THE JUICE IS WORTH THE SQUEEZE

Saving time and resources by unifying your on-prem and cloud-based IAM

E-BOOK

SecurID™

TABLE OF CONTENTS

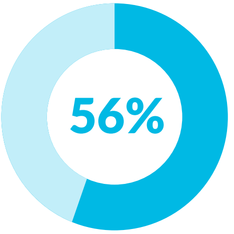
The Future of Identity Access Management

Securing Your Assets No Matter The Location

As we continue into the 2020s, one thing is for certain: As the percentage of remote workers continues to grow, so too will new security threats. However, successful financial service organizations will be those who can prioritize flexibility and efficiency. So how do organizations balance these benefits while simultaneously protecting key resources?

The first step is to accept the fundamental facts. 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 will not eliminate the need for on-premise security, but it will expand the security perimeter 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 over any other industry. This is a potential boon for those organizations who embrace this shift. But every new remote employee means another new user and another brand-new access point to be protected. 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-based identity access management.



Of organizations already maintaining **more than half** of their **business in the cloud**

With these facts in mind, there are questions that financial service organizations must be able to answer if they intend to thrive in the future. Some of the key issues are:

- Can we integrate identity access management across all our systems?
- Do we have *both* a cloud-based and on-prem security solution?
- Are we partnered with a security vendor who can help us with a seamless adoption?

And perhaps most importantly:

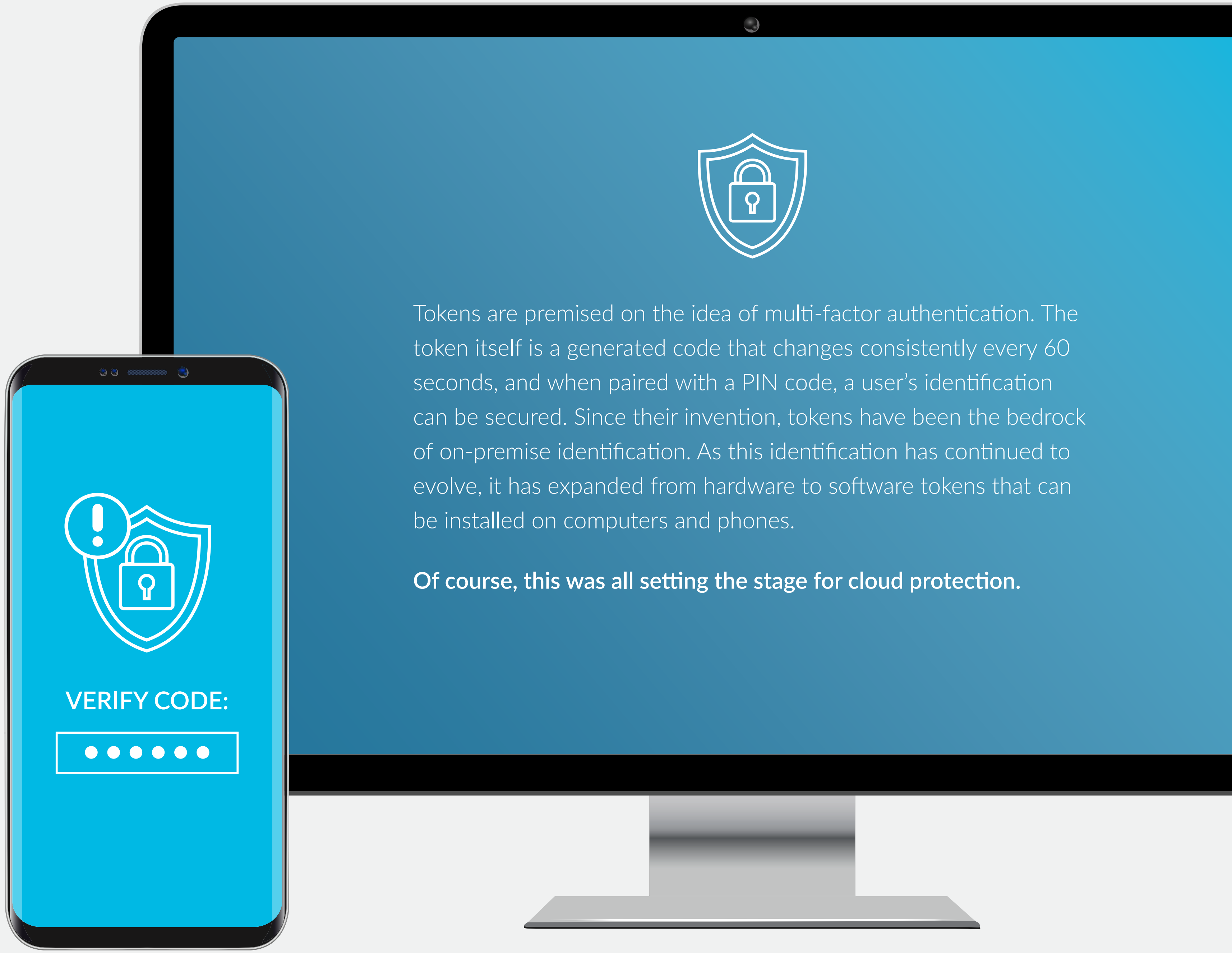
- What is the most cost-effective way to meet these needs?

The Present

On-Prem and Cloud Security Divergence

AT A GLANCE:

Two-factor identification is not a new concept for the financial service industry. In fact, it has been the pillar of financial security for more than 30 years. When banking protection first took a major step forward from one-time password identification of the 80s, it did so with two-factor identification in the form of tokens.



Tokens are premised on the idea of multi-factor authentication. The token itself is a generated code that changes consistently every 60 seconds, and when paired with a PIN code, a user's identification can be secured. Since their invention, tokens have been the bedrock of on-premise identification. As this identification has continued to evolve, it has expanded from hardware to software tokens that can be installed on computers and phones.

Of course, this was all setting the stage for cloud protection.

The divergence of two-factor authentication practices to the cloud from on-premise solutions coincided with the rise of SaaS, IaaS, and other cloud-based advantages to business. With business being split between the two, it was only natural that cloud-based vendors rose to fill the gaps in organization's cybersecurity postures.

But this shift created issues surrounding cost and implementation. Suddenly, organizations had multiple vendors for the same service operating in different locations. This resulted in increased legwork for IT and security staff, who became tasked with security and visibility across multiple platforms. This effectively created a system far more complex than it needs to be — demanding more resources than organizations need to devote.

Though it is easy to see how we got here, this divergence between on-prem and cloud security isn't an advantage to anyone: in fact, it's hurting the bottom line of countless organizations.

The Rules are Different Now

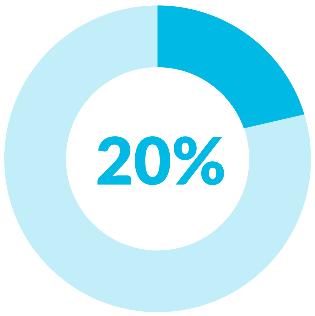
Post COVID-19, there has been a major shift in the way business is conducted, and the financial services industry is no exception. As operations shifted to remote work, the concept of the traditional brick-and-mortar office shifted with it. Of course, customers will always want a physical location to do their banking. But as more and more businesses come to terms with the needs of their employees and hybrid office benefits, the need for cloud security becomes more prevalent.

CHANGE IS COMING:

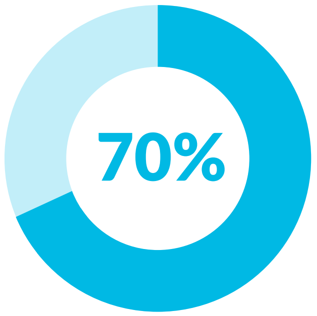
In the wake of this in-office vs remote work debate, there will be a negotiation between financial service employers and their employees. According to a December 2020 survey by PwC, only **20% of employees will want to be in the office three or more days each week** once COVID-19 is no longer a major concern to them and their family.

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, organizations are now hiring at previously unheard-of rates with candidates viewing remote work as a benefit. The strain of this hybrid model falls on the shoulders of managers who are tasked to navigate between different sets of employees.

No matter your organizational decision, it is clear 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, think about how much the industry changed overnight.



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



Of employers who believe employees should be at their desks a minimum of **three days per week**

It’s Simple, Really

The Future, Now

There is no better way to prepare for the future of identity access management than implementing to seamless security practices. For some, this will mean adding cloud-based security on top of their on-prem solutions. For others, it will mean unifying their cloud-based and on-prem vendor to reduce costs and improve efficiency. Either way, the choice is clear: If organizations want to be future-ready, they must be willing to make adjustments to their strategy now — and not when it is 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: **The cost of a data breach in 2021 cost $4.24 million, a 10% rise over two years;** additionally, the cost was **$1.07 more for breaches involving remote work.** Malicious actors aren't affected by sunk cost fallacies, nor will financial anxieties stop your organization from losing money.

ARE YOU IN FOCUS?

In another McKinsey & Company financial services insight, CEOs asked their leadership: **Does our IT project portfolio reflect our strategy 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 be as large as possible and move as quickly as they can. 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.

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

Customers want to know that they are being supported whenever and wherever they access critical accounts, and companies that cannot provide protection will stand to lose big.

What Should Your Considerations Be?

Comprehensive IAM solutions utilize machine learning and advanced risk-engines to assemble intelligence that distinguishes a user from a device. Additionally, behavioral-profiling creates a standard of identity assurance that minimizes risk and elevates security against threat-actors.

When deciding whether to adopt a new IAM strategy, there are some key factors your organization must be ready to account for. Importantly, your implementation must meet the standards previously discussed for future-readiness, which means balancing your current needs as you forecast forward.

What Should Your Considerations Be?

1 **A Hybrid Approach** – With the growing increase in security threats and breaches, organizations can no longer afford to opt-out of cloud adoption. The goal is to find an approach that encourages adoption while ensuring that modern authentication methods will protect both on-prem 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 to provide the easiest solution across as many platforms as are available.

3 **Conditional Access and Threat-Aware Authentication** – It may seem clichéd, but the truth of identity access management is that every threat is uniquely different. Any solution you employ 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 users limited their access attempts to traditional business hours. So, too, are the days when your organization could employ a solution without failover capabilities. In the event of a cloud outage, you must still provide constant protection; if not, you risk not only your organizational health 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** – The goal for your IAM security should be the same for your vendor selection: Work smarter, not harder. Vendors who can offer top-of-the-line on-prem and cloud solutions will not only streamline the user experience and implementation process, but they 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 actually account for the future.* Any cloud-based solution you adopt must enable next generation capabilities, eliminate time-consuming multi-step serial upgrade processes, and improve your organization's total cost of ownership.

SecurID Can Help

THIS IS WHAT WE DO

SecurID has always been on the forefront of IAM security protection, and that hasn't changed. The same token technology we invented is the foundation upon which cloud-based solutions are built. However, the good news is that you don't have to go to other vendors for your cloud-based needs: **SecurID offers best-in-class solutions on-prem and in the cloud.**

More than 500 global organizations and over 13,000 customers trust SecurID for their on-prem solutions — and we can help streamline your management under one identity platform. There is no aspect of IAM security we can't assist you in. **After all, we invented encryption.**

But if you're still wondering whether you should make the switch now to our cloud-based IAM solutions, consider what it will cost to not switch. Simply put: **The only way to prepare yourself against an attack is before it happens.** And there is no question that your organization will need to make the switch to the cloud; the risk of waiting will come in the form of security breaches and cyberthreats. It is impossible to quantify the number of attacks that your organization will avoid by adoption. But what is easy to quantify are the losses you'll avoid on your bottom line.