for reporting any deficiencies with regards to Prezent policies and procedures is clearly spelled out in each relevant policy.

Logging and monitoring Prezent instances

Prezent uses a combination of services to monitor its network and systems. These monitoring tools allow for gaining insights and improving network usage, availability, and overall performance and health of our network resources.

Automated tools are deployed to enhance our risk management capabilities, identify security incidents, improve security operations visibility, and continuously discover and manage vulnerabilities at scale.

Prezent is constantly striving to improve our security monitoring capabilities and uses AWS documentation on best practices to inform the alerting and logging measures we take.

Logging and monitoring Prezent security infrastructure

A key component of any security program is to maintain detective controls to monitor for potential threat actors and intrusion attempts into the Prezent environment.

Prezent has a formal, documented security incident response policy, process, and workflow. Prezent's incident response process includes event discovery; triage and analysis; investigation; containment and neutralization; recovery and vulnerability remediation; and hardening and detection improvements.

The primary goal is to investigate, contain any exploitations, eradicate any threats, recover Prezent systems, and remediate any vulnerabilities. Throughout this process thorough documentation will be required as well as a post-incident report. Prezent will inform all necessary parties of the incident without undue delay.

Contractual commitments can be viewed by accessing the customer contract and the Data Processing Addendum.

14. Encryption

Encryption overview

Prezent provides all customers with encryption for data in transit and at rest. This section summarizes encryption capabilities at a high level.

Encryption in transit

To protect data in transit between our app and our servers, Prezent supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols and above, Advanced Encryption Standard (AES 256) encryption, and SHA 256 signatures, whenever supported by the customers.

Encryption at rest

Data at rest in Prezent's production network is encrypted using industry-standard 256-bit AES256, which applies to all types of data at rest within Prezent's systems—Serverless NoSQL databases, Relational databases, file stores, database backups, etc.

Usernames and passwords

Prezent encrypts customer usernames and passwords used to access the Prezent using cryptographic hash functions. Prezent also supports single sign-on to integrate with the customer's own authentication service. In this configuration, Prezent uses an authentication token provided by the customer's identity provider in lieu of a stored username and password to identify and authenticate the user.

Data communication

Prezent uses a fully encrypted channel to communicate with and access its network and applications. All traffic within the network is redirected from HTTP to HTTPS.

Access Control to the production code base is limited via the following controls:

- Multi factor authentication must be used to access any part of Prezent's codebase
- The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- RBAC approach is used for accessing the application code repository.
- All default regular-user accounts have been removed.

Key management

Access to keys and secrets are secured in accordance with the Access Control Policy.

15. Conclusion

Prezent is a cloud-based platform that supports a logically separated tenant architecture that enables isolation of customers from each other.

Key security benefits are provided through the application of extensive automation, implementation of standardized operational processes, and built-in platform security features such as data encryption and access control.

We at Prezent believe that our customers are well-served by our application of relevant, measurable, and industry recognized information security frameworks. These include ISO/IEC 27001:2013, as well as accreditation with regional standards and regulations such as CCPA and GDPR. Transparent disclosure is an additional element of assurance available to all customers. This includes, but is not limited to, provision of the SSAE 18 audit SOC 1, SOC 2 Type I & II reports, and ISO certificates.

For more information about Prezent, please contact your account representative or visit us at:

https://www.prezent.ai/