RSA

SOLUTION BRIEF

Zero Trust

Identity and Access Management Paves the Way

As organizations pursue more digital projects, adapt to a workforce that works from anywhere and explore new possibilities in the cloud, the idea of zero trust is central to IT security today.

People have been talking about zero trust ever since Forrester introduced the term back in 2010—but adopting zero trust has never felt as urgent as it does now. As organizations pursue more digital projects, adapt to a workforce that works from anywhere and explore new possibilities in the cloud, the idea of zero trust is central to IT security today. And identity—the very notion of who can be trusted and with what—is central to zero trust. As you contemplate the role of zero trust in your organization's security strategy, keep the following fundamentals in mind.

Zero trust is about the right level of trust

The name suggests having no trust, but it is more specifically about not assuming trust unless there is a clear basis for trust—even inside an organization's network perimeter. In that sense, zero trust means establishing the right level of trust, whether in a user or a device, before allowing access to the organization's resources. The level of trust required will differ depending on who or what wants to be trusted with access, what they want access to and other factors—all of which will change as the access environment and context change.

Zero trust is an ongoing endeavor

Zero trust isn't a technology or a product; it's a mindset. Employing the principles of zero trust is therefore an ongoing endeavor, not a one-and-done deployment. Zero trust is about thinking of trust as something to be established continuously, through a process of dynamic decision-making that is constantly informed by changing context and risk.

Zero trust is in the details (defined by NIST)

NIST has defined seven tenets of zero trust as part of its zero trust architecture. Adhering to these tenets requires attention to a multitude of detailed tasks in the service of key goals: securing all communications regardless of location, granting access on a per-session basis and determining access by dynamic policy. Multiple

components of identity and access management—including a policy engine, policy administrator and policy enforcement informed by data access policy—are essential to realizing these goals.

RSA: Assembling key components of zero trust

RSA offers the requisite identity and access management capabilities needed to address NIST's tenets of zero trust, with:

- **Role- and attribute-based access**, conditional access and risk-based analytics—all fundamental to establishing a policy engine and policy decision point as required by NIST
- **The ability to act as policy administrator**, with a range of authentication methods to determine access when requested at the policy enforcement point
- **Governance and lifecycle capabilities** that provide the foundation for governance-focused and visibility-driven authorization of access to resources
- **Integration with identity systems** such as Microsoft Active Directory (AD) and cloud-based Azure AD and Amazon Web Services (AWS) AD to integrate identities with the policies, administration and methods required by a zero trust architecture

Learn more about how RSA addresses the IAM challenges zero trust presents, with comprehensive capabilities from authentication to identity governance and lifecycle.

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.