Teamflect Organizational Measures

Product Security

Audit Logging

We monitor and analyze information gathered from services, internal traffic in our network, and usage of devices and terminals. We record this information in the form of event logs, audit logs, fault logs, administrator logs, and operator logs. These logs are automatically monitored and analyzed to a reasonable extent that helps us identify anomalies such as unusual activity in employees' accounts or attempts to access customer data.

Data Security

1. Secure by design

Every change and new feature is governed by a change management policy to ensure all application changes are authorized before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, cross-site scripting, and application layer DOS attacks.

2. Data isolation

Our framework logically separates customer data and prevents access to non-authorized data. Each customer's service data is logically separated from other customers' data using a set of secure protocols in the framework. This ensures that no customer's service data becomes accessible to another customer.

The service data is stored on our servers in Microsoft Azure when you use our services. Your data is owned by you, and not by Teamflect. We do not share this data with any third-party without your consent.

3. Encryption

In transit: All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers, for all connections including web access. This ensures a secure connection by allowing the authentication of both parties involved in the connection, and by encrypting data to be transferred.

We have enabled HTTP Strict Transport Security header (HSTS) to all our web connections. This tells all modern browsers to only connect to us over an encrypted connection, even if you type a URL to an insecure page at our site. Additionally, on the web we flag all our authentication cookies as secure.

At rest: Sensitive customer data at rest is encrypted using 256-bit Advanced Encryption Standard (AES). We provide additional layers of security by encrypting the data encryption keys using master keys. The master keys and data encryption keys are stored using Azure Key-vault service.

4. Data retention and disposal

We hold the data in your account as long as you choose to use Teamflect Services. Once you terminate your Teamflect user account, your data will get deleted in 3 months. The data deleted from the active database will be deleted from backups after 1 month.

Integrations

Teamflect supports integrations with:

Microsoft Active Directory

Microsoft Teams

Microsoft Graph

Microsoft 365

Multi-Factor Authentication

As Teamflect only allows sign-ins through Microsoft authentication, organizations may enable MFA through their Microsoft 365 settings.

Product Architecture

Our product architecture at Teamflect is designed with a similar approach to Azure Geo-distributed applications. Just like Azure's Geo-distributed app architecture, our product is designed to operate across multiple geographic regions, with distributed components and services that are strategically located to provide optimal performance, resilience, and fault tolerance. This architecture allows us to deliver a scalable and reliable solution that can withstand failures in individual regions, ensure high availability, and provide low-latency access to our services for users around the world. Similar to Azure's geo-redundant approach, our product architecture includes redundant components and services deployed in multiple regions, with data replication and synchronization mechanisms in place to ensure data consistency and integrity. This enables us to provide a robust and resilient product infrastructure that can handle high traffic loads, maintain data integrity, and deliver a seamless user experience, even in the face of regional failures or disruptions.

Role-Based Access Control

Teamflect users can be assigned one of four roles:

User

Administrator

Configuration editor

Report reader

Scoped administrator

Service-Level Agreement

At Teamflect, we are committed to delivering a reliable and high-performance product to our customers. As part of our service level agreement (SLA), we provide a 99% uptime guarantee. This means that our customers can expect our product to be available and operational for at least 99% of the time, ensuring minimal disruptions and downtime.

SSO Support

At Teamflect, we have implemented Single Sign-On (SSO) as our authentication method both internally for our team members and for our customer logins. SSO allows us to provide a seamless and secure authentication experience for both our internal users and customers, eliminating the need for separate login credentials for different applications and services. We use Azure AD to manage authentication and authorization for all our user accounts, whether it's for our internal team members or our customers accessing our services. This ensures that our authentication process is consistent, secure, and user-friendly across all our systems, helping to protect sensitive information and mitigate potential security risks. By leveraging SSO, we simplify access management, enhance security, and provide a smooth user experience for both our internal team and our valued customers.

Data Security

Access Monitoring

We employ technical access controls and internal policies to prohibit employees from arbitrarily accessing user data. We adhere to the principles of least privilege and role-based permissions to minimize the risk of data exposure.

Access to production environments is maintained by a central directory (Azure AD) and authenticated using a combination of strong passwords and multi-factor authentication. Additionally, we log all the operations and audit them periodically.

Backups Enabled

We run full backups of our databases every day. Backup data in the DC is stored in the same location and encrypted using the AES-256 bit algorithm. All backed-up data are retained for a period of six months. If a customer requests for data recovery within the retention period, we will restore their data and provide secure access to it. The timeline for data restoration depends on the size of the data and the complexity involved.

To ensure the safety of the backed-up data, Microsoft use a redundant array of independent disks (RAID) in the backup servers. All backups are scheduled and tracked regularly. In case of a failure, a re- run is initiated and is fixed immediately.

Data Erasure

We hold the data in your account as long as you choose to use Teamflect Services. Once you terminate your Teamflect user account, your data will get deleted in 3 months. The data deleted from the active database will be deleted from backups after 1 month.

Encryption-at-rest

Sensitive customer data at rest is encrypted using 256-bit Advanced Encryption Standard (AES). We provide additional layers of security by encrypting the data encryption keys using master keys. The master keys and data encryption keys are stored using Azure Key-vault service.

Encryption-in-transit

All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers, for all connections including web access. This ensures a secure connection by allowing the authentication of both parties involved in the connection, and by encrypting data to be transferred.

We have enabled HTTP Strict Transport Security header (HSTS) to all our web connections. This tells all modern browsers to only connect to us over an encrypted connection, even if you type a URL to an insecure page at our site. Additionally, on the web we flag all our authentication cookies as secure.

Physical Security

All Teamflect employees work remotely, hence Teamflect does not have office buildings since March 2021.

Teamflect uses Microsoft's Azure Datacenter, and these datacenters are secured and monitored by Microsoft in terms of physical security. Microsoft Azure employs a multi-layered physical security strategy to safeguard its data centers and, by extension, the data stored within. This strategy includes:

Physical Access Control: Access to Azure data centers is tightly regulated through biometric scans, motion sensors, and video surveillance, ensuring only authorized personnel can enter.

Surveillance and Detection: Continuous monitoring via video surveillance, intrusion detection systems, and environmental sensors protect against unauthorized access and environmental hazards.

Environmental Controls: Azure data centers feature climate control, fire suppression systems, and power backups to mitigate risks from environmental threats and ensure uninterrupted service.

Infrastructure Security Design: The physical infrastructure of data centers is designed to be resilient against physical threats through strategic location choices, physical barriers, and secure loading zones.

Compliance and Certifications: Azure's physical security measures are regularly audited and certified against international standards like ISO 27001, SOC 1 and 2, and PCI DSS, demonstrating a strong commitment to data protection and privacy.

These components together form the backbone of Azure's physical security framework, aimed at protecting customer data against a wide range of physical threats and ensuring compliance with global standards.

App Security

Bot Detection

At Teamflect, we take proactive measures to safeguard our application from malicious bots, and one of the tools we rely on is Azure Front Door. Azure Front Door is a cloud-based service that acts as a global entry point and security layer for our application, enabling us to optimize and secure traffic to our web applications and APIs.

Furthermore, Azure Front Door is integrated with other Azure services, such as Azure Web Application Firewall (WAF) and Azure Content Delivery Network (CDN), which further enhance our application's security posture. Together, these features help us in effectively mitigating bot attacks, ensuring the availability and reliability of our application, and protecting our users' data.

Code Analysis

Every change and new feature is governed by a change management policy to ensure all application changes are authorized before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, cross-site scripting, and application layer DOS attacks.

Credential Management

At Teamflect, we prioritize the secure management of cryptographic keys, which is why we leverage Azure Key Vault as a best practice. Instead of hardcoding keys directly in our code, we utilize Azure Key Vault as a secure key management solution. This allows us to store and manage cryptographic keys, certificates, and secrets in a central, cloud-based vault, with robust access controls and auditing features.

Azure Key Vault provides us with multiple layers of security, including encryption at rest and in transit, hardware security modules (HSMs) for key storage, and integration with Azure Active Directory for authentication and authorization. This ensures that our keys are protected from unauthorized access, and enables us to follow the principle of separation of duties, where different roles have limited access to specific keys or secrets based on their permissions.

By using Azure Key Vault, we can easily manage and rotate our cryptographic keys without having to modify our application code. This helps us in maintaining a more secure and compliant software environment, as we can effectively manage and monitor access to our keys, track key usage, and generate audit logs for compliance and regulatory requirements.

Additionally, leveraging Azure Key Vault reduces the risk of accidental exposure or leakage of keys through code repositories or backups, as the keys are securely stored in a dedicated key vault and not hardcoded in our code. This strengthens our overall security posture and helps us meet our commitment to protecting sensitive data and ensuring the confidentiality and integrity of our software and services.

Secure Development Training

At Teamflect, we prioritize the security of our SaaS platform through rigorous Secure Development Testing practices. Our security experts use techniques such as SAST, IAST, code review, threat modeling, secure configuration review, and code analysis to identify and mitigate vulnerabilities. We conduct thorough scans, manual code reviews, and configuration checks to ensure compliance with secure coding practices. Our Secure Development Testing process is an integral part of our software development lifecycle, allowing us to proactively address security issues early on. We are committed to providing a secure and reliable SaaS platform, and our ongoing efforts in Secure Development Testing help us achieve that goal.

Software Development Lifecycle

Every change and new feature is governed by a change management policy to ensure all application changes are authorized before implementation into production. Our Software Development Life Cycle

(SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, cross-site scripting, and application layer DOS attacks.

Vulnerability & Patch Management

We have a dedicated vulnerability management process that actively scans for security threats using a combination of certified third-party scanning tools and in-house tools, and with automated and manual penetration testing efforts. Furthermore, our security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to spot security incidents that might affect the company's infrastructure.

Once we identify a vulnerability requiring remediation, it is logged, prioritized according to the severity, and assigned to an engineer. We further identify the associated risks and track the vulnerability until it is closed by either patching the vulnerable systems or applying relevant controls.

Web Application Firewall

Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We use firewalls to prevent our network from unauthorized access and undesirable traffic. Our systems are segmented into separate networks to protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting Teamflect's production infrastructure. All crucial parameters are continuously monitored using our proprietary tool and notifications are triggered in any instance of abnormal or suspicious activities in our production environment.

Access Control

Data Access

At Teamflect, we have implemented comprehensive access management practices to ensure the security and integrity of our systems and data. These practices include assigning permissions to users based on predefined roles that are determined by their managers. This helps ensure that users only have access to the resources they need to perform their job functions and minimizes the risk of unauthorized access.

We also adhere to the principle of least privilege, which means that we only grant users permissions that are absolutely necessary for their job responsibilities, and avoid giving them excessive or admin-level access. This minimizes the potential impact of a security breach and reduces the attack surface.

To maintain ongoing security, we conduct quarterly reviews of permissions for critical services to identify any excessive or outdated permissions that may have been granted over time. This allows us to promptly revoke unnecessary permissions and keep access privileges up-to-date.

As part of our access management strategy, we utilize Azure AD, a robust identity and access management solution, to manage user authentication and authorization. This allows us to leverage pre-existing groups and security features provided by Azure AD to grant access in a secure and efficient manner.

By implementing these access management practices, we strive to maintain a strong security posture and safeguard our systems and data against unauthorized access and potential security threats.

Logging

At Teamflect, we rely on Azure Log Analytics for managing our application logs and internal logs. Azure Log Analytics is a powerful cloud-based logging and monitoring service provided by Microsoft that allows us to collect, analyze, and query logs generated by our applications and systems.

Password Security

At Teamflect, we leverage Azure AD to effectively manage the complexity of our passwords. Azure AD provides robust password policies and security features that enable us to enforce strong password requirements, such as minimum length, complexity, and expiration. This helps ensure that user passwords are secure and not easily guessable, reducing the risk of unauthorized access due to weak passwords.

Furthermore, Azure AD offers additional security features, such as multi-factor authentication (MFA), which adds an extra layer of protection to user accounts by requiring additional verification beyond just a password. This enhances the overall security of our authentication process and helps safeguard against password-related attacks, such as brute-force attacks or credential stuffing.

Infrastructure

Status Monitoring

At Teamflect, we leverage the comprehensive monitoring services provided by Microsoft Azure. Azure offers a wide range of monitoring and observability tools that allow us to gain deep insights into the performance, availability, and security of our applications and infrastructure. We utilize Azure Monitor, Azure Log Analytics, and Azure Application Insights, among others, to monitor various aspects of our applications, including system metrics, logs, traces, and application performance data. These monitoring services enable us to proactively detect and diagnose issues, set up alerts, and gain visibility into the health and performance of our systems. By leveraging Azure monitoring services, we can ensure the reliability and availability of our applications and promptly address an

Anti-DDoS

At Teamflect, we rely on Azure Front Door as a crucial component of our DDoS (Distributed Denial of Service) protection strategy. Azure Front Door provides us with a powerful and scalable solution to mitigate and prevent DDoS attacks, ensuring that our applications and systems are safeguarded against malicious traffic and potential disruptions. With Azure Front Door, we can leverage its advanced features, such as intelligent threat detection and filtering, to proactively detect and block malicious traffic, minimizing the risk of DDoS attacks impacting our services. This helps us ensure the availability, performance, and reliability of our applications, providing a secure and seamless experience to our customers and users.

Azure

Teamflect infrastructure is fully hosted on Azure

BC/DR

At Teamflect, we rely on Azure as our trusted solution for managing Disaster Recovery (DR) and geo-redundancy. Azure provides us with robust and scalable tools that allow us to implement effective DR strategies, ensuring the resilience and availability of our critical applications and data. With Azure, we can replicate and store our data across multiple geographical regions, ensuring geo-redundancy and data durability. In the event of a disaster or system failure, we can quickly failover to the replicated data and maintain business continuity. Azure's comprehensive DR features and global presence enable us to implement a reliable and secure DR plan, minimizing downtime and ensuring our services are always available to our customers and users.

Separate Production Environment

At Teamflect, our developers adhere to best practices by utilizing test data during the development and debugging phases of our software development process. Test data is an essential component of our testing strategy, allowing our developers to thoroughly test the functionality, performance, and security of our applications. By incorporating carefully crafted test data, our developers can simulate real-world scenarios and validate the correctness of their code, identifying and resolving issues early in the development cycle. This helps us ensure that our software is reliable, secure, and free from potential bugs or vulnerabilities before it is released into production. Our commitment to utilizing test data during development and debugging reflects our dedication to delivering high-quality and robust software solutions to our customers and users.

Network Security

Data Loss Prevention

At Teamflect, we rely on Microsoft 365 as our Data Loss Prevention (DLP) solution. Microsoft 365 offers a comprehensive suite of security and compliance tools that help us protect sensitive data and prevent data breaches. With Microsoft 365 DLP, we can create and enforce policies to automatically identify, monitor, and protect sensitive information across various Microsoft 365 services, such as Microsoft Office, Outlook, SharePoint, and OneDrive. We can configure rules and actions based on predefined or custom classifiers to detect and prevent the unauthorized sharing or leakage of sensitive data. Microsoft 365 DLP also provides reporting and auditing capabilities, allowing us to monitor and track data protection activities in real-time. By utilizing Microsoft 365 as our DLP solution, we can ensure the confidentiality and integrity of our data and comply with relevant data protection regulations.

Firewall

As a fully remote organization, Teamflect does not have physical offices, and as such, we do not rely on traditional firewalls as a part of our security infrastructure. Instead, we employ robust security measures to protect our digital assets and ensure the confidentiality, integrity, and availability of our systems and data. Our security strategy includes implementing strong authentication methods, utilizing virtual private networks (VPNs) and secure connections for remote access, employing encryption and multi-factor authentication for data in transit and at rest, and implementing strict access controls and permissions. Additionally, we regularly monitor and audit our systems and networks for any potential security risks or vulnerabilities and proactively address any identified issues. Our security measures are designed to mitigate risks associated with remote work and safeguard our operations and data without relying on physical firewalls typically used in traditional office environments.

Security Information and Event Management

At Teamflect, we have chosen Microsoft Azure Sentinel as our Security Information and Event Management (SIEM) solution. Azure Sentinel is a cloud-native SIEM and Security Orchestration, Automation, and Response (SOAR) platform that helps us collect, analyze, and respond to security events and threats across our cloud and on-premises environments. With Azure Sentinel, we can efficiently detect, investigate, and respond to security incidents in real-time by leveraging advanced analytics, machine learning, and automation capabilities. We can also integrate Azure Sentinel with other Microsoft cloud services, such as Azure Active Directory and Microsoft 365, to gain deeper insights into our security posture and enhance our threat detection and response capabilities. Azure Sentinel provides us with a scalable and flexible solution that enables us to proactively manage our security posture and safeguard our systems and data from potential cyber threats.

Corporate Security

Email Protection

We rely on Exchange Online Protection (EOP). EOP is a cloud-based service provided by Microsoft that helps us protect our organization's emails from spam, malware, phishing attacks, and other email-based threats.

EOP uses advanced threat intelligence and machine learning algorithms to identify and block malicious emails before they reach our users' inboxes. It scans incoming and outgoing emails for spam, viruses, and other malicious content, and applies multiple layers of filtering to detect and block different types of threats. EOP also uses real-time threat intelligence from the broader Microsoft Intelligent Security Graph to stay up-to-date with the latest threats and adapt its defenses accordingly.

EOP provides us with a variety of security features, including anti-spam and anti-malware filtering, message encryption, and data loss prevention (DLP) policies. It also includes features such as sender and recipient verification, DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance) authentication, and email quarantine for suspicious messages. These features help us in mitigating the risk of email-based attacks and ensuring that our emails are secure and trustworthy.

Furthermore, EOP is tightly integrated with other Microsoft cloud services, such as Office 365 and Microsoft Defender for Endpoint, providing us with a unified and comprehensive security ecosystem. This allows us to have a consistent and coordinated approach to email security across our organization and helps us in protecting our sensitive data, maintaining compliance with regulatory requirements, and safeguarding our email communications from potential threats.

Employee Training

At Teamflect, we prioritize ongoing security awareness and training. We conduct quarterly security trainings, provide specialized training to new joiners, and conduct attack simulations to identify vulnerabilities. These measures help us create a security-conscious culture among our team members and empower them to recognize and respond to security incidents effectively. By continuously improving our team's security knowledge and skills, we are better positioned to defend against potential threats and protect our systems, data, and users from potential attacks.

HR Security

As part of our robust security measures at Teamflect, we require background checks, non-disclosure agreements, and policy acceptance for any employee who will have access to customer data. Background checks are conducted to ensure that our team members meet our strict security standards and do not pose any potential risks. Additionally, we require all employees with access to customer data to sign non-disclosure agreements (NDAs) to legally bind them to maintain confidentiality and protect sensitive information. Furthermore, employees are required to accept and adhere to our comprehensive security policies, ensuring that they understand and comply with our security protocols at all times. These measures help us maintain a high level of security and trust in handling customer data.

Internal SSO

At Teamflect, we utilize Azure Active Directory (Azure AD) as our internal Single Sign-On (SSO) solution to minimize cyber attack risks. Azure AD provides us with a secure and centralized way to manage access to our applications and systems, reducing the potential attack surface and mitigating the risk of unauthorized access. With Azure AD, we can enforce strong authentication measures, implement multi-factor authentication (MFA), and monitor and manage user access effectively. This helps us enhance our overall security posture and safeguard against potential cyber threats.

Penetration Testing

As part of our proactive security measures, Teamflect conducts penetration tests with reputable security consultancy companies every six months. These tests involve controlled and authorized attempts to exploit vulnerabilities in our systems and applications, identifying potential weaknesses before they can be exploited by malicious actors. By conducting regular penetration tests, we are able to proactively identify and remediate vulnerabilities, strengthen our security posture, and ensure that our systems and applications are resilient against potential cyber threats. This helps us maintain a robust and secure environment for our customers and users.