RSA ADAPTIVE IAM
Solutions for the Hyper-Connected World

WHAT IS ADAPTIVE IAM?
- Securing the Dynamic Perimeter
- Risk-based Identity and Access Controls
- Extending IAM to the Cloud
- Protecting Mobile Access
- Aggregating & Synchronizing Identities
- Continuously Verifying Trust

THE CHALLENGE
Today we live in a hyper-connected world, which confronts traditional Identity and Access Management (IAM) with new challenges. The volume of identities is growing exponentially in both the number of users and devices. Organizations are rapidly extending access to applications internally and externally, not just to employees but also to an ecosystem of customers, clouds, service providers, and supply chains. While online openness enhances enterprise productivity and agility, it also exposes organizations to security risks such as new avenues for cyber attacks.

The increasing adoption of cloud-based services has also pushed data access outside the traditional perimeter of an organization. These compounding complexities in the volume of identities, data, mobility, BYOD, and cloud have made secure access management increasingly more challenging.

Access management technologies that are built around the traditional perimeter are falling short. What’s needed is a new approach to IAM as mobile users and Cloud Services are driving a transformation towards risk-based, adaptive solutions.

A NEW APPROACH TO IAM
IAM solutions must adapt to protect corporate data and users wherever they are, even when they’re outside the traditional boundaries of the organization. Security needs to be an outcome of the fluid interaction between identity and data, based on attributes, and the proportionate with the level of risk. The modern session risk assessment is a combination of knowing identity and data attributes, and the means by which that identity and data are trying to meet. This is about knowing the authorization context, in addition to the authentication context – to be able to do fine grained controls in “time and space”. The new enforcement point is a dynamic security perimeter around user access that is adaptive to changing risk levels based on different contextual risk factors for each online session or transaction.

Several key tenets are essential to ensuring trusted identities and access across enterprise and cloud environments:
- Access management and identity federation must be tightly integrated with dynamic, risk-based authentication and with an eye toward user convenience.
- Trust must be constantly verified, not just at the start of a session but throughout.
- There is also a strong need for next generation identity infrastructure that aggregates and correlates identities to presents a single, flexible source of identity information.
- Enterprises need to augment and extend their existing on-premise IAM deployments with capabilities delivered from the cloud. A new, more dynamic and scalable approach must be taken.
THE RSA SOLUTION

Whether you are using IAM internally or securing access for millions of external users to a consumer portal, RSA delivers on these guiding principles to address evolving IAM challenges. RSA can put you on a secure path with the most effective combination of user authentication methods, access management controls, federated identity management and virtual directory solutions. Seen in isolation, these technologies are very effective - but the sum of these solutions is certainly larger than the parts. We call this sum Adaptive IAM. Adaptive in the face of cloud and mobile. Adaptive in the face of ever changing risk profiles. Adaptive in the face of increasing number and richness of identities.

RSA® ACCESS MANAGER

RSA Access Manager secures access to web applications with transparent, single sign-on (SSO) based on coarse to fine-grained control policies. Additionally, RSA Access Manager supports a wide range of authentication methods, including RSA SecurID two-factor authentication and RSA Adaptive Authentication. RSA Access Manager also integrates with RSA Adaptive Directory so that organizations have a single logical view of all identities and attributes to ensure safer authorization of access to all their web applications. When authentication and access management are matched to the risk of the situation along with a single source of identity truth, organizations benefit from reduced fraud with minimal user impact.

RSA® ADAPTIVE DIRECTORY

RSA Adaptive Directory delivers a global view of identity on top of your existing identity infrastructure. It uses model-driven virtualization to externalize identity out of disparate data silos into a common, interoperable service. A flexible identity service is critical to enabling any initiative requiring secure access to a global list of identities.
“Through the strategic use of RSA technology, we have been able to accelerate our plan for an integrated regional health information organization. The Keystone Health Information Exchange pilot, secured by RSA Access Manager and RSA Federated Identity Manager, allows Emergency Departments within participating hospitals to share patient health information in real time. We were particularly attracted by the way RSA Adaptive Authentication offers layers of security in addition to the standard user name and password, but without inconveniencing the user. It is ideal for clinicians working in a busy and often pressured hospital and clinic environment.”

DAVID YOUNG, IT DIRECTOR, GEISINGER HEALTH SYSTEM

users, along with their complete identity profiles—including web access management with RSA Access Manager, authentication, identity federation and fine-grained authorization.

**RSA® FEDERATED IDENTITY MANAGER**

RSA Federated Identity Manager secures access to external applications by providing federated single sign-on for both identity provider and service provider models. RSA Federated Identity Manager installs on-premise and provides a standard-based method to leverage trusted identities between organizations, their partner and their customer ecosystems.

**RSA® ADAPTIVE FEDERATION**

RSA Adaptive Federation provides easy-to-use, federated single sign-on for both identity provider and service provider models to popular cloud-based applications. As a cloud-based service, RSA Adaptive Federation provides flexible, scalable support without additional hardware, software, agents or data stores—enabling, faster, simplified deployments. For even stronger security, existing user credentials can be extended securely to the cloud without leaving your enterprise.

**RSA® ADAPTIVE AUTHENTICATION**

RSA Adaptive Authentication, with its advanced self-learning risk engine, calculates a risk score based on the user behavior profile, the device fingerprint, and the eFraudNetwork match. This risk score is provided to a policy engine and the user is either granted access, required to provide an alternate authentication credential, or denied access. RSA Adaptive Authentication tightly integrated with RSA Access Manager, including out-of-band phone and out-of-band email support. RSA Adaptive Authentication is a proven solution protecting thousands of organizations and users worldwide today.

**RSA® SECURID®**

RSA SecurID is the market leading two-factor authentication solution. The RSA SecurID authentication mechanism consists of either a hardware or software token that generates unique authentication codes at fixed time intervals using the token’s factory-encoded random key.

**RSA® IDENTITY VERIFICATION**

RSA Identity Verification uses dynamic knowledge-based authentication to provide reliable identity assurance in real-time through a top-of-mind identity quiz generated from public and commercially available data.