PROTECTING THE NEW PERIMETER:

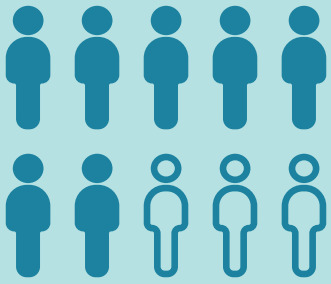
1Password

Identifying and securing shadow IT

In a hybrid world, not only do we work from everywhere, we use a huge number of apps – 130 at the average organization – to get work done. Some apps are sanctioned by the IT or Security team. Many are not.

Those apps not managed by IT/Security are, by definition, a blind spot known as shadow IT. If IT doesn't know about it, it's shadow IT.

And if they don't know about it, they can't secure access to it.



7 in 10 organizations have been compromised by an unknown or unmanaged asset in the past year.

Four considerations to securing your hybrid workforce:

1. **Identity:** How do you validate the person signing in is actually that person?
2. ✓ **Shadow IT and BYOD:** How can you ensure security when access can be from any device or to any application–even those not managed by IT?
3. **Security adoption:** How do you drive adoption of critical security tools while ensuring that productivity is not compromised?
4. **Security costs**: How can you make sure that your investments in security tools are actually worth the cost?

Shadow IT by the numbers

- On average, 30% of applications used by employees are not managed by the company.[1]
- 7 in 10 organizations have been compromised by an unknown or unmanaged asset in the past year.[2]
- 30%-40% of IT spending in enterprises now goes to shadow IT, according to Gartner.[3]

1 Gartner Market Guide for SaaS Management Platforms Dec 22
2 IBM, State of attack surface management, 2022
3 How to eliminate enterprise shadow IT

By some estimates, shadow IT comprises as much as 50 percent of the apps we use to get work done. Employees access those apps from airports and coffee shops, from home and on their commute, from their phones and tablets and personal laptops.

That's the new perimeter businesses are tasked with defending. And that's why, in the world of hybrid work, securing that perimeter starts with identity: by verifying that the people accessing those apps are who they say they are.

We use shadow IT because we bump up against a limitation in the suite of approved/managed apps at our disposal. For that reason, shadow IT can boost productivity. Sometimes it's the difference between whether employees complete a task or not. This is why a growing number of CIOs and CISOs see it as an opportunity to align IT's goals (strong security) with business goals.

30%

the average # applications used by employees are not managed by the company

How to secure shadow IT

1 Understand what workers are trying to accomplish – and help them accomplish it.

Say Sam in Sales needs to share a file with a prospect, but no approved/managed applications allow them to do that. As a workaround, they create an account on a file-sharing service, upload their files, and send the link to the prospect. IT has no way of knowing whether the password Sam created for the file-sharing service is weak, reused, or even compromised.

2 Understand the (growing) risks of shadow IT

1Password research found that 63.5% of respondents had created an account their IT department didn't know about in the previous 12 months. Gartner estimated that one-third of successful cyberattacks will be on data stored in shadow IT infrastructure.

3 Incorporate an EPM into your identity and access management (IAM) stack

Single sign-on (SSO) can help by signing employees in to a portfolio of apps using a single, strongly vetted identity. But SSO only protects managed apps, not shadow IT.

Enterprise passwords managers (EPMs) fill the gaps in your sign-on security model by securing access to the unmanaged applications that SSO doesn't. They do the work of logging in so workers don't have to by generating strong, unique, random passwords, then automatically filling in those credentials. Leading EPMs also support passkeys, a more secure alternative to passwords.

Your business needs 1Password

1Password was built to secure hybrid workforces, making it easy to:

- Protect company data in both managed and unmanaged apps. Ensure your employees can secure any app with strong, unique credentials while giving them the flexibility to choose their own apps for work.
- Prevent breaches with active threat detection. Spot security issues quickly with a single view that brings together data breaches, password vulnerabilities, and employee usage insights.
- Manage access to company data. Control which groups can access specific vaults, and limit who can create a vault or invite new users. You can also set custom policies – minimum password requirements or mandating two-factor authentication, for example – to align with company security policies.

For more information on securing your hybrid workforce, download The new perimeter: Access management in a hybrid world, or contact us to speak with a 1Password security specialist.

1Password