responsiv

simple · effective · distinctive

Responsiv Cloud Security Service

RA002CN-PD

Product Description

Responsiv Cloud Security Service (RC-SS)

Responsiv Cloud Security Service (RC-SS) is used by Responsiv Cloud Platforms for authentication and authorisation services. It provides an identity provider that locally manages users, connects to external identity providers for single-sign-on, and uses federated trust associations to avoid password challenges by trusting unified credentials.

The service is attached to Responsiv Cloud Platforms. Once connected, you can access the service through the Responsiv Cloud Console to add users and manage their access. Policies can be defined to deliver role, context, attribute, and user-based security controls.

RC-SS supports multiple ways to control access to your Responsiv Cloud Platforms.

This service is pre-integrated with Responsiv Cloud Platforms and Responsiv Cloud Services. Each customer is assigned a primary identity store and additional identity stores, and user registrations may be configured as required.

This product description describes the key features, functions, and capabilities of the product or service. It is not intended to fully document the product or to provide support.

Audience

This description is for architects and technical specialists to give a high-level, brief description of the product or service. It is intended to be used to inform users of the broad functions and scope of capability. Refer to linked product documentation for details. Responsiv reserve the right to change the specification at any time and without notice.

Obligations

This document is not an offer or contract. Neither Responsiv nor you have any obligations or liability to the other unless our authorized representatives enter into a separate definitive written agreement. Terms included in this document are not binding unless they are included in such a written agreement.

Observations and recommendations in this document are based on our opinions, experience, and knowledge of the product. Responsiv makes no representation as to accuracy or fitness for purpose.

Underlying Software

This description is for a Responsiv product that is implemented using a combination of capabilities delivered by pre-existing products. References to those products and their documentation are required to improve understanding of the capabilities that are available and how to access them using the available tooling. Responsiv makes no claim that our product provides all documented features. If a feature is of particular interest, please seek clarification with Responsiv.

Developers use a low-code graphical development environment that allows them to move into Extended SQL, Java, and other languages that may be more appropriate for a particular problem, or that already exist and can be reused.

Responsiv provide and support all software embedded in this product.

Table of Contents

Service Overview

Responsiv Cloud Security Service (RC-SS) protects Responsiv Cloud Platforms and your automation, integration, business rule, and custom applications.

On the Responsiv Cloud, each Responsiv Cloud customer is assigned their own “Customer Place”.

This is a walled garden network environment that is private and secure and may span multiple physical locations. Customer places are protected by state-of-the-art firewalls, governance, and management practices. Cloud services and cloud platforms are made accessible from the customer place to simplify construction of installations that involve more than one capability.

Responsiv Cloud Platforms are deployed or attached to the customer’s place, creating a secure region of capabilities that can be connected. Responsiv Cloud Security Service is attached to each platform and to the Customer Place.

User Management

Users can be removed or added to the service by adding them to the appropriate identity store. For local users this is done through the Responsiv Cloud Console. For external identity stores use the appropriate process. User authorisations can be configured in the same way.

Additional identity stores can be added to the service to allow segregation of user categories, for example guests and external users separated from internal staff.

User Protection

The service is integrated to Responsiv Cloud Services and Responsiv Cloud Platforms to protect all direct user access. The service intercepts access requests and checks for credentials. If credentials are not appropriate, then the user is redirected to authenticate themselves.

API Protection

Trust Interceptors can be configured to protect API access to services. The service also supports standard API protective protocols, including OAuth2, OpenID, JWT.

Accessing the Service

The service is hosted in Responsiv Cloud datacentres located in the UK and accessible over the public Internet or using optional dedicated MPLS[1] connections. Refer to Cloud Service Terms and Conditions for information about hosting providers.

https://responsiv.co.uk/wp-content/uploads/2023/09/TC-RL0002O-Aug2023-Terms-and-Conditions-for-use-of-Responsiv-Cloud-v3-0.pdf

Recommendation: An optional service preparation package can be purchased to help you set up connections, share certificates for security, and mentor staff on the use of this platform (See Optional Services).

There are three points of connection to Responsiv Cloud Services.

Public Connections

Public Connections are used by customers and users that are accessing the platform from the public, untrusted, internet. Most Responsiv Cloud Platforms do not allow public access.

Responsiv Cloud Platforms may be accessed from the public internet by routing the connection through your own firewalls and intrusion detection arrangements. This ensures that we see the connection as originating from an internal network, and responsibility for its protection is with your security defences.

The only platforms that allow direct access to the public Internet is the Responsiv Cloud API Platform.

User Connections

User Connections are used by staff and others to access the platform from your internal (semi-trusted) networks. User connections are tunnelled over encrypted, mutually authenticated virtual private networks (VPN), or transport layer security (TLS) connections. These connections are explicitly allowed through our firewalls from a named set of Internet Protocol (IP) addresses.

Responsiv Cloud Security Service intercepts all user traffic. Depending on how the service is configured, the user will be challenged for a security token, then for a username and password. The username and password is checked against the identity store, which can be local to the cloud or external in your own control.

Recommendation: To reduce the management overheads of setting up new users, and the risk that they remain after the user no longer needs them, Responsiv recommends configuring external identity storage and/or federated trust.

Data Connections

Data Connections are used by systems inside your private network to connect to and from the cloud platform using specific protocols. Connections are tunnelled over encrypted, mutually authenticated virtual private networks (VPN), or transport layer security (TLS) connections. These connections are explicitly allowed through our firewalls from a named set of Internet Protocol (IP) addresses.

Administrative Connections

Administrative Connections are used by our administrators and by the Responsiv Cloud Console to allow administration of the platform, including patching and upgrades. These connections are not directly accessible to customers or from public internet connections.

Customer Place Connections

Each Responsiv Cloud customer is assigned their own "Customer Place".

This is a walled garden network environment that is private and secure and may span multiple physical locations. Customer places are protected by state-of-the-art firewalls, governance, and management practices.

Responsiv Cloud Platforms are deployed or attached to the customer's place, creating a secure region of capabilities that can be connected. Responsiv Cloud Security Service is attached to each platform and to the Customer Place.

Platforms and Services deployed to the same Customer Place can be connected or clustered to deliver reliable and available business solutions.

Platforms and Services deployed in separate customer places cannot be directly connected.

[1] See optional services

Features

Responsiv Cloud Security Service (RC-SS) supports fine-grained authorisation policies and combinations of access control mechanisms.

Attribute-based Access Control (ABAC)

Attribute-based access control (ABAC) uses information about the subject rather than predefined roles to determine authorisation. It can be used to protect data, services, and IT resources from users that don't have "approved" characteristics. Approved characteristics are defined in a security policy. For example, read access given to a user in department IT Admin, accessing from a listed mobile device, and accessing a resource designated as owned by IT Admin. The rule is assigned permissions.

Role-based Access Control (RBAC)

Role-based access control (RBAC) uses predesignated roles to determine access to resources. For example, a user is placed into the IT Admin (Read Only) or IT Admin (Read-Write) group in the identity store. Multiple users are simply added to the appropriate groups to give them access. The group is assigned permissions.

User-based Access Control (UBAC)

User-based access control (UBAC) assigns permissions to individual users. While it is better to manage users' permissions in the other available ways, this is a foundational element of the solution and allows single users to be assigned specific permissions.

Context and Time-based Access Control (CBAC)

Users with the right role, user, or attribute security can be further restricted by the context. This means that a user with permission is only allowed to enter during working hours and from a company location or using a company device.

Authorisation Policies

Centralised Resource, Permission, and Policy Management using user interfaces accessible from the Responsiv Cloud Console, including the ability to simulate authorisation requests to test policies.

Identity Store Configuration

Responsiv provide an identity store to be used to control access to services hosted in your customer place. The identity store can be used to define local users and/or roles, and to federate with an existing identity store. Identity Stores are private to each customer with no access allowed directly between them.

Optional Services

Optional services are available to extend the capabilities or capacity of Responsiv Cloud Platforms and other products.

RT00094 Responsiv Assist Flex Support

Use flex support credits to prepare the service for use by new customers to (1) securely connect to Responsiv Cloud, and to get started with the Responsiv Cloud Service, or (2) to establish a managed service.

RA002DO Responsiv Cloud Security Identity Store Expansion

Additional identity stores can be used to separate groups of users, for example customers, suppliers, and staff. The identity store includes an entitlement for a maximum number of registered users. Additional expansions can be used to add users to an existing store or to create a new store.

RA001RD, RA001SE Responsiv Cloud Connection Service

Create private, dedicated network connections between your systems and the Responsiv Cloud. Improve security, reliability, and performance. Remove the need for VPN and reduce the cost of data egress from Azure and other super-scale clouds. Establish connections from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider. A one-time connection applies.

RA002EH Responsiv Cloud Security User Expansion Annual Subscription

Purchase additional users for an existing security installation.

Developer and Administrator Tooling

Unified Management

Security management is provided by the Responsiv Cloud Security Service console. Responsiv creates all identity stores and configures all connectivity to external identity stores and certificate authorities.

Using the Responsiv Cloud Console, you may manage identities and set policies, allowing you to add users, register applications and services, and protect your cloud installation.

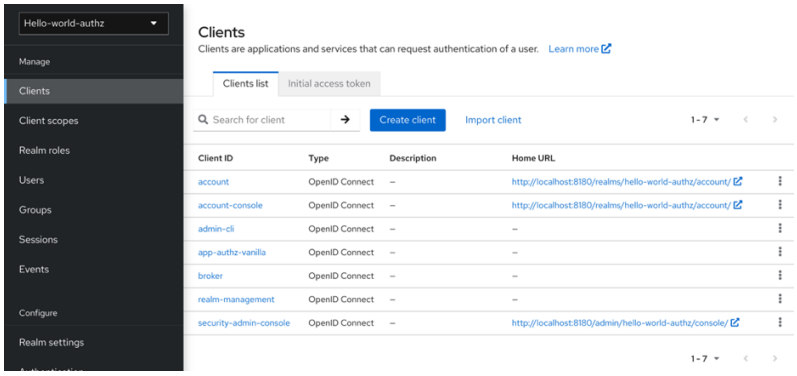


Figure 1; Registration of applications and services authorised to use the service.[2]

Policy Evaluation Tool

When designing policies, you can simulate authorisation requests to test how your policies are being evaluated.

You can access the Policy Evaluation Tool by clicking the evaluate tab when editing a resource server. There you can specify different inputs to simulate real authorisation requests and test the effect of your policies.

The policy evaluation tool is used to test changes to your policies. Policies are enforced at the policy enforcement points (PEP) in each Responsiv Cloud Platform.

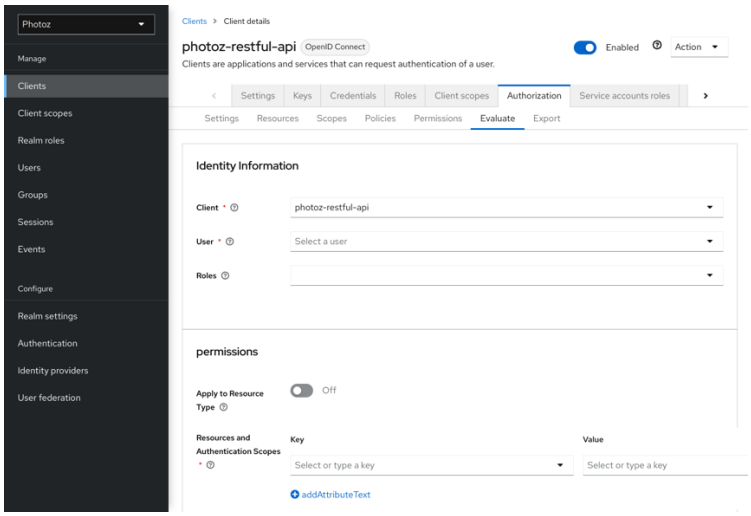


Figure 2; Policy Evaluation Tool user interface.

[2] https://www.keycloak.org/docs/latest/authorization_services/index.html#_getting_started_overview

Service Management

Responsiv manages this service, including active health monitoring, patching, upgrades, and general maintenance. The service is available 7x24.

Service Preparation

This service is prepared by configuring the Identity Store to manage users locally, or to attach to an external identity store to allow customers to retail control and management of their users. Federated trust can be configured at this point. To properly configure this service the following steps are followed.

1. **Plan**
    i. **Select Security Pattern** that you prefer to use. Note that combinations are perfectly reasonable and can be added later. One or more of Attribute-based access control (ABAC), Role-based access control (RBAC), User-based access control (UBAC), Context and Time-based access control (CBAC).
    ii. **Document** attributes, roles, contexts, and the authorisation that will be associated with those things. For example, the role "ADMIN" will have these authorisations.
    iii. **Decide** whether to implement local, SSO, or federated trust. For SSO implementations the subset of identities that are in-scope for the Responsiv Cloud Services should be marked to allow filtering.
2. **Execute**
    i. Configure the service to connect to external identity store for SSO.
    ii. Configure a federated trust association to remove the authentication challenge.
    iii. Configure users as members of groups with roles etc.
    iv. Describe authorisation policies and use the service to test them.

Service Level Agreement

This service is supported by Responsiv from our UK offices.

The service includes product/platform support only and is triggered by automated monitoring built into the platform or manually accessed from our website https://responsiv.co.uk/support-hub/support/.

The service level agreement (SLA) for Responsiv Cloud services (RL000F6 Responsiv Support Services Addendum v1.0) can be found here: https://responsiv.co.uk/wp-content/uploads/2023/11/TC-RL000F6-Aug2023-Responsiv-Support-Services-Addendum-v1-0.pdf. The SLA defines support available for the platform including support hours of availability, response times, severity level, Service Down definition, the claim process and other support information. Responsiv provides the Customer with the following availability service level agreement (SLA). Responsiv will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below.

Upgrade and Patching Schedule

We expect to perform a single upgrade annually and to install security and critical patches efficiently as they become available. Patches are categorised as follows:

- Security – Patch specifically or including for a security flaw or weakness.
- Critical – Patch will be required to be applied before support attempts to resolve a problem.
- Optional – Specific function bug resolution. Optional depending on use cases.

Continuous Improvement

Responsiv does not commit to future development or support beyond our contractual obligations. Responsiv Cloud Platforms and Responsiv Cloud Services are continually developed and maintained.

New features may be provided as optional expansions to the base platform, or may be installed as standard.

Format and Charging Measures

This product is available in the following formats:

- Software as a Service (SaaS) product that is bundled with each Responsiv Cloud Platform
- Individually as a Responsiv Cloud Service

This product supports charging by instance, registered users, and duration. Entitlements use a combination of charging measures that are appropriate to the intended purpose.

Architecture

The Responsiv Cloud Security Service is hosted in a secure part of the Responsiv Cloud.

It connects to external identity stores and certificate authorities using TLS encrypted connections. Users accessing services in your Customer Place are intercepted and checked for authenticity before allowing access or redirecting for credential challenge.

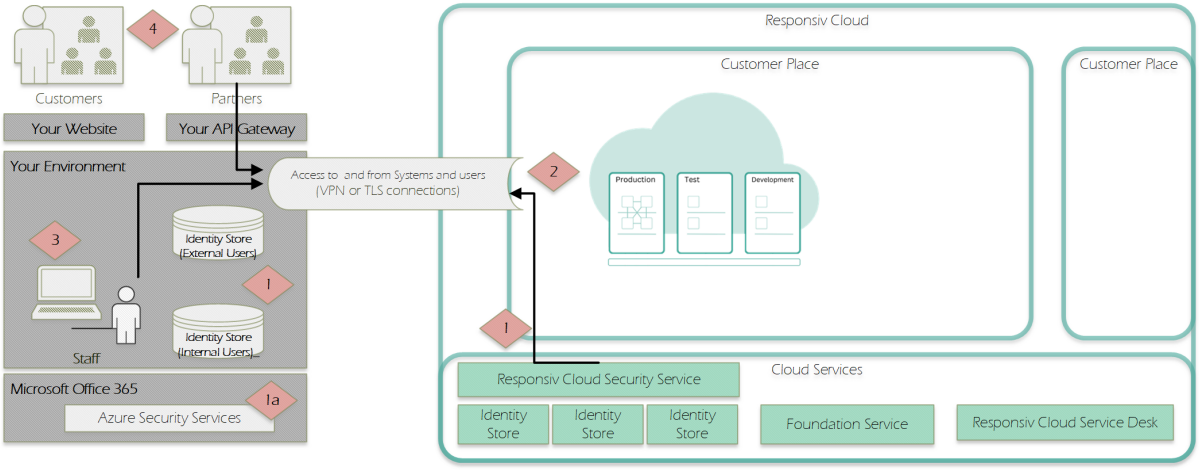


Figure 3; Service Architecture

[1] The Responsiv Cloud Security Service is optionally attached to an existing identity store located in your environment or perhaps the Microsoft Azure Security Service [1a] to simplify user management and reduce the number of challenges for credentials that a user will typically encounter. If this connection is not made, then users can be manually managed inside the service.

In either case, user groups are assigned cloud groups to allow the cloud services to be consistent in their application of protection.

[2] An enforcement point is placed in front of your Service or Platform to check for credentials and redirect those without valid credentials. In these cases, the security service will request credentials. Enforcement uses OAuth2 cookies.

[1a] Other systems can be protected using this service, and this service can integrate with cloud security services, for example Azure security services and identity stores.

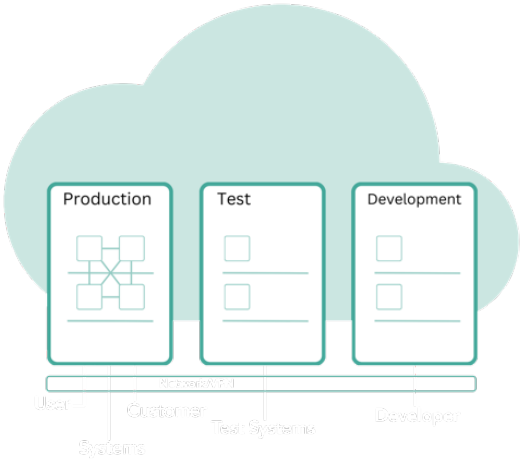
[3] The same credentials can be used to raise tickets in the Responsiv Cloud Service Desk, to access The Responsiv Cloud Console, and to download tools and client programs from The Responsiv Asset Distribution System (ADS).

[4] Your partners and customers can access Responsiv Cloud Platforms by connecting through your API gateway and/or website. Their access is challenged and you can allow them to register (guest).

Infrastructure Architecture

This service is delivered as a production service only. It is available and configured to protect services and user access to Responsiv Cloud Platforms and their environments.

The implementation is a multi-tenant installation with secure separation of user realms and identity stores.



Physical Location

Responsiv operate cloud platforms from locations that are hosted by different cloud providers and chosen for qualities of service and benefit optimisation.

Cloud providers include Red Centric, IBM Cloud, AWS, and Microsoft Azure.

Responsiv Platform data processing and data storage is, by default, performed in the United Kingdom.

All data centres used by Responsiv are Tier 3, ISO27001 certified locations, with 7x24 security and electrical backup facilities.

Supported Protocols

Responsiv Cloud Security Service supports the following protocols:

LDAP and Active Directory

Lightweight Directory Access protocol (LDAP) is a standard protocol for accessing directories. It is more commonly used to refer to implementations that include a database and accessed using the protocol. LDAP defines a standard schema to consistently describe characteristics of people and in particular, their usernames and passwords.

Active Directory is a Microsoft product that has an LDAP interface and provides identity and access management (IAM).

OpenID Connect (OIDC)

OpenID Connect simplifies verification of user identity based on the authentication performed by an Authorization Server and allows the target system to obtain user profile information using APIs. This is an authentication protocol based on OAuth 2.0.

OpenID Connect compliant server.

https://www.keycloak.org/docs/latest/securing_apps/

https://wjw465150.gitbooks.io/keycloak-documentation/content/securing_apps/topics/overview/supported-protocols.html

OAuth 2.0

Open Authorisation (OAuth) version 2.0 is a standard to allow a websites and applications to access resources hosted externally on behalf of a user. It is part of a framework of specifications (IETF RFC 6749 and 6750).

OAuth2 compliant server.

SAML 2.0

Security Assertion Markup Language (SAML) is an XML based language used to describe security assertion/tokens carried in the security header of network connections. Tokens authenticate the user's identity and are understood by Responsiv Cloud Security Service, which can be configured to trust specific issuers. The result is that users can access protected resources without being challenged for credentials.

SAML compliant server.

JWT

JSON web token (JWT) is an open standard (RFC 7519) used to securely transmit information as a JSON object. JWT can be configured to secure APIs on the Responsiv Cloud Platforms.

http://ibmacejwt.rf.gd

https://www.ibm.com/docs/en/app-connect

Single Point of Authentication

Responsiv Cloud Security Service can be the central identity provider used to create the SAML assertion, and can be configured to trust external providers.

Improved User Experience and Directory Isolation

Users sign in once to access multiple service providers, making authentication faster and avoiding password lists. User information does not need to be accessible from Responsiv Cloud Security Service or synchronised across directories because it is the certificate that authenticates.

NCSC Cloud Security Principles

Responsiv Cloud Security Service and associated policies and governance are used to comply with UK National Cyber Security Centre (NCSC) Cloud Security Principles.

Principle 1: Data in transit protection

Data should be adequately protected against tampering and eavesdropping as it transits networks inside and external to the cloud. This should be achieved using a combination of encryption, service authentication and network-level protections.

Responsiv provide data in transit protection using mutually authenticated connections and encryption of data as it passes around each Responsiv Cloud Platform. Data passed in message format can be configured to the encrypted at all stages of transfer. Networks are protected by physical access restrictions to prevent an attacker from intercepting data.

Connections between Responsiv Cloud Platforms and user systems and applications are protected by VPN, TLS, and pre-authenticated network addresses.

https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data

https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data

https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks

Principle 2: Asset protection and resilience

Data, and the assets storing or processing it, should be protected against physical tampering, loss, damage, or seizure. Protections should include cover for the legislation that your data is subject to, as well as mitigations such as encryption, data centre security, secure erasure, and service resilience.

2.1 Physical location and legal jurisdiction

Data maintained by Responsiv Cloud Platforms is physically located and processed in our UK datacentres and administered by a UK based team. Responsiv Cloud Platforms are physically installed on hardware dedicated to Responsiv.

Location	Activity
England, UK	Security, Support, Hosting, and Processing

All data remains under UK legal jurisdiction. Responsiv contracts are subject to the same, UK legal jurisdiction. For reference, our default cloud hosting locations are 4D data centres owned and operated by RedCentric.

See TC-RL000CQ Responsiv Data Processing Addendum (DPA)

https://responsiv.co.uk/wp-content/uploads/2023/09/TC-RL000CQ-Aug2023-Responsiv-Data-Processing-Addendum-DPA-v2-0.pdf

https://www.redcentricplc.com/about-us/4d-data-centres/

2.2 Data centre security

Responsiv use physical datacentres with 7x24 security and power backup including fuel reserves. Hardware is protected in separated cages. These facilities offer security and low latency to provide reliable and resilient managed hosting solutions. Accredited with ISO 27001, ISO 9001, and ISO 14001, providing peace of mind that your data and systems are always accessible.

https://www.redcentricplc.com/public-sector/

https://www.redcentricplc.com/uk-data-centres/london-data-centre/

2.3 Data encryption

Data is encrypted when written to disk and in backups. Physical media is dedicated to Responsiv use.

2.4 Data sanitisation and equipment disposal

Responsiv securely erases data on request, and when a customer closes a platform or customer place.

Principle 2.5: Physical resilience and availability

Responsiv service availability and service level agreements (SLA) are defined generally in the TC-RL000F6 Responsiv Support Services Addendum, and the product entitlement for each cloud platform. Platforms are available 7x24 and historically achieved over 99.99% availability.

https://responsiv.co.uk/support-hub/terms-and-conditions/

Responsiv Cloud Platforms are deployed to remove single points of failure in the production environments using an active-active configuration to reduce failover delays. Databases and singleton components (those hosting state) are deployed with automated fault detection and failover configured.

Hardware is deployed in a resilient cluster with RAID protected disk. System backups and snapshots are used to assure recovery of the working system. Additional services are available to provide the same assurance for user data.

Responsiv offer multi-zone/multi-centre deployments to suit requirements. We can achieve the level of availability you need by introducing redundancy into your architecture. We use a high-availability architecture built across multiple data centres or geographic regions, within a single Responsiv Cloud service. Please contact Responsiv for information.

See RA002BM Responsiv Cloud Backup Service for information about user-data backups triggered by changes made to the data and based on a defined schedule.

Principle 3: Separation between customers

A malicious or compromised customer of the service should not be able to access or affect the service or data of another. It will need to implement effective security boundaries in the way it runs code, stores data, and manages the network.

Responsiv Cloud customers are assigned a "Customer Place". This is a walled garden network area that separates their installations from all other customers. Each cloud platform is installed into this "place" with its own isolation between platforms and between environments (Production, User test, and Development). This allows tight control over data flows, including the ability to detect anomalous traffic more easily.

Unless otherwise indicated in the product entitlement or product description, Responsiv Cloud Platforms and services are single tenant. Responsiv Cloud Security Service separates user groups from different customers, and controls access from a separate and secure region of the Responsiv Cloud.

It is not possible to create a direct connection between customer places without passing out of the Responsiv Cloud and returning through the authorised channel to the second place.

https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/technically-enforced-separation-in-the-cloud

https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

Principle 4: Governance framework

The service provider should have a security governance framework which co-ordinates and directs its management of the service and information within it. This will give you confidence that other controls will continue to be effective through the lifetime of the service.

Responsiv has a governance framework that prescribes how our assets are securely handled, and how we adopt new technology to deliver our services. For more information, please contact Responsiv.

- POL21-SEC-015 Password Management
- POL21-SEC-019 Technology Adoption
- POL21-SEC-020 Data Protection
- POL21-SEC-021 Data Security

Principle 5: Operational security

The service is operated and managed securely to impede, detect, or prevent attacks. It will achieve this through a combination of effective vulnerability management, protective monitoring, configuration & change management, and incident management.

Principle 5.1: Vulnerability management

Only selected Responsiv Cloud Platforms can be attached to the public Internet. In every case, we recommend that connections to cloud platforms are internal to your organisation, and that your partners and customers pass through your integrated security barriers before entering the Responsiv Cloud.

This means that the attack surface for Responsiv Cloud is dedicated to defending against contagion from customer networks, and from attacks that have already passed through your defence in depth.

5.2 Protective monitoring

Responsiv monitors for attacks, misuse, and malfunctions withing components of each customer place. Security, Audit, and Problem alerts are raised to our service desk, and if appropriate forwarded to you. Our monitoring includes network, hardware hosting, virtualisation, and platform software.

5.3 Incident management

Responsiv has pre-planned incident management processes in place to assure recovery from predictable unexpected problems.

https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

5.4 Configuration and change management

Responsiv know the components and configurations for all Responsiv Cloud Platforms. Configuration and deployment of the service is automated and audited. We can identify and manage changes affecting security of the service.

Principle 6: Personnel security

Service provider personnel with access to your data and systems, you need a high degree of confidence in their trustworthiness and the technical measures in place that audit and constrain the actions of those personnel.

Responsiv use a third-party organisation to screen all staff with access to our cloud platforms. Staff are given access to limited parts of the cloud environment, and different levels of access are used to protect against malicious activity as well as accidental damage. Privileged access is only available to Responsiv screened and authorise personnel.

Role based access (RBAC) and detailed planning is used to reduce the possibility of human error. Runbooks are an important part of our control process.

Principle 7: Secure development

Cloud services should be designed, developed, and deployed in a way that minimises and mitigates threats to their security. This will include a robust software development lifecycle that uses an automated and audited integration and deployment pipeline.

Responsiv license world leading, best in class, software from IBM and other vendors. Our own software is developed, tested, and verified in the UK by dedicated programming teams.

Development considers security as a primary design concern for software development. We use industry standard encryption and security practices and components.

Principle 8: Supply chain security

Ensure that supply chain meets the same security standards that the organisation sets for itself. This includes where a third party has access to customer data or the service, and where the provider has dependencies on a third party such as when procuring hardware and software.

The supply chain for Responsiv Cloud Platforms generally involve a relatively small number of suppliers, including cloud hosting, software product provision, firewall and network providers, and us. For all suppliers, we assure ourselves that the software is developed in a secure manner, and that for any open-source components, we can support the software ourselves if the support project is retired.

Principle 9. Secure user management

Your provider should make the tools available for you to securely manage your use of their service, preventing unauthorised access and alteration of your resources, applications, and data. This will usually include an access model that allows you to implement role-based access controls across the service and the data held in it.

Responsiv Cloud software, including virtualisation, middleware, applications, and managed service, is completely controlled by Responsiv. Our services are hosted on hardware dedicated to our use. The result is that we have no unnecessary separation of responsibilities, reduced internal attack surfaces, and reduced access to your enterprise data.

Sensitive data

If your application or data is particularly sensitive, you will need to discuss use of sovereign cloud and dedicated hosting, which gives you control and oversight of the entire underlying stack of services.

Data sharing

Our cloud services describe data sharing relationships with third parties, and we have a separate privacy policy. We do not share your enterprise data, and cloud user personal data is only shared to enable and facilitate the services provided to your organisation.

Principle 10: Identity and authentication

Access to service interfaces should be constrained to a securely authenticated and authorised identity, which may belong to either a human user or a machine.

Responsiv make the tools available for you to securely manage your access to our service and to prevent unauthorised access and alteration of your resources, applications, and data. We use a single, coherent access control mechanism.

We have a single well-defined user account model for the Responsiv Cloud and administrative access to Cloud components. Each customer has an identity store and region within which they control access. Control is through graphical browser-based interfaces.

- Support requests are accepted only by the Responsiv service desk, which uses the same authentication mechanisms and credentials.
- Granular access control, according to the 'principle of least privilege', enabling 'standard' and 'administrative' user accounts, as well as several different authorisation schemes.
- Customer access is separated. Other customers cannot in any way effect your security settings.

Principle 11: External interface protection

External or less-trusted interfaces of the service should be identified and defended appropriately. This includes external APIs, web consoles and command line interfaces.

External Interfaces are authenticated using mutually authenticated connections. See principle 1. We require multi-factor authentication (MFA) for administrative user access for both customers and Responsiv staff.

joiners, movers, and leavers

Responsiv security integrates with your internal processes to manage joiners, movers, and leavers. We offer federated trust, shared identity store, and API management of user security profiles.

Principle 12: Secure service administration

The design, implementation, and management of the cloud service provider's administration systems should follow enterprise good practice, recognising their high value to attackers.

Defensive measures include application programming interfaces (APIs), web consoles, command line interfaces (CLIs), and direct connect services. Our administrative interfaces are only available through our internal security jump-points and bastion servers.

Principle 13: Audit information and alerting for customers

Identify security incidents and should have the information necessary to find out how and when they occurred. The service will need to provide you with audit information, and issue security alerts when attempted attacks are detected.

Responsiv will provide the audit data needed to investigate incidents related to customer use of the Cloud Service and the data held within it. We audit our response to all service request tickets in a tamper proof system. This includes information for actions taken by Responsiv personnel that affect your service or the data held within it. Audit information cannot be deleted by the customer or Responsiv during the retention period.

Principle 14: Secure use of the service

Easy to meet your data protection responsibilities. Services should be secure by design and by default. Wherever this is not the case, the provider should help you meet your security responsibilities.

Responsiv make it easy for you to use their services in a way that is defended against common attacks. We do not allow connections that are considered dangerous, and our service preparation service will help setup and configure secure connections as well as mentor your staff on its maintenance.

Common attacks, for example DOS, DDOS, SQL Injection, and other known attach vectors are protected by default. Cloud connections are generally only allowed from known addresses using known certificates (mutual authentication), which protects individual customers at the same time as preventing contagion between customer networks and their cloud platforms.