Security FAQ

1. The general setup

How would you describe the products' security setup at high-level?

Tricent for Google Workspace and Tricent for Microsoft 365 both run as a managed Software-as-a-Service (SaaS). Each customer runs in their own isolated data environment without any data sharing between customer domains, and all customer data is stored encrypted at rest and in transit using standards-based encryption algorithms.

All customer data access keys are stored encrypted and only exposed in memory for the Tricent service when needed. All data access, user actions, and admin access to the customer's Tricent application in support scenarios are logged and kept for the duration of the service contract to fulfill compliance and regulatory requirements.

What technology frameworks, languages, platforms, stacks, etc. are used in the scope of the application/service?

Python, React JS, .NET Core, Google Cloud Platform, Microsoft Azure.

Do you use any third parties for data processing purposes?

Yes, the complete list is here.

Do you have an easy way to report security vulnerabilities in your systems?

Yes, any concerns can be submitted here.

Which best describes your web application?

The web application is only available over HTTPS.

Who do you use as your data center provider(s)?

Google Cloud Platform and Microsoft Azure

Which best practice technologies are in place in your cloud infrastructure?

Network segmentation, security groups, IAM, encryption at rest & in transit, MFA, HSM, IAP, SSH, TLS, and others.

In which data center regions are you currently deployed?

EU West & EU North.

Does your service get audited against external standards (such as ISO 27001, PCI, SOC 2 Type 2)?

We have SOC 2 Type 1 and are currently working towards Type 2 and plan to achieve a ISO 27001 attestation afterward.

Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?

We enforce separation of duties, peer reviews, and static code analysis tools, as well as weekly vulnerability scans.

Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc)?

Our service is highly available - in case of outages in critical components, a failover will happen naturally without downtime for the customer.

Do you restrict, log, and monitor access to your critical systems (e.g., firewalls, vulnerability scanners, APIs, etc.)?

Yes.

Do you have incident response in place?

Yes.

2. Passwords and access

Do your services support Single Sign-on?

Yes, on the Tricent for Google Workspace product it is provided in turn via upstream GWS authentication. On the Tricent for Microsoft 365 product we use the native Azure AD Authentication upstream.

Do your services support Multi-factor Authentication?

Yes, on the Tricent for Google Workspace product MFA is provided via upstream GWS authentication. On the Tricent for Microsoft 365 product we use native Azure AD Authentication upstream.

Do your services offer role-based access controls?

Yes. You can read more about the access setup of the individual roles here (Tricent for Google Workspace) and here (Tricent for Microsoft 365).

Can we create custom roles?

No.

Who assigns user roles in the product?

The customer creates and assigns user roles.

On Tricent for Google Workspace, a Super Admin role is created in connection with the product onboarding who can then promote other users to admin roles. Standard role is user access only.

On Tricent for Microsoft 365, the customer assigns Super Admin and Admin roles via their Azure Active Directory admin center using a Global Admin role.

Which roles in the Tricent application can access Personal Identifiable Data across the organization in Tricent?

In Tricent for Microsoft 365: Super Admins and Admins can see Team/file names, user names, and email addresses, but no file content. Team-owner/team cleanup responsible can see Team/file names, user names, and email addresses, on the teams that they are responsible for but no file content. End-users can see their own data only including a link to content via the M365 upstream platform.

In Tricent for Google Workspace: Super Admins and Admins can see file names, user names, and email addresses, but no file content. End-users can see their own data only including a link to content via the GWS upstream platform.

Read more about roles in Tricent for Google Workspace here and in Tricent for Microsoft 365 here.

Is the allocation of user accounts controlled through a formal process ensuring that all accounts are unique and that users are only granted the necessary access to perform their daily duties?

Yes, we require both unique accounts, MFA, and adhere to least-privilege access control principles.

Is a process in place to ensure access control alignment when faced with joiners and leavers situations (onboarding and offboarding cycles)?

Yes, we have a procedure in place that ensures that offboarded employees are removed from systems within 24 hours after leaving the company.

Do you periodically review employees' access to systems and align access control afterwards?

Yes, we regularly review access to our systems and align if anomalies are found.

3. Data encryption

Is data encrypted in the product?

Yes, using AES 256 on both our Google and Microsoft platforms.

Can clients encrypt data using a key from a separate key management system (KMS) to which the provider does not have access?

On our private tenant solution you can generate and store your own data access keys.

Is all data to and from the product, including user interactions, encrypted?

Yes, using up to TLS/SSL v 1.3.

Which encryption protocols/standards do you support?

Up to TLS/SSL v 1.3.

4. Backups and logs

Do you create backups of data?

Yes.

How frequently do you backup?

Daily.

How long does it take to restore backups?

Less than an hour.

Is there an audit log of authentications and authorizations?

On Tricent for Google Workspace: OAuth grant mechanism is used for authentication

towards GWS user data. All authentication and authorization is logged upstream in GWS token audit log for customer inspection offsite. In addition, we also log locally user and admin authentication - these are viewable in the web application system event logs.

On Tricent for Microsoft 365: OAuth grant mechanism is used for authentication towards M365 user data. All authentication and authorization is logged upstream in Azure token audit log for customer inspection offsite. In addition, we also log locally user and admin authentication - these are viewable in the web application system event logs.

Is there an audit log of all user activity? Who looked at what data etc.?

Yes, all data-changing actions are logged in the application event log.

Where are logs stored, and who has access to this data?

Logs are stored in each customer's private database. They are available in the web application to end users (own actions and cleanup engine actions), and super/admins (sitewide actions and cleanup engine actions).

What is your SLA for vulnerability updates in the products or underlying architecture?

Our infrastructure is patched weekly and on demand such as when a zero-day is announced.

Do you sync your (customer) data to an offsite location in real-time?

We do full data backups hourly. In the event of an incident, very little data will be subject to potential loss.

Do you store your backups on tape or other types of removable media?

No, we only use disk-to-disk transfer.

Do you have procedures in place for restoring data and general business continuity?

Yes.

Do you audit your 3rd party providers to ensure compliance with your policies and general use of best practices?

Yes, we ensure our vendors live up to the same strict demands we impose upon ourselves.

5. Privacy

Do you support Data Leak Prevention (DLP) for the detection of private data being leaked?

We do regular scans for potential data leaks.

Do you handle any Cardholder data?

No.

Do you support private data to be encrypted at rest?

Yes, metadata and personal data is encrypted in transit and at rest.

Do you support the right to be forgotten?

Yes.

Is all data stored in the EU?

Our own infrastructure runs solely in the EEA. We only use our own private keys for encrypting data, and customer data is, as such, inaccessible to any third parties.

All customer data is encrypted in transit and at rest using our own keys. We ensure our sub-processors live up to the same high data protection standards as us and for transfers to/from third countries mandate that they use EU GDPR-approved mechanisms such as SCC.

Do you seek rights to use customer-derived data for your own purposes?

No.

Is your Privacy Policy externally available?

Yes, right here.

What specific controls do you have in place to prevent unauthorized access to your employees' workstations?

Strong passwords, malware detection, mandatory screen locking, and managed software updates.

How often do you scan your systems for vulnerabilities?

Weekly and on demand.

Which operating systems do you use?

Linux, Windows, macOS, and Android.

How often do you patch your systems with security updates?

Weekly or more often depending on criticality.

Do you have your backup data stored offsite?

Yes, we use a separate cold data backup site.

Do you use unique admin accounts (no shared accounts)?

Yes, we only employ uniquely identifiable high-privilege accounts.

6. Endpoint security

Are all your endpoints that can connect to production networks managed centrally via MDM?

Yes.

Does sensitive or private customer data ever reside on user endpoints?

No.

How is this enforced?

Internal data management policy forbids this, and technical controls disallow it.

Do you have a breach detection system (such as HIDS) that includes anomaly detection and alerting capability?

Yes.

Do you harden your end-user platforms via relevant standards (such as CIS)?

Yes, we enforce configuration management via our MDM solutions.

Do you have an emergency process for evaluating and patching critical software OS and software vulnerabilities?

Yes, we do this on an ongoing basis.

Do you have a process for inventorying which systems are affected by vulnerabilities and need patching?

Yes, this is done via our MDM solutions and general config management software.

7. Firewalls/networks/zones

Does your public-facing infrastructure reside in a filtered DMZ zone separated from internal network structures?

Yes.

Do you segregate your application-carrying networks into multiple zones based on purpose and risk?

Yes.

Do you employ encryption for any network traffic that may carry sensitive information?

Yes.

Have you deployed monitoring, management, and alerting of your networks?

Yes.

8. Monitoring

Do you continuously monitor the availability of your networks and the assets in them?

Yes.

Do you centrally retain the logs produced in your networks from assets and store them for at least 6 months?

Yes.

Which companies do you use for your Infrastructure as a Service needs - if any?

Google (GCP) and Microsoft (Azure).

Do you operate any wireless networks that allow access to private parts of your infrastructure?

Only staff employees are allowed access to our private networks.

Do you have mechanisms to detect any changes in data (intentionally or accidentally)?

We use host-based IDS, which monitors in real-time for changes in infrastructure and audit logs that keep track of changes to customer settings and data. For persistent data storage, we have transaction logs.

Does the product support a High Availability configuration?

Our web architecture is load balanced and highly available. Our database architecture is highly available and distributed across data centers offering geo-diversity.

Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?

We continuously scan for vulnerabilities in our code and fix any critical issues with priority.

Do you conduct application and network penetration tests of your infrastructure at least annually?

Yes.

Have you recently reviewed your SSL configuration to ensure that only secure protocols and ciphers are offered to clients?

Yes, we regularly review the cipher suite advertised by the server and the protocols it uses.

9. Web vulnerabilities and controls

Are there any potential risk areas in your web application platforms?

The applications use a persistent database storage backend that can be queried via SQL. The applications do not support file uploads.

The applications may load active content (scripts, applets, style sheets) from external sources. The applications use cryptography to protect data and integrity.

How often do you run vulnerability scans?

At least every week.

Which strategies do you employ to avoid being vulnerable to XSS?

We use a templating system/web framework that automatically escapes all user input before displaying it back.

What is your specific strategy for protecting against any future XSS vulnerabilities?

Our web frontend is written in React which provides strategies to escape string variables in views and allows first-class functions that mitigate the need to pass strings in event handlers (which may contain malicious code).