RSA® VIA

The first Smart Identity solution that protects from endpoint to cloud

IT is struggling to keep pace with new business realities – more people, more devices, and more data in more places. Each one of these requirements adds more risk to the system. And with 76% of breaches exploiting weak or stolen credentials1 – it is clear that identity is a major attack vector.

But traditional Identity and Access Management (IAM) systems that are meant to address these risks are letting users and businesses down. They fail to keep up with the constant flow of new users – employees, customers and partners. They can't be extended to new mobile, web and SaaS applications that the business wants to run. They don't allow users to interact with devices and information the way they need to get the job done. The biggest issue? These systems use static rules to manage a dynamic environment, leaving businesses profoundly at risk.

Many IT organizations respond by buying point IAM products that solve specific problems, but this piecemeal approach creates silos of rules and information that hamper consistent control and limit visibility.

The outcome? Productivity slows and users are frustrated as IT struggles to keep pace with new business demands. New employees are not on-boarded properly, access requests get lost or delayed, and both users and business units start taking matters into their own hands, triggering "bad habits" like Shadow IT. Perhaps that is why nearly half of all employees in an IT survey admit to bypassing security regulations in order to get their job done.ii

All of this leaves organizations profoundly at risk – driving employees and business units to clamor for something better.

RSA® Via: a smarter way to secure today’s extended enterprises

RSA Via is different. It is the first Smart Identity solution that helps enterprises protect identities from the endpoint to the cloud.

Unlike today’s solutions:

- **RSA Via relies on context, not just static rules**, so it can adapt quickly to constant environmental changes
- **RSA Via is business-driven**, so informed decisions keep it in lock-step with the business as it evolves
- **RSA Via enables comprehensive visibility** across traditional silos, providing greater insight into how users and information interact
- **RSA Via delivers consumer level usability**, making lives easier for end users while enabling the business

RSA Via is a set of SaaS and software solutions that work together to protect the entire identity and access lifecycle. It features a governance-driven approach to ensure consistency in access controls, regardless of the user’s location, device or where the resources reside. RSA Via ensures continuous compliance with changing rules and regulations without rendering current IAM investments obsolete.

KEY BENEFITS

Because it’s smart, RSA Via:

- **Streamlines** access control, enabling companies to embrace cloud-based applications without sacrificing security
- **Simplifies** how user access is governed across the enterprise, making it possible to achieve sustainable compliance
- **Shrinks** identity as an attack vector by coordinating access management, governance and lifecycle segments into an integrated solution
- **Reduces** friction between security owners and business users, leading to fewer instances of Shadow IT
- **Automates** how user access is requested, approved and delivered
- **Extends** access protection to web, mobile and SaaS applications, enhancing the value of your current security technology investments
RSA Via offers three key benefits:

**Shuts Down Rogue Access**

*RSA Via transforms traditional access security, by integrating separate identity and access management silos, with full visibility and control over user identities and activities. The result, IT can now:*

- Deliver secure access for all users, through flexible strong authentication methods.
- Track unusual activity that may indicate stolen credentials or an insider threat.
- Apply integrated, end-to-end access security across diverse systems and users.
- Confidently know who has access to what and if the access is appropriate and compliant.

**Removes Access Barriers so you can say “Yes” to the Business**

*RSA Via helps boost user and business productivity while substantially enhancing enforcement of appropriate access:*

- Mobile employees get simpler authentication and single sign-on. RSA Via eliminates confusing multiple passwords and authentication interfaces.
- IT eliminates resistance between users, IT and compliance, and - with integration to hundreds of applications - it removes business barriers that can trigger departmental Shadow IT initiatives.
- With business-driven access reviews and access requests, you’ll remove a key barrier to increased productivity while ensuring that appropriate access is enforced.

**Achieves Compliance Without Chaos**

*RSA Via’s centralized, automated processes help you:*

- Establish strong compliance processes to assess identity policy and controls violations and manage remediation.
- Define and enforce access policies, including segregation-of-duties policies.
- Streamline and document compliance processes with robust identity controls.
- Respond to compliance gaps, reduce cost and limit exposure to risk.

**RSA VIA OFFERINGS**

**RSA Via Access**

*Enables secure and convenient user access*

RSA Via Access delivers secure and convenient access to any application, from any location, on any device. Companies use RSA Via Access to regain control of a disrupted perimeter with strong, secure access and single sign-on to the leading Web and SaaS applications, native mobile apps and non-standard, cloud-based or legacy web applications. Administrators apply consistent and centrally enforced contextual access policies to efficiently configure access for users based on the business areas they operate in, application sensitivity, session and network info, and device type.

With RSA Via Access, organizations can:

- **Apply the same highly secure access levels** for SaaS and mobile apps that you already provide for on-premises applications.
- **Confidently access SaaS applications from any device** located inside or outside your network, while sensitive user credentials stay safe on-premises.
- **Speed user access to applications** with a frictionless user experience.
- Provide **user friendly step-up authentication** options from the user’s own device.
- **Govern access using context sensitivity policies** that look at application type, location of user and more
RSA Via Lifecycle
Simplifies and automates the access request process

RSA Via Lifecycle simplifies and automates how access is requested, approved and delivered. RSA Via Lifecycle combines a business-friendly interface for access request and approval with an innovative approach to provisioning user access changes automatically across all target systems. RSA Via Lifecycle can be layered on top of existing provisioning systems, extending their value.

With RSA Via Lifecycle, organizations can:

- Provide a business-relevant, easy-to-use service for requesting and approving access.
- Execute user access changes rapidly and reliably, across all key applications – whether on premise or SaaS – without manual effort.
- Orchestrate the entire access request, approval, and provisioning process.
- Enforce policies and ensure sustainable access compliance through preventative controls, enforced at the time of access request.
- Efficiently onboard or transfer users, ensuring that users quickly obtain appropriate access through suggested entitlements based on similar users’ attributes and job roles.
- Connect quickly to commercial or custom applications via configuration-based adapters, avoiding long and expensive deployment projects.
- Leverage existing provisioning systems instead of ripping and replacing them.

RSA Via Governance
Centrally manages and governs access

RSA Via Governance simplifies how user access is governed across the enterprise, making it possible to achieve sustainable compliance by fully automating the monitoring, reporting, certification and remediation of user entitlements.

With RSA Via Governance, organizations can:

- Gain enterprise-wide visibility into all user access privileges.
- Identify orphan user accounts and remEDIATE inappropriate user access.
- Engage the line of business for user access review and certification processes.
- Manage and audit all entitlement changes through integration with enterprise-wide access fulfillment and enforcement systems.
- Implement security and compliance controls such as segregation of duties and ensure that policy and control objectives have been met to provide evidence of compliance.
- Deploy efficient and consistent processes around lifecycle events.

RSA SecurID™
World-leading two-factor authentication

More than 25,000 organizations depend on RSA SecurID to protect over 400 on-premises resources including VPNs, firewalls, virtual desktops and Windows or Linux servers. Now, by operating RSA Via Access and RSA SecurID together, companies can seamlessly use their SecurID authenticators to protect cloud-based SaaS applications like Workday, Office 365, Google Apps, Salesforce and Box.

RSA Adaptive Authentication
Balance security and usability for strong authentication

RSA Adaptive Authentication is a risk-based authentication and fraud detection platform that protects users accessing web sites and portals. Available as a SaaS or on-premise solution, Adaptive Authentication combines strong authentication, emerging threat protection, flexibility and confidence in one product to address consumer identity assurance.

RSA Via – NAVIGATING TODAY’S CHANGING IT ENVIRONMENT

RSA Via is the first Smart Identity solution that protects from endpoint to cloud—regardless of where users are located and where the resources reside. It ensures that your company is constantly in compliance with changing rules and regulations.
RSA Via Access, RSA Via Lifecycle and RSA Via Governance create a governance-driven approach to access, regardless of the user’s location, device or where the resources reside. Their shared intelligence forms a coordinated response to combat threats and enable continuous compliance, while allowing users to get on with their work.

---
