Insightful

We Keep Your Data Safe and Confidential

At Insightful , we live by a privacy-first approach that's built on multi-layered security that protects your sensitive information. Whichever industry you're in, rest assured that your business-critical data stays confidential with Insightful .

Book a Demo

Enterprise On-Premise Deployment

Enterprises need next-level security – and Insightful delivers it with our enterprise-grade on-premise solution. Experience the security and flexibility of storing data on-premise in your private cloud or physical servers located on your private network. Once set up, your data is completely isolated from outside networks (except for a single licencing endpoint).

Learn more about how Insightful works in Enterprises →

Powerful Configurability to Reduce the Collection of Sensitive Data

As Insightful collects and stores data, we know some of it may be sensitive. This is why Insightful secures your data via multi-level security at all access and storage points. Plus, highly flexible security features enable you to manage and restrict which data is collected in the first place.

Full control is in your hands:

- Disable activity tracking for specific apps and websites
- Disable screenshots for specific apps and websites

Note: Insightful doesn't have keylogging features.

Let's Talk About Data Security

Encryption

Data At Rest

- All data at rest is encrypted with AES-256.
- All keys are stored and managed by Google Cloud KMS.
- Data is broken into subfile chunks for storage, and each chunk is encrypted at the storage level with an individual encryption key.

Data in Transit

- HTTPS, SSL, TLS 1.2
- All data is fully encrypted when in Transit.

Access

By the Client

- Client data is accessed through a secure HTTPS connection.
- Activity Log Data and screenshots can be exported via a variety of methods in compliance with Right to Data Portability (GDPR, Article 20).
- Passwords are protected using an advanced hashing algorithm.
- Two-factor authentication can be enabled for additional account protection.

By Third Parties

- Insightful will never sell or disclose your data to a third party - not even anonymized.

By Insightful

- You're the owner of your data - our team never views the information collected by our software. We operate on a 'Least privilege' policy – we only request access your data if an account admin requests support.
- All Insightful employees go through a rigorous background screening process and sign a strict NDA.

Retention

We retain your Account data for as long as you maintain your Insightful account, or as otherwise needed to provide you with our Services.

Screenshots are stored for up to two months. All other data Insightful collects is kept for up to 24 months.

Partners and Thirds Party Service Providers

stripe · mongoDB · elastic

Multi-Tenancy

While Insightful is a multi-tenant cloud SaaS provider, we've established a strict protocol to ensure that all key/private customer data is isolated to safeguard against access and data breaches.

Multi-tenant

- Insightful User and Access Management

Isolated

- Employees' activities, time on tasks, and fragments live in isolation
- Screenshots live in total isolation for each account

Security Testing

Insightful infrastructure and apps are rigorously security-tested on a continuous basis to identify and resolve potential vulnerabilities. As an extra layer of security, we work with leading security teams and specialists to provide your data with the highest level of security.

Our data is stored in a secure data center managed and protected by Google Cloud Platform (GCP), which undergoes its own rigorous security testing against the latest standards.

Unmatched Reliability and Transparency

We pride ourselves on our server reliability, boasting an uptime track record of +99.9%. What this means to you is that your data is always secure and available to you when you need it most.

To provide the highest level of service and operational transparency you can check on uptime anytime through our 'Status Dashboard'. Here you'll find a history of both scheduled and unscheduled maintenance windows and real-time updates of platform status.

Business Continuity and Disaster Recovery

Data Backups

To ensure that your customer data is always safe and accessible, we perform backups to two different cloud locations every 30 minutes.

Uptime

Insightful boasts an impressive server availability uptime track record of +99.9%. Users can check on uptime anytime through our Status Dashboard to receive real-time updates.

Recovery

In the unlikely event of a full system outage, Insightful customer data and applications will be restored and running in a new cloud region in less than 6 hours.

Maintenance

When downtime-causing maintenance is required, you'll be notified well in advance. And we always aim to perform maintenance in off-peak hours to minimize impact.

FAQ

How are user passwords stored?

All client passwords are stored encrypted and hashed. They are never stored in plain/human readable text.

How does Insightful handle credit cards?

Insightful never stores credit card details associated with your account. All credit card information is collected and processed by our third-party provider, Stripe. Stripe is a PCI compliant payment processor. Your card information is passed directly to them, meaning your credit card information never touches our servers.

What happens to my data after I terminate my Insightful Contract?

Once you delete your Insightful account, or otherwise terminate the use of our services, we may continue to store certain information as needed to comply with our legal obligations, or to resolve any disputes, prevent fraud, enforce our agreement or to protect our legitimate interests.

What is Insightful ' uptime track record?

Our uptime track record is quite impressive: +99.9% for system availability. You can check the uptime information anytime through our Status Dashboard.

The dashboard is updated with the latest information on scheduled maintenance, as well as unscheduled downtime. During downtime, the page is updated in real-time, but you can also subscribe to receive the latest updates.

When will you notify customers of a security breach?

When we detect a data breach, we will notify affected customers as soon as possible and always within 72 hours. The security of your data is our primary focus.