RSA

Top Trends in Identity for 2024

Securing the Future of Identity in the AI Era

January 2024

RSA.com

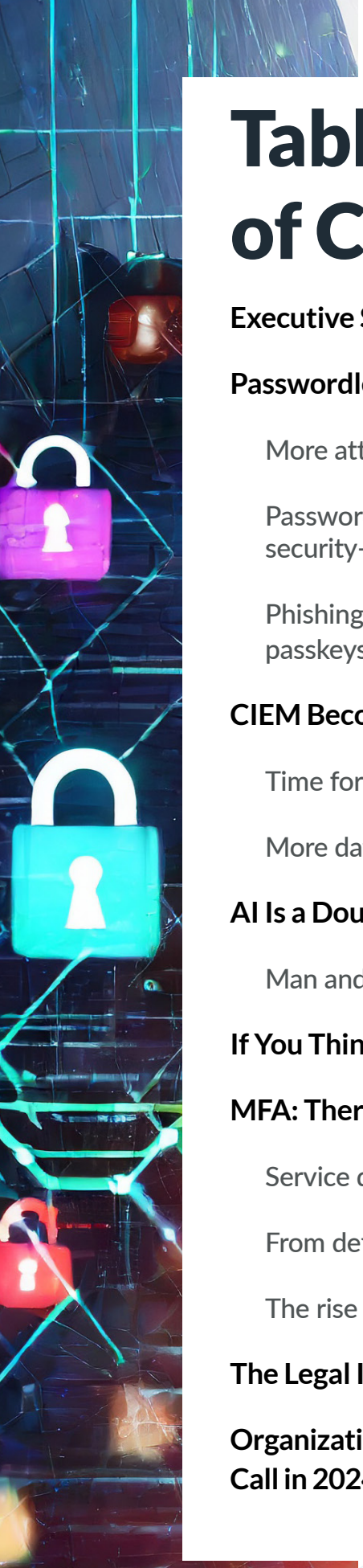


Table of Contents.

Executive Summary: Don't Predict—Prepare.

One of the most interesting things about chaotic systems is that they tend to be predictable in the short term. Think about the weather: As much as we love to make fun of meteorologists, they're actually pretty good at predicting the weather through the end of the week.

But even as they get only a couple of weeks out, making any accurate prediction over the long term becomes nearly impossible. There are too many variables—too much chaos—for any model to account for: Will it be hot or cold in a month? Rainy or sunny in a year? There's no way of knowing except to live it.

The same is true for cybersecurity. After speaking with customers, partners, analysts, and researchers across industries, and after surveying more than 2,300 people across more than 90 countries on their identity security knowledge, behaviors, and beliefs, we know that organizations will need to account for growing numbers of users, devices, entitlements, and environments. Moreover, if the past is any indicator, we know that that growth will create a larger, more vulnerable attack surface. The Identity Defined Security Alliance's 2023 Trends in Securing Digital Identities survey found that 90% of businesses had an identity-related incident in the past year, and 98% agreed that the number of identities they need to manage is increasing.

The pace of change will only accelerate. Look at how generative artificial intelligence (AI) has completely altered the threat landscape—and introduced new cybersecurity capabilities to defend against those threats. Look at the progress we've made enabling

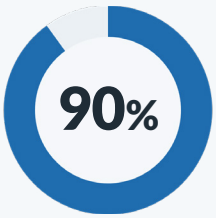
multi-factor authentication (MFA)—and the ways that cybercriminals are adapting. Consider how threat actors have found a new favorite target in IT service desks, or how progress on passwordless authentication will minimize hackers' favorite vulnerability, even as it introduces new ones.

The following sections detail some of the new risks we see emerging as a result of a growing attack surface, new threat vectors, progress on instituting MFA, and other changes. RSA leaders describe the innovations we think will enable organizations to adapt to those new risks, explain how our role will evolve alongside AI, and examine the ways that cybercriminals will look for gaps in identity security to launch attacks.

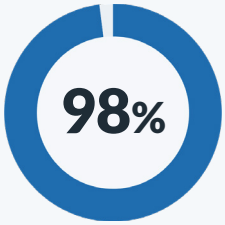
We're not trying to predict the weather. We know we can't—that there are too many variables, too much interaction, too much chaos for any organization to control for.

But that admission doesn't absolve us of inaction. To the contrary. When you admit the limits of your foresight, it becomes incumbent on you to prepare for what might come next.

The Identity Defined Security Alliance's 2023 Trends in Securing Digital Identities survey found that:



of businesses had an **identity-related incident** in the past year



agreed that the number of identities they needed to manage is **increasing**

“The future will be passwordless.”

Passwordless Authentication Will Finally Become a Reality in 2024.

"The future will be passwordless." That was how former *New York Times* cybersecurity reporter Nicole Perlroth began a blog detailing new innovations that would send an "encrypted key from a user's phone to the desktop computer," making the "often painful process of logging into a site" a little less aggravating.

Perlroth was cagey about exactly when we'd arrive at that passwordless future. That omission turns out to have been a smart decision. She made that prediction on December 18, 2013, and while passwordless and passwordless authentication have long been popular topics, the tech industry hasn't really made significant strides in replacing Something-You-Know-based authentication. If they had, there would be far fewer data breaches.

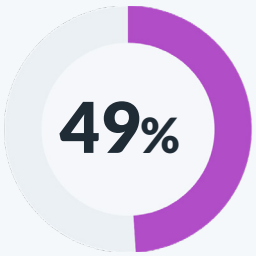
Unfortunately, credentials (and specifically stolen passwords) have continued to be one of the leading causes of breaches. The Verizon 2023 Data Breach Investigations Report found that the use of stolen credentials "became the most popular entry point for breaches" over the last year, and that 49% of all data breaches involved credentials. Microsoft found that password attacks "increased more than tenfold" compared to 2022, "from around 3 billion per month to over 30 billion."

More attacks—but also stronger defenses

Thankfully, in 2024, we expect more users to deploy passwordless authentication. While enterprises have long understood that passwords are insecure and wanted to embrace passwordless authentication, they've been slow to do so because FIDO was viewed as a consumer technology and there had been major gaps in native platform support.

Those objections have been resolved—passwordless standards are far more mature, and there's a flourishing passwordless ecosystem that's poised to grow even faster because of consumer acceptance. In 2022, Apple, Google, and Microsoft "announced plans to expand support for a common sign-in standard created by the FIDO Alliance and the World Wide Web Consortium," noting in a joint press release that their new support would "allow websites and apps to offer consistent, secure, and easy passwordless sign-ins to consumers across devices and platforms." In 2023, Amazon joined in the broader effort to drive passwordless authentication.

As an active member of the FIDO Alliance's board of directors since 2014 and a member of the Alliance's Enterprise Deployment Working Group (EDWG), the FIDO2 Technical Working Group (TWG), and the



of all **data breaches** involved credentials.

Verizon 2023 Data Breach Investigations Report

FIDO User Experience Working Group (UXWG), RSA knows that it's important to both have enterprises sign off on passwordless standards and have consumers use it to grow acceptance with the technology. Security companies can bang the drum on the need for passwordless until they're blue in the face (and trust us, we have), but that message won't land until consumers see, use, and benefit from passwordless in their everyday lives, or until employers feel that passwordless can adequately secure authentication.

The big four's commitments, more mature standards, and a thriving passwordless ecosystem will translate into real progress—finally!—for passwordless in 2024.

Passwordless authentication progress will inflame security-vs.-convenience debate

Overall, any progress toward passwordless authentication will be worthwhile. But not all passwordless authentication is created equal. Moreover, that progress will result in new risks and vulnerabilities.

One challenge we expect is that the progress tech makes in driving passwordless authentication will throw gasoline on the security-versus-convenience debate. Given that the big four cater to consumers, we expect that the passwordless authentication they will institute will lean more toward convenience and will likely use synched passkeys relying on cloud platforms to synchronize and manage these passwordless authenticators' passkeys.

Enterprises, on the other hand, will look at that debate differently, and will likely look to improve on credential recovery use cases while still maintaining high assurance with device-bound passkeys. Ultimately, companies will need to consider how passkeys are managed and what that means to their security posture.

Phishing-resistant MFA leads to more synched passkeys; more synched passkeys lead to more security breaches

It's not just the big four endorsing passwordless that will change authentications in 2024. Executive Order M-22-09, "Moving the U.S. Toward Zero Trust Cybersecurity Principles," and the Federal Risk and Authorization Management Program (FedRAMP) will require the use of phishing-resistant MFA by the end of fiscal year 2024.

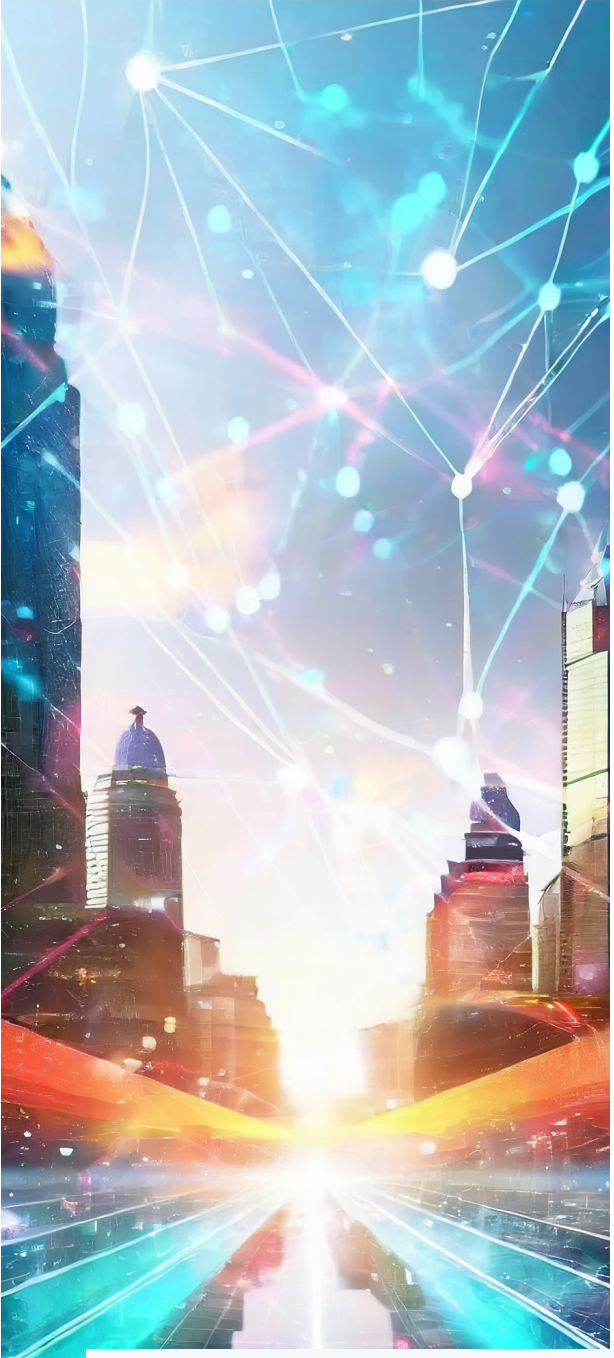
It's not exactly an earth-shattering revelation for us to predict that the U.S. government's requirement to use phishing-resistant MFA in 2024 will result in the wider use of phishing-resistant MFA next year (we might as well predict: "The sun will rise in the east next year").

But it is worth gaming out the effects of that requirement. Next year, more government agencies will use phishing-resistant MFA. Between the government's requirements and the big four's push for passwordless, we expect that many users will deploy FIDO-synchronized passkeys for personal use. Both consumers and enterprises should be aware that these keys will be synched to the cloud—we suspect that some might not know that's occurring, or the risks that result. As we noted above, synched passkeys prioritize convenience over security and may introduce new vulnerabilities for their organizations.

With more phishing-resistant capabilities deployed because of the government's requirements, we expect more threat actors to target users' personal accounts and exploit users' password vaults and wallets. If users and their organizations are using certain passwordless configurations and defaults, then threat actors may be able to use compromised personal accounts to launch attacks on professional resources.

This isn't entirely theoretical: Last year, software development vendor Retool claimed that 27 of its cloud customers were breached, in large part due to a "Google Authenticator synchronization feature that syncs MFA codes to the cloud." In their report on the breach, Retool noted that this "is highly insecure, since if your Google account is compromised, so now are your MFA codes."

Organizations should prepare for this now. It's well worth looking for solutions that make it possible to disable synchronized passkeys for certain use cases, as a way of keeping passwordless authentication both secure *and* convenient.



> **....the more complex a multicloud configuration, the more it becomes a minefield for zero-trust implementation.”**

CIEM Becomes Key.

It should come as no surprise that most businesses are using cloud services to at least some degree: In the PwC Cloud Business Survey, 78% of executives said that "their companies had adopted cloud in most or all parts of the business." This year, the U.S. government planned to spend $9 billion on cloud computing. Gartner predicted that half of enterprise IT spending will shift to the cloud by 2025. The Identity Defined Security Alliance's 2023 Trends in Securing Digital Identities survey found that the adoption of more cloud applications was the #1 factor driving an increase in the number of identities across respondents.

We won't list all the reasons for moving to the cloud—there are plenty. But for all the advantages that come with using hosted and managed services, organizations also need to understand that every cloud environment scales an organization's risks. Citing a Gartner report, *Venture Beat* reported that the "more complex a multicloud configuration, the more it becomes a minefield for zero-trust implementation."

That was borne out by the data: The Verizon 2023 Data Breach Investigations Report found that among the 602 confirmed security incidents resulting from miscellaneous errors, 23% were caused by publishing errors ("showing something to the wrong audience") and 21% resulted from misconfiguration. The IBM Cost of a Data Breach Report found that cloud misconfiguration was "the initial vector for 11% of attacks," and that those breaches had an average cost of $4 million.

That's an awful lot to spend on a mistake, and it's why we expect more organizations to prioritize cloud infrastructure entitlement management (CIEM) in 2024 and the vendors that can provide the most secure cloud environments. By integrating cloud environments, organizations inherit secondary risk from their vendors—how third parties manage their entitlements, tools, and insider threats extends to the customers themselves, and their data. For regulated organizations in healthcare or financial services, losing direct ownership of patient or financial data expands their risk significantly.

Time for SMBs to implement CIAM

Cloud services inflate an organization's attack surface from the top down, importing new risks as the business makes infrastructure changes.

Customers, contractors, and third-party users inflate an organization's attack surface from the bottom up. As organizations grow, they take on more users and need to manage more of their information. That information in turn can be regulated by compliance mandates like GDPR and CCPA. And even if it isn't regulated, losing a customer's information is never a good look.

That's why we expect more organizations to implement customer identity and access management (CIAM) capabilities, which extend identity controls associated with users to customers, contractors, temporary workers, and others. And, similar to what we've said about organizations bringing more than simply authentication to customers, they also need to bring governance, lifecycle, and access capabilities to manage third-party users' identities.

Importantly, it's not just large enterprises that need to emphasize IAM or CIAM. Cybercriminals won't distinguish between the Fortune 500 and mom-and-pops. As more information is exploited, used, retained, and stored, whether in the cloud or on-premises, the size of the organization doesn't really matter—the same requirements still apply. What changes instead is the number of people it would take to handle the work and the impact that a given security incident could have.

That overlap is driving a growing interest in CIAM from small and midsize businesses (SMBs). In fact, given the actions that led to security events for SMBs this year, Verizon recommended "Access Control Management" as one of the controls for the incidents that

most frequently affect SMBs. Those capabilities should include the use of "processes and tools to create, assign, manage and revoke access credentials and privileges" and should extend to a broad range of user, administrator and service accounts.

> **"Increasingly, both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked."**
>
> *Verizon 2023 Data Breach Investigations Report*

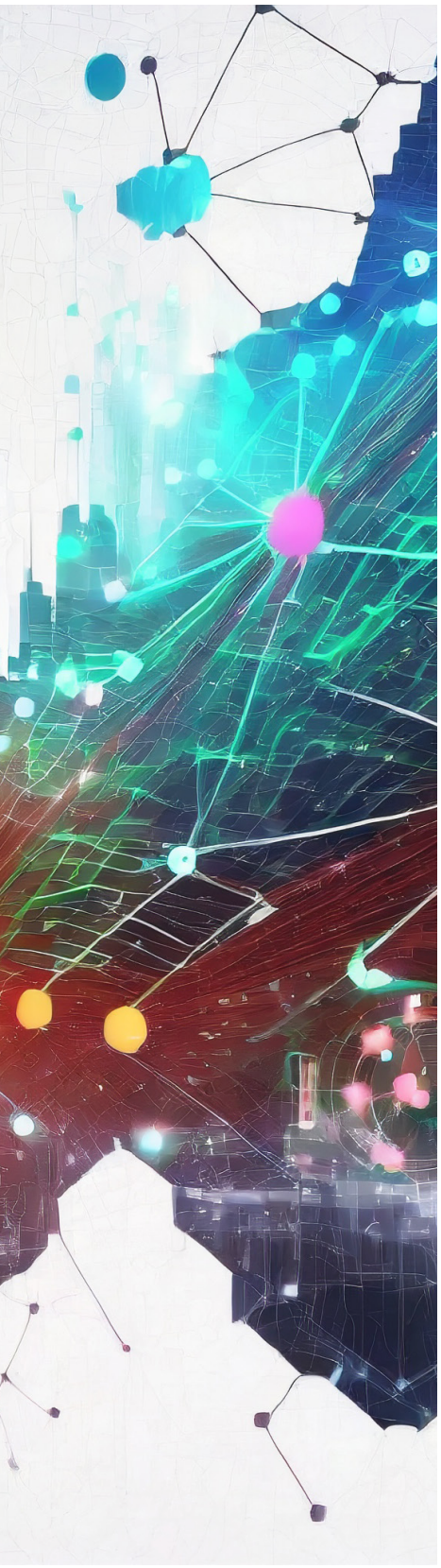
More data, smarter decisions

One of the great myths of TV is when an investigator zooms in on an image, says "Computer, enhance," and then the image becomes even sharper. Watch this with a graphic designer, and they may have to take a long walk: In the absence of AI (which can increase resolutions of photos and images in addition to all its other neat tricks), images need to begin with the highest resolution and scale down. Experts know that to get a clearer picture at scale, you need to begin with more information, not generate it by magic or special effects.

The good news is that the trends we've described above—more information combining together in the cloud, more users bringing even finer-grained information to organizations, and more organizations merging their information with others in the cloud—will give organizations the data they need to construct a sharper, clearer image of any user, machine, service, or other entity.

By leveraging more directory information and federated data and attributes, we'll have a much larger scope of data that can help us better triangulate who needs access to given resources. That growing quantity of information will provide organizations with far more advanced intelligence, dashboards, and better-informed decision-making and automation. Having more attributes will allow organizations to set better, more restrictive policies and move even closer to zero trust.

> “Just because we need AI in cybersecurity doesn’t mean that human operators are going away.”



AI Is a Double-Edged Sword. In 2024, It Will Cut Even Deeper.

If you consumed any media in 2023, then you might have come across AI a couple of times. AI was nearly everywhere, from passing the bar exam to (spoiler alert) squaring off against Ethan Hunt in *Mission: Impossible*.

There's a lot of hype around AI. But there's also a lot of potential, both as a new risk and a new cybersecurity tool. In 2023, researchers and attackers used AI to write polymorphic malware, develop a deepfake ad of Tom Hanks promoting dental insurance, and drive a 1,265% increase in phishing emails. The Verizon 2023 Mobile Security Index white paper reports that "seven words can be enough of a sample to create a believable impersonation of an individual's voice." With AI creating more—and more convincing—phishing lures, deepfakes, and other social engineering attacks, organizations must prioritize strong MFA to help keep themselves safe.

While AI represents a growing risk, it can also be a significant asset in enhancing organizations' cybersecurity posture. The 2023 RSA ID IQ Report found that 91% of respondents believed that AI has a role to play in improving identity security. In fact, the report found that people trust technology with their security and privacy: 64% said they would trust a computer or password manager to secure their information instead of their partner, closest friend, or financial advisor.

The Identity Defined Security Alliance's 2023 Trends in Securing Digital Identities survey found that 98% of identity and security stakeholders believe that AI and machine learning are beneficial.

Those perceptions are informing significant investments in AI. The AI software market is set to expand by $64 billion by 2024, with cybersecurity among the fastest-growing industries benefiting from those investments, per Forrester Research.

AI can help accelerate detection, reduce the financial cost of a breach, and improve an organization's overall cybersecurity posture. The IBM Security Cost of a Data Breach Report 2023 found that organizations that use security AI and automation "experienced, on average, a 108-day shorter time to identify and contain" a data breach. Saving time also saves money; organizations with sophisticated AI and automation "reported USD $1.76 million lower data breach costs."

Man and machine—not man versus machine

Just because we need AI in cybersecurity doesn't mean that human operators are going away. Far from it: We'll continue to need humans' expertise in defending against cybersecurity threats. But the particulars of what humans will do and how we'll interact with AI will change.

In the near term, we expect that AI will manage day-to-day operations, including automating account provisioning for new users, ensuring that users enable MFA, and monitoring for account irregularities. While AI is managing rote operations, human experts will supervise higher-touch and more impactful choices, like what happens when a user needs a resource that other peers don't require, or uses out-of-band authentication to respond to a high-risk request like disabling MFA.

In time, AI will become a core part of organizations' cybersecurity architecture. By then, threat actors will start to target AI in a similar way to how they launch prompt bombing and MFA fatigue attacks today to try to get around an organization's security functions. With AI, that will mean data poisoning and prompt injections, or trying to make AI hallucinate and work against us.

What this means is that AI will secure us—and we'll need to secure AI.

> One emerging ransomware risk to keep an eye on in 2024? **Bring Your Own Device (BYOD).**

If You Think Ransomware Attacks Are Bad Now, Just Wait Until 2024.

"If it ain't broke, don't fix it" applies to everyone—bad guys included. Ransomware will continue to be a useful tool for them, still dominating headlines and driving up costs in 2024.

The Verizon 2023 Data Breach Investigations Report found that 24% of data breaches involved ransomware, and that ransomware "is ubiquitous among organizations of all sizes and in all industries." Microsoft's Digital Defense Report 2023 found "an increased rate of ransomware attacks compared to last year," with human-operated ransomware attacks "up more than 200 percent since September 2022."

That's in large part because ransomware *pays*. The 2022 FBI Internet Crime Complaint Center (IC3) found that, among incidents where the victim paid a ransom, the median loss more than doubled year over year to $26,000, and the range of losses in 95% of cases was between $1 million and $2.25 million. The IBM Security Cost of a Data Breach Report 2023 found that the average cost of a ransomware attack "increased 13%" year over year to an average cost of $5.13 million.

We expect that the 2023 ALPHV ransomware attacks will drive up the 2023 costs. Caesar's Entertainment reportedly paid $15 million, and MGM Resorts International expected a $100 million cost impact as a result of the breach. Because ransomware is on the rise and can make such a significant financial impact, organizations must implement strong MFA and other cybersecurity measures to stay safe.

One emerging ransomware risk to keep an eye on in 2024? Bring Your Own Device (BYOD). Microsoft found that "80%-90% of all successful ransomware compromises originate through unmanaged devices," which "typically have fewer security controls and defenses" than managed hardware.

Ransomware by the numbers:

$5.13 million
average cost of a ransomware attack

13%
year-over-year growth in the average cost of a ransomware attack from 2022 to 2023

$100 million
expected cost of the ALPHV 2023 ransomware attack on MGM Resorts International

Human-operated ransomware attacks increased 200 percent since September 2022.

MFA: There's Good News and Bad News.

The good news is that regulations requiring MFA will help create a higher ceiling for cybersecurity. In England, the National Health Service's (NHS') requirement to institute MFA by June 2024 will help secure healthcare and patient data. By October, the European Union will require its member states to begin applying the Network and Information Security directive (NIS2), which includes "the use of multi-factor authentication" where appropriate. In the U.S., the Biden Administration's Executive Order on Improving the Nation's Cybersecurity required that all Federal Civilian Executive Branch agencies begin implementing MFA in 2022.

The bad news is that, while MFA is essential to cybersecurity, some of the worst data breaches of the last few years demonstrated that MFA is insufficient on its own:

New AI threats, ransomware, and a growing attack surface underscore the urgent need for organizations to prioritize MFA as their first line of defense. Cybersecurity begins with authentication.

MFA: There's Good News and Bad News.

Timeline

March 2022

Russian threat actors breached a non-governmental organization by enrolling a new device in MFA, then "took advantage of a misconfigured account [that was] set to default MFA protocols," which effectively allowed them to bypass MFA by disconnecting from the internet

The LAPSUS$ hacking group compromised Okta's third-party customer service provider, then used that access to add a new account to the "tenant administrators group" and in turn breach 366 customers

September 2022

After obtaining an Uber employee's Active Directory password, the attacker impersonated Uber IT and used an MFA fatigue attack to flood the user with MFA prompts until they approved the request, providing them access to Uber's bug bounty program

November 2022

Attackers managed to steal cloud tokens issued to users who had enrolled in MFA; they then used the stolen tokens to gain access from a different device

June 2023

Microsoft observed "[a]pproximately 6,000 MFA fatigue attempts....per day by the end of June 2023."

August 2023

A campaign targeting Microsoft 365 used EvilProxy, "a phishing toolkit that uses reverse-proxy tactics to bypass" MFA, successfully compromising senior executives

September 2023

Caesars Entertainment, MGM, and other organizations were breached after threat actors phished customer service desks, allowing the attackers to reset MFA to allow access to Okta super-admin accounts

October 2023

BeyondTrust and CloudFlare discovered attacks against their identity infrastructure; the attacks originated in part because attackers gained access to Okta's support desk and HAR files

The Citrix Bleed vulnerability provided attackers with a method to bypass password and MFA requirements

Because MFA is a critical cybersecurity component, and because of the work that government and business have done to implement MFA, we expect that attackers will continue to look for ways to bypass MFA in 2024. Moreover, we expect that the successful attacks will exploit the gaps in organizations' identity infrastructure.

MFA is the first line of defense—it just can't be the last line of defense.

"Even though there are many ways to steal credentials, we have many ways to protect them as well. One of the best ways (stop me if you have heard this one before) is the use of MFA. Before you recline in your chair and "Well, ACKtually …" us, we do realize there are limitations to some MFA implementations. As you're undoubtably aware, some very high profile breaches this year demonstrated some of those shortcomings.

In some cases, criminals used social engineering to convince users to accept the authentication attempts. In other instances, they stole the session cookie and used it to masquerade as the user. Of course, some MFA bypasses weren't really bypassing MFA because some of the services weren't properly configured to ONLY use MFA."

Verizon 2023 Data Breach Investigations Report:

"A false sense of security."

"MFA is supposed to help improve security. But as we've discussed in previous reports, it's not a panacea. In fact, the false sense of security that having MFA in place can generate is a risk in itself.

Increasingly, SMS- and authenticator-app-based types of MFA are being supplanted. Many applications now use a form of MFA where users are asked to respond—typically accept or reject—to an alert on their mobile device. In an MFA spamming attack, the perpetrator bombards the user with prompts in the hope that the person will click 'accept' to make the annoyance go away. Some do.

In 2022, Uber suffered a high-profile—although, it said, fairly harmless— breach due to MFA fatigue. The attacker used a contractor's compromised VPN credentials to repeatedly attempt to log in. When this didn't succeed, the attacker contacted the victim on WhatsApp and, pretending to be Uber IT support, encouraged the employee to accept the request. They did. The attacker was able to exploit access to the VPN to move laterally to breach critical systems such as the company's email, cloud storage and code repository."

Verizon 2023 Mobile Security Index white paper

Service desks should be a lifeline for users—not a gold mine for attackers

For years, threat actors have been impersonating IT or organizations' help desks to socially engineer their targets (the attacker that breached Uber posed as part of the company's tech support team).

But recently, attackers have adjusted their targets and attacked help desks themselves. You can see the appeal: Help desks have wide latitude to create accounts, suspend MFA, and reset passwords, which is more or less what an attacker would want to do themselves. Moreover, they are used to receiving "urgent" requests from VIPs. And because organizations want their users and employees to stay connected and productive, it's easy to find help desk contact information online.

Those factors all make help desks an appealing—and lucrative—target. MGM estimated $100 million in losses following the ransomware attack that began when threat actors phished customer service desks and allowed the attackers to reset MFA; Ceasars paid the attackers a reported $15 million to restore their systems. Support systems also collect a vast amount of information on their users that could be used in future attacks: An October 2023 breach allowed a threat actor to download all the names and email addresses of a support system's users, which may lead to "an increased risk of phishing and social engineering attacks."

Organizations need to prevent their help desks from causing harm. To do so, they'll need to:

- **Understand** what actions help desks can take and what they have access to
- **Document** their runbooks and process documentation, as well as when the help desk brings in another group
- **Establish** the high-risk actions that must follow change management processes
- **Create** a security-first culture that involves more than rolling out annual compliance training, including leadership consistently communicating that security is paramount
- **Demonstrate** that leadership will support the help desk when it does things by the book
- **Integrate** identity verification to bootstrap credentials during onboarding

That last point will become particularly important as hybrid work cements itself across industries. Onboarding may not be conducted in person as frequently as it was even five years ago. That represents a significant shift for cybersecurity, as authentication can only be as strong as its initial enrollment. Organizations will need broader identity verification capabilities to establish a strong ceiling for new identities.

From defense to self-defense

Identity has always been the defender's shield: Creating accounts, establishing authentication, and provisioning entitlements all result from the need for organizations to account for, manage, and secure resources.

But if identity is an organization's shield, then that also makes it an attacker's target. That's not necessarily news—look through any year's Verizon Data Breach Investigations Report and you'll likely find that identity was one of the leading initial attack vectors that year. But even while it's not a new problem, identity as a growing security vulnerability is poised to get much worse. Growing numbers of users, devices, entitlements, and environments make for a larger, more complex, and more vulnerable identity attack surface. In last year's data breaches, attackers used that growth to their advantage.

It's not enough for identity to be good at defense—it needs to become good at self-defense. Identity threat detection and response (ITDR) is an emerging capability that can

help identity become more than a stronger shield; instead, it can give identity something akin to an immune system that actively looks for and defends against threats.

It's clear that we need that latest booster to our immune system. Humans can't parse the logs that result from hundreds of thousands of events and see what's anomalous, and static rule sets aren't adaptive enough to respond to thinking adversaries. But AI can—in fact, unlike humans, AI improves as you feed it more data.

Not all AI is created equal when it comes to cybersecurity. Deterministic AI tends to provide security and audit teams with the transparency they need to maintain compliance and automate security operations. AI is particularly good at assessing:

1. **Authentication data** to understand who is trying to get in
2. **Account and entitlement** information to understand what someone could access
3. **Usage data** to see what someone is really doing

The rise of the machines

It's not just human users: Cybersecurity needs to account for machine, internet of things (IOT), and service accounts in addition to the real humans who log in. And we have to do this for every stage of the identity lifecycle.

In 2023, a hacking group used an API to find the passwords transmitted between an identity vendor and its customer. The attacker used the API to try to create a backdoor service account. They were prevented from doing so, but they should have never had the chance: The initial API exchange—one service account sending information to another—introduced the risk, which grew worse because there was limited oversight on what those service accounts were transmitting. Even service accounts shouldn't be transmitting cleartext passwords, and any password should be tied specifically to the machine it's operating on. We saw similar risks at play at Colonial Pipeline, where an inactive VPN account that wasn't protected by MFA was used to launch a ransomware attack against the energy provider.

That risk is poised to grow. The number of IOT-connected devices grew by 18% in 2022 to 14.3 billion endpoints and was expected to grow another 16% this year to 16.7 billion. That's a lot of non-user-based accounts exchanging information—and a lot more ground for cybersecurity teams to cover.

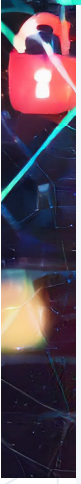
> “Law and professional services represent a perfect storm of risks.”

The Legal Industry and Professional Consulting Will Come Under Attack.

In the United States, there are sixteen critical infrastructure sectors, including chemicals, communications, energy, and financial services. The U.S. Cybersecurity Infrastructure & Security Agency (CISA) defines these sectors as "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

Many cybersecurity requirements focus on these sixteen sectors and the organizations that work within them; those requirements have helped create a higher cybersecurity standard for critical infrastructure. Moreover, the 2024 deadline for federal civilian agencies to adopt some level of zero trust architecture means that energy, transportation, and other critical infrastructure will be hardened to many attacks—and that attackers will look elsewhere for softer targets.

We expect that adversaries will focus on the sectors that lack cybersecurity requirements—particularly law offices and professional consulting firms. These industries represent a perfect storm of risks: They trade in privileged, confidential information, but they are not required to develop cybersecurity capabilities.



> “...mobile devices have become indispensable tools. They serve as vital entry points to a company’s key systems, data and cloud-based resources. They can also put these resources at risk.”

Organizations Will Look for a New Way to Answer the Mobile Security Call in 2024.

It is a truth universally acknowledged that we love our phones. By the end of 2022, more than 5.4 billion people subscribed to a mobile service, and 4.4 billion accessed the internet from a mobile device. Mobile apps generated more than $400 billion in revenue in 2022.

Shockingly, phones also can help users stay more secure: they fulfill the something-you-have and something-you-are factors that serve as identity proofs in MFA. At the end of 2023, 86% of people used their phone as their primary authenticator (73% believed that smartphones were the most convenient MFA method). That in turn helps to eliminate passwords, which are involved in the vast majority of data breaches.

But for all their cybersecurity potential, phones and other devices haven't ushered in a golden age of perfect security. Threat actors just won't let us have nice things: Mobile malware samples increased 51% year-over-year from 2021 to 2022. In detailing ransomware targeting patterns, Microsoft has "observed that 80 to 90 percent of all compromises originate from unmanaged devices." Forrester found that employee-owned mobile devices were the second most common target of external attacks, following IOT devices.

Despite their MFA potential, users' phones introduce significant risks. Nearly three-quarters of all 2023 RSA ID IQ respondents (72%) believed that people frequently use personal devices to access professional resources. The same survey found that nearly all (97%) cybersecurity experts believed that users' phones represented critical cybersecurity risks because users:

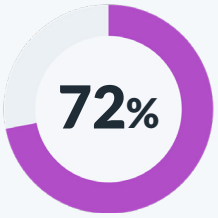
- **Opened more emails** on their mobile devices than on desktops
- **Had more difficulty** scrutinizing those emails on mobile devices
- **Accessed professional resources** from personal devices

Throw in the fact that personal devices tend to have fewer security controls than managed devices, and it's clear that mobile phones are expanding the attack surface.

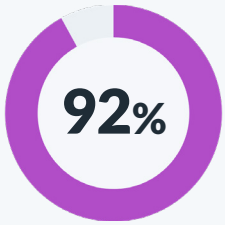
And unlike other risks, businesses aren't about to reverse bring your own device (BYOD) policies: A 2023 Samsung report found that only 15% of businesses issue mobile devices to all their employees. Last year, Zimperium found that 60% of endpoints accessing enterprise assets were on mobile assets. It's no wonder that some outlets were referring to bring your own device (BYOD) as "entrenched" as far back as 2015.

What's an organization to do? Employers can't require users to install security or monitoring software on their personal devices without significant resistance. But they also need a way to control and maintain the inherent security weaknesses that are part and parcel to personal device use within the organization.

2023 RSA ID IQ Report highlights mobile device risks:



of respondents believed that people frequently use personal devices to access professional resources



of cybersecurity experts believed that users' phones represented critical cybersecurity risks

That's why we predict that in 2024, organizations will focus on ways to balance both security and convenience when it comes to users' personal phones. If users are going to use their phones as authenticators, then look for solutions that protect the authentication process itself, without imposing multiple apps and downloads on users' personal devices.

"…mobile devices have become indispensable tools. They serve as vital entry points to a company's key systems, data and cloud-based resources. They can also put these resources at risk.

Mobile devices offer vast improvements in productivity and flexibility, but they also introduce a myriad of security challenges. Striking a balance between robust security, productivity and cost isn't easy. And organizations also need to factor in user experience and privacy too.

Overburdening users with intrusive security measures can deter productivity. But lax security protocols would expose critical company systems and assets to threats. Getting this balance right is a career-determining, future-deciding, board-level issue.

Effectively protecting mobile devices and preventing them becoming the organization's Achilles heel entails leveraging solutions that provide robust security while ensuring seamless user experience."

Verizon 2023 Mobile Security Index white paper

Secure Your Identity Future With RSA.

Sign up for a free trial of RSA ID Plus to see firsthand how we can help keep your organization secure. Whether it's adapting to new threats, harnessing the power of AI, instituting MFA, or developing a full component of identity security capabilities, RSA can prepare your organization for whatever 2024 has in store. As you look for new ways to stay secure, connected, and productive, RSA is here to help.

Start your free 45-day trial of ID Plus

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.