RSA

Top Trends in Identity for 2025

Incremental progress, exponential effects

January 2025

RSA.com

Table of Contents.

Executive summary: More is more.

Where were you on July 19, 2024?

With any luck, you weren't traveling. That day, a combination of a CrowdStrike update and limitations with Microsoft environments reportedly crashed 8.5 million Windows systems, delayed or cancelled 10,000 flights, and cost Fortune 500 companies more than $5 billion in direct losses. Importantly, the outage wasn't due to cybercriminals or threat actors. Instead, infrastructure simply failed—and when it did, nearly everything broke.

That one day looms large over 2025 and foreshadows what we expect to see this year in security. Not because we expect any of the particulars to reoccur, but because the overall environment really hasn't changed all that much since last July.

Organizations will largely have the same technologies and capabilities at their disposal this year as they had last year. They will continue making progress in implementing multi-factor authentication (MFA), deploying passwordless authentication, and honing their use of AI in their tech stacks. And they will continue working in hybrid environments and generating increasing numbers of machine identities. At the same time, threat actors will continue attacking passwords, using their own instances of AI in attacks, and trying to find ways to bypass MFA. Researchers will continue making incremental progress on new technologies like quantum computing, and security experts will continue preparing for threats that are ten years away.

For the most part, the same systems, capabilities, risks, and threats will play out in 2025 as they did in 2024. We don't expect a revolution in any one of those variables. Instead, we expect evolutions in each.

However, if a single software update can crash millions of computers, as it did in 2024, then evolutions will become revolutions. Even without marquee new technologies hitting the market in 2025, with interconnected systems, growing numbers of users and agents, and AI that can make decisions and generate outputs faster than any human, incremental progress will have exponential effects in 2025.

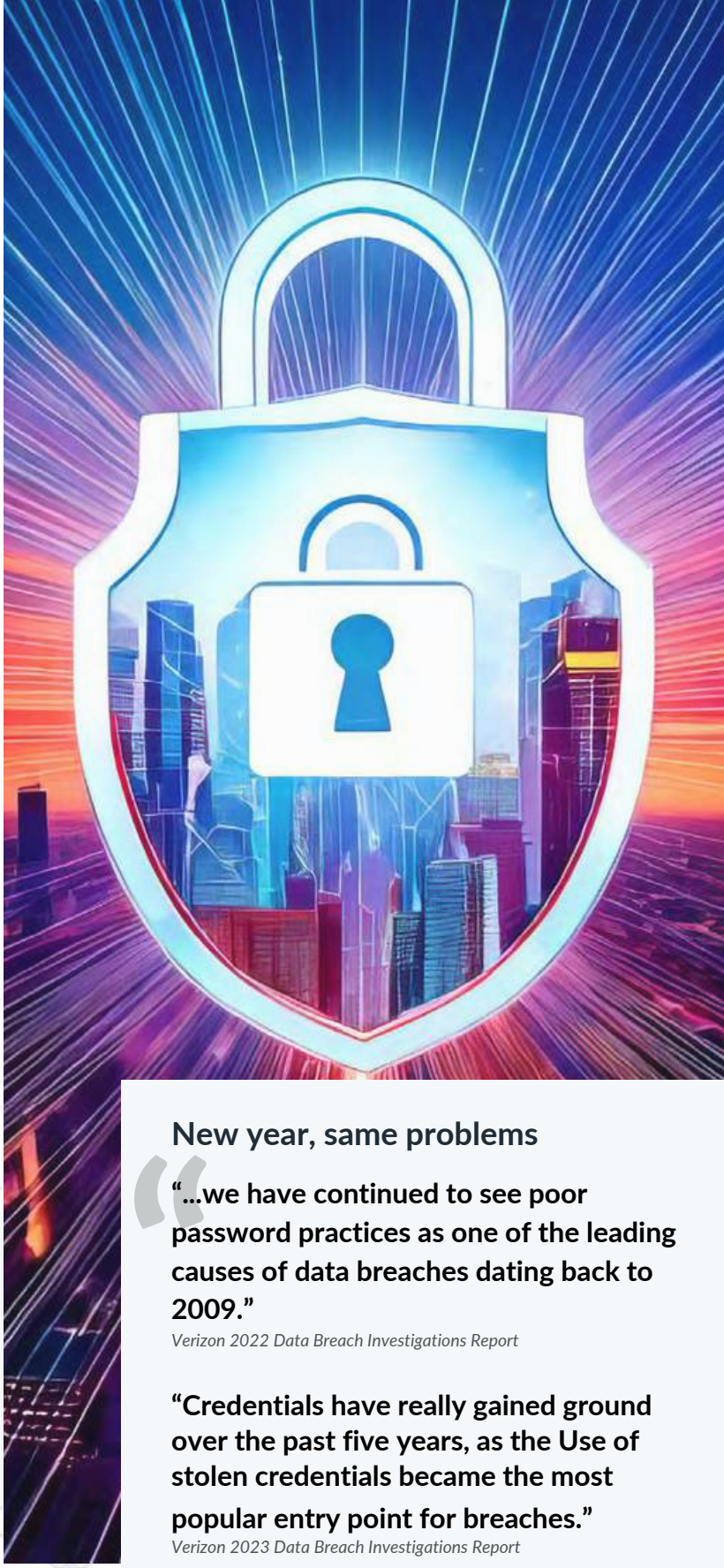
We expect there to be more of everything in 2025: more MFA, more passwordless authentication, more AI deployed in cybersecurity stacks, and more users (especially more machine users), as well as more attacks on passwords and more data breaches that do even more damage.

Add in a new presidential administration in the United States with shifting cybersecurity priorities, and new global regulations emphasizing resilience after that July 19 incident, and we expect a bigger, louder, and riskier 2025.

That's not to deter action. To the contrary: organizations should continue investing in cybersecurity and infrastructure capabilities that will help them weather a perfect storm. They should use history to guide them: historically, most data breaches were caused by some weakness in an organization's identity infrastructure. That can mean a password that is vulnerable to compromise, a failure to implement MFA, or an attacker exploiting some other vulnerability in an organization's identity lifecycle to move laterally, gain more permissions, and do more damage. Likewise, interconnected systems built on single points of failure will do just that. Resilient systems will thrive when fragile ones fail.

I don't know what date will define cybersecurity in 2025. But I do know that day is coming—and it may be coming soon. I urge you not to wait to find out when it will be, but instead to take action now to prepare.

Rohit Ghai
RSA CEO



> **“MFA will be everywhere in 2025.”**

New year, same problems

“...we have continued to see poor password practices as one of the leading causes of data breaches dating back to 2009.”

Verizon 2022 Data Breach Investigations Report

“Credentials have really gained ground over the past five years, as the Use of stolen credentials became the most popular entry point for breaches.”

Verizon 2023 Data Breach Investigations Report

“Over the past 10 years, stolen credentials have appeared in almost one-third (31%) of breaches.”

Verizon 2024 Data Breach Investigations Report

A 60-year old problem will continue in 2025.

Digital passwords have been in use since the 1960s, when Fernando Corbató needed a way for multiple users to operate a computer system via their own private access. In the decades since, they've become entrenched in nearly every aspect of our lives.

That won't change in 2025. Passwords will still be in use, and threat actors will use them whenever possible. Between the arrival of ubiquitous MFA, which will pressure cybercriminals to adapt their tactics, and AI that can automate password spraying attacks, we expect to see significant growth in data breaches caused by passwords in 2025.

But things are changing. The 2025 RSA ID IQ Report found that 61% of organizations planned to implement passwordless authentication in the next year. The survey's findings are reflective of larger trends: passwordless authentication is gaining ground, and passwordless will be widely favored by the end of the year. Consumers will start to view the traditional username/password log-in process as clunky and exert competitive pressure on organizations to evolve their authentication processes.

Organizations will find this preference for passwordless difficult to navigate. Businesses will need to find ways to cater to user demand without compliance mandates requiring passwordless, without having an agreed-upon passwordless standard, and without disrupting operations built on something-you-know authentication. Those pressures will make it difficult for organizations to implement enterprise-ready passwordless authentication—and may cause them to remove passwords from processes where they had been operating effectively.

Consumers' preference for passwordless and the absence of a global standard will also influence broader ecosystem battles, as Google, Meta, Apple, and Microsoft continue pushing their own passwordless standards and jockeying for dominance over the others.

“Cybercriminals will still find ways to bypass MFA”

44%

of 2025 RSA ID IQ respondents estimated that the total costs of identity-related data breaches exceeded the costs of typical incidents”

Ubiquitous MFA will push cybercriminals to raise their game in 2025.

Another trend we expect to transform cybersecurity in 2025 is that many more organizations will achieve ubiquitous multi-factor authentication (MFA). With Google and Microsoft announcing plans requiring MFA, regulatory mandates for MFA and phishing-resistant authentication, and high-profile incidents like the United Healthcare data breach, MFA will be everywhere in 2025. We also expect that financial institutions will reduce their use of SMS-based MFA due to SIM-swapping and attacks on telcos, and that Meta will follow Google and Microsoft's lead in requiring MFA.

The bad news is that, despite universal MFA and passwordless' slow advance, organizations will still need to negotiate the weakness that is passwords. Even with advancements like MFA, FIDO, and other passwordless innovations, many enterprise systems still start with passwords and layer advancements on top of them or use passwords as the recovery mechanism when a system is compromised.

MFA on its own does not eliminate data breaches. User and authenticator onboarding isn't strong enough in many areas, and authenticators are only as strong as the trust established in them during the onboarding process. Cybercriminals will still find ways to bypass MFA via attacks targeting enrollment and credential recovery, session hijacking, and social engineering of IT help desks.

In 2025, it won't be enough for organizations to do the bare minimum to meet compliance regulations. A check-the-box approach to cybersecurity simply won't work when threat actors are rewarded when they think outside the box. Organizations will need a more holistic view of security that starts with MFA and addresses any relevant mandates—but doesn't end there.

While we don't expect threat actors to abandon tried-and-true attacks like phishing or social engineering, we believe that threat actors will adapt to ubiquitous MFA by attacking other points in the identity lifecycle with greater frequency and urgency. The organizations that have unified their identity components will be better prepared to recognize and stop these attacks and stay safe in 2025.

> **Expect to see more AI-driven password spraying and social engineering attacks in 2025.”**

AI will lose its shine and hone its edge in 2025.

In December 2024, the FBI warned that "criminals exploit generative artificial intelligence (AI) to commit fraud on a larger scale which increases the believability of their schemes. Generative AI reduces the time and effort criminals must extend to deceive their targets."`

That will continue in 2025. Cybercriminals will continue using AI and machine learning to attack individuals and organizations: the technology will make it quicker, easier, and more affordable for threat actors to launch and automate attacks. Expect to see more AI-driven password spraying and social engineering attacks in 2025. We also believe that cybercriminals will use AI to attack biometrics more this year. As cybercriminals use AI to create deepfakes and socially engineer their targets, liveliness—natural, on-camera and in-the-moment responses—will emerge as a line of defense against these attacks.

On the cybersecurity side, organizations will start defining their terms when it comes to AI. The term won't have as broad a definition in 2025, with organizations narrowing their AI focus to stress proven techniques that can drive insights and deliver value, like machine learning.

In the short term, cybersecurity teams will prioritize analytics as an initial use case—ingesting their own data to surface insights and prioritize actions. Organizations will come to learn that if different layers share signals information, then each will get better at recognizing and defending against observed behavior. Organizations that have implemented a more holistic approach to their cybersecurity will be better at realizing these benefits, as integrated capabilities will be well-suited to sharing signals between systems. We also expect that vendors will start to offer internal assistants that tell customers how to better leverage the technology that they've purchased.

The obverse is also true: cybersecurity will start to articulate the AI models that are not acceptable for them. For example, cybersecurity will not use commercially available engines or large language models. And organizations will make the reasonable decision not to open their data to train public AI models. Rather than rely on third parties, the AI that cybersecurity will use will be built by and for cybersecurity specifically.

“Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud”

The following techniques are excerpted from FBI Alert Number: I-120324-PSA

“Criminals embed AI-powered chatbots in fraudulent websites to prompt victims to click on malicious links.”

“Criminals generate short audio clips containing a loved one’s voice to impersonate a close relative in a crisis situation, asking for immediate financial assistance or demanding a ransom.”

“Criminals generate videos for real time video chats with alleged company executives, law enforcement, or other authority figures.”

“10x-50x

Factor by which machine identities outpace normal accounts.

Machine identities will grow exponentially in 2025.

Machine identities have always been a known unknown for IT: they're used to run databases, microservices, firewalls, root/admin accounts, and nearly every other process that's not tied to a human or device. They've always outpaced other types of accounts by several orders of magnitude.

But in 2025 they're set to grow exponentially, as adding on cloud services or creating a new project will create hundreds of machine accounts at the click of a button.

Each of those machine accounts in turn will have its own set of permissions. Many of these accounts will act independently as agents on users' behalf. They also authenticate using a wide variety of means, including passwords, authentication tokens, security keys, and x509 certificates. These accounts are mostly created by developers and through software provided by cloud and SaaS providers, not through the business' internal IT operations.

Growing numbers of machine accounts, limited visibility into when they are created or how they authenticate, and more expectations that they'll act without oversight will give threat actors a new asset: cybercriminals will try to impersonate or log-in as these accounts.

To prevent breaches and threat actors from moving laterally, organizations will need to monitor these accounts in real-time and apply Zero Trust principles like least privilege.

This may be a challenge for some organizations, as architectures for access-data collection tend not to be tuned to the cloud accounts and systems that will generate these new machine identities. In fact, we don't expect all organizations to be capable of managing this change and expect several data breaches exceeding $10 million in costs to be caused at least in part by machine identities next year.

> **“Regulators will be less lenient in evaluating organizations’ resilience.”**

What new global regulations and a US presidential administration will mean for cybersecurity.

While we believe that certain US Department of Defense (DoD) regulations like the Cybersecurity Model Certification (CMMC 2.0) will stay in place, the start of the second Trump administration will reset the cybersecurity agenda in the US and influence regulations around the world.

In fact, organizations may see a reduced compliance burden for certain security requirements. If that's the case, then organizations may shift their spending away from initiatives intent on achieving regulatory compliance to instead pursuing more proactive measures, like moving from public clouds to private instances or returning data back on-premises to protect customer data.

It may also mean that organizations that do the bare minimum to meet requirements may pull back on their cybersecurity spending—and leave themselves at risk. Should organizations pull back on cybersecurity programs, those spending changes and reduced regulations may cause insurers to perceive greater risks and demand higher cybersecurity insurance premiums.

Outside of the US, laws and regulations like the EU's Network and Information Systems Directive 2 (NIS2) and Digital Operational Resilience Act (DORA) will emphasize resilience or have resilience as a critical component. Given the CrowdStrike / Microsoft outage last year that affected some 8.5 million devices, regulators will be less lenient in evaluating organizations' resilience.

To prepare, organizations should think through scenarios like "What happens if the MFA cloud provider has an outage or becomes unavailable?" By gaming out situations like that, organizations can see where their dependencies are, and which processes or security components might break in the event of a third-party outage.

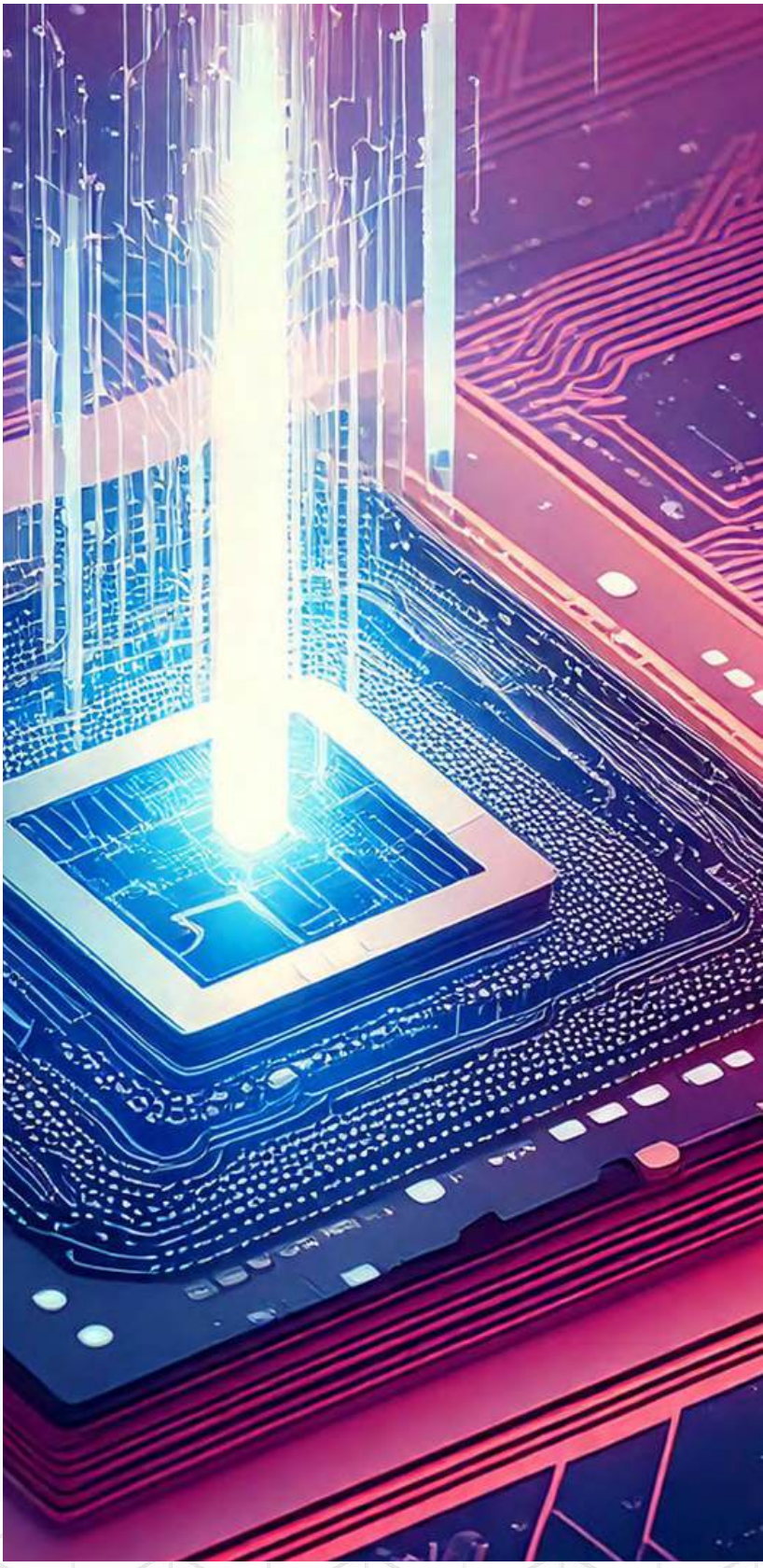
As regulations ebb, the organizations that maintain services and protect consumer data will stand out. Those that don't will develop untrustworthy brands that employees and customers will avoid. Resilience and security will be valuable in and of themselves and brand assets to the organizations that exemplify them.

70%

of organizations operate in hybrid deployments

80%

of IDC study respondents "expected to see some level of repatriation of compute and storage resources in the next twelve months"



> **...organizations will be well-prepared for any post-quantum capabilities long before they arrive.”**

Quantum computing will not pose a threat to encryption in 2025.

Quantum computing will continue making incremental advancements in 2025. However, given the significant resources needed to operate quantum computing, the state of quantum computing (which is still predominantly in the research stage), and new guidance from NIST, the technology will not pose a significant threat to encryption this year.

By implementing new NIST guidance, organizations will be well-prepared for any post-quantum capabilities well before they arrive. The guidance recommends deprecating 112-bit-equivalent (2048-bit keys) RSA keys by 2030 and will disallow all RSA digital encryption signature algorithms by 2035. The same is also true for Elliptic Curve cryptography: ECDSA and EdDSA will meet their end-of-life in 2035.

The guidance also recommends increasing the key size to 3072- or 4096-bit RSA keys. Doing so is a relatively easy fix for organizations to implement that will add five years to existing encryption standards' viability. To meet the new guidance, organizations need to generate new key pairs and issue new certificates, and the software that will work with those new pairs and certificates will need to accommodate longer key sizes. Most recent software should be able to adapt to those new requirements. RSA will follow NIST guidance and adjust product default configurations where needed.

Importantly, as promising as quantum computing may one day be for medical research, finance, and aerospace, and as dangerous as it could be for encryption, quantum computing's effects and applications are still largely theoretical. Focusing on quantum's theoretical future distracts from the very clear, present, and low-tech exploits that cybercriminals succeed with today:

- Change Healthcare was compromised by stolen credentials and didn't have MFA enabled on some of its accounts
- Scattered Spider convinced IT help desk staff to disable or reset MFA credentials in order to launch a ransomware attack
- Colonial Pipeline was breached in part due to an orphaned VPN account

Quantum computing requires massive funding and resources. The three data breaches listed above—and the countless others caused by phishing, weak credentials, or any other by-the-book tactic—did not.

A good problem to have

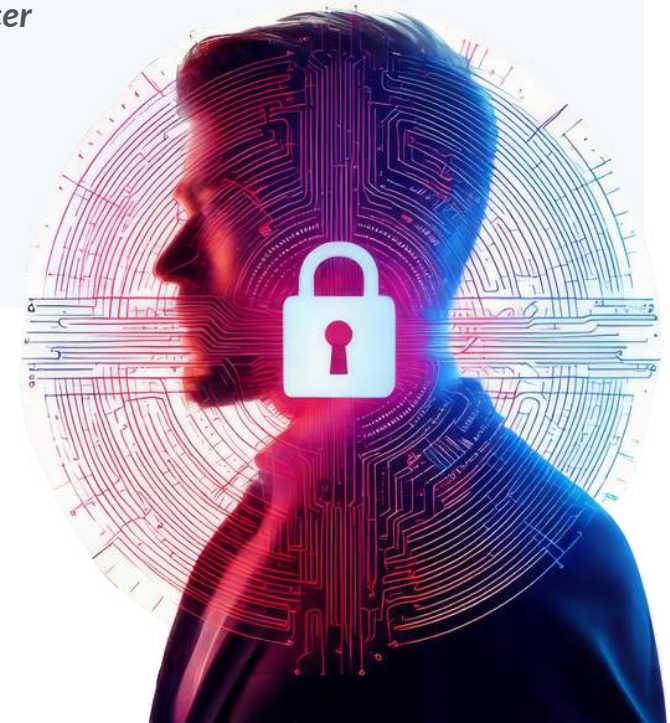
“You’d be hard pressed to name three people who have done more for computing than Ron Rivest, Adi Shamir, and Leonard Adleman. Beyond building one of the most widely used and longest-lasting encryption methods, their names are also tied to the world’s biggest tech conference and the world’s most secure identity company: RSA Security.

Having a brand as recognized, widespread, and enduring as RSA is a major asset for us: organizations know that RSA stands for security. But when you’re tied to three transformative technologists, sometimes there can be a little confusion about which ‘RSA’ does what.

RSA Security and the RSA cryptosystem are two separate entities. RSA Security released the public-key cryptosystem into the public domain in 2000—our company hasn’t maintained the standard in decades.

While the algorithm is associated with our founders and our brand, it is not part of our products or solutions today.”

Jim Taylor, RSA Chief Product and Technology Officer



Forewarned is forearmed.

RSA secures the most secure. For decades, leaders in government, financial services, energy, healthcare, and more have turned to RSA for the identity and access management (IAM) capabilities needed to secure access, prevent risks, and accelerate productivity.

Learn why and prepare for whatever 2025 has in store: start your RSA ID Plus trial now to accelerate your Zero Trust maturity by implementing the world's most secure multi-factor authentication (MFA), access, single sign-on (SSO), directory, and other critical cybersecurity features across cloud, hybrid, and on-premises environments.

We're known by the company we keep.

9,000+
Customers

99.99%
Uptime

13 Trillion
Entitlements

70%
of Fortune 100 Financial Firms

13
US Federal Executive Departments

40
Years of Innovation

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For more information, go to RSA.com.