1Password

Managing the unmanageable

Wrangle shadow IT and unmanaged access across every team

Shadow IT and access management: A universal challenge

If you've worked in IT or security for any amount of time, you're undoubtedly familiar with shadow IT: any technology being used by employees without centralized management or oversight.

Shadow IT is a major concern, and it's not hard to understand why; 1Password's 2025 annual report, *The Access-Trust Gap,* found that over half (52%) of employees have downloaded apps without IT's approval. Furthermore, the report also found that shadow AI is a growing problem within organizations. 24% of employees have used unsanctioned AI tools, and 37% of employees admit they don't always follow their company's AI policies.

Vulnerability exploits and credential compromise are the leading attack vectors used to breach companies, meaning that every unmanaged entry point represents risk. If IT and security don't know that a specific tool or application exists, it's impossible to manage or secure it. Among other issues, it's impossible to know how access to shadow IT applications is being managed. Are employees using weak, default credentials? Are they sharing them across teams or with outside vendors? Are they retaining access to them after they leave the company?

The reality is that virtually every organization has shadow IT being used across any number of teams. And for the most part, there's nothing malicious about it; employees just want to use whatever tools will make them most productive.

The challenge for IT and security teams is twofold: discover these shadow IT applications and apply proper governance to them.

Why SSO is not enough to manage shadow IT

Most enterprise organizations attempt to manage access with single sign-on (SSO) tools. This is an important first step, but SSO has significant limitations, and is only effective for the tools that IT and security teams manage. This leaves critical gaps in an identity and access management (IAM) strategy, such as:

- Websites and applications that can't be federated via SSO (such as social media accounts)
- Tools for which SSO integration is prohibitively expensive (known as the "SSO tax")
- Tools for which SSO integration is either impossible or technically unfeasible
- Shadow IT

It's not hard to understand why 70% of IT and security professionals say that SSO is not a complete solution for securing employee identities. All of these systems and sites that aren't managed by SSO represent risk to your company.

Note: To learn more about the limitations of SSO, check out 1Password's ebook: Why SSO is not enough for identity security.

Shadow IT: Securing it means enabling it

Shadow IT is a growing problem, and it poses serious risks to organizations. 1Password's annual report surveyed over 5,000 knowledge workers, and found that:

52%

of employees have downloaded apps without IT approval.

73%

of employees use personal devices for work, at least half of which are not managed by their organization.

34%

(on average) of apps are not protected by SSO.

Brian Morris,VP & CISO at Gray Media, pointed out that "The real number of employees using shadow IT is probably much higher than 52%... 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."

According to IBM, 35% of breaches involve data stored or shared through unauthorized applications or cloud buckets. What's more, breaches involving unmanaged data tend to cost 16.2% more for the impacted company, while also taking more time to identify and contain. Companies can't afford to do nothing about the rising issue of shadow IT, but the question of what they should do is far from simple.

There are really only two options when it comes to dealing with shadow IT: say "no," or move to the rule of "yes."

IT and security teams have traditionally defaulted to “no,” but that philosophy has failed to eliminate shadow IT. Organizations have spent millions of dollars on SSO, IAM, and privileged access management (PAM) tools for more than a decade to stop employees from using shadow IT, yet the issue persists.

The old approach to security – restricting access to tools, devices, and apps in the name of control – made sense when IT managed every network, device, and system. But that world is rapidly changing.

Today’s IT and security teams should find ways to enable everyone at their company to use the tools they need to be successful, while also securing access to those tools.

It’s important to take a holistic approach to tackling shadow IT. Historically, the security of certain teams has been prioritized over others, but today, nearly every department deals with sensitive data that could harm the company if exposed, or serve as an entry point for bad actors. So IT and security should begin by understanding and prioritizing the risks that shadow IT can pose to different teams.

	Information Technology (IT)	Engineering	Finance	Human Resources (HR)	Marketing
What level of security risk do these teams possess?	High	High	High	High	High
Priority of security for these teams	High	Medium	Low	Low	Low

How to manage shadow IT across different teams

Engineering

Developer secrets need an extra layer of protection from code to cloud

Team	Engineering
Responsibilities	Developing and building a company's products and/or internal and external applications
Shadow IT & Access Challenges	• Developer secrets need an extra layer of protection because of privileged access to sensitive data and infrastructure • Developers often require additional tools or services to meet deadlines or work efficiently; for instance, they may need both an Apple and Windows computer to use for testing purposes • Teams struggle to gain visibility into the health and security of developer credentials like SSH keys • Developers often feel that security/IT policies and processes interfere with productivity and innovation

Meet the engineering team

Engineering teams often have access to a company's most critical infrastructure and data. They also use specialized secrets like SSH keys, API tokens, and other infrastructure secrets to access systems and integrate applications. As such, it's critical to empower them to stay secure.

Engineering and security

As Siri Varma, tech lead with Microsoft Security, put it, “Developers often prioritize speed, functionality and time-to-market, while cybersecurity teams prioritize safety and risk mitigation. This can lead to friction when security policies impose measures that developers feel slow down their workflow.”

Developers often look for faster workarounds to get around that friction - like hard-coding credentials or storing secrets in plain text. It’s a risky habit: GitHub found 39 million secret leaks in 2024, and Verizon found that the average time to remediate leaked GitHub secrets is 94 days. And these bad habits are only getting more dangerous with the advent of agentic AI tools that need broad permissions to operate and can wreak havoc if left to operate without proper controls.

The key to securing the engineering team – and driving adoption of security tools and policies – is to reduce friction as much as possible. This means creating streamlined approval workflows when an engineer requests access to a new tool. It also means enabling developers to work without directly exposing secrets. For instance, 1Password’s developer tools let developers generate, store, and share secrets while they remain encrypted. With these safeguards in place, engineers can experiment with new tools or build AI agents without handing over the keys to the kingdom.

Finance

Managing finances and reputational risk

Team	Finance
Responsibilities	Organizational finances, managing financial and reputational risk
Shadow IT & Access Challenges	• Services used often not supported by SSO, such as bank accounts • Sharing of sensitive data across internal and external teams • Financial impact of trying to secure everything possible behind SSO

Meet the finance team

In addition to meticulous budgeting and forecasting, the finance team actively maintains accurate financial reporting to adhere to compliance standards. Finance handles critical financial data such as the company’s banking credentials, confidential audit reports, and financial reporting.

Finance also often has access to customer information and payment systems, data which requires strict security protections under standards like PCI DSS. As such, the Finance team requires robust measures to protect every user and, in turn, the organization.

Finance and security

Finance teams face distinct challenges, as they have access to the organization's most sensitive financial data. Malicious access to this data can significantly impact the company's reputation and financial standing, so it's absolutely necessary to protect every user on this team.

One example of a critical access point for finance is the organization's banking credentials. Mismanagement of these credentials exposes the organization to significant risk, as it could lead to direct access to the company's cash flow.

Finance teams not only have access to confidential financial data, they also often need to share documents with external partners like auditors, investors, or board members. External sharing may happen through unencrypted email or a messaging application, causing risk to the business and its confidential information.

Safeguarding finance requires proper credential storage and the ability to securely share sensitive data. Furthermore, every finance team wants to avoid the high costs that come from a breach, making security a key priority for this team.

Your finance team also has to manage and forecast budgeting and spend for the entire organization. A large portion of that spend includes the cost of the software and tools each team needs to perform their day-to-day roles. Trelica by 1Password helps teams eliminate unnecessary spend by identifying unused licenses and redundant applications, driving significant cost savings while reducing the attack surface.

Human resources

Building a strong workforce and workplace

Team	Human Resources
Responsibilities	Workplace environment, and attracting, developing, and retaining talent
Shadow IT & Access Challenges	• Access to highly sensitive employee data that must be protected • Sharing of sensitive data across internal and external teams • Managing the employee lifecycle, including a critical role in onboarding and offboarding

Meet the human resources team

The human resources (HR) team is dedicated to employee management, nurturing employee growth through training and development initiatives, and ensuring a positive workplace culture. This team also focuses on making sure your organization is compliant with labor laws, benefits administration, and enhancing overall employee satisfaction. All of this means they need to access and share confidential employee information, including personal identifiable information (PII), day in and day out.

HR and security

In their daily workflows, HR teams need to use, access, and share credentials to platforms that manage confidential employee details, process applicants, background checks, and other recruitment details. HR teams also often need to share sensitive company or employee documentation with external partners such as prospective employees, contractors, or employment agencies.

This information often needs to be quickly accessible and shareable, but it's also a critical security and compliance concern. Viking Line, for instance, was fined 230,000 euros under GDPR, after it was found that they were improperly storing and handling employee health data in their HR system.

Without a standard protocol or process to securely share with staff outside the company, your HR team may share confidential information through unsafe channels, greatly increasing the risk of a data breach or compliance failure.

Marketing

Building brand, pipeline, and a successful go-to-market strategy

Team	Marketing
Responsibilities	Company brand and reputation, product marketing, and supporting go-to-market functions
Shadow IT & Access Challenges	• Services used often not supported by SSO, such as social media platforms • Sharing of sensitive data across internal and external teams • Teams often have access to sensitive customer data

Meet the marketing team

The marketing team tends to work closely with cross-functional teams to generate leads, nurture customer relationships, and optimize the customer journey.

The marketing team has direct access to your company's social media accounts, handles confidential campaign spending and reporting, and often has access to sensitive customer data. It's incredibly important to safeguard this data and place guardrails on how users access this data.

Marketing and security

The marketing team accesses a variety of applications for customer relationship management, project management, email marketing, and website analytics, many of which may not be covered by SSO.

Marketers require quick, easy access to a large number of platforms to maximize their productivity, but they are often faced with friction when it comes to managing secure credentials. This growing need to maximize productivity means users often take shortcuts in their management practices (shared spreadsheets or reused credentials, for example), which sacrifices company data security. These productivity needs have also driven marketing organizations to be at the forefront of AI adoption, with 59% of global marketers considering AI to be a top trend for campaign optimization.

If companies don't enable marketing orgs to use cutting-edge AI tools, it can easily lead to a proliferation of shadow AI. Unsanctioned AI tools can be malware in disguise, but even legitimate tools can pose serious risks to organizations if they're given unmonitored access to sensitive data. It's a risk that security teams should take seriously, as 27% of employees have worked on AI-based applications that their employers did not approve.

The marketing team also collaborates heavily with external partners like analysts, agencies, and contractors, who need access to company information to support various initiatives. The marketing team must be empowered to securely share analytics, credentials, campaign spend details, and more with external collaborators, while adhering to the principle of least privileged access, so that only *intended* individuals have access to intended data.

Information technology

Supporting and enabling the entire organization

Team	IT
Responsibilities	Acquisition, provisioning, and management of technology tools and services
Shadow IT & Access Challenges	• Procurement and implementation of tools and applications • Making sure technology and services meet organizational and security requirements • Securing all of the teams above

Meet the IT team

As you likely know, information technology (IT) teams touch on many areas of a company's operations. They're the front line of a company's defenses. In addition, IT teams play a critical role in actively educating and empowering employees to foster a culture of strong security practices. Finally, the IT team aims to streamline operations and enhance efficiency in managing company information.

IT and security

Where the teams discussed earlier have specific tools, services, or sharing that must be secured, IT teams play a central role in securing all those aforementioned tools, and all the users who access them. Unique vulnerabilities exist across every department, and IT is in need of comprehensive solutions to keep each user protected.

Unfortunately, IT is often bogged down by manual processes, such as onboarding or offboarding employees. At the same time, IT is in charge of responding to tickets requesting access to software or tools. All this can make it difficult for teams to find time to take a broader look at their company's security needs.

With the ever-growing number of managed and unmanaged SaaS applications, security solutions need to reduce IT's burden and help them focus on issues like shadow IT. SaaS management tools like Trelica by 1Password help teams automate manual processes related to securing SaaS access.

As Carol Atkins, Software License Asset Manager at Zuora, put it after the company adopted Trelica by 1Password, “I now spend less than 10% of my day doing routine SaaS management, which is impressive bearing in mind the number of apps we use.” Trelica by 1Password delivered 10x ROI for Zuora in just six months, indicating just how impactful it can be to manage SaaS access and shadow IT.

Enable and secure

Managing shadow IT across the organization

Given the security challenges posed by each team, how should companies safeguard their entire organization?

The key is to empower every employee across each department with solutions that can make sure that every sign-in and access point is secure, while also giving IT and security teams full control to enforce access permissions.

How 1Password secures and enables access

The 1Password Enterprise Password Manager (EPM) provides teams with a centralized solution to use, access, and share critical company data with role-based access controls, while ensuring that users adhere to security policies.

1Password can do this while also streamlining end-user workflows to maximize productivity so that employees don’t need to take shortcuts to stay productive.

1Password Vaults enable IT admins to securely allocate credential access to users based on factors like their role and the length of time they require access. For instance, teams that work with third-party partners can give temporary and encrypted access to sensitive data on an as-needed basis.

Trelica by 1Password is a SaaS Management Platform that provides full-lifecycle governance to every SaaS app, even those that aren’t behind SSO. With continuous app discovery, it also uncovers the use of any unapproved applications across the company, to help uncover and manage the use of shadow IT and AI.

1Password also provides specialized tools to meet the security needs of different teams. For instance, 1Password’s developer tools provide specialized means for engineering teams to manage SSH keys, API tokens, and other infrastructure secrets.

With a partner like 1Password, IT and security teams can begin to manage the unmanageable across every part of their organization. That's why more than 175,000 businesses rely on 1Password to secure their businesses:

Engineering	"As a Senior Data Engineer I appreciate how 1Password simplifies secure credential management for both personal and team use. It allows me to safely store SSH keys, API tokens and database credentials and easily share them with teammates when necessary. The browser extension and mobile app are seamless, and the overall interface is intuitive even for non-technical staff." **Lakshmi B., G2 Quote**
Finance	"With 1Password we set up a shared vault, and there we have everything, and there is no risk of disclosing data. I remember one Friday, in full urgency with a client, that we needed the corporate card to pay for a license. Instead of wasting time searching for it, it was already saved in 1Password, and we used it with secure autocomplete in seconds. That day we finished on time thanks to that, and I thought, "It's over; this app has earned its place here." **Jordan M., Sales Associate, G2 Quote**
HR	"I was able to successfully onboard 300+ users with ease... my adoption rate was 82% in <1 week! Setting up the SCIM bridge for automated user provisioning was key in ensuring my users had a seamless and simple authentication experience to get them going." **Matt S., Head of North American IT Operations and Global IT Security Officer, G2 Quote**
Marketing	"1Password is helping us securely store and share credentials across teams without relying on insecure methods like spreadsheets or emails. It eliminates password fatigue by generating strong, unique passwords for each account and autofilling them across devices. This reduces the risk of breaches, improves compliance, and saves time for both individuals and teams." **Shakhawet Hossain C., Marketing Officer, G2 Quote**

IT	“With 1Password, we consolidated all credentials, API keys, and sensitive notes into a single, encrypted platform. Secure sharing eliminated the need to exchange passwords via email or chat. Role-based access controls and audit logs streamlined compliance reporting and reduced the burden on IT. The elimination of weak, reused, and compromised passwords improved our overall security posture. We no longer waste time on password resets or manual credential updates, productivity has increased, and security risks have decreased across the board.” **Michael M.,IT Manager, G2 Quote**
	“1Password was very easy to get setup and get our users added. We used the user import to manually add all of our users since we have less than 100, it was fast and efficient. We've made several groups and shared vaults and they are being utilized by our end users. Everyone has enjoyed the benefits of using 1Password and not having to remember a ton of passwords for all of the different sites and apps they have to use daily. **Michael M.,IT Manager, G2 Quote**