RSA® Adaptive Authentication and Citrix NetScaler SDX Platform Overview
RSA and Citrix have a long history of partnership based upon integration between RSA Adaptive Authentication and Citrix® NetScaler® application delivery solutions. The next generation of SDX platform provides the foundation for further integration. Today, Citrix NetScaler SDX appliances enable consolidating multiple NetScaler instances onto a single purpose-built appliance. Working together, RSA and Citrix will jointly deliver RSA Adaptive Authentication on the next generation NetScaler SDX platform. This enables RSA and Citrix to jointly deliver consolidated, best-in-class L4-7 networking services on an open, unified platform.

**Citrix NetScaler Next Generation SDX Overview**

The next generation of the NetScaler SDX platform provides an open platform that makes the whole network **app-driven**. Unlike monolithic approaches that compromise functional depth for functional breadth by adding piecemeal extensions to existing products NetScaler SDX consolidates best-in-class application delivery services onto an open, unified platform.

The next generation of SDX platform unifies best-in-class L4-7 network services into an application control layer, and can integrate this application control with both existing transport networks and emerging SDN technologies. This application control layer can make emerging L2-3 SDN architectures completely app-driven by using app-centric definitions and policies to simplify network design while making the whole network more intelligent.

The next-generation of SDX provides:

- **Control** by creating a unified application control layer composed from best-in-class L4-L7 network services.

- **Simplified** administration by using a prescriptive, app-driven approach for defining networking policy and topology and automating network configuration.

- **Consolidation** of network services while preserving best-in-class network functionality.

- **Intelligence** by ingraining application intelligence and comprehensive control into both existing L2-3 infrastructures and emerging SDN architectures.

The dynamic nature of cloud services requires a level of app-awareness, control and flexibility and that go beyond the capabilities of today’s data center networks. Together, by integrating RSA Adaptive Authentication and NetScaler SDX, RSA and Citrix are delivering this app-awareness, control and flexibility to today’s networks and tomorrow’s SDNs in an open and unified manner.
RSA Adaptive Authentication Solution Overview

RSA Adaptive Authentication is a comprehensive risk-based authentication and risk management platform that balances security, usability and cost. Adaptive Authentication offers a layer of security on top of existing user credentials that is convenient for any client type or location. Adaptive Authentication monitors and authenticates user activities based on risk levels, institutional policies and user segmentation. Adaptive Authentication protects against the risk of unauthorized access without compromising the user experience.

Adaptive Authentication is powered by the RSA Risk Engine. The Risk Engine measures a series of indicators behind the scenes to validate user identities and behaviors. The majority of logins are “invisibly” authenticated by using analytics. This transparent authentication creates a superior user experience as users are only challenged in the highest risk scenarios. In addition, RSA Adaptive Authentication is self-learning and thus constantly improves detection accuracy.

The RSA Risk Engine measures over 100 different risk indicators for every login. These risk indicators typically involve device identification, behavioral profile, and a check against the RSA eFraudNetwork™. The RSA Risk Engine is a self-learning technology. It recognizes and adjusts to threat patterns using a Naïve Bayesian Algorithm. A unique risk score, between 0 and 1000, is generated for each activity. The higher the risk score, the greater the likelihood that an activity is fraudulent.
Device identification analyzes the device from which the user accesses a web site or mobile application. Several devices can be associated with each end-user. The behavioral profile is a record of what activities the end-user usually performs. Both the device identification and behavior profile match behavior and profiles of typical users against themselves as well as against global profiles.

Once the degree of risk has been assessed, the Policy Manager determines what action to take. Depending on the level or risk, an organization can decide to block, monitor, allow or force a “step up” authentication. The Policy Manager enables organizations to instantly react to emerging localized fraud patterns according to their business policies, and effectively investigate activities flagged as high risk. The Policy Manager is used to translate organizational risk policy into decisions and actions through the use of a comprehensive rules framework that can be configured in real time.

The RSA eFraudNetwork service is a cross organization repository of threat patterns gleaned from RSA’s extensive network of customers, internal research labs, ISPs and third party contributors across the globe. When a threat pattern is identified, the threat data, transaction profile and device fingerprints are moved to a shared data repository. The eFraudNetwork provides direct feeds to the Risk Engine so that when activity is attempted from a device or IP that appears in the eFraudNetwork, it will be deemed high risk and prompt a request for additional authentication.

When a particular user activity crosses the risk threshold as defined by the RSA Risk Engine and the Policy Manager, Adaptive Authentication can further assure the identity of the user by initiating a “step up” authentication. A step up authentication is an additional factor or procedure that validates user identities. Following are some examples of step up authentication methods:

- **Challenge questions** – Secret questions that have been selected and answered previously by the end user.

- **Out-of-band (OOB) phone authentication** – Via SMS, phone and email. When properly utilized, OOB authentication can stop MITB and MITM attacks.

- **Multi-credential framework** – Adaptive Authentication is integrates with existing and 3rd party authentication methods. The Multi-credential Framework allows organizations to develop authentication methods via RSA Professional Services, “in-house”, or to integrate with existing or new 3rd party authentication methods.
RSA Adaptive Authentication 7.0 features a unique and dedicated risk model to analyze mobile channel activity. Mobile browser activity is detected automatically and analyzed by the mobile risk model. The analysis performed by the mobile risk model is enhanced by such features as location awareness and mobile device identification. Location awareness detects the location of the device using a series of time and geography based algorithms and can access location data gathered through Wi-Fi, cell-tower triangulation, and GPS. Anomalies such as locations which are new to the user, or impossible user ground speeds, are flagged. Device characteristics can be gathered either through JavaScript if the end user is accessing via a mobile browser or directly through an API. Mobile applications feature enhanced device identification, including device name, device model, language, screen size, and number of address book entries.

Finally, Adaptive Authentication 7.0 protects against threats from hackers who set up proxy attacks to log on to institutions from “proxy” IP addresses. These attacks allow hackers to penetrate user accounts via the genuine end user IP and thus gain positive device identification. Proxy attacks install malicious code on the victim’s device and open a back door that allows the hacker to connect. Adaptive Authentication 7.0 is able to determine when a log on or transaction is being performed via a proxy which is anomalous to the user and IP, and adjust the risk score appropriately. The Adaptive Authentication customer can use the policy manager to either deny, challenge, or monitor activity coming from a proxy address.

RSA Adaptive Authentication is a proven solution that is currently deployed at over 8,000 organizations worldwide and across multiple industries including financial services, healthcare, and government. It is currently being used to protect over 200 million online users and has processed and protected over 20 billion transactions to date.

Customer Value

Integrating the advanced authentication features in RSA’s Adaptive Authentication services with The next-generation SDX platform substantially enhances the security of the enterprise and cloud applications delivered through the NetScaler while providing a seamless end user experience.

- **Added Agility**: Organizations become more agile by providing on-demand, anytime, anywhere secure remote access to systems and applications.

- **Strong Layered Security**: Extend user identity across enterprise and SaaS applications with strong, multifactor security beyond username and password.

- **Superior User Experience**: Transparent authentication methods offer the lowest impact on genuine users providing a convenient online experience as users are only challenged when suspicious activities are identified and/or an organizational policy is violated.

- **Low Total Cost of Ownership**: Enables user self-enrollment with no need to deploy additional hardware.
Integration Strategy and Use-Cases

Figure 2: RSA Adaptive Authentication