Infrastructure Services

As a Microsoft Teams App, SalesTim relies on several “first-party” components and services such as the Microsoft Teams platform and Microsoft Azure.
In addition the SalesTim platform uses several “second-party” or “third-party” services, especially: - GitHub Enterprise is our source code repository platform and issue tracking tool. Learn more… - Intercom is our chat application for communication with our prospects and customers from our website, and users in our apps. Learn more… - As SalesTim is not in the business of storing or processing payments, all payments made to SalesTim goes through our partner, Stripe. Learn more…

Microsoft Teams

SalesTim relies on the Microsoft Teams extensibility platform to automate governance, bring business solutions and integrate LoB and CRM apps seamlessly into Microsoft Teams.
Microsoft Teams is a chat-based workspace in Office 365 that integrates with the apps and services that people use to get work done together.

Especially, SalesTim leverages the following Microsoft Teams extensibility components:

Service	Role
Embedded web experiences with Tabs	SalesTim brings 5 custom tabs to meet specific audiences expectations and requirements
Bots in Microsoft Teams	SalesTim intelligent assistant relies on the Microsot Bot Framework and is fully integrated with Microsoft Teams to bring a seamless experience across devices, desktop and mobile
Adaptive Cards	SalesTim intelligent assistant brings actionable notifications through Adaptive Cards
Microsoft Graph	Secure and cross-platform authentication with Azure AD. Cross-functional features across the whole Office 365 suite through the Microsoft Graph unified programmability model.
Messaging Extensions (Search & Share)	Search for CRM objects right from conversations
Messaging Extensions (Custom Actions)	Initiate actions from conversations
Deep links	Initiate conversation based on business processes

Microsoft Azure

The SalesTim Platform relies entirely on the Microsoft Azure platform.
Here is a summary of the key architecture components involved:

Service	Role
Azure Traffic Manager	Azure Traffic Manager is a DNS-based traffic load balancer that enables us to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. We're using it to increase application availability, improve application performance and perform service maintenance without downtime. Learn more…
Azure App Service	The SalesTim Platform is hosted as a containerized app on Linux, enabling vertical and horizontal scale-up based on application needs and reach high availability. Learn more…
Azure Application Insights	Application Insights is an extensible Application Performance Management (APM). We're using it to monitor our live production environments, gather telemetry such as performance counters, Azure diagnostics, Docker logs and diagnostic trace logs. Learn more…
Azure Cache for Redis	Azure Cache for Redis is based on the popular software Redis. It is used as a cache mechanism to improve the performance and scalability of the SalesTim Platform, especially for back-end data store access and external APIs requests. Learn more…
Azure Cosmos DB	Azure Cosmos DB is a globally distributed, multi-model database service that supports document, key-value, wide-column, and graph databases. The SalesTim Platform relies on it as the main back-end data store. Learn more…
Azure Key Vault	Microsoft Azure Key Vault is a cloud-hosted management service that allows the SalesTim Platform to encrypt keys and small secrets by using keys that are protected by hardware security modules (HSMs). The SalesTim Platform relies on it to store securely its encryption keys. Learn more…
Azure Blob Storage	Azure Blob Storage is a massively scalable object storage for unstructured data that allows the SalesTim Platform to store securely blobs contents such as images. Learn more…

Learn more about Azure Data Residency from our Data Management Practices page

GitHub

Security Measures	Description
HTTPS	All data received from and sent to GitHub is encrypted in transit.
Verified Domains	You can verify the domains controlled by your organization to confirm your organization's identity on GitHub. Organization owners are be able to verify the identity of organization members by viewing each member's email address within the verified domain.
2FA	Access to our private repository requires two-factor authentication for everyone in the SalesTim organization. Learn more...
Protected Branches	Protected branches ensure that collaborators on our repositories cannot make irrevocable changes to branches. Enabling protected branches also allows us to enable other optional checks and requirements, like required status and security checks and required reviews. Moreover, deployment to production environments requires at leats two human validation steps. Learn more...
Security Alerts	GitHub automatically tracks public vulnerabilities in packages from supported languages on MITRE's Common Vulnerabilities and Exposures (CVE) List, and use a combination of machine learning and human review to detect vulnerabilities that are not published in the CVE list.

Learn more about GitHub Security.

Intercom

Security Measures	Description
HTTPS	All data received from and sent to Intercom is encrypted in transit.
2FA	Access to our Intercom dashboard requires two-factor authentication for everyone in the SalesTim organization.Learn more...
Verified Domains	We created a whitelist of specific SalesTim domains that the Intercom Messenger can be seen on. The Intercom Messenger will only appear on these domains (it won't appear in unintended locations). Learn more...

Security Measures	Description
Identity Verification	Identity Verification helps to make sure that conversations between you and us are kept private and that one user can't impersonate another. Identity Verification works by using a server side generated HMAC (hash based message authentication code), using SHA256, implemented using the Node Crypto API. Learn more…
Cookies Policy	Learn more about Intercom cookies policy…

Learn more about Intercom Security.

Stripe

Security Measures	Description
HTTPS	All data received from and sent to Stripe is encrypted in transit.
2FA	Access to our Stripe dashboard requires two-factor authentication for everyone in the SalesTim organization.Learn more…
Platform Security	Stripe has been audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. To accomplish this, we make use of best-in-class security tools and practices to maintain a high level of security at Stripe.
Compliance	SalesTim integration with Stripe follows the Stripe Integration Security Guide.

Learn more about Stripe Security