www.worktime.com info@worktime.com 1-877-717-8463

WORKTIME®

SECURITY & RELIABILITY FEATURES

NON-INVASIVE MONITORING

- ✓ CERTIFIED SECURE DATA CENTER
- ✓ MULTI-TIER SYSTEM ARCHITECTURE
- ✓ AES-256 ENCRYPTION
- ✓ TWO-FACTOR AUTHENTICATION
- ✓ ROLE-BASED/ IP ACCESS CONTROL
- ✓ AUDIT LOGS
- ✓ REGULAR AUTOMATIC BACKUPS

AICPA Service Organization Control Reports
AICPA
SOC 2

Gramm-Leach-Biley Act

GDPR

HIPAA

IN THIS DOCUMENT

WorkTime - safety features

Certified secure data center
All WorkTime data is hosted in certified secure facilities that comply with international security standards. This guarantees physical protection, controlled access, and reliable infrastructure for your monitoring data.

Multi-tier system architecture
WorkTime is built on a robust multi-tier system architecture designed for high availability, scalability, and fault tolerance. This structure isolates different components of the platform, ensuring consistent performance, minimizing downtime, and providing a reliable foundation for enterprise-level operations.

AES-256 encryption
WorkTime uses AES-256 encryption, the industry standard for protecting sensitive data. This advanced encryption method ensures that all information — both in transit and at rest — remains secure and unreadable to unauthorized parties, providing strong protection against data breaches and cyber threats.

Two-factor authentication
WorkTime supports two-factor authentication (2FA) to add an extra layer of protection. Even if login credentials are compromised, unauthorized access is prevented by requiring a second verification step.

Role-based access control
WorkTime provides role-based access settings, ensuring that each user only has the level of permissions required for their role. This reduces security risks and keeps sensitive data available only to authorized personnel.

IP access control
WorkTime enhances security by allowing you to restrict system access to approved office IP addresses or secure VPN connections. This feature ensures that only trusted networks can connect, reducing the risk of unauthorized logins and external threats.

Audit logs
WorkTime records every action taken by administrators and users in detailed audit logs. These logs support internal investigations, improve accountability, and help meet compliance requirements such as SOC 2 and GDPR.

Regular automatic backups
WorkTime performs scheduled automatic backups to ensure that your data is never lost. Even in case of unexpected failures, information can be quickly restored, keeping monitoring uninterrupted.

Full customer control over security configuration
Organizations retain complete authority to configure and manage all security settings within WorkTime, aligning data protection practices with their internal policies and compliance requirements.

WorkTime uses AES-256 encryption

WorkTime ensures enterprise-grade data protection by using industry-standard AES-256 encryption

All employee activity data is securely encrypted both in transit and at rest, safeguarding it against unauthorized access. By applying the same encryption standard trusted by financial institutions and government organizations worldwide, WorkTime guarantees that information remains fully protected while delivering accurate, non-intrusive productivity analytics.

Protection of data at rest and in transit

WorkTime applies strong AES-256 encryption to secure all information, whether it is stored on servers or transmitted between systems. This ensures data remains safe from unauthorized access at every stage.

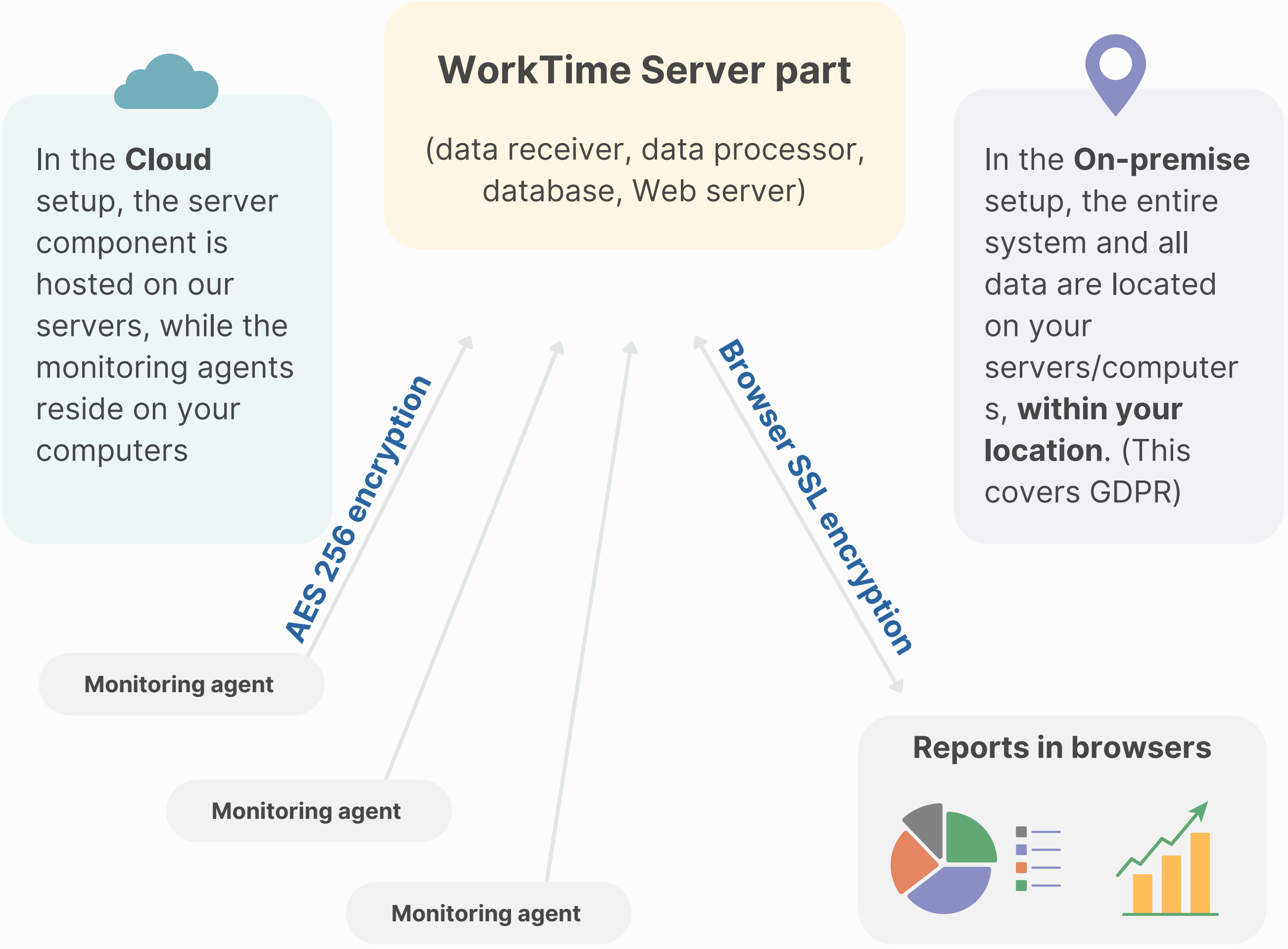
Encrypted storage locally or in the cloud

Whether deployed on-premise or in the cloud, all collected data is consistently stored in encrypted form. This guarantees that sensitive business information remains secure regardless of the chosen infrastructure.

Reliability

WorkTime is built on a robust multi-tier system architecture that ensures both stress resistance and fault tolerance

This design guarantees that monitoring data is never lost and the monitoring process remains stable, even under heavy workloads. Proven in real-world deployments, WorkTime has been successfully implemented in organizations ranging from small teams to enterprises with 15,000+ employees and environments with over 300 Citrix servers.



WorkTime Server part

(data receiver, data processor, database, Web server)

In the **Cloud** setup, the server component is hosted on our servers, while the monitoring agents reside on your computers

In the **On-premise** setup, the entire system and all data are located on your servers/computers, **within your location**. (This covers GDPR)

SOC2, HIPAA, GDPR compliance

SOC 2 compliance

WorkTime follows SOC 2 principles to ensure data security, availability, and confidentiality. By adhering to industry-recognized auditing standards, WorkTime demonstrates reliable safeguards for handling sensitive business information. This gives organizations confidence that their monitoring data is managed with strict controls and operational integrity.

GLBA compatible

WorkTime is designed with financial organizations in mind, offering a GLBA-safe mode that ensures nonpublic personal information (NPI) is never collected or exposed. The system monitors productivity through safe metadata only, without accessing financial records, customer data, or private content. This makes WorkTime a secure solution for financial institutions that must comply with GLBA requirements.

HIPAA compatible

WorkTime is designed with healthcare organizations in mind, offering a HIPAA-safe mode that ensures protected health information (PHI) is never collected or exposed. The system monitors productivity through metadata only, without accessing electronic health records, patient data, or private content. This makes WorkTime a secure solution for healthcare providers that must comply with HIPAA requirements.

GDPR compatible

WorkTime fully supports GDPR requirements by applying privacy-first monitoring practices. The software collects only the data necessary for productivity reporting, encrypts all information, and gives customers complete control over their data. Employees' personal content, messages, and credentials remain private, ensuring transparency and trust in compliance with GDPR standards.

Non-intrusive & productivity oriented

WorkTime is non-invasive and collects only selective productivity-related data, focusing on key performance indicators (KPIs) for accurate workforce analytics. It never captures passwords, message texts, or the content of communications, ensuring full respect for employee privacy.

WorkTime monitoring: safe & privacy-first

✓ WorkTime **NEVER** records screens, keystrokes, passwords, chats, emails, or documents. Instead, it collects only data which is sufficient to produce **70+** productivity and workforce analytics reports. This approach eliminates the risks tied to capturing personal content while still delivering accurate, actionable insights.

✓ **Safe screen analyzer:** In WorkTime, screen activity is represented strictly as numerical data — no images, no personal content. Numbers are straightforward to analyze, making it easy to identify patterns, measure productivity, and track progress over time.

✓ **Safe keystroke counter:** WorkTime measures keystroke activity — such as typing speed per application and per employee — without capturing any content. This privacy-first feature is fully user-controlled and can be turned on or off at any time.

Traditional monitoring: content recording risks

⚠ **Content recording risks:** conventional monitoring tools capture personal information — including screens, keystrokes, passwords, chats, emails, and documents — creating serious security and privacy concerns.

⚠ **Traditional screenshots:** all you receive are raw images that are difficult to interpret and offer no reliable way to track productivity progress.

⚠ **Traditional keystroke logging:** keystrokes are recorded in full, exposing sensitive content and credentials, yet providing little to no value for meaningful productivity analysis.

⚠ Conventional monitoring tools often rely on **methods similar to those of spyware**, raising serious privacy concerns. They not only raise serious privacy concerns, but also fail to provide meaningful insights into employee performance KPIs.

Try WorkTime!

WorkTime offers a **14-day free trial of its top-tier Enterprise** plan with unlimited employees. The trial includes access to **70+ reports** - such as attendance, active time, productivity, progress, alerts - as well as **HIPAA- and GDPR-safe modes**, and more. WorkTime supports monitoring across **remote**, **hybrid**, and **office** environments!

WorkTime: Privacy-first monitoring

Experience privacy-first, performance-focused monitoring

Questions? We're here to help!
info@worktime.com 1-877-717-8463

Try WorkTime now