teamflect

Data Security at the Core:

TEAMFLECT'S SECURITY ASSURANCE

teamflect

Content

Overview

Welcome to Teamflect's Trust Center, where data privacy and security are paramount. We're dedicated to safeguarding your data and ensuring a strong security posture. This portal offers insights into our proactive security measures

99%
Satisfaction

47K
Monthly **Active** users

100%
Secure Data

teamflect

Teamflect is trusted by 1000+ forward-thinking organizations

Schréder
Experts in lightability™

espyr®

RIMAC

AMWINS™

DSM

isabel group

Product Security

teamflect

- Audit Logging
- Data Security
- Integrations
- Multi-Factor Authentication
- Product Architecture
- Role-Based Access Control
- Service-Level Agreement
- SSO Support

Product Security

Audit Logging

- Detailed audit logs.
  - ❑ Event records
  - ❑ Audit trails
  - ❑ System logs
- Continuous monitoring and analysis.
- Detect and respond to unusual activities.
- Safeguard your sensitive data.

Product Security

Data Security

- **Secure Design**:
  - Authorized changes via change management.
  - Adherence to secure coding.
  - OWASP-based security framework.
- **Data Isolation**:
  - Customer data separation.
  - Strict access protocols.
  - Data ownership assurance.
- **Encryption**:
  - TLS for data in transit.
  - HSTS for web security.
  - 256-bit AES encryption at rest.
  - Master keys in Azure Key Vault.
- **Data Handling**:
  - Data retained while using Teamflect.
  - Deletion after account termination.

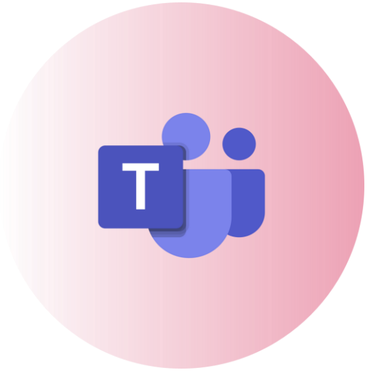
Product Security

teamflect

Integrations

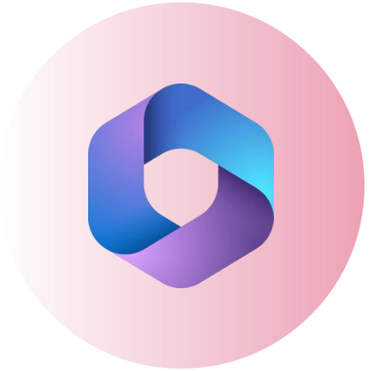
Teamflect supports integrations with:

Microsoft Active Directory



Microsoft Teams

Microsoft Graph



Microsoft 365

Product Security

Multi-Factor Authentication

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

Product Security

Role-Based Access Control

teamflect

Teamflect users can be assigned one of four roles:

User

Scoped Administrator

Global Administrator

Configuration Editor

Report Reader

Product Security

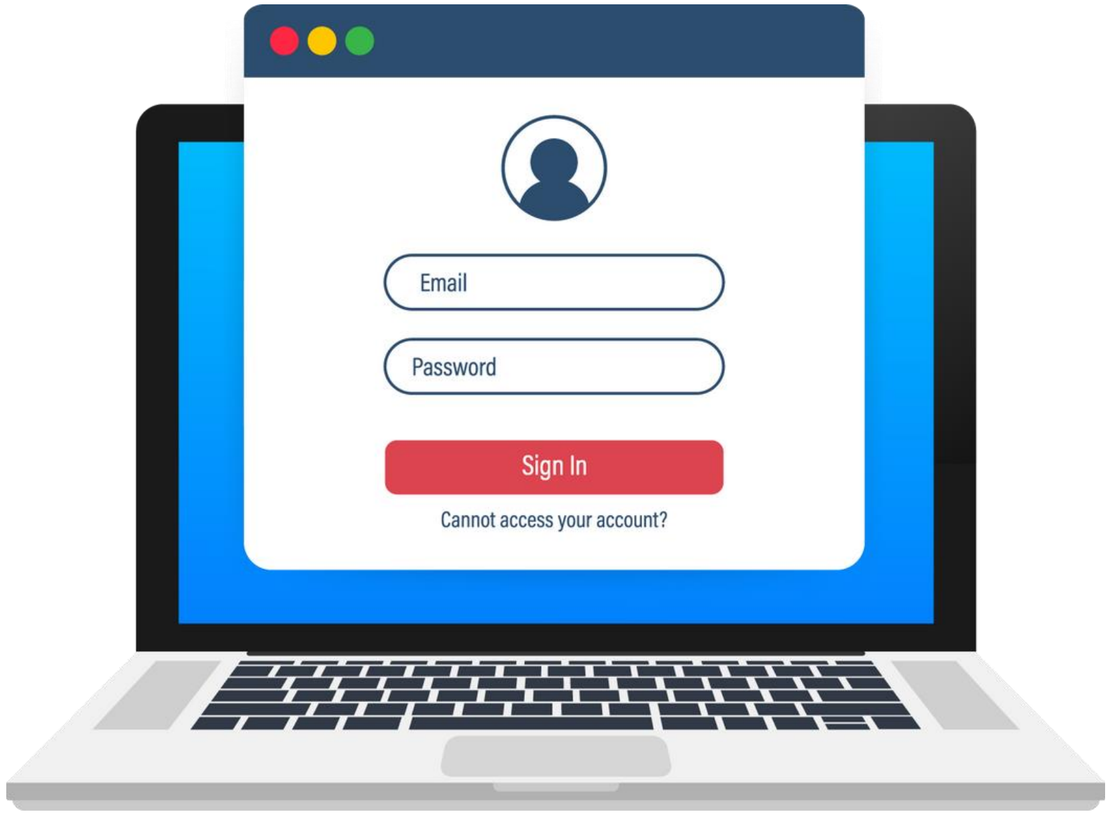
Service-Level Agreement

- Teamflect is committed to reliability.
- SLA includes a 99% uptime guarantee.
- Minimal disruptions and downtime for customers.

Product Security

SSO Support

- Teamflect employs Single Sign-On (SSO) for seamless authentication - no need for separate login credentials.
- Azure AD manages authentication for all users.
- Consistent, secure, and user-friendly experience.
- Simplifies access management and enhances security.



Data Security

teamflect

- Access Monitoring
- Backups Enabled
- Data Erasure
- Encryption-at-rest
- Encryption-in-transit
- Physical Security

Data Security

Access Monitoring

At Teamflect, we prioritize data security through stringent measures:

- Limited Access: We strictly control employee access to user data, following the principles of least privilege and role-based permissions to minimize data exposure.
- Secure Authentication: Access to production environments is managed through Azure AD, protected by robust passwords and multi-factor authentication.
- Detailed Logging: We maintain thorough logs of all operations, subjecting them to regular audits to ensure data integrity and security.

Data Security

Backups Enabled

We take data protection seriously, with these robust measures in place:

- Daily Backups: Our databases are fully backed up daily, with data encrypted using the AES-256 bit algorithm. Backed-up data is stored in the same secure location.
- Retention Policy: We retain all backup data for a period of six months. If a customer needs data recovery within this timeframe, we'll restore it securely. The restoration timeline depends on data size and complexity.
- Redundant Storage: To enhance safety, we use a redundant array of independent disks (RAID) in our backup servers, ensuring data resilience.
- Regular Monitoring: Backups are scheduled and monitored routinely. In case of a failure, we initiate a re-run to rectify the issue promptly. Your data's security is our priority.

Data Security

Data Erasure

Your data's lifecycle is managed as follows:

- Data Retention: Your data remains in your Teamflect account as long as you use our services.
- Account Termination: If you decide to terminate your Teamflect user account, your data will be deleted within 3 months.
- Backup Data: Data removed from the active database is purged from backups after 1 month. We prioritize swift and secure data removal when requested.

Data Security

Encryption-at-rest

We employ robust encryption measures for sensitive customer data at rest:

- AES-256 Encryption: Your sensitive data is safeguarded with 256-bit Advanced Encryption Standard (AES), providing a strong security layer.
- Key Encryption: To enhance security, data encryption keys are themselves encrypted using master keys.
- Secure Storage: Both master keys and data encryption keys are stored within Azure Key Vault service, a trusted and secure environment.

Data Security

Encryption-in-transit

We take data protection during transmission seriously:

- Robust Encryption: All customer data sent over public networks is safeguarded using TLS 1.2/1.3 encryption with strong ciphers, ensuring secure and authenticated connections.
- HSTS for Web: We've enabled HTTP Strict Transport Security (HSTS) for web connections, ensuring secure connections only.
- Cookie Security: Authentication cookies are flagged as secure on the web, bolstering data protection during interactions.

Your data's safety during transmission is our priority, and we employ these measures to guarantee a secure and encrypted connection.

Data Security

Physical Security

Our physical security strategy consists of two key elements:

- Remote Workforce: Since March 2021, our entire team operates remotely, eliminating the need for physical office spaces and enhancing data security.
- Azure Datacenters: We utilize Microsoft's Azure Datacenters, which are rigorously safeguarded and monitored to guarantee the physical security of your data.

App Security

teamflect

- Bot Detection
- Code Analysis
- Credential Management
- Secure Development Training
- Software Development Lifecycle
- Vulnerability & Patch Management
- Web Application Firewall

App Security

Bot Detection

We employ Azure Front Door, a cloud-based service, as a global security layer for our application. It optimizes and secures traffic to our web applications and APIs while seamlessly integrating with Azure Web Application Firewall (WAF) and Azure Content Delivery Network (CDN). This combination effectively safeguards against bot attacks, ensuring continuous application availability and data protection.

App Security

Code Analysis

- Change Management Policy: Every code change and new feature requires authorization before production deployment.
- SDLC Security: Adherence to secure coding guidelines, including vulnerability scanning and manual reviews.
- OWASP-Aligned Framework: Application layer security framework to mitigate threats like SQL injection, cross-site scripting, and application layer DOS attacks.

App Security

Credential Management

- Azure Key Vault Integration: We prioritize secure cryptographic key management and integrate Azure Key Vault as a best practice.
- Centralized Vault: Azure Key Vault allows centralized storage and management of cryptographic keys, certificates, and secrets in a secure cloud-based vault.
- Robust Security Layers: Azure Key Vault provides encryption at rest and in transit, utilizes hardware security modules (HSMs) for key storage, and integrates with Azure Active Directory for authentication and authorization.
- Access Control: Different roles have limited access to specific keys or secrets based on permissions, following the principle of separation of duties.

App Security

Credential Management

- Key Rotation: Effortless key management and rotation without code modification, enhancing software security and compliance.
- Access Monitoring: Enables effective access management, usage tracking, and audit log generation for compliance and regulatory requirements.
- Reduced Risk: Minimizes the risk of accidental key exposure or leakage, as keys are securely stored in Azure Key Vault and not hardcoded in code.
- Overall Security: Strengthens our security posture, ensuring data protection, confidentiality, and software integrity.

App Security

Secure Development Training

- Rigorous Security: We prioritize platform security through thorough Secure Development Testing practices.
- Expert-Led: Security experts employ techniques like SAST, IAST, code review, and threat modeling to identify and mitigate vulnerabilities.
- Compliance Assurance: Comprehensive scans and manual code reviews ensure adherence to secure coding practices.
- Integrated Process: Secure Development Testing is seamlessly part of our software development lifecycle, enabling early security issue resolution.
- Commitment to Security: Our ongoing Secure Development Testing underscores our commitment to a secure and reliable platform.

teamflect

App Security

Software Development Lifecycle

- Change Authorization: All changes and features require prior authorization for production.
- Secure Coding Guidelines: Adherence to secure coding standards is mandatory.
- Vulnerability Screening: Code changes undergo comprehensive vulnerability scans for potential security issues.
- Manual Reviews: Additional manual reviews enhance code security.
- OWASP-Aligned Security: Our security framework, following OWASP standards at the application layer, protects against SQL injection, cross-site scripting, and application layer DOS attacks.

App Security

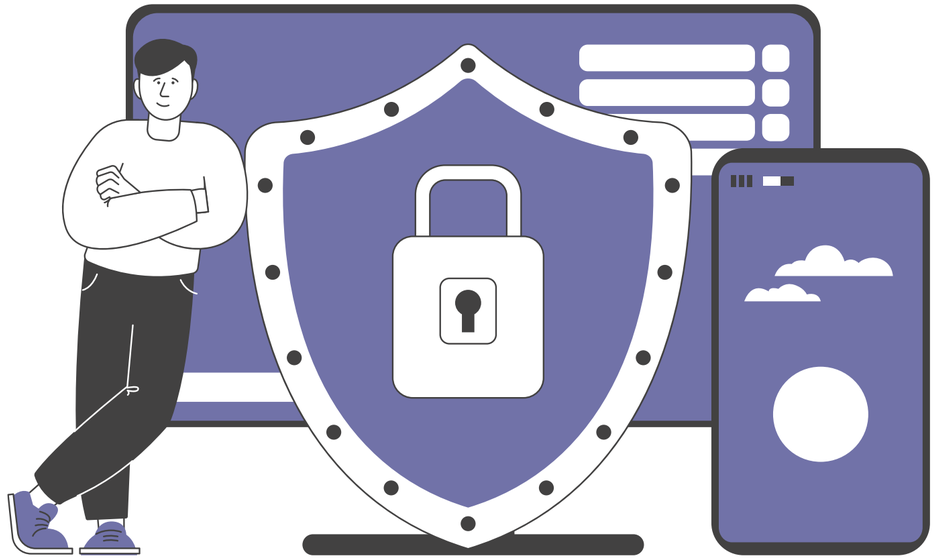
Vulnerability & Patch Management

- Proactive Scanning: We employ certified third-party and in-house scanning tools, along with automated and manual penetration testing, to actively identify security threats.
- Continuous Monitoring: Our security team vigilantly reviews inbound security reports, monitors public sources, and keeps an eye on potential security incidents that could impact our infrastructure.
- Rigorous Process: Vulnerabilities are logged, prioritized based on severity, and assigned to engineers for resolution.
- Risk Assessment: Associated risks are identified, and we diligently track vulnerabilities until they are mitigated, either through patching or the application of relevant controls.

App Security

Web Application Firewall

- Multi-Layered Protection: Our network security employs multiple layers of defense. We utilize firewalls to block unauthorized access and unwanted traffic.
- Network Segmentation: We segregate systems into distinct networks to safeguard sensitive data. Systems for testing and development are isolated from those supporting our production infrastructure.
- Continuous Monitoring: Key parameters are under constant surveillance through our proprietary tool. Any unusual or suspicious activity in our production environment triggers immediate notifications, allowing rapid response to potential threats.



Access Control

teamflect

- Data Access
- Logging
- Password Security

Access Control

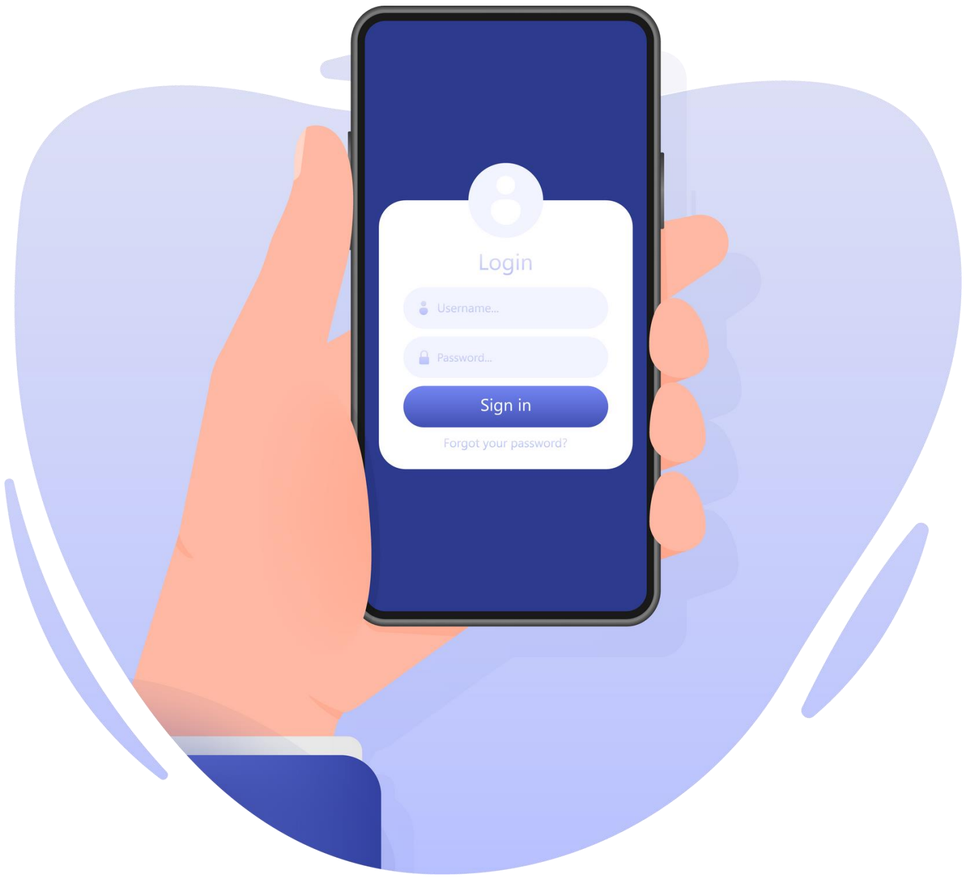
Data Access

- Role-Based Permissions: Users are assigned permissions based on predefined roles set by managers, ensuring resource access aligns with job functions.
- Least Privilege: We strictly grant necessary permissions to reduce the potential impact of a security breach.
- Regular Reviews: Quarterly assessments identify and revoke outdated permissions for up-to-date access privileges.
- Azure AD Integration: We leverage Azure AD for secure and efficient access management.
- Enhanced Security: These practices fortify our security, safeguarding our systems and data against unauthorized access and potential threats.

Access Control

Logging

- Azure Log Analytics: We utilize Microsoft's Azure Log Analytics, a cloud-based logging and monitoring service, to manage our application and internal logs.
- Powerful Logging Service: Azure Log Analytics enables the collection, analysis, and querying of logs generated by our applications and systems, providing robust logging capabilities.



Access Control

Password Security

- Robust Password Policies: Azure AD enforces strong password requirements to prevent weak passwords and enhance security.
- Multi-Factor Authentication (MFA): MFA adds extra protection, strengthening authentication security against password-related attacks.

Infrastructure

- Status Monitoring
- Anti-DDoS
- Azure
- BC/DR
- Separate Production Environment

Infrastructure

Status Monitoring

- Comprehensive Azure Tools: We use Microsoft Azure's powerful monitoring tools to gain insights into performance, availability, and security.
- Monitoring Services: Azure Monitor, Log Analytics, and Application Insights track system metrics, logs, traces, and app performance.
- Proactive Detection: These tools proactively identify issues, set alerts, and offer visibility into system health.
- Reliability Assurance: Leveraging Azure monitoring ensures app reliability, availability, and rapid issue resolution.

Infrastructure

Anti-DDoS

- Crucial Defense: Azure Front Door is our shield against DDoS attacks.
- Powerful Safeguard: It provides robust, scalable DDoS protection, ensuring our systems run smoothly.
- Smart Threat Detection: With intelligent threat detection and filtering, we proactively block malicious traffic.
- Reliable Experience: Azure Front Door ensures application availability, performance, and a secure user experience.

Infrastructure

BC/DR

- Reliable Azure Solution: We rely on Azure for Disaster Recovery (DR) and geo-redundancy.
- Effective DR Strategies: Azure provides scalable tools to ensure application and data availability.
- Geo-Redundancy: Data replication across regions for resilience and durability.
- Swift Continuity: Quick failover to replicated data in disasters.
- Comprehensive Plan: Azure's global presence and features ensure minimal downtime, offering uninterrupted services to customers and users.

Infrastructure

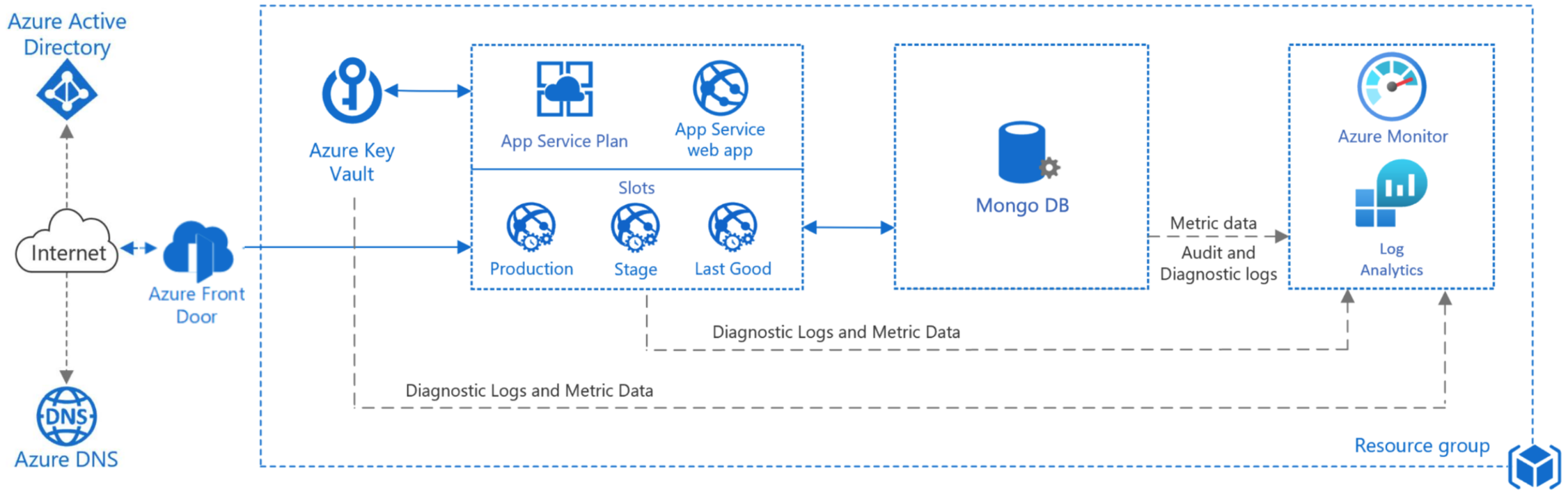
Product Architecture

Our architecture mirrors Azure's Geo-distributed approach.

- Distributed components for performance and resilience.
- Ensures fault tolerance and high availability.
- Low-latency access for global users.
- Data replication for consistency and integrity.
- Handles high traffic and disruptions seamlessly.

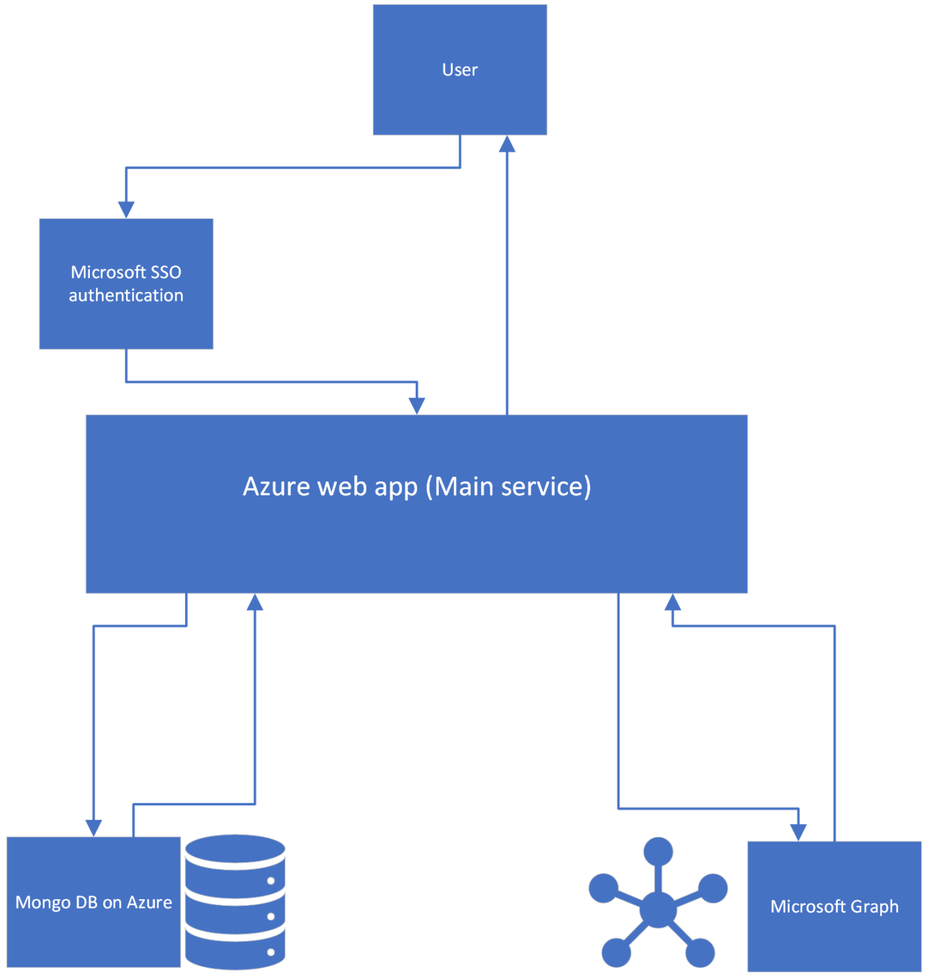
Infrastructure

Teamflect App Architecture



Infrastructure

Main Data Flow



Infrastructure

teamflect

Separate Production Environment

Testing Strategy

We follow best practices by using test data during development and debugging.

Thorough Testing

Test data is crucial for testing functionality, performance, and security.

Real-World Scenarios

Carefully crafted test data helps simulate real-world scenarios, ensuring code correctness and early issue resolution.

Reliability and Security

This commitment to test data reflects our dedication to delivering high-quality and secure software to our customers and users.

Network Security

teamflect

- Data Loss Prevention
- Firewall
- Security Information and Event Management

Network Security

Data Loss Prevention

- Comprehensive Security: We rely on Microsoft 365 for Data Loss Prevention (DLP).
- Policy Enforcement: Automatic identification and protection of sensitive data across Microsoft 365 services.
- Custom Rules: Configurable rules and actions for preventing unauthorized data sharing.
- Real-time Monitoring: Microsoft 365 DLP offers real-time monitoring and reporting.
- Data Confidentiality: Ensuring data confidentiality and compliance with relevant regulations.

Network Security

Firewall

- No Physical Offices: Teamflect operates remotely.
- Robust Digital Security: We prioritize digital asset protection, data integrity, and availability.
- Key Measures: Strong authentication, VPNs, encryption, and strict access controls.
- Continuous Monitoring: We regularly audit and monitor for potential security risks.
- Remote Risk Mitigation: Safeguarding remote operations without traditional physical firewalls.

Network Security

Security Information and Event Management

At Teamflect, our proactive security management relies on Microsoft Azure Sentinel, a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform.

- Effective Incident Response
  - Real-time security incident detection and response.
  - Utilizes advanced analytics, machine learning, and automation for efficient handling.
- Integration with Microsoft Cloud Services
  - Seamless integration with Azure Active Directory and Microsoft 365.
  - Enhances threat detection and response capabilities.
- Scalable and Flexible
  - Provides scalability to manage security posture.
  - Safeguards systems and data from cyber threats.

Azure Sentinel

Corporate Security

teamflect

- Email Protection
- Employee Training
- HR Security
- Internal SSO
- Penetration Testing

Corporate Security

Email Protection

- Cloud-Based Security: EOP by Microsoft safeguards emails from spam, malware, and phishing using advanced threat detection.
- Real-Time Protection: Utilizes threat intelligence and machine learning to identify and block malicious emails in real-time.
- Comprehensive Filtering: Scans emails for various threats, applying multiple layers of filtering.
- Integrated Security: EOP is integrated with Microsoft's cloud services, ensuring consistent and comprehensive email protection.

Corporate Security

teamflect

Employee Training

Our commitment to security includes:

01 Quarterly Security Training

Every three months, our team members receive essential security training.

02 Specialized Training

New team members get specialized training for secure onboarding.

03 Attack Simulations

We regularly conduct attack simulations to identify vulnerabilities and ensure our team is security-aware.

Corporate Security

HR Security

To bolster security, we:

Conduct Background Checks: Ensuring our team meets stringent security standards.
Implement NDAs: Legal agreements to uphold data confidentiality.
Enforce Security Policies: Employee acceptance and adherence to comprehensive security protocols.

Corporate Security

Internal SSO

- Azure Active Directory (Azure AD): Our centralized SSO solution.
- Enhanced Security: Strong authentication, MFA, and access monitoring.
- Reduced Attack Surface: Minimizing unauthorized access risks.

By using Azure AD, we bolster our security and efficiently manage user access.

Corporate Security

Penetration Testing

- Proactive Security: Regular tests every six months.
- Identifying Vulnerabilities: Controlled attempts to find system weaknesses.
- Strengthened Security: Remediation and resilience against threats.

Our regular penetration tests help us maintain a secure environment and protect our customers and users.

teamflect

Get in touch with us

- +1 323 591 8419
- info@teamflect.com
- https://teamflect.com