1Password

The Access-Trust Gap

2025 ANNUAL REPORT

1Password

Table of contents

2025 has been a pivotal year for identity security, marked by extraordinary technological breakthroughs and escalating risk.

Artificial intelligence has emerged as the most transformational force since the Internet. And now we are entering a new chapter: The era of agentic AI, where autonomous agents act on our behalf across multiple systems to accomplish jobs previously only achievable by humans.

Yet this wave of innovation is arriving at a moment when the rise of SaaS, generative AI, unmanaged devices, and identity sprawl already strains identity security. Security and IT leaders are grappling with unmanaged and unsafe forms of access that far exceed the capabilities of traditional identity and access management tools. Tools like SSO, which were once touted as universal solutions for managing and securing access, have proven to have significant limitations.

The primary culprit here is *sprawl*. SaaS sprawl has led to inadequate access governance and the proliferation of shadow IT. Device sprawl has led to employees accessing company data on unmanaged and otherwise vulnerable devices. And identity sprawl has contributed to unsafe forms of authentication that circumvent our best security tools.

The result is what we call the Access-Trust Gap: The widening divide between the types of access that security and IT teams can control and the reality of how people – and now AI agents – access sensitive systems and data *in practice*.

Every security tool we've trusted to govern access – SSO, IAM, MDM – is being outpaced by the reality of how people actually work today.

Now we're adding agentic AI into this already fragile ecosystem. It's time to repair the foundations of access management and extend beyond our previous capabilities to ensure contextually aware access everywhere work gets done.

Crucially, security must act as an enabler for workers in this new world. Instead of resorting to the old tactics of locking down tools and devices, modern IT and security teams must empower employees to use the applications and tools they need to be productive, within reasonable guardrails. Failing to consider the needs of workers not only hurts business outcomes but also incentivizes employees to find unsafe workarounds to company policies.

The data in this report shows where we're falling short today, but it also provides a clear roadmap for a future in which we have closed the Access-Trust Gap, empowered our employees, and are ready to embrace the next era of work.

Key insights

The 1Password 2025 Annual Report is based on a survey of over 5,000 knowledge workers commissioned by 1Password. It uncovers several areas where the Access-Trust Gap is widest and where access to protected resources lacks proper governance and controls, including: generative AI, SaaS applications, credentials, and end user devices.

01

AI use is high, but policy compliance is low

73% of employees are encouraged to use AI for some part of their workloads, but 37% admit they do not always follow their company's AI policies.

27% of employees have worked on AI-based applications that their employer did not approve.

02

The app ecosystem is plagued by SaaS Sprawl and Shadow IT

70% of IT and security professionals say that SSO tools are not a complete solution for securing employee identities.

52% of employees have downloaded apps without IT approval.

03

Companies embrace passwordless authentication as credential risks grow

89% of security and IT professionals say their company is actively encouraging employees to use passkeys.

44% of CISOs report that employees using weak or compromised credentials is one of their top challenges.

04

The challenges of endpoint security have evolved past the capabilities of MDM

75% of CISOs believe that MDMs do not fully protect their managed or corporate devices.

73% of employees use personal devices for work, at least half of which are not managed by MDM.

Key insights and findings by country

US Canada France
UK Singapore Germany

01

AI use is high, but policy compliance is low

% employees who only follow their company's AI policy "most of the time:"

↓	30%	38%
	40%	33%
↑	43%	40%

% of employees who have worked on AI-based applications that their employers did not approve:

↓	25%	26%
↑	40%	28%
	30%	27%

02

The app ecosystem is plagued by SaaS sprawl, shadow IT, and invisible access

% of employees who have successfully accessed a prior employer's account, data or applications after leaving the company:

	36%	↓ 31%
	34%	34%
↑	43%	46%

% of employees who have downloaded apps wtihout IT approval:

↑	56%	↓ 45%
	51%	50%
↑	56%	51%

03

Companies embrace passwordless authentication as credential risks grow

% of security & IT professionals who say their company is actively encouraging employees to shift logins to passkeys:

	91%	91%
↓	87%	90%
	88%	↑ 92%

% of IT & security professionals who say that employees using weak or compromised credentials is a top security concern:

	49%	↑ 51%
↓	43%	50%
	49%	47%

04

The challenges of endpoint security have evolved past the capabilities of MDM

% of IT & security professionals that believe that MDM does not fully protect their managed devices:

↓	57%	73%
	73%	↑ 75%
	69%	70%

% of employees who use a personal device for work at least once a month

	75%	69%
	66%	↓ 63%
	70%	↑ 76%

01

As AI adoption surges, security struggles to keep pace

Businesses and employees are rapidly deploying generative AI tools to boost productivity, but security policies and controls have not kept pace. While 73% of employees are encouraged to use AI for some part of their workload, only a fraction operate under clearly defined policies, and this lack of clarity and enforcement exposes organizations to avoidable compliance and data exposure risks.

The results also highlight an alarming lack of safeguards for what AI-based tools employees are permitted to use and how they are permitted to use them. Forty percent of survey respondents say they can only use “company licensed and approved AI for specific tasks,” but 30% say they are “encouraged to experiment with generative AI for any task.”

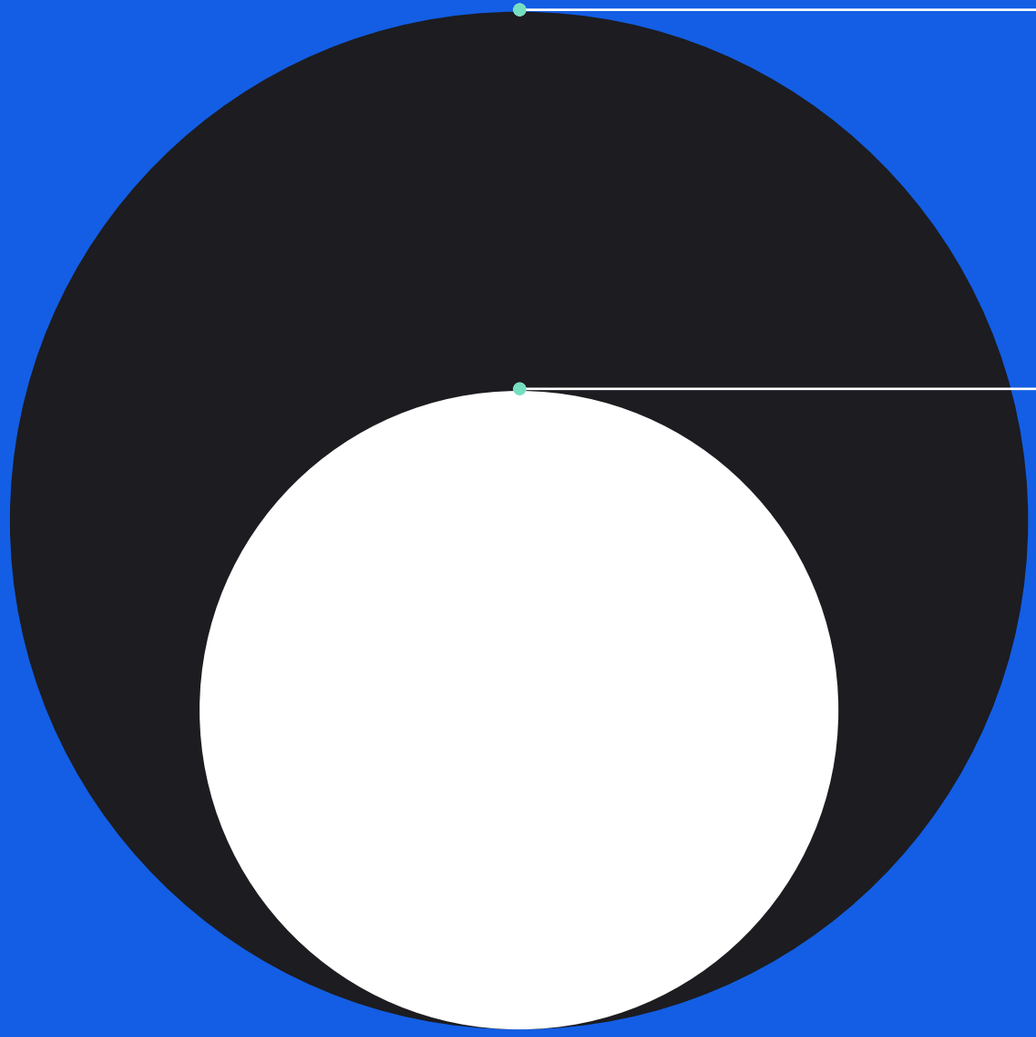
The data suggests that companies lack considered and detailed AI usage policies, as well as the means to enforce them.

This policy gap is compounded by a lack of awareness among less technical employees that their company has an AI policy at all. While only 6% of IT and security professionals believe their company lacks an AI policy, that number rises to 16% among other employees, suggesting that even when guardrails exist, they are not clearly communicated across the workforce.

Likewise, only 1% of IT and security professionals reported not knowing their company AI policy, compared to 11% of other employees.

Q. Do you follow your company's policies regarding the user of generative AI applications?

When workers are aware of their companies' AI policies, the next question is: do they follow them? At first glance, the data here appears supportive: 94% of respondents report following company policies regarding generative AI. But a closer look reveals that 37% of employees only follow company AI policies "most of the time," which means that over a third of respondents actively and knowingly disregard policy when it suits them.



94%

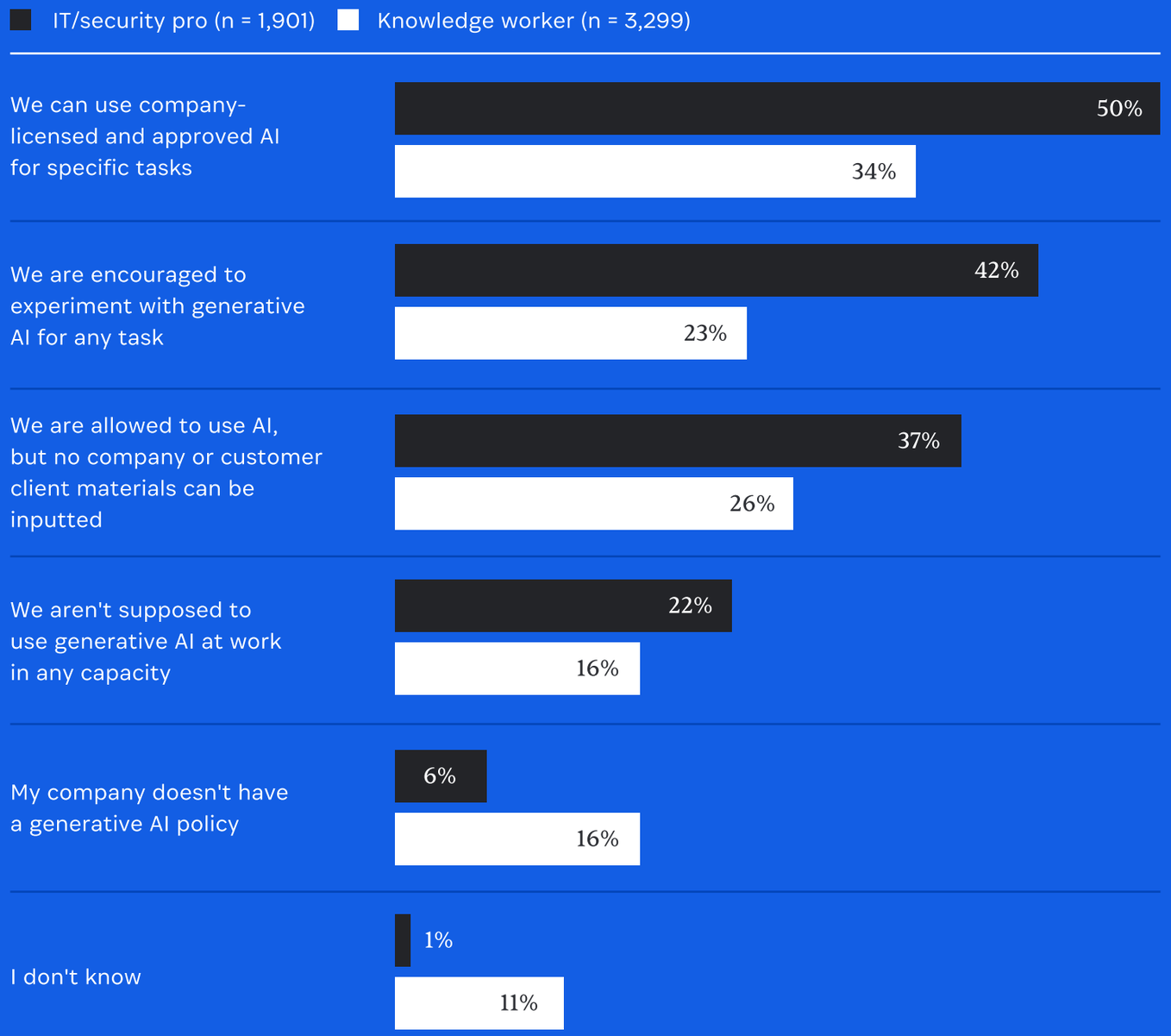
of employees report following company policies regarding generative AI

37%

only follow company AI policies "most of the time"

Base: Total respondents with AI policies, n = 4,198

Q. What is your company's policy regarding employees using generative AI tools at work?



Base: Total respondents, n = 5,200

> The need to balance security and productivity has never been more visceral for security leaders than it is now with the rapid proliferation of AI tooling. The various ways employees are using AI are growing faster than policies can keep up with. Security and privacy teams need the tools to help them understand the usage, put in place controls, and grow with the adoption of these technologies."

Jacob DePriest, CISO & CIO, 1Password

Shadow AI

Shadow AI – the unauthorized use of generative AI tools – has quickly emerged as one of the most pervasive and dangerous forms of shadow IT. AI-based tools used by workers without company oversight or visibility present significant risk; they can absorb sensitive information into their training data, violate legal and compliance mandates, or function as outright malware.

Disturbingly, the data shows that shadow AI is the second-most prevalent form of shadow IT, ranking only behind email.

One in four employees (27%) has used AI-based applications that were not purchased or approved by their company.

> “I know we’ve got data going into these LLMs that we don’t have control over. The best we can do is sign enterprise agreements that offer some legal protections, but if someone uses a tool we don’t have an agreement for, there’s no protection for us.”

Nick Tripp, CISO, Duke University

“

An AI-driven calendar optimization service integrating directly into corporate email systems through ‘read-only roles’ and ‘authentication tokens’ can no doubt boost productivity when functioning correctly. Yet, if compromised, this direct integration grants attackers unprecedented access to confidential data and critical internal communications. In practice, these integration models collapse authentication (verifying identity) and authorization (granting permissions) into overly simplified interactions, effectively creating single-factor explicit trust between systems on the internet and private internal resources. This architectural regression undermines fundamental security principles that have proven durability.”

Patrick Opet, CISO, J.P. Morgan Chase[1]

[1] An open letter to third-party suppliers, JP Morgan, 2025

The security risks of generative AI can be severe; even seemingly innocuous applications can expose sensitive data, produce biased or incorrect outputs, or function maliciously. The risks escalate when AI tools are used for higher-order tasks. If an employee uses an unsanctioned AI tool to input sensitive customer information or IP, and makes an important decision based on the AI’s output, those actions could expose data to training models and potentially fall afoul of legal and compliance obligations. The research indicates that these sensitive AI uses are quite widespread.

Q. When using AI at work, what kind of actions have you taken?

22%
Shared customer call notes to transcribe & summarize

21%
Analyzed customer data with the help of AI

21%
Wrote a report or presentation using company data

19%
Made an important decision by sharing company data

16%
Analyzed company data with the help of AI

16%
Worked on performance reviews or hiring, using employee data

Base: Employees, n=3,292

How to mitigate AI security risks

Generative AI tools offer transformative potential, but like any powerful technology, they introduce new categories of risk, from unintended data exposure to prompt injection attacks. And these risks require a new approach to access governance.

But the genAI revolution happened so quickly that it caught even the most seasoned security professionals off guard, forcing them to adapt to multiple types of risk at once. To improve security for generative AI tools, businesses must shift their approach from reacting to AI to anticipating it.

As a baseline, this requires continuous monitoring for the presence of unsanctioned tools and AI agents and the ability to effectively block them before they can cause any damage.

However, blocking alone cannot be a CISO's entire strategy for managing AI security risks. As we've seen, employees are already willing to go around policies that they don't understand or agree with. This means that security and IT teams must craft detailed, relevant policies for AI usage and ensure the entire workforce truly understands them.

In addition, when workers are discovered using unsanctioned tools, it's vital to understand what benefits they derive from these tools, so they can be directed toward more secure applications to meet the same needs.

Finally, it's vitally important that business leaders design security and access management with the future of AI in mind. The next wave is agentic AI, and it's already upon us. AI agents act autonomously, make decisions, and cross application boundaries without oversight. This requires businesses to tailor their access management approach to these agents, giving them access to the data they need to function, preventing them from exceeding defined parameters, and revoking access when appropriate.

> As these AI-driven solutions continue to proliferate, they will replace legacy enterprise applications that rely on manual user input and static authentication model. Securely managing access for this army of agents will require new tools, explicitly designed to manage the unique needs of non-human identities.
>
> Omdia[2]

[2] How Extended Access Management (XAM) closes the gaps in security, Omdia, 2025

Imperative: AI governance

AI governance is one area where every company must extend beyond its current capabilities, and where best practices and principles are still being defined. Any sensible approach to AI governance must start with discovery, and include the participation of stakeholders from across the organization to balance the (sometimes competing) demands of productivity and security.

01.

Maintain a complete inventory of AI tools in use at your organization and conduct regular audits.

02.

Establish clear policies, enforce appropriate AI usage, and guide users toward safe tools and behaviors.

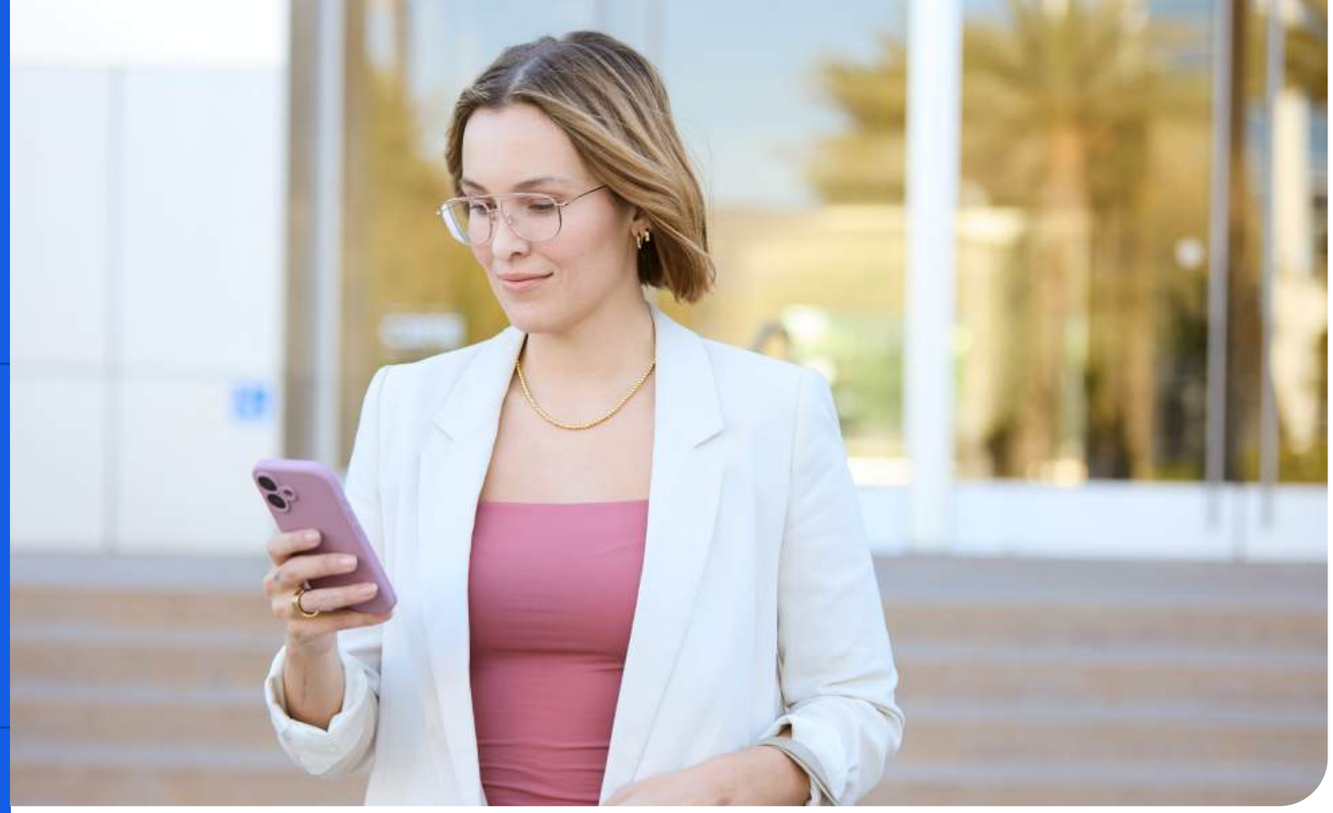
03.

Invest in controls to ensure only company-sanctioned AI tools can access company data.

02

SaaS sprawl and shadow IT are evading security tools

The “SaaS explosion” has been going on for so long that “There’s an app for that” is a punchline old enough to have its own driver’s license. But the proliferation of apps (including web apps) shows no sign of slowing down, so we should probably update the joke to “there are fifteen apps for that, but only one is approved for employee usage and at least two are actually malware.”



The SaaS explosion has long outpaced traditional IT oversight. Today, enterprises face an environment where hundreds of cloud- and browser-based applications are in active use, many without IT’s knowledge or control. Shadow IT is no longer a fringe behavior; it's a foundational threat to modern access governance. And even sanctioned apps pose risks when access is poorly managed, offboarding is incomplete, or they are not protected by SSO.

> “SaaS sprawl has led to a dramatic rise in shadow IT: apps and tools used without the approval or knowledge of security teams. Protecting organizations means securing all the apps used by employees, not just the managed apps.”
>
> Omdia, How Extended Access Management (XAM) closes the gaps in security, 2025

Our survey data highlights the two primary problems that organizations face when attempting to manage their SaaS ecosystem.

Shadow IT

The use of tools outside IT's visibility and control is rampant.

Even known and company-managed applications aren't properly governed across the employee lifecycle.

Applications

In both cases, existing security tools, particularly SSO, are inadequate to discover and govern applications. And in both cases, the potential fallout includes improperly managed permissions, data breaches, compliance violations, and wasted budget on software licenses.

Employees routinely use unsanctioned apps for work

Shadow IT isn't just common, it's systemic. 52% of employees report that they have downloaded work-related apps without IT approval. Furthermore, this is almost certainly an undercount, as many users don't consider browser-based web apps, such as Grammarly or Perplexity, when estimating their usage.

> The real number of employees using shadow IT is probably much higher than 52% because we're not just talking about downloading apps – people use web apps like Grammarly and Monday all the time that expose company data. But because they work through the browser, they don't really think of them as apps."

Brian Morris, VP & CISO, Gray Media

When we asked employees why they downloaded apps without checking with IT, the answers clustered around convenience and productivity. Very few respondents claimed they didn't know they were supposed to ask permission.

Q. Is there a reason you download apps without checking with IT?

Employees engage in high-risk behaviors on these sanctioned apps, from experimenting with AI tools to cloud-based file sharing to software development.

The risks of shadow IT can lead to catastrophic consequences; IBM[4] found that one in three breaches involved shadow data.

45%

It's more **convenient** to use them

44%

My **entire team** uses them

43%

I'm more **productive** while using them

21%

Our company-approved software **doesn't meet my needs**

4%

I **didn't know** I needed to

Base: Employees who have downloaded apps without checking with IT, n=1,709

[4] Cost of a Data Breach Report, IBM, 2025

SaaS access governance and the shortcomings of SSO

SSO is the go-to solution for organizations that want to centrally manage access to their company's apps. SSO positions itself as a complete identity solution that enables secure and streamlined onboarding and offboarding, as well as effective permissions management and the ability to detect unused licenses. In practice, however, 70% of IT and security professionals say that SSO tools are not a complete solution for securing employees' identities[5].

SSO can be plagued by implementation difficulties, is often prohibitively expensive due to the so-called "SSO tax," and there are many types of identities (superadmins, multichannel guests, and legacy accounts) that can circumvent SSO and log into apps via other means.

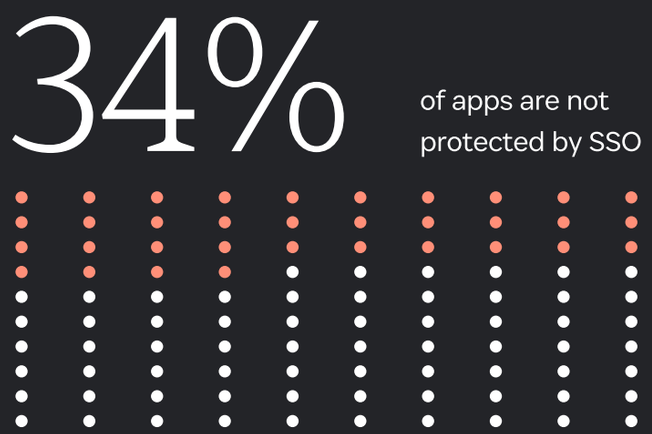
The survey data confirms that SSO usage is far from universal. IT and security professionals reported that an average of 66% of apps are behind SSO. This not only leaves a third of apps unprotected, but it also fails to account for unsanctioned shadow IT.

One major indicator of how SSO is falling short is the amount of access that comes from employees whom IT believed to have been successfully offboarded. Over one-third (38%) of employees have successfully accessed a prior employer's account, data, or applications after leaving the company.

[5] The explanation for this is multifaceted and is examined in detail in Why SSO is Not Enough (1Password, 2025), in which we conduct an in-depth analysis of SSO's advantages and inherent limitations.

1Password

of IT and security professionals say that SSO tools are not a complete solution for securing employees' identities.



Off-boarding is challenging because so many apps are outside SSO, and additionally, SCIM's effectiveness varies by vendor implementation. As a result, you can disable someone's access through your SSO provider, but it's easy to miss something and ongoing monitoring is required."

Mark Hillick, CISO, Brex

How to manage SaaS access governance & shadow IT

Reducing SaaS sprawl, eliminating shadow IT, and instituting more rigorous employee lifecycle management are all interrelated problems. IT and security teams should seek out solutions that can accomplish all three: identifying, securing, and managing access across the entire SaaS ecosystem. But it's important when managing SaaS that the cure not be worse than the disease, and that administrators seek to understand how employees are using SaaS apps before simply cutting off access to them.

Imperative: SaaS governance

To secure the SaaS ecosystem, CISOs must think holistically. Merely discovering shadow IT is insufficient if you lack the means to enforce policy around it. Likewise, managing access via SSO is important, but admins cannot neglect apps outside of it.

01. Invest in technology that allows for the continuous discovery of shadow IT. To be effective, this must include web-based apps as well as locally hosted software.

02. Ensure compliance across your entire SaaS stack: Discover applications and tools that require security and bring them into compliance to meet modern security standards (NIST, CIS, CISA, etc.) and compliance mandates (ISO, SOC, GDPR, etc.).

03. Detect all forms of access to apps and mandate SSO where possible.

04. Manage and secure authentication for apps that cannot be federated behind SSO.

05. Automate SaaS access governance to ensure complete lifecycle management, including for non-SSO managed apps.

06. Maintain a detailed audit trail of your app inventory and employee lifecycle access to apps.

03

The next frontier: Passwordless

Despite years of effort to harden the enterprise perimeter, compromised credentials remain the single most common entry point for attackers[6]. Our own data reinforces this trend: nearly half of security leaders cite weak or compromised credentials as the top impediment to securing their organizations.

This is not a new problem. What has changed is the context. As identity becomes the new perimeter, the authentication stack is no longer a secondary concern – it is the foundation of digital trust. And that foundation, in many organizations, is showing signs of strain.

[6] Data Breach Investigations Report, Verizon, 2025

Credentials remain a persistent risk

Credential hygiene remains poor. Two-thirds of employees admit to engaging in unsafe practices, such as reusing passwords across work and personal accounts, relying on default credentials, or sharing passwords via email or messaging apps. Alarmingly, security professionals – those charged with defending against credential compromise – report higher rates of poor hygiene than their non-technical peers.

These practices have real consequences. Among CISOs who experienced a material breach in the past three years, 50% identified compromised credentials as a root cause, second only to vulnerability exploits.

Indeed, CISOs said that "employees using weak or compromised credentials" was the number one thing impacting their ability to deliver adequate security protections.

Base: CISOs n = 638

Q. What has impacted your team's ability to deliver adequate security protections for your company?

44%

Employees using weak or **compromised credentials**

44%

Employees using **unapproved software**

41%

Inability to enforce security policies on **personal or unmanaged devices**

40%

Lack of **comprehensive device security** capabilities

39%

Inability to stay on top of the latest **patches and updates**

38%

Poor identity **threat detection response** (ITDR)

We also found that among the 34% of IT and security professionals who had experienced a breach with a material impact in the past three years, compromised credentials were the second-most common factor, after vulnerability exploits.

Q. What were the primary factors that contributed to the data breach or security incident?

42%

DATA EXFILTRATION

50%

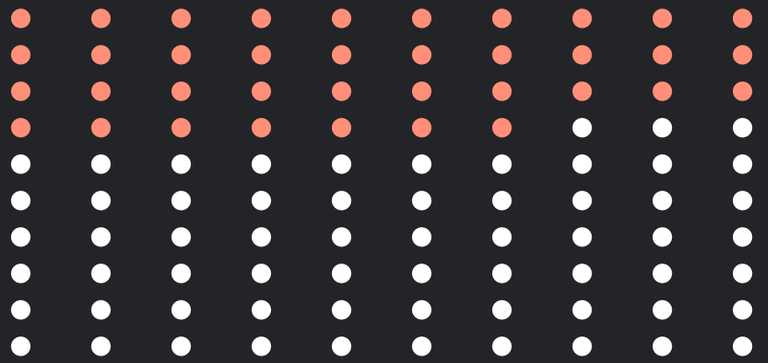
COMPROMISED CREDENTIALS

38%

UNMANAGED/ UNAPPROVED APPLICATIONS

37%

UNMANAGED/ UNAPPROVED DEVICES



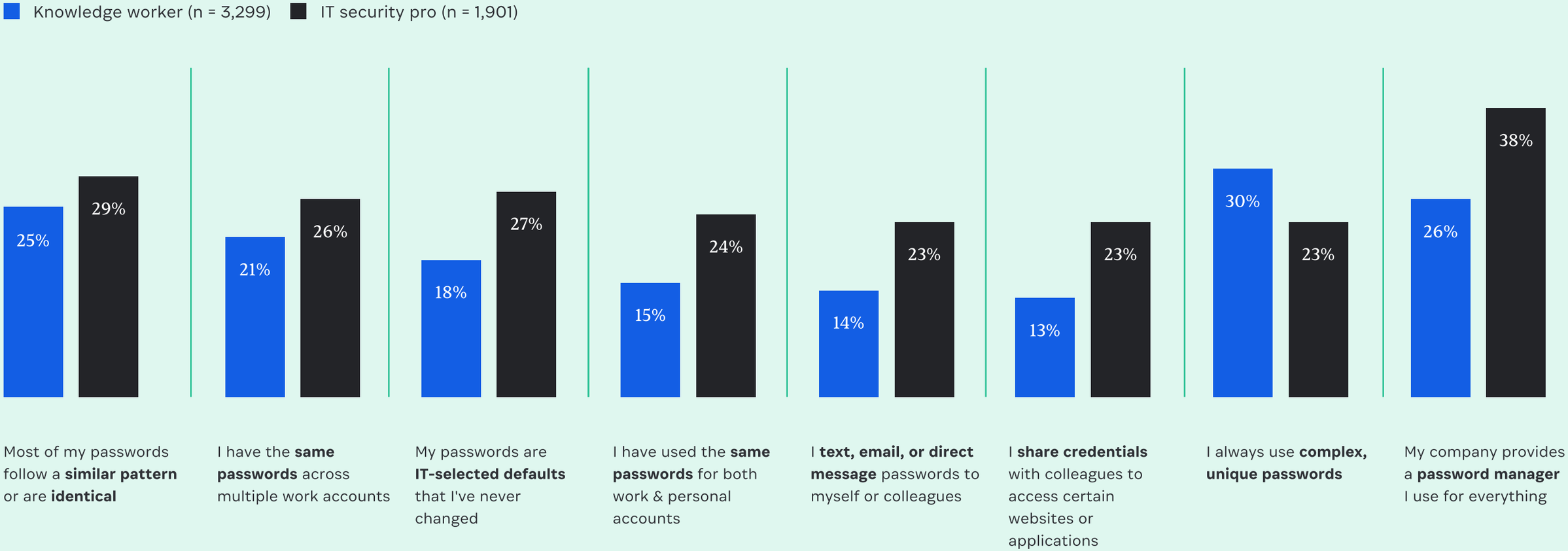
53%

VULNERABILITY EXPLOIT

Base: IT/Security pros who have experienced a data breach in the last three years, n = 884

Q. Which of the following are true about the passwords you have used at work within the last year?

Password threats may persist even in the face of stronger authentication because **employee password practices are actually getting worse.** Our data poor password practices, an increase from last year[7] (61%). Additionally, IT and security professionals tend to report worse practices than their peers.



Base: Total respondents, n = 5,200

[7] Security and productivity in the age of AI, 1Password, 2024

In F1, data is everything, so we can't compromise on security, but we also can't afford tools that slow us down. Credential and secrets management was an area where we saw an opportunity to improve on both security and speed, by reducing the amount our team has to directly handle credentials.”

Mark Hazelton, CSO, Oracle Red Bull Racing

Leaders & employees are embracing passkeys

It's unrealistic to phase out password-based authentication entirely, but our survey found a high degree of enthusiasm for replacing it with passkeys, where possible.

89% of security and IT professionals say their company is encouraging or planning to encourage employees to shift their logins to passkeys. Meanwhile 41% of employees have adopted passkeys where they're available, and 25% say they haven't but would happily switch from passwords to passkeys if that were an option. These biometric-based credentials offer phishing-resistant authentication without requiring hardware keys or introducing friction.

Passkeys are appealing to security leaders because they're so much more secure than passwords, and they support numerous regulatory and compliance standards, including GDPR, HIPAA, and CCPA, which require phishing-resistant authentication, data minimization, and encryption. For employees, passkeys appeal because they are intuitive and seamless to use across their devices.

89%

of security and IT professionals say their company is encouraging or planning to encourage employees to shift their logins to passkeys.

> "I'm not surprised by the enthusiasm for passkeys, because the companies pushing passkeys are making it so easy to convert to them—one click and it's done."
>
> Brian Morris, CISO, Gray Media

How to chart a course to passwordless

The movement toward passwordless authentication is not binary. For most enterprises, it will be a multi-year transformation – one that must be carefully sequenced across technologies, workflows, and regulatory frameworks. During this transition, passwords will continue to coexist with newer methods of authentication. With that in mind, organizations must simultaneously strengthen the credentials they still depend on and accelerate the deployment of those that will eventually replace them.

The push toward passwordless authentication is not only a security imperative, but also a response to broader shifts. The proliferation of unmanaged devices, the decentralization of SaaS, and the emergence of agentic AI all point toward a future in which human and machine identities access sensitive systems from multiple endpoints, outside traditional control planes.

Legacy authentication paradigms cannot scale to meet this reality. Passwordless authentication offers a more durable solution: one that enables strong identity assurance without sacrificing user experience.

[8] How Extended Access Management (XAM) closes the gaps in security, Omdia, 2025

> “A truly passwordless environment has long been the dream of security leaders. However, fully eliminating passwords is a years-long undertaking, and authentication must be as secure as possible at every step along the way.”
>
> Omdia[8]

Imperative: Passwordless

As we've established, "passwordless" authentication isn't a binary, and passwords are unlikely to be fully deprecated anytime in the foreseeable future. With that in mind, the goal of passwordless should be to remove users as much as possible from the authentication flow, so their exposure to raw credentials is minimized.

01. Define your roadmap and process to replace weak passwords with unique passwords, add MFA, and transition to passwordless authentication, including passkeys.

02. Task your Compliance Officers with verifying that the passwordless implementation aligns with regulatory frameworks, such as ISO, SOC 2, and GDPR.

03. Deprecate knowledge-based authentication factors like SMS codes wherever possible.

04. Equip employees with clear guidance and ongoing support with transitioning to strong passwords, MFA, and passwordless solutions.

05. In the cases where passwords remain necessary, require the use of an enterprise password manager to facilitate secure storage and sharing of credentials.

04

Endpoint security neglects too many devices and too many risks

Today’s security architecture was built for a world where people worked in corporate offices, on company-owned devices, using applications provisioned by IT. Plainly, this world no longer exists, and the disparity between past and present is particularly evident when we consider endpoint security and management.

Mobile Device Management (MDM) is still the default solution for employee devices, but it has fundamental shortcomings. While MDM is capable of implementing baseline compliance settings on company-owned devices, it is not designed to assess the constantly shifting variables of a hybrid, multi-device, SaaS-heavy workforce. MDM is only capable of assessing a limited number of device attributes, is not a suitable solution for personal devices, and most crucially, does not make device health part of every authentication attempt – a core requirement of Zero Trust security.

To adapt to the new reality of work, security and IT leaders should explore contextual access, particularly in the case of devices. Under this approach, device access is dynamically granted and revoked based on device posture, which can change frequently. Instead of falling back on rigid binaries, like managed vs unmanaged, this approach allows companies to tailor device compliance to their specific needs.

MDM leaves holes in endpoint security

Unmanaged personal devices pose particular risks for cybersecurity, but security professionals acknowledge that “managed” devices can also be vulnerable. When asked how well they felt that MDM protected their managed devices according to various considerations, the answers were stark.

MDM solutions are a foundational part of endpoint management, but they are only one component of device security and are constrained by fundamental limitations.

> Our MDM solution doesn't provide real-time device health checks or proactive monitoring, which makes it difficult to quickly identify and address vulnerabilities or performance issues."

CISO, multi-billion dollar sports franchise

CISOs believe that MDM does not fully **protect** their managed devices

75%

CISOs think that MDM doesn't allow them to keep their devices fully **compliant**

64%

CISOs think that MDM doesn't fully keep their devices **healthy**

61%

> MDM can do very little for compliance issues that can't be solved through blunt automation. MDMs have fairly limited abilities to report on and enforce device posture, usually by acting as an admin over basic settings. That leaves teams with no solution for – or even awareness of – major risks to their fleet."

1Password[9]

[9] Why MDM isn't enough for device security, 1Password, 2025

Most workers use personal devices, often in violation of company policy

Nearly three-quarters (73%) of employees use their personal devices for work at least once a year.

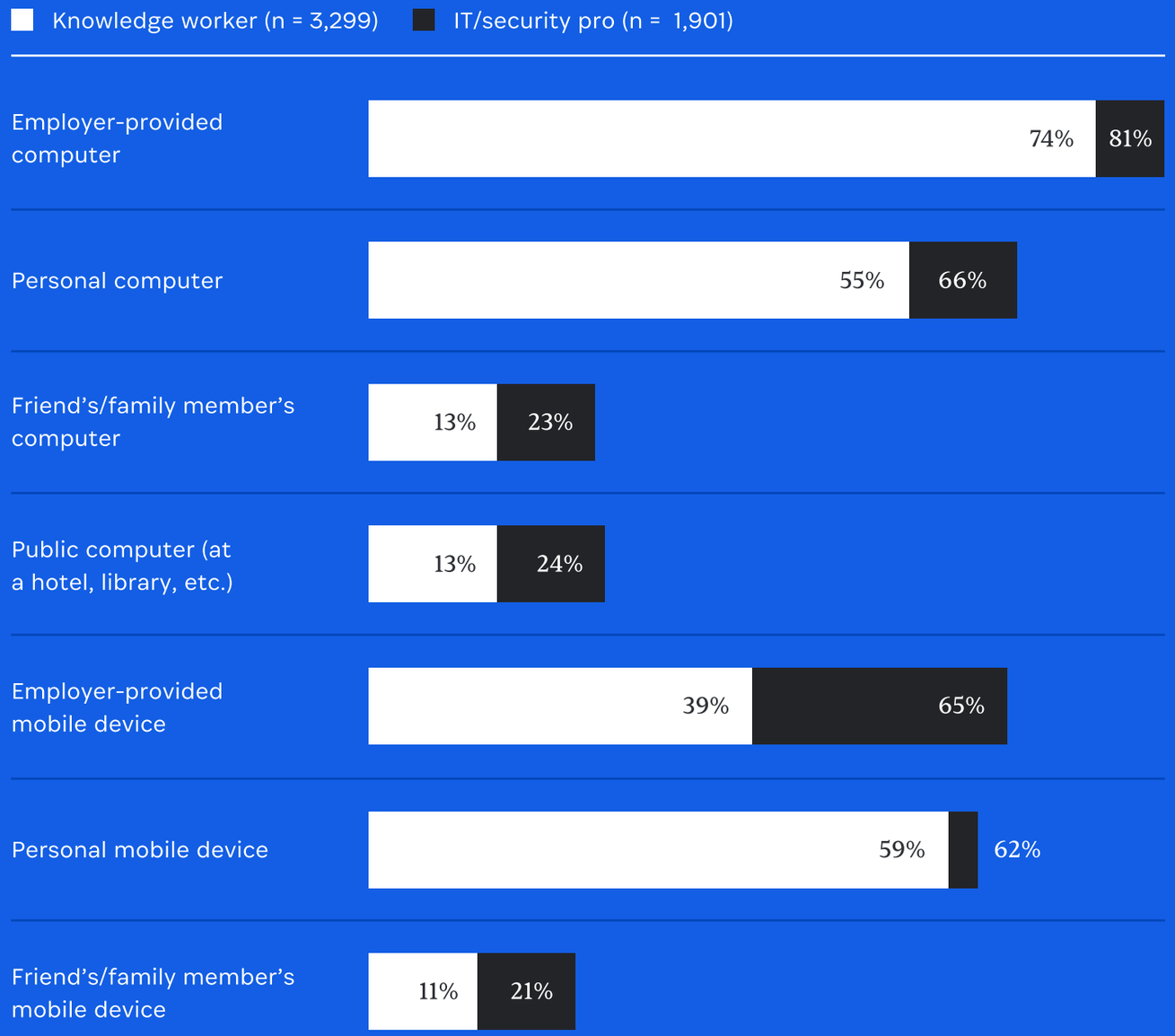
56%

of employees use a personal device on a weekly basis

67%

of IT and security professionals use a personal device on a weekly basis

Q. Which of the following devices have you used for work in the past year?



Personal and BYO-devices are much more vulnerable to compromise than company-owned devices. They are less likely to have antimalware and updated software, and more likely to contain unsanctioned shadow IT and improperly stored sensitive information. This is partly because they often lack MDM and EDR tools to ensure they meet baseline security requirements. Among IT and security professionals with a BYOD policy, roughly half reported that these BYO-devices were enrolled in security tools.

It would be alarming enough simply to say that half of all personal devices used for work lack basic protection. But this data does not account for employees who use personal devices in violation of their company's policy. Hence, the number of unmanaged devices being used for work tasks is undoubtedly higher than 50%.

Indeed, 21% of respondents report that their company has an anti-BYOD policy, but it is not actually enforced.

> "It's so hard to control BYOD. For example, if you've got Office 365, it's very hard to keep people from putting it on their personal devices. We are anti-BYOD for computers, but if you don't have an MDM that evaluates devices to see if they're company-owned, it's hard to stop."
>
> Brian Morris, CISO, Gray Media

The risks associated with personal devices vary depending on how employees use them. A worker checking Slack or email on their phone isn't totally without risk; nation-state threat actors are known to target emails because they're rich with sensitive data and provide an opportunity for impersonation.

Still, this threat pales in comparison to a high-level admin accessing a company's production environment on an unmanaged device. Indeed, according to Microsoft[10], 92% of all successful ransomware compromises originate through unmanaged devices.

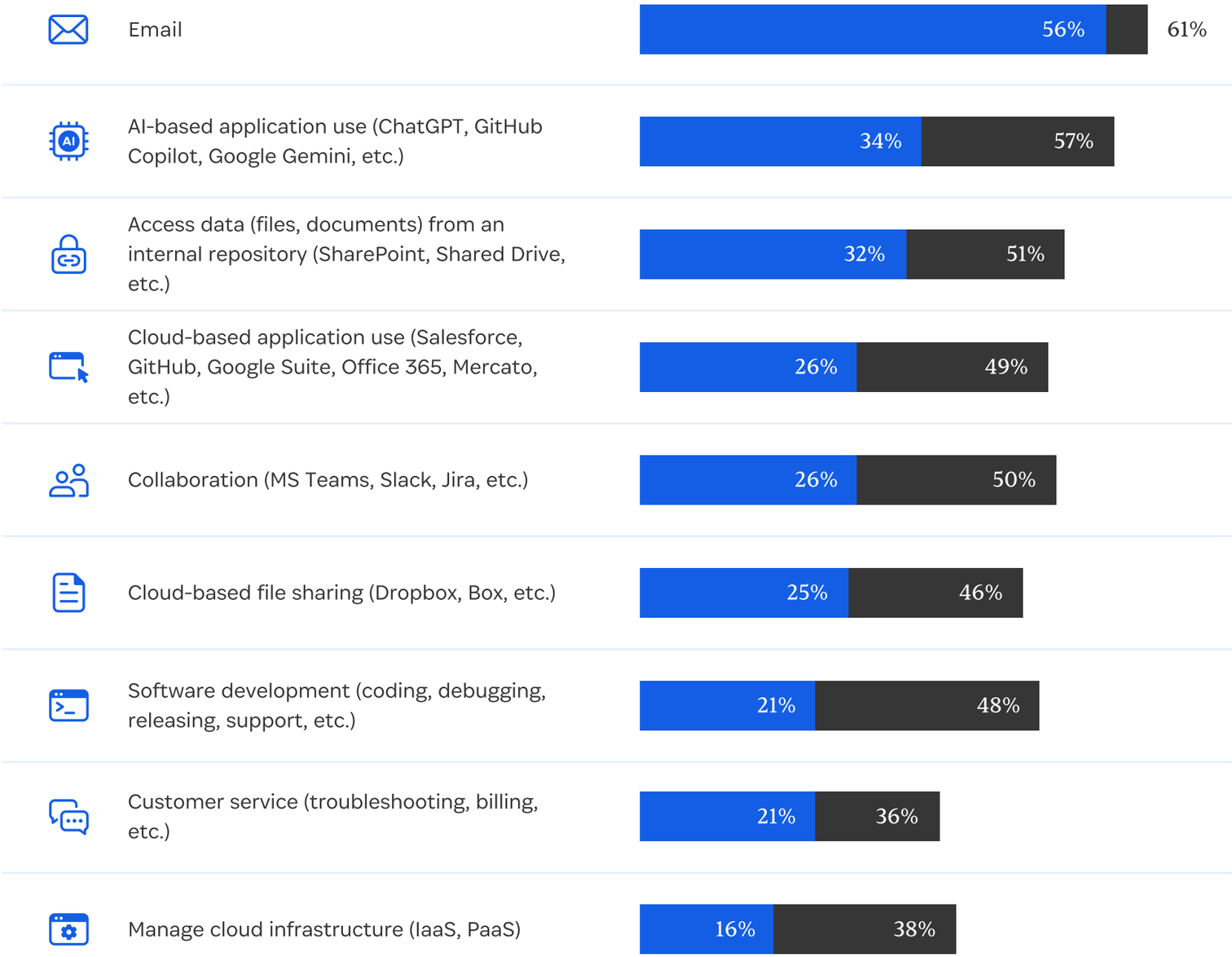
Concerningly, many respondents who use personal devices report engaging in risky behaviors that could expose sensitive data if their devices were compromised. Additionally, IT and security professionals were much more likely to report using personal devices for sensitive tasks.

[10] Microsoft Digital Defense Report, Microsoft, 2024

Q. What types of work tasks have you done on a device that's not provided by your employer?

Knowledge worker (n = 3,299) IT/security pro (n = 1,901)

The data shows that personal device usage goes far beyond workers occasionally checking their work email on their phones. Instead, workers are regularly performing sensitive tasks on these devices.



Base: Employees + IT/Sec Pros using personal devices for work, n = 4,642

Q. Please indicate the reasons why you would use a device that was not provided by your employer for work purposes.

So why do workers use personal devices instead of company-provided ones? The answers often came down to simple preference, but in some cases, respondents admitted their goal was to avoid their companies' security policies.

Convenience

34%
I like my device better

29%
Using the same device for personal and professional purposes is convenient

30%
I am allowed and encouraged to use my personal device for work-related tasks when I am away from my work computer

Productivity

21%
I left my device in the office

12%
My corporate device is unable to handle my work responsibilities

20%
Devices are not provided for remote work (working from home, etc.)

Policy workarounds

24%
Certain websites that I need to do my job are restricted on work devices

23%
Certain applications that I need to do my job are restricted on work devices

17%
Getting through work-related security requirements (usernames/passwords, VPN, etc.) is frustrating

Base: Employees using personal devices, n = 2,915

> The reason employees use personal devices is because it's more convenient for them, and if it's more convenient, they'll use it for everything, and that introduces risk to any machine that has Duke data on it. We're working toward a future where we have more insight into these devices."

Nick Tripp, CISO, Duke University

How to secure access from all end user endpoints

As previously stated, security leaders and IT must invest in solutions that can supplement MDM.

> Recent years have seen an onslaught of ransomware attacks, phishing schemes, and evolving regulatory and compliance standards. They have also seen new security and compliance challenges posed by remote and hybrid workforces, and the increasing use of personal devices in corporate environments. These changes require IT and security teams to gain more visibility into “unmanaged” devices and call for more robust security on managed devices.”
>
> 1Password[11]

[11] Why MDM isn't enough for device security, 1Password, 2025

Imperative: Endpoint security

Any strategy for securing devices must consider employee productivity and convenience in order to be effective. As previously discussed, these are some of the most common drivers employees give for going around company policies. When possible, allow users to remediate their own device issues, rather than forcing them to file an IT ticket. Blocking users on unsafe devices is only half the battle; the other half is getting them unblocked.

01. If allowing personal devices, then ensure all devices meet compliance requirements. Adopt privacy-conscious solutions that employees will tolerate on their personal devices.

02. If banning personal devices, then ensure unmanaged devices cannot access data.

03. In all cases, verify that only secure, compliant devices can access company resources.

04. Guide users to self-remediate compliance issues.

05. Invest in technology, such as device trust, that can dynamically block access based on real-time device posture checks. Establish a single, cross-platform pane of glass for all devices.

1Password

Methodology

1Password conducted this research using an online survey distributed by PureSpectrum among n=5,200 adults aged 18+ who currently work in a desk job position, with n=1,500 North American respondents (U.S. + Canada), n=1,000 United Kingdom, n=1,000 Germany, n=1,000 France, and n=700 Singapore.

Within each country, the sample included a subset of IT security professionals: n = 500 in North America (U.S. and Canada), n = 400 in Germany, n = 400 in France, and n = 200 in Singapore. The sample also included a further subset of contractors, manager titles or greater, and CISO titles. The sample was balanced by gender, age, and company size, with an international geographic spread of respondents.