RSA ID Plus Hybrid Failover

Ensuring uninterrupted security and access

RSA ID Plus Hybrid Failover provides a resilient authentication solution, ensuring continuous security and access during unexpected disruptions. By seamlessly integrating cloud and on-premises authentication systems, RSA ID Plus Hybrid Failover mitigates risks from cloud service outages, infrastructure faults, and cyberattacks.

Hybrid Failover ensures that your organization's critical on-premises systems remain protected, enabling operational continuity and reducing downtime:

- **Enhanced Security:** Hybrid Failover maintains strong security protocols and user authentication during service disruptions.
- **Operational Continuity:** Hybrid Failover ensures uninterrupted access to essential systems, minimizing business impact.
- **Cost Efficiency:** Hybrid Failover reduces potential for financial losses from downtime and security breaches.

Architected to protect

RSA ID Plus provides organizations with the market's only hybrid authentication platform, through which cloud and on-premises authentication can be integrated to ensure uninterrupted availability of authentication and verification capabilities.

The RSA ID Plus Cloud Authentication Service (CAS) offers secure and convenient multi-factor authentication (MFA) methods such as push-to-approve, passwordless (biometrics, QR code, FIDO passkeys) and one-time passcode (OTP) for mobile or hardware devices.

RSA CAS is tightly integrated with the on-premises RSA Authentication Manager (AM). This integration creates a single authentication backend, proxying authentication requests between RSA AM and RSA CAS to maximize security and user convenience. With this integration, OTP authenticators enrolled via RSA My Page are enabled for "High Availability OTP," allowing the RSA AM to verify OTP authentication requests even when the cloud service is unreachable.

94%

of business and IT leaders have moved some of their workloads back to on-premises from the cloud due to unexpected security issues based on a Citrix 2024 survey.[1]

RSA ID Plus Hybrid Failover limits your risk from outages and attacks

Mitigating cloud service outages

Cloud services are essential for your daily operations, but there's always a risk of an outage. With RSA Hybrid Failover, you ensure that your critical on-premise systems remain secure even if the cloud service is unreachable. When activated, RSA Hybrid Failover immediately switches to OTP-only mode, maintaining security and access continuity.

Resilience from infrastructure misconfigurations and faults

To protect your systems, MFA needs reliable communication with the authentication backend. Unexpected issues from planned maintenance or third-party outages can disrupt this connection. RSA Hybrid Failover detects when the cloud service cannot be contacted; in those scenarios, it automatically ensures that users can still authenticate with OTP, ensuring that users stay secure even when they can't connect.

Defending against malicious attacks

In the event of an attack, threat actors might try to disable your security controls by making the cloud service appear offline. RSA Hybrid Failover counters this by recognizing when the cloud service is unreachable; in the event of a cloud outage, Hybrid Failover will still require users to provide OTP authentication. This prevents attackers from compromising your security, ensuring that your defenses remain strong.

[1] *https://www.itbrew.com/stories/2024/03/01/nearly-all-business-and-it-leaders-surveyed-have-shifted-some-cloud-workloads-back-to-on-prem*