RSA BUSINESS-DRIVEN SECURITY™

SECURING CUSTOM AND LEGACY APPS

Three Reasons to Add MFA at the Network Level

EXTENDING AUTHENTICATION TO LEGACY SYSTEMS AND CUSTOM APPS

Multi-factor authentication (MFA) is a powerful tool for enforcing secure access across an organization. But applying it everywhere to everything—from legacy systems and custom applications to IoT environments and isolated networks—is a tall order.

While using MFA to enable legacy and custom applications (without native support for SAML and RADIUS protocols) can involve complex point-to-point integrations, implementing MFA at the network layer is a much more straightforward process.

RSA SecurID® Access and Palo Alto Networks' next-generation firewall make it far easier and more cost-effective to extend MFA protection to critical legacy and custom applications. When you add MFA at the network level, you:

Protect against compromised credentials.

Reduce the burden on internal resources.

Strengthen firewall administration.

THREE REASONS TO ADD MFA AT THE NETWORK LEVEL

1 PROTECT AGAINST COMPROMISED CREDENTIALS

Despite being essential to day-to-day operations, legacy systems and custom apps are often inadequately secured with just usernames and passwords—leaving them vulnerable to credential-based attacks. Even one compromised credential can allow attackers to move through a network undetected, infiltrating sensitive applications and data. In contrast, network-level MFA provides increased protection to all applications.

2 REDUCE THE BURDEN ON INTERNAL RESOURCES

Deploying MFA to each of your applications can be slow and costly, requiring one-off coding for custom apps and legacy systems that are not SAML- or RADIUS-enabled. But without MFA, you leave sensitive systems and data exposed and vulnerable. Putting MFA at the network layer gives you more control over access, without the cost of a separate integration for each legacy app.

3 STRENGTHEN FIREWALL ADMINISTRATION

Any security technology is only as good as its administration safeguards—who can access the system and perform certain tasks. Compromised admin credentials can let bad actors into your network, or leave you open to insider threats. Integrate MFA at the network level, and you can use the RSA policy engine to define, manage, and verify authentication requirements based on each admin group's roles and permissions, rather than storing usernames and passwords in a local database.

SECURE ACCESS AT THE NETWORK LEVEL: INTEGRATED FIREWALL AND MFA

RSA SecurID Access integrates with Palo Alto Networks' next-generation firewall to secure legacy systems, custom apps, mainframe servers, networking equipment, SCADA systems and IoT devices from credential abuse.

RSA and Palo Alto Networks bring the benefits of MFA to custom apps and legacy systems, without custom coding. Authentication happens at the network level, before access to applications and systems is granted. The firewall acts as an authentication gateway, extending MFA protection to critical older systems—challenging access requests and thwarting the use of stolen credentials. Enforcing secure access at the network level also extends authentication to isolated networks that can't otherwise connect to identity management systems.

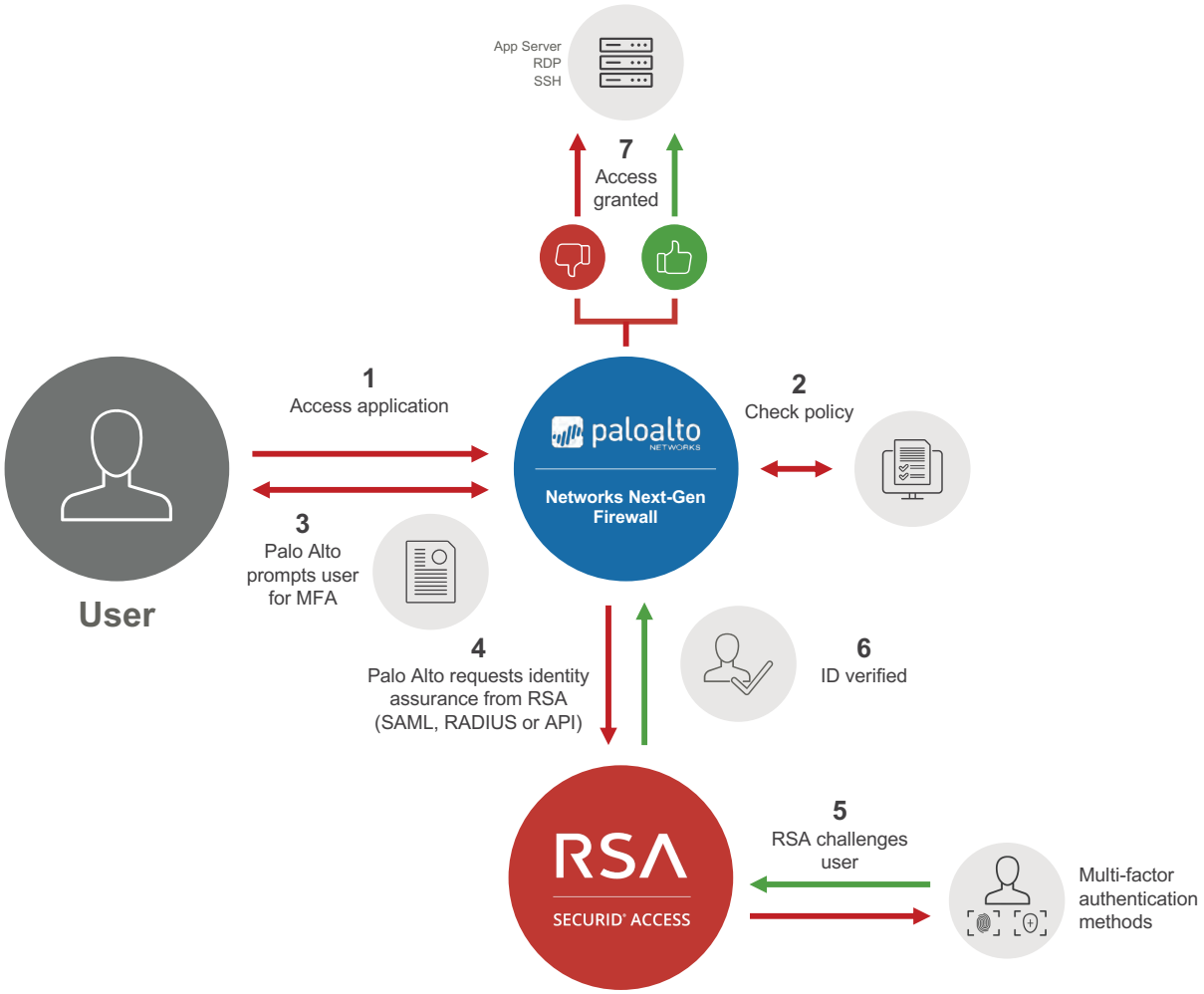
THE RESULT? YOU CAN:

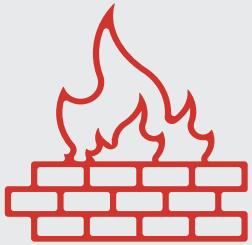
Prevent credential abuse

Quickly provision MFA without application updates

Provide role-based identity assurance to privileged users

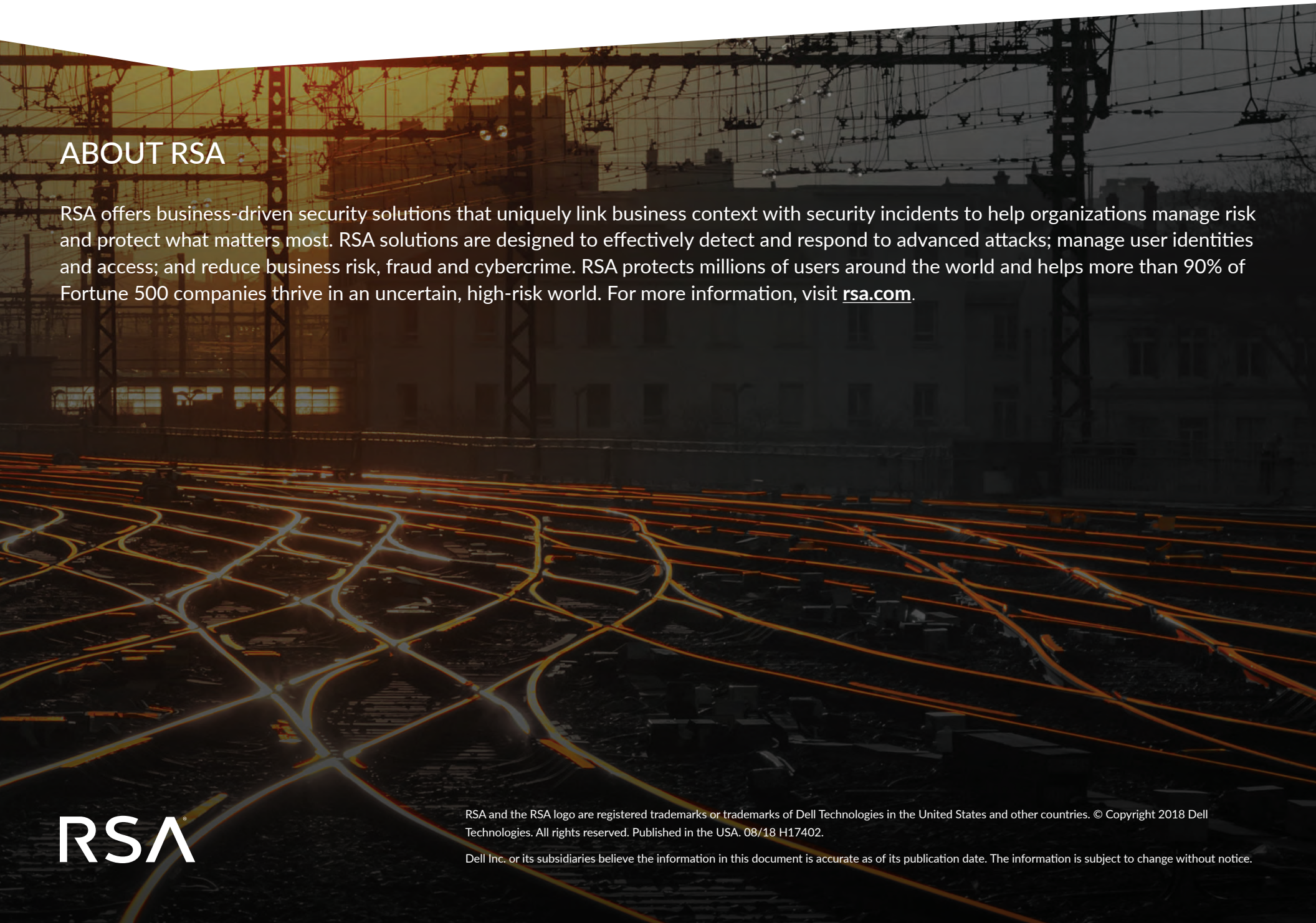
HOW IT WORKS





RSA SECURID ACCESS

RSA SecurID Access enables businesses to empower employees, partners and contractors to do more without compromising security or convenience. Embracing the security challenges of today's blended-cloud and on-premises environments, bring-your-own-device trends and mobile policies, RSA SecurID Access ensures that users are who they say they are, and that they get timely, convenient access to the applications they need—from any device, anywhere.



ABOUT RSA

RSA 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 Fortune 500 companies thrive in an uncertain, high-risk world. For more information, visit **rsa.com**.

RSA