RSA

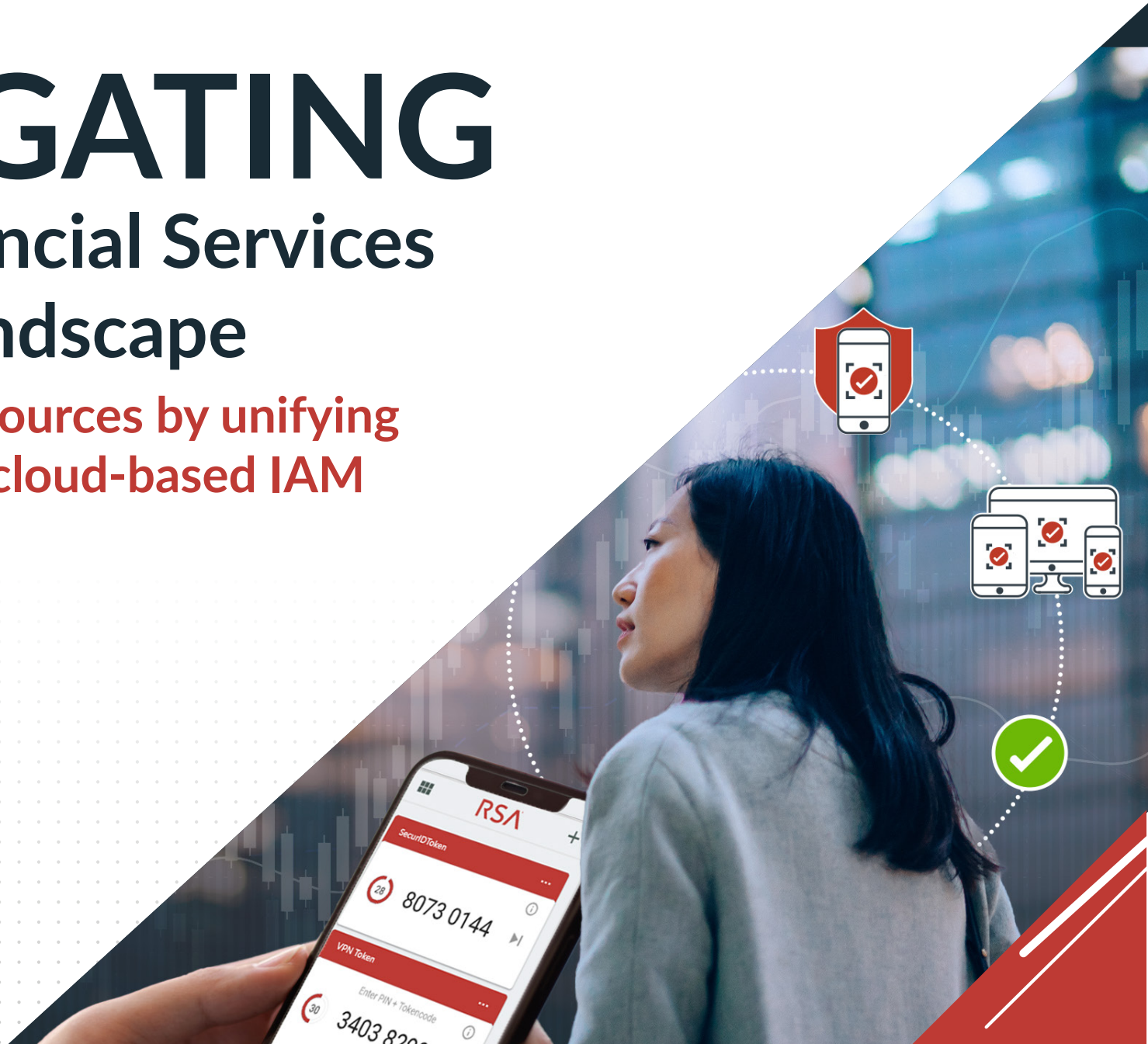
RSA.com

NAVIGATING

A New Financial Services Security Landscape

Save time and resources by unifying on-premises and cloud-based IAM

EBOOK | June 2022



The Future of Identity and Access Management

Securing your assets no matter the location

Key lessons from the 2020s: Organizations that adapt, survive. Organizations that adapt quickly, thrive. Nowhere is this truer than in financial services.

From a rapidly evolving workforce, to ever-changing regulations and mounting pressure to scale, it's more important than ever for financial services organizations to prioritize operational efficiency and flexibility. But that's easier said than done. How can financial services organizations deliver a seamless experience, navigate compliance hurdles, scale efficiently—and protect key resources?

We know that a truly hybrid future—one where workforces are split between on-site and remote workers—is coming for most organizations. We know that this change will not eliminate the need for on-premises security. But it will expand the attack surface that organizations need to protect. And there will be a lot to protect.

A 2020 McKinsey & Company study found that the financial services industry has the highest potential for remote work of any sector.[1] This change is a potential boon for organizations that embrace this shift. But every new remote employee means another new user and another brand-new access point to protect.

Forcing employees back into the office is a non-starter. Providing a remote work option has become table stakes for employers. Flexibility is now a recruiting tool. Consequently, leveraging cloud applications is a "must" to maintain efficiency. When considering the desires of the financial services employee, a recent PwC survey determined that 40% of financial services employees want a mobile experience for work applications and data. And with 56% of organizations already maintaining more than half of their business in the cloud, it's clear that there needs to be a substantial investment in cloud applications and the cloud-based identity and access management (IAM) that protects it.[2]

40%

of financial services employees want a mobile experience for work applications and data

50%

of organizations maintain more than half of their business in the cloud[2]

The Present

On-premises and cloud security coexistence

Background

Two-factor authentication is not a new concept for the financial services industry. In fact, it's been a pillar of enterprise security for more than 30 years. Hardware tokens improved banking security by providing the financial services organization the two-factor authentication needed to move on from one-time passwords.

Today, tokens deliver stronger security through multi-factor authentication. By pairing the user PIN with a unique code that changes every 60 seconds, organizations can eliminate password-based authentication.

Since their invention, tokens have been the bedrock of on-premises authentication. And as organizations' security needs have changed, authentication has evolved from hardware to software tokens that can be installed on computers and phones.

This evolution set the stage for cloud protection.

The cloud changed everything

Software as a service (SaaS) provided organizations with major advantages: It reduced total cost of ownership, built resilience, and allowed global collaboration. But as financial organizations and other businesses moved more resources to the cloud, they effectively split their authentication needs between the on-premises resources they already had and the new SaaS applications that were becoming essential.

Security-ready financial services organizations must be able to answer the following questions:

- Can we integrate IAM across all our systems?
- Do we have both cloud-based and on-premises security solutions?
- Are we partnered with a security vendor who can help with a seamless adoption?
- Can we gain visibility and control over who has access to what?

And perhaps most importantly:

- Can we scale responsibly and budget accordingly?

This shift created significant issues: Suddenly, organizations had multiple vendors providing the same service in different locations. This resulted in weaker security, more friction on users, and higher costs. It was an expensive and complex system—demanding more resources, costing more money, and providing less value.

And the situation is further complicated for financial services organizations, which must navigate multiple federal and state regulations and comply with evolving laws (like the Gramm-Leach Bliley Act, Sarbanes-Oxley Act, and the Consumer Protection Act). Moreover, as margins get squeezed on traditional banking products, banking organizations are expanding into other products (e.g., insurance), adding even more regulatory hurdles. A strong IAM solution will help financial services organizations remain in compliance with the regulations protecting users' personal information and other data.

Though it is easy to see how we got here, this divergence between on-premises, cloud identity, and access management providers ultimately means that organizations may pay more for weaker security.

The Rules Are Different Now

Changes in business mean changes in security

Due to COVID-19, there has been a major shift in the way business is conducted, and the financial services industry is no exception. As operations have shifted to remote work, a new normal has emerged and changed our perception of the traditional brick-and-mortar office. Though customers will always want a physical location to do their banking, customers, employees, and businesses all recognize the benefits—if not the necessity—of hybrid offices.

These new needs demand new security.

Change is coming

In the wake of the in-office vs. remote work debate, financial services organizations and their employees will need to have a conversation. According to a December 2020 survey by PwC, only 20% of employees will want to be in the office three or more days each week once COVID-19 is no longer a major concern to them and their families.

This is compared to the 70% of employers who believe employees should be at their desks a minimum of three days per week to maintain a distinctive culture. However, in the wake of the Great Resignation, it's clear that current and prospective employees view remote work as an important benefit. The strain of this hybrid model falls on the shoulders of managers who must lead different sets of employees.

No matter your organizational decision, it's clear that remote work will become more prevalent in the coming decade, whether as a perk of the job or the cost of doing business. If your organization wonders whether it needs to adapt now, consider how drastically the industry changed overnight.

20%

of employees want to be in the office three or more days each week once COVID-19 is no longer a concern

70%

of employers believe employees should be at their desks a minimum of three days per week[2]

4.5M

American workers left their jobs voluntarily in November 2021, a 20-year high[3]

It's Simple. Really.

The Future. Now.

There is no better way to prepare for the future of IAM than implementing seamless security practices. For some, this will mean adding cloud-based security on top of their on-premises solutions. For others, it will mean unifying their cloud-based and on-premises vendors to reduce costs and improve efficiency. Either way, the choice is clear: If organizations want to be future-ready, they must be willing to adjust their strategy now—and not when it's already too late.

Understandably, there will be organizations resistant to adopting a new IAM solution. Typical concerns revolve around cost, ease of adoption, and choice of vendor. But keep this in mind: according to a recent IBM study, the cost of a data breach in 2021 was $4.24 million, a 10% rise over two years—additionally, the cost was $1.07 million more for breaches involving remote work.[4]

Are you in focus?

In McKinsey & Company's Insights on Financial Services, CEOs asked their leadership: Does our IT project portfolio reflect our strategic focus? In many cases, that answer is "no." But in an industry as competitive as financial services, speed and efficiency are at a premium. Companies want to grow and scale as quickly as possible. If your company needs to constantly backtrack to secure yourself ad hoc against attacks from hackers or investigate breaches, forward progress will be a challenge.[5]

Additionally, in a world where everything is digitally transforming, your organization needs to ask whether it's doing enough to simplify the digital experience of your customer—and this is not as simple as evaluating your mobile app or interface.

Customers want assurance that identities are verified when they access company resources, and end-users demand intuitive digital experiences to work productively.

Comprehensive IAM solutions use contextual information—including who is requesting access, from where, and from what device—and machine learning to create advanced risk engines and behavioral profiling that determine standards of identity assurance, minimize risk, and elevate security against threat actors.

What Should Your Considerations Be?

7 key factors

When deciding whether to adopt a new IAM strategy, there are seven key factors your organization must consider. That said, your implementation must meet the standards previously discussed for future readiness, balancing your current needs as you forecast forward.

1 **A Hybrid Approach** – As cloud adoption expands the attack surface, generates more threats, and increases the impact of breaches, businesses must find new ways to secure their resources. The goal is to find an approach that will protect both on-premises and cloud resources.

2 **Easy-to-Use Authentication Methods** – Not all authentication methods are equal. The goal for your organization should be to adopt a flexible and convenient solution across as many platforms as are available.

3 **Conditional Access and Threat-Aware Authentication** – It may seem clichéd, but the truth of IAM is that every user is different. Any solution you deploy must be able to provide superior detection of abnormal users, devices, and network activities.

4 **24/7 Authentication Availability and Protection** – Gone are the days when your organization could employ a solution without failover capabilities. In the event of a cloud outage, you must provide constant protection. If not, you risk not only your organizational health and reputation but also the safety of your users.

5 **Offline Authentication for Non-Network Users** – Depending on how your additional network security functions (whether it be SASE or otherwise), your users may not always be connected to a network. However, this connection does not change the needs of your organization: Users must have access availability regardless of whether they are online.

6 **One Point of Contact for all Solutions** – As cloud adoption increases, your vendor list can become extensive. You can simplify and fortify your IAM security by choosing one vendor who can offer on-premises and cloud coverage. This will not only streamline the user experience and solution management process, but also simplify the procurement process, saving your organization valuable time.

7 **Continuous Innovations and Direct Upgrade Features** – In order for a solution to be future-proof, it needs to account for the future. Any cloud-based solution you adopt must enable next-generation capabilities, eliminate time-consuming multi-step serial upgrade processes, and reduce your organization's total cost of ownership.

Security Starts with Identity

RSA has always been at the forefront of IAM security, and that hasn't changed. Our cloud-based IAM solutions are built on the same token technology we pioneered decades ago. Today, we offer best-in-class identity solutions on-premises and in the cloud. That means you can rely on a single trusted vendor for all your identity needs, wherever you are on your cloud journey.

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

1. McKinsey Global Institute, "What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries." https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries

2. PwC, "Hybrid work comes to financial services: The when, why and how often of the physical office." https://www.pwc.com/us/en/industries/financial-services/library/hybrid-work.html

3. New York Times, "Department of Labor. You Quit. I Quit. We All Quit. And It's Not a Coincidence. Why the decision to leave a job can be contagious." https://www.nytimes.com/2022/01/21/business/quitting-contagious.html

4. IBM, "Cost of a Data Breach Report 2021." https://www.ibm.com/security/data-breach

5. McKinsey, "How US mid-cap banks can solve the conundrum of scale in technology." https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/how-us-mid-cap-banks-can-solve-the-conundrum-of-scale-in-technology

OWN YOUR IDENTITY.