TIMIFY Security Whitepaper

last update: 21.06.2023

Introduction

In today's globally interconnected environment, the primacy of data security has never been more apparent. At TIMIFY, we are keenly aware that our role extends well beyond providing top-tier scheduling solutions - we are guardians of the data that our clients entrust us with.

This whitepaper stands as a testament to our dedication to security, offering a thorough exploration of our advanced security protocols and architectural safeguards. Not only will it give stakeholders a transparent view into our security practices, but it will also break down the elements of our multi-tiered security strategy. This strategy encompasses a myriad of elements from the physical security mechanisms in place at our data centers to the state-of-the-art network defenses designed to thwart potential breaches.

Our commitment to data security is unwavering and is reflected in our investments in cutting-edge security technology, the constant vigilance of our security team, and the rigorous controls and protocols we implement.

As the digital landscape evolves, so does our approach to cybersecurity at TIMIFY. Recognizing the importance of flexibility in dealing with emerging threats, we've designed our systems to dynamically adapt to new challenges.

In this whitepaper, we explore our strategies in detail. We explain how we utilize advanced technologies, strong encryption techniques, and policy enforcement to secure your data. Our goal is to stay one step ahead, pre-emptively fortifying our system against potential threats.

The trust our clients place in us is paramount. We ensure data integrity, confidentiality, and availability through stringent practices and industry-leading security protocols.

This whitepaper aims to reaffirm our commitment to security in the digital age. It emphasizes our promise to provide a secure platform that our users can trust and depend on. We invite you to continue reading to further understand our steadfast dedication to your data security.

Briefly overview

Data Storage and Encryption:
This involves the protection of client data both when it is in transit (moving from one place to another) and at rest (stored on our servers). We use industry-standard encryption algorithms to safeguard the client data at all times.

Access Control and Authentication:
We control who has access to certain data and systems by implementing strong authentication methods and restricting access based on user roles, ensuring only authorized individuals can access sensitive information.

Data Backup and Recovery:
To protect against data loss, we regularly back up data and have robust recovery procedures in place. These measures ensure data redundancy and business continuity in case of unforeseen events.

Network Security:
We implement measures like firewalls and intrusion detection systems to protect our network infrastructure from unauthorized access or breaches, ensuring our system's integrity and confidentiality.

Monitoring and Auditing:
We regularly track and review system events to detect any suspicious activities early and maintain system integrity. These auditing processes help us ensure accountability and compliance.

Incident Response:
In case of a security incident, we have a planned response to quickly identify, contain, and eradicate the threat, minimizing potential damage and recovering the system to normal operation.

Patch Management:
Regular system updates and patches are essential for addressing potential vulnerabilities. We ensure all systems are updated timely, thereby reducing the risk of security breaches.

Reliability and Availability:
We strive to provide a consistently available service. Thanks to the robust infrastructures of AWS and MongoDB Atlas, we ensure a high uptime and service reliability, allowing your business operations to run smoothly.

Data Storage and Encryption

At TIMIFY, we place the utmost importance on data security. Our data storage and encryption practices are designed with this in mind, adhering strictly to industry best practices.

Encryption at Rest:
We ensure all data stored within our databases, including backups, is fully encrypted. This means that even when your data is not actively being used, it is safeguarded against unauthorized access. Our systems convert the stored data into an unreadable format that can only be reverted to a readable format with the correct decryption key.

Encryption in Transit:
All data moving through our system is also encrypted, with a minimum standard of TLS 1.2 (Transport Layer Security). This means that any data communicated between our servers, internal systems, databases and client devices is converted into an unreadable format during transmission, preventing any unauthorized access or interception.

Together, these measures provide a comprehensive layer of security for your data, regardless of its state or location.

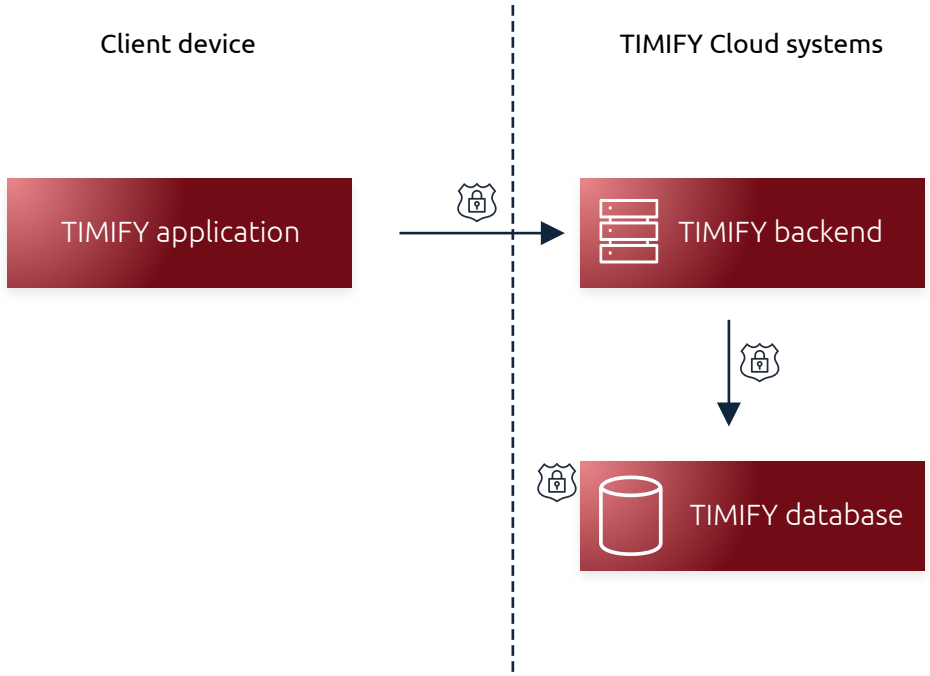


Figure 1 - Flowchart of data movement between the TIMIFY application, the server and the database.
All communication between the client and the server is encrypted with TLS 1.2+
The stored data in the TIMIFY database is encrypted ar rest.

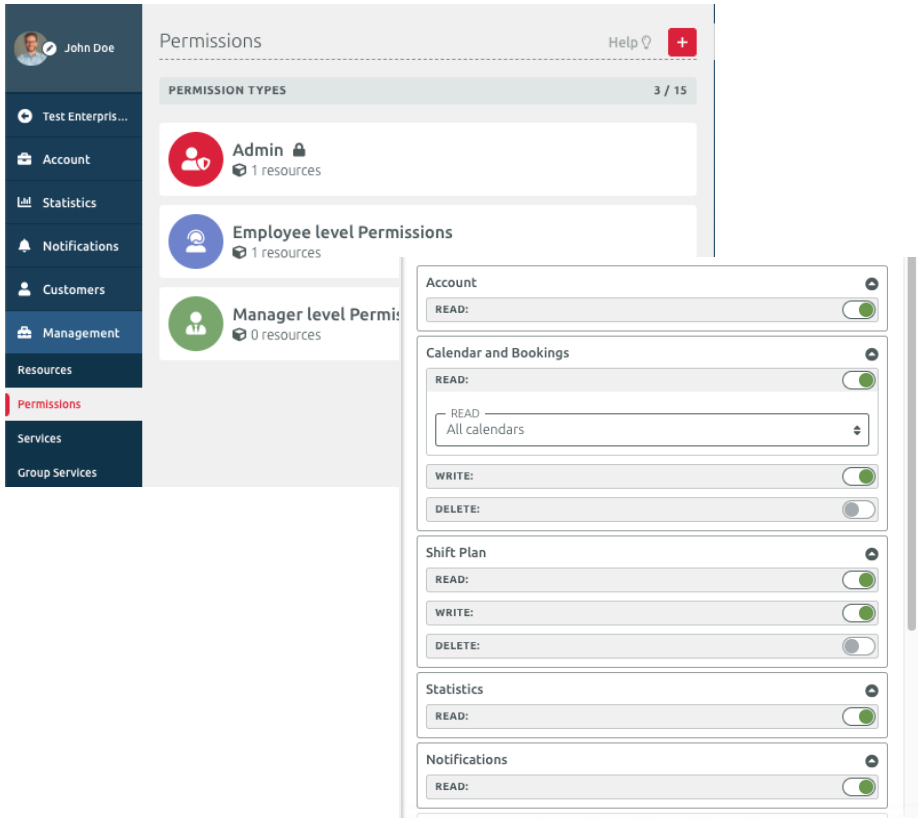
Access Control and Authentication

At TIMIFY, we've implemented rigorous Access Control and Authentication measures to ensure the security of our system and the confidentiality of your data.

Access Control:
Our systems operate on the principle of least privilege, meaning users are only granted the minimum levels of access necessary to perform their roles. We manage this through Role-Based Access Control (RBAC). With RBAC, access permissions are associated with roles, not individuals, providing strict control over who can access what within our system.

Authentication:
Authentication is the process through which users prove their identities before accessing their assigned resources. We use robust authentication methods, including multi-factor authentication (MFA), requiring users to provide multiple pieces of evidence to confirm their identity.

Protection against Brute Force Attacks:
To protect against brute force attacks, where an attacker attempts to gain access by trying multiple login combinations, we've implemented a limit on login attempts. If a certain number of incorrect attempts are made, the system will temporarily lock out the user, thwarting any potential brute force attacks.



Picture 1 - TIMIFY WebApp: Permissions Management screenshots

In addition to these measures, we continuously monitor and audit access patterns within our system to swiftly identify and respond to any suspicious activities.

Through these Access Control and Authentication practices, we strive to ensure your data is accessed only by authorized users and remains secure from unauthorized access.

Data Backup and Recovery

At TIMIFY, we understand the importance of your data and its pivotal role in your operations. That's why we've implemented comprehensive data backup and recovery procedures to ensure data continuity and to minimize any potential impact of unforeseen events.

Data Backup:
We regularly create backups of your data to ensure its safety in the event of system malfunction or any external threat. These backups are encrypted and stored securely in separate locations, thereby ensuring data redundancy and adding an extra layer of protection against data loss.

Data Recovery:
In the unfortunate event of data loss or corruption, our recovery processes come into play. Our systems are designed to restore data from our secure backups swiftly and effectively, allowing you to resume operations with minimal downtime.

This proactive approach to data backup and recovery is a crucial part of our commitment to safeguarding your data and ensuring the resilience and reliability of our services.

Picture 2 - TIMIFY places its trust solely in globally recognized leading technology corporations.

Network Security

At TIMIFY, we are committed to providing a secure network environment that safeguards your data and maintains the integrity and functionality of our services.

Firewalls:
We use sophisticated firewall systems to form a barrier between our trusted internal network and untrusted external networks. These firewalls are designed to filter incoming and outgoing traffic, allowing only legitimate traffic to pass through and blocking any suspicious activities.

Intrusion Detection and Prevention Systems (IDPS):
To further enhance our network's security, we implement IDPS. These systems continually monitor our network for signs of possible incidents, log information about these events.

Secure Network Architectures:
Our network architectures are designed with security as a priority. This includes using secure virtual private cloud (VPC) instances, subnets (public & private) for separating and categorizing resources, and utilizing network access control lists and security groups.

Encryption:
All data in transit within our network is encrypted using industry-standard encryption protocols. This ensures that even if data traffic were intercepted, it would remain unreadable without the decryption keys.

Monitoring and Auditing

At TIMIFY, we firmly believe in the importance of ongoing monitoring and regular auditing as essential elements of maintaining a secure and reliable service.

Monitoring:
We employ advanced monitoring systems that continuously track activity across our network and applications. These systems detect and alert us to any unusual or suspicious behavior that could indicate potential threats. We monitor a wide range of parameters, including system performance, data access, and usage patterns, to maintain system health and ensure security.

Auditing: Regular audits form an integral part of our commitment to transparency and adherence to established security practices. These audits involve rigorous examinations of our system configurations, access controls, and data handling practices to ensure they meet or exceed industry standards and comply with applicable regulations. In addition, audits are performed following any significant system changes or in response to a detected incident.

Our real-time monitoring coupled with periodic auditing enables us to maintain a high level of security awareness. This proactive approach allows us to rapidly detect, respond to, and rectify any potential issues, reaffirming our commitment to data security and the reliability of our service.

Incident Response

Security incidents are a reality of the digital world, and at TIMIFY, we recognize the importance of being prepared. Our comprehensive Incident Response strategy ensures we can quickly and effectively address any potential security threats.

Incident Detection:
Our systems are designed to vigilantly monitor network and application activity. Using sophisticated detection tools, we swiftly identify any anomalies or suspicious activities.

Incident Analysis & Containment:
Once a potential incident is detected, our dedicated security team jumps into action. They perform an immediate and thorough analysis to understand the incident's scope, impact, and potential risk.

Response and Recovery:
After the incident's immediate threat is neutralized, our team shifts focus towards system recovery. We work to restore any affected services to their normal function.

Post-Incident Follow-up:
We believe in learning from each incident. Therefore, every incident is followed by a detailed review to understand its root cause and to identify any adjustments required to our security protocols.

With our robust Incident Response process, we assure you that we are committed to maintaining a secure and reliable environment and ensuring the uninterrupted operation of our services.

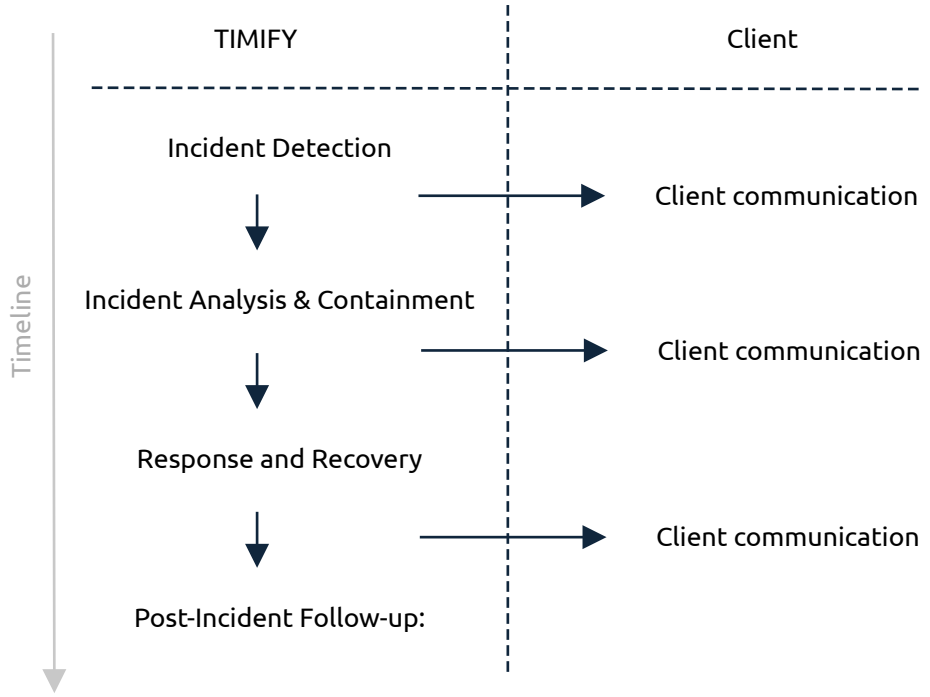


Figure 2 - TIMIFY incident response plan - overview

Patch Management

At TIMIFY, we've implemented a robust patch management process to ensure that our services remain secure and perform optimally.

Routine Monitoring: Our team continually monitors for new patches or updates released by AWS and other software vendors we rely on. This constant vigilance allows us to stay ahead of potential vulnerabilities that could be exploited.

Risk Assessment:
Each identified patch is thoroughly assessed for relevance and potential impact on our systems. This includes understanding the security enhancements it offers, its compatibility with our current systems, and the potential risks it may introduce.

Testing:
Before a patch is rolled out, it undergoes rigorous testing in a controlled environment. This step is vital to ensure the patch will not cause system instability or other adverse effects.

Patch Deployment:
Once a patch has been approved, it's deployed across our systems. For critical security patches, we prioritize swift deployment to quickly mitigate any potential risks.

Post-Deployment Review:
After a patch is deployed, we continue to monitor system performance and stability. This post-deployment review allows us to identify and quickly rectify any unforeseen issues.

Reliability and Availability

Ensuring that our services are consistently available and perform reliably is a fundamental priority at TIMIFY. Our infrastructure, built largely on Amazon Web Services (AWS), employs a variety of strategies to ensure high availability and reliability.

AWS Infrastructure:
We leverage the robustness and reliability of AWS, which provides a high degree of fault tolerance and operational stability. AWS's global infrastructure offers a secure, scalable, and reliable environment for our operations.

Load Balancing:
To ensure seamless performance even during peak usage times, we use load balancing techniques. This involves distributing workloads across multiple computing resources, thereby maximizing throughput, minimizing response time, and ensuring that no single server bears too much load. AWS's Elastic Load Balancing service aids us in this task, dynamically distributing incoming application traffic across multiple targets.

Multi-Region Availability Zones:
In our commitment to provide a highly available and reliable service, we take advantage of AWS's global infrastructure, which spans multiple geographic regions and availability zones. By strategically spreading our resources across these zones, we ensure that even if an issue arises in one zone, our service can continue uninterrupted, and our users remain unaffected.

Conclusion

At TIMIFY, we recognize our role as not just a provider of premier scheduling solutions, but also as the custodians of our clients' data. This understanding drives our relentless commitment to data protection and secure operations.

Leveraging the robust AWS infrastructure, we implement stringent access controls, comprehensive encryption, and advanced network security measures. Our proactive patch management strategy ensures timely upgrades, while sophisticated monitoring tools aid in early detection of potential threats.

The resilience of our service is a testament to our strategic data backup and recovery plans, alongside our effective use of load balancing and multi-region availability zones for enhanced reliability and availability. Furthermore, our efficient incident response strategy emphasizes swift detection, containment, and system recovery, minimizing the potential impact of security incidents.

In summary, our holistic approach to security makes TIMIFY a trusted partner in managing your scheduling needs. By placing data security at the core of our operations, we ensure that our commitment to safeguarding your data mirrors our commitment to your peace of mind.

www.timify.com
security-team@timify.com