InVision Enterprise Security

May 2020

Introduction

Your team's digital product design work is a core part of your company's success. That's why we go to extensive measures to protect it. InVision uses industry-best, market-leading security tools to protect our customers' most sensitive and confidential data. We also provide configurable security enhancements to your InVision account to help you efficiently adhere to organizational and compliance standards.

This white paper provides an overview of InVision's security program, controls, and functionality employed within our production environment, including several new features available in the latest version of InVision (Version7).

Organizational Security

InVision's best-in-class security program is built against the ISO 2700x standard, with supplementary controls added for NIST framework alignment and compliance with European privacy regulations. Our security team, led by InVision's VP of Information Security, implements and maintains appropriate controls to protect customer data and assets. Specific areas of focus for the security team feature network, database, system, and application security—and 24x7 monitoring and alerting, risk management, and compliance.

Protecting Customer Data

Secure by Design

The principle of security by design is not new, nor is it complex in theory; however, many organizations struggle to fully bring this concept into practice.

InVision is an exception.

InVision's Engineering organization utilizes a squad methodology for product development, which provides our application security team the perfect opportunity to integrate and embed themselves in the development process throughout the development lifecycle. This methodology enables the application security team to preemptively advise and enable team members, and retrospectively assess features, components, and releases through continuous internal and external security testing.

To supplement internal vulnerability testing, InVision performs semi-annual third party network and application penetration tests and participates in two leading bug bounty programs. These programs allow the world's most gifted and talented hackers and penetration testers to test our security measures in a dedicated and tightly controlled test environment for monetary gain.

Encryption

Data in Transit

All data transmitted to and from the InVision platform is protected using Transport Layer Security encryption. InVision utilizes the strongest available ciphers and protocols, including support for both TLS v1.2 and TLS v1.3 (new!) .

Data at Rest

Data at Rest: All design files, personal data, authentication data, and session tokens are encrypted at rest using AES-256 encryption. Encryption is managed through the FIPS 140-2 compliant Amazon Key Management System (Amazon KMS). Key Encryption Keys (KEKs) are rotated annually and managed with dual controls.

Network and Server Security

Distributed Denial of Service (DDoS) Protection

InVision usesa best-in-class DDoS protection service that can auto-detect and mitigate layer 3, 4, and 7 network attacks. This service protects the platform from availability disruptions, but more importantly, it identifies and prevents brute force attacks, keeping your account credentials safe and secure.

Web Application Firewall (WAF)

InVision applications and services are also protected with an enhanced Web Application Firewall that can detect and block more than 600 web-based attacks and payloads, including OWASP top 10 attacks. In addition to typical signature-based solutions, this market-leading solution learns "normal" application behavior and correlates this with threat intelligence to provide advanced alerting and blocking capabilities. This is one of the most important components InVision utilizes to protect our customer data from attack, compromise, and data leakage.

Intrusion Detection and Prevention

The InVision production platform is equipped with the latest in-network and host-based security monitoring tools, designed to detect and prevent malicious attacks against our customers, site, and services.

Advanced Container Security Tooling

InVision uses one of the most advanced container security tools on the market, providing our production environment with advanced features such as automated hardening of images, continuous vulnerability scanning, real-time patching, real-time threat and anomaly detection, role-based access control, and policy enforcement.

Endpoint Security

All workstations comply with InVision Endpoint Security Standards, encompassing the deployment of full disk encryption, encrypted VPN, and advanced threat detection software. Additionally, a mobile device management (MDM) agent is deployed and utilized to ensure that systems adhere to our password policy, are kept up-to-date, and do not install or run prohibited software.

InVision Employee Access Control

Provisioning

To reduce the risk of data exposure, InVision adheres to the principle of least privilege and role-based access control. As a result, all employee requests for access require formal documented access requests, including access request duration and justification, and must be reviewed and approved by both their manager and a member

of the Security team. Production access is reviewed quarterly.

Authentication

InVision requires Multi-Factor Authentication for all production access for all employees, reducing the likelihood of unauthorized or compromised user accounts accessing customer data.

Continuous Monitoring

InVision monitors all production networks, systems, containers, and applications for suspicious and unusual behavior. Logs are generated from events such as administrative access, use of privileged commands, system calls, and application restarts. These logs are analyzed in near realtime to detect and alert on potential issues, and are retained for at least 12 months for forensic and auditing purposes. Access to production logs is restricted to security personnel on a need-to-know basis.

Data Retention and Disposal

Customer data is retained throughout the duration of the Service agreement, after which the customer is granted an additional thirty (30) days to retrieve designs and other content from the platform.

Upon expiration of the extension period, or earlier upon request, InVision will destroy, or render unreadable, all live customer data. Backups that contain recently deleted data will be purged within 14 days.

Incident Response

InVision has established a mature Security Incident Response framework for reporting and responding to potential security incidents. Security incidents are managed by knowledgeable Security Engineers, and escalated to appropriate leadership based upon analysis, validation, and severity. In the event of a customer impacting security incident, affected customers will be informed via email by our customer support team. Incident response procedures are tested and updated at least annually.

Disaster Recovery and Business Continuity

InVision utilizes a best-in-class hosting provider that distributes platform operations across multiple availability zones, protecting our platform availability against failures caused by insufficient power infrastructure, loss of network connectivity, and ineffective environmental controls. In the event of a catastrophic incident that is not handled seamlessly by our service provider, InVision's Disaster Recovery and Business Continuity Plan will be invoked. This plan provides guidance, process, and procedures to restore platform

availability under a variety of circumstances. The Disaster Recovery and Business Continuity Plan is tested and updated at least annually. Nightly backup snapshots are encrypted, retained for 14 days, and validated through quarterly restoration testing.

Vendor Management

InVision utilizes a number of sub-processors as part of the delivery of our Services, some of whom also act as data processors with access to certain customer personal data. InVision assesses the security of our sub-processors at least annually and contractually requires that they maintain the security standards of InVision and our customers. Get detailed information about InVision sub-processors and sub-contractors.

Service Security

The following security configuration controls are available, and highly recommended, for InVision v7 Enterprise customers.

Dedicated Name Space

Dedicated name spaces, with custom URLS, enables you to create a customized look-and-feel for your users' experience, and provides your users with a customized login experience.

IP Whitelisting

InVision offers application-based IP Whitelisting, which prohibits access to anyone not explicitly authorized. This feature provides an additional layer of protection against unauthorized access, account compromise, and brute force attacks. Find out more about IP whitelisting.

Audit Logs (new!)

InVision now provides an audit logging feature that is clear, concise, and readily available within the InVision application. Audit logs now track who made what modifications, to which design, and when. It's that simple. Logs can be viewed via the administrative console or downloaded as a CSV. No need to request logs from Support or sifting through backend application logs for what you need.

User Provisioning and Deprovisioning (new!)

InVision now supports user provisioning and deprovisioning through the SCIM (system of cross-domain identity management) protocol. SCIM integrates with industry leading Identity Providers (IdPs) and introduces a simple way to automate the onboarding and offboarding process, and addresses required access modifications due to changes in roles and responsibilities. The effect on your team will be a reduction in manual overhead and a decrease in potential exposure caused by inadvertent continued access following termination.

User Authentication and Access

Customer administrators have the option to configure user authentication in one of the two following ways:

1. Local Authentication

Customers utilizing local authentication will use InVision-specific usernames and passwords for each platform user. Customers who select this authentication mechanism should strongly consider enabling both of the following supplementary configurations:

- **Password Policies**

  InVision provides customers with the ability to meet organizational or compliance password requirements by configuring password policy length, complexity, duration, and history. Learn how to configure a password policy.

- **Enforced Multi-Factor Authentication**

  InVision also offers application-based two-factor authentication, preventing compromise from leaked credentials or brute force attacks. Learn how to configure two-factor authentication.

2. Single Sign-On (SSO) Authentication

Customers who leverage Single Sign-On (SSO) reap the benefits of both a seamless user experience when they access InVision applications and effortless enforcement of company security requirements through authentication rules. SSO is supported over SAML 2.0. Learn how to configure SSO for your service.

Whether your team utilizes local authentication or SSO, you should consider using our session timeout configuration feature and share link enforcement controls.

Session Timeout

Session timeouts protect users whose devices may be accessed by another individual, compromised, lost, or stolen by terminating the active session in a predefined amount of time. Learn how to configure a session timeout in the section titled "Timing Out."

Document Sharing Controls

Sharing documents is a key part of the InVision collaboration workflow—but without the proper controls sensitive documents can end up in the wrong hands. InVision offers granular controls to give you the security you need without impeding your end-user's sharing workflow.

Compliance

InVision knows how important your data is, which is why we're committed to ensuring that the security controls we have put in place are effective against today's and tomorrow's threats. To that end, we have sought and maintained the following third-party assessments, attestations, and certifications:

- **SOC2 Type 2** – Annual examination and attestation to the AICPA SOC2 Type 2 security and confidentiality trust principles
- **PCI** – PCI certified service and payment processor
- **CSA** – Attestation to and observance of Cloud Security Alliance security recommendations and requirements
- **EU-US Privacy Shield** – EU-US and US-Swiss Privacy Shield framework

InVision uses a third-party, top-tier data center that maintains several industry-recognized certifications, including FedRAMP, ISO, SOC, and PCI.

Our hosting provider is compliant with numerous regulations, privacy standards, and frameworks, including HIPAA, HITECH, GLBA, the EU

Data Protection Directive, EU-US Privacy Shield, FISMA, and more than 30 others.

Summary

InVision understands the importance of your Intellectual Property, your team's valuable work, and your employees' personal data. We do not take this responsibility lightly and continue to assess and improve our Information Security program to ensure you can rest easy at night.

Questions? Reach out to your account executive and they will be happy to assist or connect you to a member of InVision's security team.


in
VISION