SOLUTION BRIEF

PREVENT CREDENTIAL-BASED ATTACKS WITH RSA SECURID® ACCESS & PALO ALTO NETWORKS
KEY BENEFITS

- **Mitigate** identity risk with a multi-layer approach to secure access.
- **Save** time and money deploying multi-factor authentication by avoiding the need to modify applications.
- **Simplify** user access and deliver a high level of identity assurance with RSA behavioral analytics and mobile push and biometric authentication.
- **Bridge** the islands of identity across cloud, web, mobile and on-premises applications, and enforce consistent policies regardless of where the data lives.
- **Balance** security and convenience with RSA assurance levels and easily define unique authentication requirements based on policy.

RSA and Palo Alto Networks have teamed up to neutralize threats associated with credential abuse by empowering organizations to enforce network-level multi-factor authentication before granting access to applications—including custom or legacy applications that do not support standard authentication protocols such as SAML or RADIUS.

THE CHALLENGE

Credential theft continues to plague organizations and contributes to the ever-increasing number of data breaches. In fact, 81% of hacking-related breaches leveraged either stolen or weak passwords.¹ Once attackers infiltrate a network, they can blend in with legitimate users, move laterally and steal or destroy assets without raising any alarms.

Multi-factor authentication helps prevent credential abuse, but deployment obstacles—such as integration with custom and legacy applications—may prevent organizations from implementing it broadly across all their sensitive resources.

**RSA SECURID® ACCESS**

**RSA SecurID® Access**, the world’s most widely deployed multi-factor authentication solution, provides convenient, secure access to on-premises, web, mobile and cloud applications—giving organizations the security they need and end users the consumer-simple experience they demand. RSA offers the broadest range of MFA methods, including mobile push and biometrics, SMS, voice, hardware and software tokens, and FIDO, as well as machine learning risk-based authentication that analyzes contextual information to benchmark normal user-access behavior and eliminate end-user friction.

**RSA AND PALO ALTO NETWORKS**

RSA has collaborated with Palo Alto Networks to extend the use and simplify the deployment and management of multi-factor authentication. Now, joint customers can enforce multi-factor authentication at the network layer and deploy it across their entire network, including to applications that do not natively support authentication protocols, such as SAML and RADIUS, and therefore cannot easily integrate with identity and access management systems.

Without this joint offering from Palo Alto Networks and RSA, many organizations might only deploy multi-factor authentication to a limited number of resources and applications, to avoid the time-consuming and costly development work associated with updating countless applications for multi-factor authentication. This approach leaves organizations’ sensitive systems and data exposed and vulnerable to credential-based attacks.

Palo Alto Networks next-generation firewall integrates with RSA SecurID Access to enforce multi-factor authentication before granting access to applications and systems. By doing this, the combined solution serves as an authentication gateway for web or thick-client applications, while centrally controlling access to these applications.

¹ Verizon, 2017 Data Breach Investigations Report
By leveraging the integration of RSA and Palo Alto Networks, organizations can quickly provision multi-factor authentication—and avoid the need to manually update applications and infrastructure. Palo Alto Networks next-generation firewall, deployed in conjunction with RSA SecurID Access, provides centralized policy management and a high level of identity assurance through the RSA rich policy engine.

**HOW IT WORKS**

![Diagram of how RSA and Palo Alto Networks work together]

*Figure 1: RSA and Palo Alto Networks Together Can Simplify the Deployment and Centralize the Enforcement of Multi-Factor Authentication*

**ADDRESS A GROWING NUMBER OF COMPLIANCE REQUIREMENTS**

Multi-factor authentication not only bolsters security but it also helps organizations satisfy a broad range of regulatory compliance mandates, including PCI DSS and HIPAA.

HIPAA Security Rule subparts 164.308(a)(4)(i) and 164.312(a)(1) direct healthcare organizations to implement policies and procedures to allow only authorized users and software programs to access protected health information (PHI). Multi-factor authentication, provided by RSA and Palo Alto Networks, gives organizations the security they need to comply with this rule, while providing their end users with convenient authentication options that won’t slow them down.
Similarly, PCI DSS directs organizations that process, store or transmit credit card information to maintain a secure environment to protect cardholders against the misuse of their personal information. Furthermore, PCI DSS 3.2, which was released in 2016, requires that multi-factor authentication be used by any personnel with administrative access into environments that handle cardholder data. RSA and Palo Alto Networks together enable merchants and service providers to quickly meet this regulation by implementing the next-generation firewall as an authentication gateway—enabling multi-factor authentication for all their firewall-protected applications, without needing to update each application individually.

SAFEGUARD REMOTE ACCESS AND NEXT-GENERATION FIREWALL MANAGEMENT

Palo Alto Networks next-generation firewall integrates with RSA SecurID Access to provide federated single sign-on and strong authentication for remote users. With the integrated solution, users connecting to network resources with Palo Alto Networks GlobalProtect™ network security for endpoint clients or GlobalProtect Clientless VPN can use RSA SecurID Access for identity assurance.

Moreover, joint Palo Alto Networks and RSA customers also can prevent unauthorized access to the Palo Alto Networks next-generation firewall web management interface by enforcing a broad range of RSA SecurID Access multi-factor authentication options.

RSA identity assurance can be easily tailored to ensure that the level of access control is appropriately matched to the level of risk. Organizations have the flexibility to group firewall administrators into low, medium and high assurance levels, based on their roles and permissions. As an example, a SOC analyst with read-only privileges may only require low identity assurance, while a super admin would most certainly be at the high assurance level. Further, the RSA policy engine enables organizations to easily define what authentication methods are allowable for each of these different admin groups. With the integrated offering, administrative usernames and passwords are managed and verified by RSA rather than stored in a local database in the firewall.

ABOUT RSA

RSA, a Dell Technologies business, offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.
ABOUT PALO ALTO NETWORKS

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization’s most valuable assets. Find out more at www.paloaltonetworks.com.

RSA and the RSA logo, are registered trademarks or trademarks of Dell Technologies in the United States and other countries. © Copyright 2017 Dell Technologies. All rights reserved. Published in the USA. 11/17 Solution Brief H16832

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