TimeTrex
Workforce Management

Security White Paper

The Security Challenge

As cloud-based workforce management services are growing in popularity, organizations are finding that the ability to control and customize security features is an essential requirement for virtually every company.

With rapidly changing technology, it's common for employees to require access to their workforce management product from several locations, as well as an expanding variety of remote devices, such as laptops, tablets and cell phones. However this broader access increases the risk of accidentally losing or compromising sensitive data as each additional endpoint makes security management more challenging. The more endpoints an organization has, the more attack points IT security professionals have to manage.

Organizations that deploy their Workforce Management solution on-site, often find the security management aspects costly and time consuming. To provide remote access - while maintaining security best practices – organizations discover that they can better control and customize security features using cloud-based Workforce Management Services instead.

The Security Solution

A cloud-based system helps to maximize the safety and security of sensitive data, and provide the protection and flexibility to control and customize security features while safeguarding vital information.

TimeTrex Workplace Management Services have been developed on a cloud-based system with robust "built-in" security features that can be customized to meet your unique and individual needs. We have invested in the creation of a state-of-the-art security infrastructure, and offer over a decade of experience in the protection and management of online data.

TimeTrex Security Consists of FOUR Key Parts

1) “**Built-In” Security-hardened features to shield your information and safeguard access.** TimeTrex implements policies and controls on par with, or better than, the on-site data centers of even the most sophisticated organizations.

2) **A continuous investment in processes and technologies to stay a step ahead.** TimeTrex continuously implements practices to proactively identify and mitigate security threats before they become a risk to you.

3) **The flexibility to customize security settings that meets your unique needs.** TimeTrex supports customers in virtually every industry, including highly regulated areas such as healthcare, finance, education, and government. We are a trusted choice.

4) **Independent verification at the source code level.** TimeTrex is the ONLY software of its kind that allows customers to independently verify security claims at the source code level.

Security Aspects of TimeTrex

High Security Data Centers

We store data in tier-one data centers strategically located around the world. These data centers are securely built from the ground up to protect them from natural disasters or unauthorized access. Each data center is SOC 1/SSAE 16 (formerly SAS 70) certified and monitored 24-hours a day by security personnel. Only limited personnel can gain access to the physical hardware within this restricted access area. When maintenance or provisioning operations are needed, personnel must pass through multiple authentication and security processes, including badges and smart cards, biometric scanners, continuous video surveillance and two-factor authentication.

Data Isolation

We provide scalable Workforce Management solutions using a multi-tenant service where customers share hardware resources, but data cannot be accessed or compromised by co-tenants. A proprietary data isolation technique is used to ensure customer information is fully protected. Such a multi-tenant system allows us to keep our services secure yet affordable. If required, a custom hosting solution is available for organizations that require dedicated servers. Whether you use our multi-tenant service or dedicated servers, your security is our highest priority.

Data Backup/Disaster Recovery

All customer data is mirrored in real-time to at least four storage devices spread across multiple independent servers offering fully multi-point redundant fault tolerance. Data checksums are utilized at the network, memory (RAM), storage, database and backup system layers. Each time data is read, and at minimum once daily, checksums are compared to ensure that data still matches its original value, protecting against any hidden or latent bit rot.

In addition to that, once daily during off-peak hours this data is backed up to encrypted offsite storage in two other data centers at least 500km (310miles) apart for purposes of disaster recovery, with daily snapshots being retained for a minimum of 30 days. At least one of these data centers enforces a minimum storage retention (anti-tamper) policy to ensure once data is written, it cannot be modified or deleted for a minimum of 30 days.

Immediately after every backup, a full end-to-end restore is performed to a separate server exercising our recovery protocols and ensuring that the backups are complete and in full working order by both an automated system and a human-in-the-loop test procedure.

End-to-End Data Encryption

With our cloud-hosted service, your data will exist in two states: at rest on storage media and in transit from our data center to your employees' devices. Data at rest on storage media is encrypted at the hardware level using industry standards such as AES 256-bit encryption and data in-transit to the customer device is encrypted using SSL.

Secure, Segmented Networks

The networks within our data centers are segmented to provide physical separation of critical back-end servers and storage devices. Our clients connect to TimeTrex using encrypted, industry-standard secure sockets layer (SSL). The use of SSL establishes a highly secure client-to-server connection and provides data confidentiality and integrity between the desktop and the data center. The services we provide over the Internet originate from employees' Internet-enabled locations and end at one of our secure data centers.

Adhere to Security "Best Practices"

The advancement and enhancement of security is an ongoing process at TimeTrex. We are committed to constantly maintaining, improving and verifying our security systems in order to keep your data as secure as possible. We have highly experienced and trained personnel to keep software and hardware technologies up to date and refined through robust designing, building, operating and supporting processes. In addition to the above, TimeTrex adheres to the PCI Data Security Standard, is PCI certified and has a 3rd party conduct daily perimeter vulnerability scanning to ensure compliance.

Traffic Throttling to Prevent Denial of Service Attacks

We routinely monitor and regulate traffic to minimize congestion and provide a fast and efficient user experience. We use baselines to track normal traffic bursts and adjust bandwidth accordingly. This prevents employees from being denied access, and red flags any potential threats or service attacks. By closely monitoring traffic we will know when an employees' traffic exceed typical parameters. The traffic is throttled until usage returns to normal. Whether the excessive traffic is caused by employee behavior or a malicious attack such as a Denial of Service (DoS) we will quickly and automatically respond to the traffic changes.

Prevent, Detect, and Mitigate Breach

Prevent, Detect, and Mitigate Breach is a defensive strategy aimed at predicting and preventing a security breach before it happens. The strategy involves continuously improving our built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS Patching to latest updated security software and network level DDOS (Distributed Denial of Service) detection and prevention.

TimeTrex continues to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. Wherever possible, we replace human intervention with an automated, tool-based process. Routine functions include deployment, debugging, diagnostic collection and restarting services. This greatly enhances the security and agility of the service.

TimeTrex conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help TimeTrex security experts create a methodical, repeatable, and optimized stepwise response process and automation.

Enabling Employee Access

TimeTrex data and services are secured at the data center, network, logical, storage, and transit levels. We offer a built-in access control list (ACL) permission system and over 800 fine grained permissions to control employee access and data usage. Individual or group access permissions can also be assigned.

Customer-End Single Sign-On and Security Provisions

Administrators can federate on-site Active Directory or other LDAP based directory services. Once federation is configured, employees whose identities are based on the federated domain can use their existing corporate logon credentials to authenticate to TimeTrex services.

Auditing and Retention Policies

TimeTrex's auditing system enable customers to log events, including viewing, editing, and deletion of content including a snapshot of the data before and after every modification. Audit logs for critical data are retained for as long as you are a customer. Administrators can view the audit data and summarize current usage. Detailed reports are available to determine how information is being used within the system, what data is being modified and have the ability to investigate any areas of concern.

Conclusion

These days, businesses of all shapes and sizes can benefit from Workforce Management Services. They improve employee productivity and allow your workforce to access data from virtually anywhere around the world. With TimeTrex it’s not necessary to sacrifice security. Our cloud-based Workforce Management platform can help you get more done, AND maintain highly secure data during a time of ever-evolving threats.

Today, fewer and fewer organizations have the ability to maintain an equivalent level of security on-site at a reasonable cost. With TimeTrex, you can enjoy security at every level from application development to physical data centers to employee access and continuously maintain the highest level of security at an affordable price.