IDENTITY: A KEY ELEMENT OF BUSINESS-DRIVEN SECURITY

Identity is replacing perimeter as the primary defensive frontline

OVERVIEW

Organizations have been grappling with identity and access management since the early days of computing in the 1960s. Each year, identities and network perimeters have become more complex and more difficult to manage.

Attackers have noticed. Today, abuse of identity is a key component in virtually every sophisticated cyber attack. Data breaches that involve weak, default, or stolen passwords far outpace breaches caused by malware.

Many organizations are beginning to recognize that they are unable to answer basic questions about the user access activities of highly-dynamic user populations at the speed required to safely conduct business. For instance:

• Who is accessing what? And are users who they say they are?
• Are we meeting the fundamental authentication needs of our employees, third-party contractors, customers, and other users for convenient and secure access to any device, anywhere, at any time?
• What types of transactions and communication are occurring?
• Do we have strong assurances that only the right people have access through strong authentication, strong access management, and identity governance?

In other words, organizations are unable to put security information into business context fast enough to determine the impact on business continuity, personal data, intellectual property, and reputational damage. At RSA, we call this the "Gap of Grief". To keep up, organizations are looking for ways to gain assurance that users are indeed who they say they are and that they have only the access levels required to do what they need to do.

The solution is Business-Driven Security™, an approach that allows an organization to comprehensively and rapidly link security details with business context so it can effectively respond and protect what matters most.

THE ALWAYS-ON BUSINESS

The conversation about balancing convenience with security is not new. Both internal and external users expect to be able to work anywhere, connect to all of the applications and data they need, from any device. After all, that’s how their personal technologies work; they expect their work world to operate the same way. Security and IT teams are being called on to accommodate users where they are.

Convenience isn’t a luxury; it’s a necessity. Efficiency is a competitive advantage. Organizations that keep access simple also increase user focus on core business objectives.

Therefore, organizations have to provide convenient access without sacrificing security. Repeated authentication prompts, complex passwords, frequent password changes, and other access and identity hurdles create friction in the user experience, and a temptation for users to bypass security controls.

At the same time, effectively managing access to data and applications is more complicated with the expansion of cloud and mobile technologies and increasing business use of Internet-of-Things (IoT) devices. The data and applications being accessed are no longer contained within a clear network perimeter with a static set of users.
Organizations are:

- Managing thousands – sometimes millions – of identities for both internal and external users.
- Managing access to systems, applications, and data that exist both on-premises and in the cloud – or somewhere in between.
- Monitoring access for users from all locations and from all types of devices.
- Managing the identities of connected things just like identities for users, through accounts with assigned access.

**GOODBYE, PERIMETER; HELLO, WORLD**

Attackers see an organization’s challenges as weaknesses that can be exploited. With 63% of confirmed data breaches involving weak, default, or stolen passwords, (see Data Breach Investigations Report 2016, Verizon) identity has become today’s most consequential attack vector.

Today’s threat landscape is more sophisticated and targeted than ever before:

- **The perimeter is disrupted and traditional security controls are ineffective.** To facilitate the needs of business, an organization’s perimeter is designed with authorized pathways through which hundreds of terabytes of an organization’s data travel daily. This data may be externally hosted in cloud applications, accessed over wireless carrier networks or public WiFi, sent via email to customers and other external parties, or accessed from personal devices. In addition, the user population today is rich with third parties including consultants, customers, vendors, suppliers, audit teams, contractors, and connected devices that are given identities, each with some level of access to the organization’s data and systems. Tucked into a large volume of legitimate communication, attacks can appear to be normal traffic and remain undetected by perimeter controls.

- **Silos of identity are creating blind spots** as user access is managed at the application or system level by the respective applications (e.g. solutions from Salesforce, Marketo,) rather than being managed centrally. This lack of transparency across all systems together makes it harder for IT to effectively mitigate identity and access risks.

- **Users manage many logins.** With an ever-increasing number of applications and a shift of operational functions to the cloud, a user may have dozens of independently-managed identities, any of which can be compromised and impersonated without IT even knowing. They often force a security risk by reusing usernames and passwords across these identities.

- **Business managers often perform ineffective, check-the-box access reviews.** Regulations for publicly-traded, healthcare, financial services, and other organizations require managers to periodically review the access of subordinates. Business managers, not IT managers, are accountable for reviewing access for subordinate business users. Once seen as an IT function, identity management is transitioning to a business function since the people who manage employees are best suited to understand their access needs. However, these reviews can become “check-the-box” exercises for managers.

**INEFFECTIVE TRADITIONAL CONTROLS**

Organizations that have not aligned identity strategies to both business priorities and a modern infrastructure are doing so at their own peril. Consider this:

- Static passwords can potentially be harvested from individual devices or central password repositories.
- Security teams are aware of incidents where attackers used an algorithm to compromise a user’s single sign-on credentials and gained access to all of a user’s work accounts.
- Two-factor authentication must evolve from token-based authentication to be more risk- and context-aware. This will not only tighten security but also eliminate the friction for users as they seek convenient access.
- Authentication methods must conveniently accommodate the users and their unique environments.
- The average employee turnover rate across industries is 15%. (See 2013 Turnover Rates by Industry, Compensation Force.) Organizations must smoothly on board and off ramp users, leveraging automation wherever possible, to meet productivity targets and eliminate possible security vulnerabilities.
• Identity governance and compliance efforts are becoming less effective at mitigating true risks because the business leaders who review and approve access are overloaded and subject to “check-the-box” mentality.

**SIGNS THAT AN ORGANIZATION’S APPROACH TO IAM IS NOT WORKING**

IT security and operations teams are not equipped to deliver what’s needed today:

• **Business growth is hindered.** Lack of comprehensive identity and access assurance could result in missed revenue targets and complaints from business leaders. Without Business-Driven IAM, organizations cannot take advantage of strategies that simplify mobile access and facilitate integration of third-parties on the network.

• **Users are frustrated** and looking for workarounds to security measures in order to access the resources they need to do their jobs or to transact business. Many current commercially-available authentication technologies intrude on the user experience, are difficult to manage, and depend upon users to voluntarily comply.

• **IT is losing control.** Cloud applications have made it more difficult for IT to have comprehensive visibility of all access points and a lot easier for departments to implement shadow IT—solutions outside the purview of IT. These Shadow IT solutions create blind spots and weaken the security team’s ability to manage access.

• **Organizations are unprepared for emerging and evolving regulations.** For instance, the European Union’s General Data Protection Regulation will require organizations to consolidate security tools; they must protect data in the same way regardless of how it is accessed. Enforcement begins in 2018.

**BUSINESS-DRIVEN IAM**

Realizing that there is no longer such a thing as a defensible perimeter, many organizations are considering identity the new perimeter. This is the main business case for Business-Driven IAM.

As an additional benefit, Business-Driven IAM transforms IT from a business obstacle to a business enabler that fuels growth. In a paradigm where IT can no longer “just say no” to the business, IT must be able to meet business demands without sacrificing security or compliance. The business side of an organization depends on IT to support growth and innovation.

Business-Driven IAM is needed to:

• **Help organizations grow.** Lines of Business can easily and securely deploy applications that help grow the business with minimal IT support, eliminating the use of Shadow IT. Business-Driven IAM is scalable and can accommodate rapid growth.

• **Make access easier.** Business-Driven IAM is seamless, frictionless, and can be almost invisible to the authorized user. End users are secure without feeling it is a chore.

• **Keep pace with the business changes.** Business-Driven IAM is more intelligent, proactive, and continuous. Security teams have to meet business expectations for speed, opening up access to enterprise resources while at the same time controlling that access. Business-Driven IAM makes risk relevant to access and enables the business to move fast with security controls working in the background to make sure everything stays safe.

• **Achieve continuous compliance with regulations and internal policies.** Business-Driven IAM achieves sustainable compliance by fully automating the monitoring, reporting, certification, and remediation of user entitlements.

• **Strengthen and extend access protection** across traditional, web, mobile, and SaaS applications.

• **Link security details with business context** to protect what matters most – whether access or data.

• **Replace fear with confidence.** Business-Driven IAM gives the business the assurance that access is being delivered appropriately, that its users are who they say they are, and that users only have access to what they need to do their jobs, and nothing more. No organization is going to keep bad guys out with a complex password and challenge questions, but they can stay secure with behavior analytics and new authentication methods that are convenient yet secure. The more confident an organization is about the identity of its users, the more fearless it can be in deploying applications and adding new users.
**RSA’S APPROACH TO IAM**

The RSA SecurID® Suite is a comprehensive IAM suite that accelerates business while mitigating risk.

With the RSA SecurID Suite, organizations can improve levels of identity and access assurance without increasing the burden of security on the business and users. The RSA SecurID Suite provides full visibility across all applications and users and brings it together for a holistic view of identity with actionable insights that reduce risk. This holistic visibility also speeds threat detection and response by allowing security teams to better identify and track the behavior of potentially compromised identities.

The RSA SecurID Suite weaves risk information and context into the fabric of the enterprise’s identity infrastructure to help leaders assess, automate, streamline, and prioritize access delivery and identity risk mitigation activities, all in real-time.

**CONCLUSION**

No doubt, IT teams have a tough job securing organizations that have made their networks accessible to a plethora of mobile devices, cloud tools, and third-party users. The traditional network perimeter is gone, and user identities now form the modern perimeter. Meanwhile, many organizations are afflicted with access blind spots, for instance from isolated islands of identity created when identities are managed at the application or system level instead of centrally.

The solution to these challenges is Business-Driven IAM, an approach that links security details and strategy to business priorities. RSA’s Business-Driven IAM solution is the RSA SecurID Suite.

With the RSA SecurID Suite, there is no tradeoff of convenience for security. Exceptional IAM is delivered in a business-friendly manner through a frictionless user experience, business-friendly access review tools, and other features that reduce the level of technical knowledge required by security teams and business leaders.

The RSA SecurID Suite delivers both identity assurance and access assurance.

From an identity governance perspective, the RSA SecurID Suite allows the organization to establish that the person logging in is a legitimate user. It is preventative and provides insight about where organizations are at risk of an attack. For instance, it prompts a manager for review and authorization when access may be inappropriate for a role or when the user appears to have a conflict of interest.

From an access perspective, the RSA SecurID Suite permits the organization to ensure that users have the appropriate level of access for their roles. With access control at the user level, organizations can enjoy comprehensive visibility into all identity access points. The RSA SecurID Suite also provides effective authentication and, if a user’s behavior somehow introduces risk, allows the organization to require stepped up authentication. The added perspective of contextual awareness of the user’s behavior converts security information into business context in real-time. RSA SecurID also provides valuable data about user access to security staff during the reconstruction of an attack.

With Business-Driven IAM, organizations can reduce risk, prioritize IAM efforts, and enhance compliance by ensuring that all areas of IAM work together—while at the same time delivering a convenient user experience and accelerating business.
BUSINESS-DRIVEN SECURITY SOLUTIONS FROM RSA

RSA is a leader in advanced cybersecurity solutions delivering Business-Driven Security™ so organizations of all sizes can take command of their evolving security posture in this uncertain, high-risk world.

Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

More specifically, RSA is the ONLY company that enables the three most critical elements of a sound security strategy: rapid response and detection, control at the user access level, and business risk management. No other company does this.

The RSA® SecurID® Suite enables organizations of all sizes to accelerate their business while minimizing identity risk and delivering convenient and secure access to the modern workforce. The RSA SecurID Suite leverages risk analytics and context-based awareness to ensure the right individuals have the right access, from anywhere and any device. The RSA SecurID Suite is comprised of:

- **RSA SecurID Access** is an innovative identity assurance solution that ensures that your organization provides the right individuals appropriate access, conveniently and securely, from anywhere to anything, from any device. It enables organizations to consistently and centrally enforce dynamic risk-driven access policies based on context to balance convenience with strong security.

- **RSA Identity Governance and Lifecycle** provides organizations the ability to act with insight to reduce identity-based risks and drive informed security decisions. RSA Identity Governance and Lifecycle simplifies how access is governed and streamlines access requests and fulfillment to deliver continuous assurance of compliance by automating the management of user entitlements throughout the user’s lifecycle.

The RSA® NetWitness® Suite is a threat detection and response platform that allows security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. By aligning business context to security risks, RSA NetWitness Suite provides the most advanced technology to analyze, prioritize, and investigate threats making security analysts more effective and efficient.

The RSA® Archer® Suite empowers organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform.

The RSA® Fraud & Risk Intelligence Suite is a centralized fraud prevention platform that uniquely blends continuous monitoring, risk-based authentication and fraud intelligence to deliver rapid insight into cybercrime attacks. Leveraging data from your business and other anti-fraud tools, the RSA Fraud & Risk Intelligence Suite enables organizations to greatly improve detection and response to fraud incidents across digital channels without impacting the customer experience.

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 the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.