RSA® SecurID Access

Security Overview

RSA® SecurID Access delivers secure and convenient access to today's SaaS, mobile, enterprise and web applications so you can regain control over a disrupted perimeter and accelerate user productivity. RSA SecurID Access enables you to take advantage of:

- **Frictionless Single Sign-On.** Deploy SSO across external SaaS, internal Web or custom applications, and SAML-enabled native mobile applications for a truly unified user experience.
- **Convenient Multifactor Authentication.** Leverage your users' mobile devices for quick and convenient step-up authentication when necessary.
- **Intelligent Context-Based Access Controls.** Take advantage of attribute-based access control for increased security and a frictionless user experience. Uniform, sophisticated and flexible authentication policies balance security with user convenience.
- **Hybrid SaaS Approach.** Use RSA SecurID Access' hybrid architectural approach, combining the benefits of a multitenant cloud-based access solution with the security and control of a dedicated on-premise virtual appliance.
- **Existing Investments.** Benefit from a cloud and mobile access product that integrates with your on-premise solutions including RSA Authentication Manager and web access management (WAM) solutions to make the most of your IT assets.

Infrastructure Layer

Infrastructure Provider

RSA SecurID Access is hosted on Microsoft® Azure®, a cloud-computing platform that is hosted through a global network of Microsoft data centers. RSA SecurID Access uses a multitenant database in an environment that shares infrastructure while segregating customer data to ensure privacy. Hardware infrastructure components, including but not limited to firewalls, load balancers, web servers, database servers, and storage equipment, are shared across multiple customers. Service levels and operational procedures are standardized for all customers due to the shared nature of the platform. Additional information can be found in the Microsoft Azure Trust Center.

Service Infrastructure

The RSA SecurID Access infrastructure consists of a set of services layered on top of each other. Services in the upper layer are more widely accessible, but hold the least amount of sensitive information. Services in the lower layers have the most privileges; access to these layers is therefore more strictly controlled. RSA SaaS Operation services are at the heart of this infrastructure and are responsible for monitoring the health of the overall system and performing maintenance procedures, such as product upgrades. RSA SaaS Operations need privileged access to the entire service environment and services are performed from an audited, locked down, and tightly controlled system.

Customer Infrastructure

RSA SecurID Access enables customers to connect to SaaS, mobile or web applications. Authentication to applications is managed through the RSA Identity Router which is a virtual appliance that customers deploy in their environment.   The identity router provides policy enforcement and a central decision point that enforces authentication and authorization for all users. The identity router also serves as an audit collection point for all user actions.

Security Controls

A complete access solution for cloud, on-premise and mobile

Data Security and Encryption

The RSA SecurID Access service uses cryptographically strong encryption and key management to secure sensitive data at rest and in transit. The encryption is secured with standard, peer-reviewed cryptographic algorithms and uses an AES 128-bit key for data in transit and an AES 256-bit key for data at rest. All connections to and from the RSA SecurID Access hosted service, regardless of data sensitivity, are secured using TLS 1.2, with ECDHE key agreement, 2048 bit RSA signatures, and AES 128-bit keys. Messages exchanged between the RSA SecurID Access hosted service and the on-premise identity router use certificate based digital signatures and encryption. In addition to the multi-layered encryption, the hybrid cloud model enables RSA SecurID Access customers to keep their most sensitive data on premise and minimize the amount of sensitive data that is sent to the cloud.

RSA SecurID Access Hosted Service

RSA SecurID Access operates data centers in the US and Europe. The hosted service infrastructure provides the administrative front end to manage the RSA SecurID Access identity router, authentication policies, identity sources and application configuration. The RSA SecurID Access hosted service provides the infrastructure to send push notifications to mobile devices for strong authentication.

The RSA SecurID Access hosted service has several native security features, including:

- Firewalls, VPNs, network segregation.
- Load balancing and high availability.
- DDoS attack mitigation.
- Host based IDS and service monitoring.
- Encrypted communication among the service components.

The RSA SecurID Access hosted service is split into multiple tiers across different network segments. Communication between the tiers is restricted to ensure that an attacker that compromises the first tier is not allowed access to subsequent tiers.

RSA SecurID Access Identity Router

The identity router is a hardened virtual appliance that is hosted and managed by the customer. The identity router acts as the policy decision point (PDP) and policy enforcement point (PEP) and communicates with on-premise infrastructure (e.g. Microsoft Active Directory, LDAP v3 directory server, RSA Authentication Manager) and the RSA SecurID Access hosted service.   The identity router also acts as a reverse proxy for HTTP Federation/password vaulting or HTTP Header integration with third-party applications. The identity router enables the RSA SecurID Access service to deliver a hybrid deployment model allowing your most sensitive data to remain on premise and under your control.

The RSA SecurID Access identity router has several security features which include:

- Hardened, locked down, third-party penetration-tested appliance.
- Encrypted communication between the IDR and the RSA SecurID Access service uses TLS v1.2.
- Public key pinning is used to connect to the service on configuration.
- The IDR can only be registered with the service using a limited-life, one-time passcode generated in the hosted service administration console.
- User key chains are encrypted with user-specific keys.
- User-specific keys are encrypted with a unique tenant key.
- All sensitive data is encrypted at rest on the virtual appliance.

After installation, the identity router configuration is managed through the RSA SecurID Access hosted service.

RSA SecurID Access Mobile App

The RSA SecurID Access mobile app functions as an additional authenticator for the RSA SecurID Access service. RSA SecurID Access end users can leverage the device as a "something you have" authentication factor with device authentication, push notification approval, or RSA mobile tokencode. The app also functions as an input mechanism for "something you are" authentication factors such as fingerprint or retina scan biometrics. The RSA mobile app has several native security features that include:

- App package signature verification on installation.
- Encryption of locally stored sensitive data.
- Encryption of all traffic to and from the RSA SecurID Access hosted service.
- Secure enrollment of the device using certificate pinning.
- On Android devices, byte code obfuscation and hardware key storage.
- RSA submits all mobile apps to third-party vendors for security and vulnerability testing.

Secure and convenient access:

To anywhere, from any device

RSA SaaS Operations

Personnel Access Control

RSA has a dedicated SaaS Operations team to handle the day-to-day maintenance and operation of the RSA SecurID Access service and infrastructure. RSA maintains geographically distributed Operations Centers in the United States, Israel, and India. The service environment is managed through the RSA SecurID Access Operations Console.

- Access to the operations console is granted only to members of the operations team who are responsible for maintaining the service.
- RSA employees must complete the operations, security awareness and secure development training before being granted access to the operations console.
- The operation console utilizes a role-based access control system to restrict operator access to functionality that is required to perform that particular operator’s responsibilities.
- All actions performed in the operations console are logged for audit purposes.
- Access is revoked immediately upon employee termination.

Physical Access Controls

Physical access control systems are in place to restrict access to and within the operation centers.

- Badge access control system is in place at the perimeter and within the facilities
- Two-factor authentication is required to access the data center
- Visitor logs record visitor access to the corporate facility
- Visitors must wear visitor badges while onsite and the badges are distinguishable from employee badges
- Visitors require an escort at all times

New IAM should extend the ROI of your existing investments

Monitoring

All server infrastructure components are monitored to ensure continuous uptime. Monitoring is performed from:

- The Microsoft Azure cloud to gain visibility into the health of the internal services that are not accessible from external networks
- An external monitoring service to provide an independent uptime assessment

Established procedures are used to investigate and respond to the malicious events detected by the service for timely resolution.

Update and Patching

All of the cloud infrastructure components are hosted on Microsoft Azure with the most recent security and OS patches. All of the software updates are tested and approved in RSA’s development environment before being applied. After a software update is released, systems are carefully monitored to ensure continued and smooth operation of affected services.

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

www.RSA.com