Security, Privacy & Compliance

Security, Privacy & Compliance

11th April 2024

Version 1.2

What is SCOUT?

SCOUT is a Software-as-a-Service (SaaS) platform that provides organisations with actionable insights to maximise the value of their Microsoft 365 and Azure environments. Leveraging automatic AI-powered rules and Smart Tag capabilities, SCOUT's insights make it possible to optimise cloud financials, improve productivity and adoption, and secure identities and resources – all presented in clear, easy-to-understand dashboards to sustain your digital transformation and associated budget management.

This white paper describes SCOUT's security and compliance programme and addresses commonly asked questions about the platform from end customers and partners.

Cloud Imperatives: Cost Management and Security

Cloud computing has become an essential part of modern business operations. However, as more companies move their workloads to the cloud, they are faced with new challenges around cost management and security.

Cloud cost management is the process of monitoring and optimising your cloud spend. It involves tracking your usage and rates across cloud providers and services, identifying areas where you can reduce costs while avoiding cloud budget overruns[i], and implementing strategies to optimise your cloud spend. By continually seeking to keep cloud costs in check with FinOps practices[ii], organisations can reduce their overall cloud spend while still maintaining the performance and availability of applications.

Security is another important aspect of cloud computing. According to a 2022 report by Gartner[iii], "through 2025, 99% of cloud security failures will be the customer's fault." This highlights the importance of implementing strong security measures when moving workloads to the cloud. Cloud providers offer a range of security features and tools to help you secure your applications and data in the cloud. However, it is ultimately up to the end customer to ensure that their applications are secure – which can only be done by having full visibility across identities, endpoints, data, and resources.

To achieve this, organisations will need trustworthy cloud-native tooling, such as SCOUT, to process billing details, make sense of contract/pricing information, ingest usage data, tag to provide business relevance, enable analysis, provide optimisation recommendations, and alert on key metrics/thresholds – all with the ability to scale with them as they evolve along their digital transformation and cloud governance continuum.

In summary, by implementing effective cost management and security strategies, companies can optimise their overall cloud spend while maintaining visibility to ensure that their cloud environments are secure.

Governance and Risk Management

Our risk management-oriented Security and Compliance programme – led by our Chief Information Security Officer (CISO) who is part of the Leadership Team – aims to continuously implement industry best practices across people, processes, and technology. To ensure impartial oversight, the CISO reports to the Board on a regular basis.

As part of the programme, we leverage various policies and controls, such as in-transit and atrest data encryption, tight access controls and strong authentication,
network/infrastructure/application-layer security, and incident response across contemporary tooling. To demonstrate our transparent approach to security and privacy, we have published our Trust Centre here: https://trust.SCOUT.co. These governance measures ensure security and privacy are in practice across the breadth of our operations and software development processes.

What frameworks/standards does SCOUT have in place?

With Board support, we have set out a program to build on the current Cyber Essentials certificate and attain ISO27001:2022 certification in 2023 followed by SOC2 Type II, plus ensure alignment with the breadth of controls in the NIST Cyber Security Framework (CSF). The highlevel plan is shown in this following table:

Framework	Our Plan	Status
Cyber Essentials	Cyber Essentials Plus Q3-24	Complete – CE Certified since 2022 Pending – CE+
ISO27001:2022	Maintain	Complete – Certified September 2023
SOC2 Type II	Maintain	Complete – Certified April 2024
NIST CSF	Q1-24 onwards	In progress (60% scope achieved)

Privacy

What customer data does the SCOUT application ingest for processing?

As per the SCOUT SaaS EULA, the platform needs read-only access to a number of types and categories of personal data for processing.

In summary, they cover the following data types: identity, business contact, financial, transaction, technical, profile, usage, marketing and communication, plus aggregated data. The specific personal data types from the Azure Active Directory (AAD) user object that are required are listed on pages 55-57 in the EULA. Customer and partner passwords are not stored in the application. No sensitive or special categories of personal data is required, ingested, or processed.

How does the SCOUT application ingest customer data?

Customer data is ingested via read-only integration with Microsoft APIs. Following our SCOUT Onboarding Process, customers are guided through a very simple four-step procedure which requires Global Administrator credentials to authenticate, then authorise the cloud application registration, and finally accept the relevant EULA to finish setting up the application before signing into the user portal. This can be completed within 15 minutes and the batched data ingestion process then begins. A customer-facing onboarding document clarifies the read-only permissions being requested, and initial reports can be viewed in the application within 24 hours.

Data residency

SCOUT SaaS production runs in Azure public cloud data centres in the Germany West EU region.

What data privacy measures does SCOUT have in place?

The end customer retains ownership of their data at all times, remaining both the data owner and data controller. As SCOUT operates on a read-only basis, customer data can only be mastered at the source tenant of the customer. Appropriate organisational and technical measures are employed in tandem to ensure we process personal data securely.

We clearly define in the EULA what data is required for the service and outline how data transfers are controlled. We maintain records of processing activity and supporting procedures for data subject access rights. Policies and training are mandated for all employees and contractors on complying with data privacy and security. Data encryption is enforced when in-transit and atrest to AES standards, per-tenant data access is restricted with federated authentication against the end customer's AAD Identity Provider (IdP), and data is segregated per tenant.

Imported data can be made anonymous at the tenant-level however this limits a number of product reports and features where user-specific insights are required, for example licence optimisation recommendations. See page 30 of the EULA for details on the processing of personal data.

How is data retention managed?

Customer data is retained for as long as the account status is active and our Data Retention Policy sets a maximum of 90 days for the retention of expired account data, whereafter it will be permanently removed.

Within the SCOUT platform there are data retention settings available at the instance level via the Admin Portal. They cover monthly cost statistics and daily M365 statistics across account usage, directory audit, email usage, events, group activities, mailbox usage, OneDrive usage, sign-in log, and Teams usage. The retention periods are set to between 12-18 months as product defaults. For long-term archive purposes, these can be saved to Azure blob storage too.

How is data deleted?

The data deletion process involves a formal request initiated by a customer, partner, or account manager internally to our Customer Success team, who will purge the tenant data once the ticket has been verified and approved. Our process requires this to be completed as soon as possible, with exception approval for two 30-day extensions should commercial conversations continue. After this, the customer tenant data must be purged from the SCOUT instance, confirmed by audit log entries and closure of the ticket. The purge from the database then flows into data removal within backups, which are retained for 30 days. Once these two data removal steps are complete, customer tenant data cannot be retrieved.

What data privacy measures are in place for white-labelled partner installations?

The EULA is signed with the partner – not SCOUT – but what data and how it is ingested remains the same in white-label partner setups. The same data types are processed, but the data processor responsibility resides with the white-label partner.

The Azure data centre region/location is a decision for the partner. While the data privacy measures are the responsibility of the partner, the solution typically fits into their existing policies and processes.

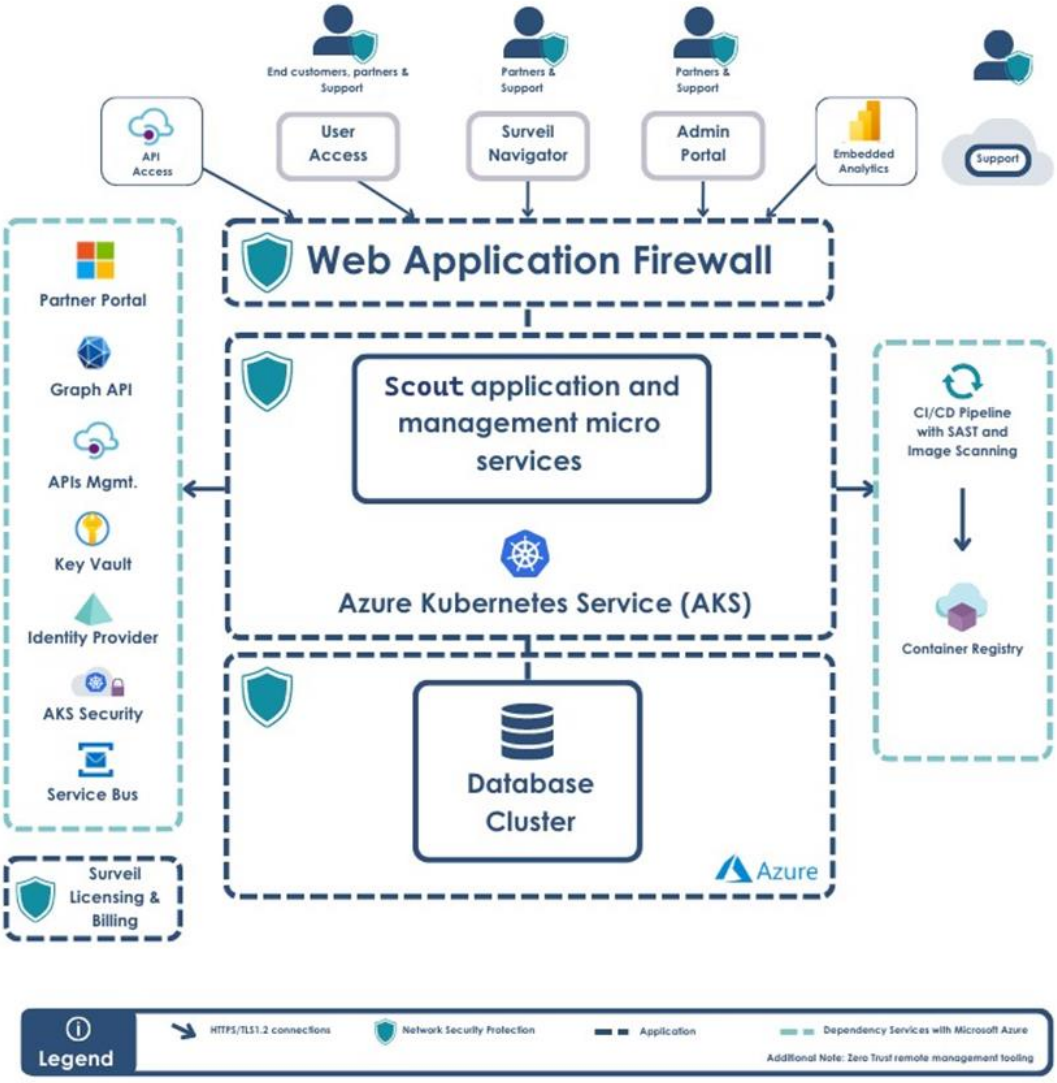
Data retention and deletion will be for the partner to decide according to their processes and policies, however the product defaults described above will apply until changed.

Architecture and Data Security

What network, infrastructure, and system security measures does SCOUT have in place?

SCOUT SaaS runs as a container-based application on the Azure Kubernetes Service (AKS) platform, with segmentation applied between running micro-services internally and externally, from the front-end web application firewall, through network security groups (NSG) and API integrations, to accessing the database layer.

SCOUT Architecture



Microsoft API integrations are exclusively read-only via REST XML, with authentication managed on an automated basis using the Azure Key Vault. We enforce privileged identity and access management for alignment with the principle of least privilege for remote management and resource access. Privileged access is reviewed on a regular basis to ensure the fewest number of staff have access. Vulnerability management is performed externally and internally, with a regular patching schedule for the non-SaaS/PaaS components we manage.

SCOUT is a 'born-in-the-cloud' business, with staff-only laptops working flexibly around the world using endpoint protection and management, disk encryption, strong authentication, and automated mandatory patching.

Additionally, staff must complete cyber and privacy awareness training which is assigned on a regular basis. Performance is monitored and tracked within our compliance automation platform for ongoing maintenance of the Information Security Management System (ISMS) for ISO27001.

How does SCOUT manage data security?

Data is encrypted in-transit using TLS1.2, and at-rest with AES. We use best-in-class database storage encryption, as well as implementing data segregation and role separation to enforce the principle of least privilege across our multi-tenant architecture.

Access is controlled via tight technical policies and strong multi-factor authentication (MFA), with row-level data masking available where required, as an advanced custom solution request. We have standard backup and data retention practices, and we proactively monitor component and system status.

How are alerts communicated?

SCOUT Alerts is a powerful feature of the platform that can alert users to financial, operational, and security changes in their Microsoft cloud. With out-of-the-box and customisable Alert Definitions, a broad range of conditions can be configured and sent via Secure SMTP.

How does the architecture and data security change with white-labelled installations?

The core SCOUT architecture does not change but the remote management, data security, and first line support ownership and responsibility is with the partner. SCOUT provides product support as the software supplier for the platform to the partner. Instance software releases are automated and take place on the first weekend of the month – partners are notified in advance for agreement to proceed. The SCOUT Licensing and Billing component is not included within white-label installations and remains a SCOUT-only back-office application.

Software

How does SCOUT secure the Software Development Lifecycle (SDLC)?

We use the agile product delivery framework, automated code review, and security assessment before entering the pipeline to Production. In our software development pipeline process, only code reviewed after successful completion of all automated security scanning and testing is permitted for production deployment, to ensure consistency across all SCOUT instances. **What are your testing processes?**

Quality and security testing is incorporated at development time with clean source code validation and static application security testing (SAST), and at the test/deployment stage with automated image scanning and policies preventing release. Once deployed, we scan for OWASP Top Ten compliance. External penetration testing security is conducted annually with specialist third-party suppliers.

How are issues or bugs reported?

SCOUT takes quality and security seriously, so we encourage the disclosure of potential bugs or vulnerabilities in our products as quickly as possible, using this Issue Submission form: https://forms.office.com/e/A4iuitW7xY

Operations

Are SCOUT application actions audited and logged?

Yes, the SCOUT platform has an audit and logging function available within the User (tenantlevel) and Admin Portals (Instance and tenant-levels for User, System and Provisioning).

The User Portal shows user management actions (e.g., add/edit/delete, licence assign, login/logout date/time/success/fail). The Admin Portal shows audit information on admin actions by Instance and per-tenant (e.g., add/edit/delete user/admin role), pricing updates, email notifications, login/logout date/time/success/fail, indexing and content refreshes, menu updates, file data exports, persona edits and assignments, repository sync, portal config exports, tenant creation/deletion, plus M365 Applications and Azure Subscriptions and their associated actions.

These audit logs are exportable but not editable and are kept for the life of the tenant or instance.

How does SCOUT manage disaster recovery?

Frequent configuration and data backups are performed and securely stored in different cloud datacentres. The team perform regular recovery verification tests to ensure data integrity and SCOUT availability to service level agreements (SLA).

What is your approach to Incident Response?

Our Security Team conduct internal exercises against various scenarios to ensure familiarity with our Incident Response Plan. The management team are included periodically to ensure familiarity with the response approach and support for communications and external notification.

Notification of security and/or data privacy incidents is required as per terms of our contracts and under a number of worldwide regulations (e.g., the General Data Privacy Regulation (GDPR) in Europe) so timely communication to affected organisations and individuals will take place.

How is disaster recovery managed in partner white-labelled installations?

Disaster recovery in white-label environments is the responsibility of the partner. Partners can choose the levels of standby and architect the SCOUT white-label setup recovery response times for their own SLAs. SCOUT support is available for service recovery should a data centre failover be required in the partner environment/service.

References

[i] Why Cloud Budgets Don't Stay in Check — And How to Make Sure Yours Do
7 Reasons Cloud Budgets Don't Stay in Check | Gartner
https://www.gartner.com/en/articles/whycloud-budgets-don-t-stay-in-check-and-how-to-make-sure-yours-do

[ii] What is FinOps? https://www.finops.org/introduction/what-is-finops/

[iii] Gartner (2021). "Gartner Top 10 Security Projects for 2021". Retrieved from https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2021/