1Password

Extending Access Management

Why zero trust requires going beyond traditional IAM – and how to do it

1

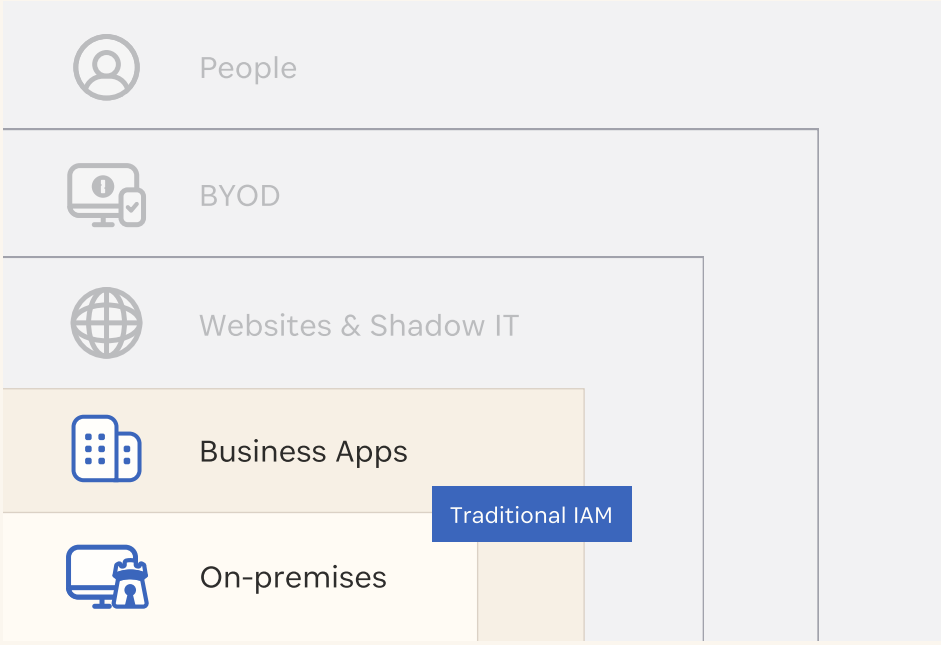
INTRODUCTION:

The Access Trust Gap

Remote and hybrid work have become the standard, not the exception – and it's clear work is never going back to how it used to be. Flexibility is increasingly becoming the expectation. Not just in terms of where and how we work, but also with regards to the devices and applications we use daily.

Traditional approaches to identity and access management (IAM) were built for another time–a time when work required employees to be in the office, on a corporate network, and working from a corporate device. The new way of working has made it virtually impossible to use those existing tools to meet the needs of remote and hybrid, BYOD, and to secure applications brought in from the edge.

As seen below, traditional approaches to IAM are leaving critical gaps in your security strategy. We call this the **Access Trust Gap**.



What is the Access Trust Gap?

In most businesses, there is a large difference between the goal of securing **all** devices, applications, and identities in an organization, and the reality that current security tools can only secure a fraction of those devices, applications, and identities.

This is what we call the Access Trust Gap.

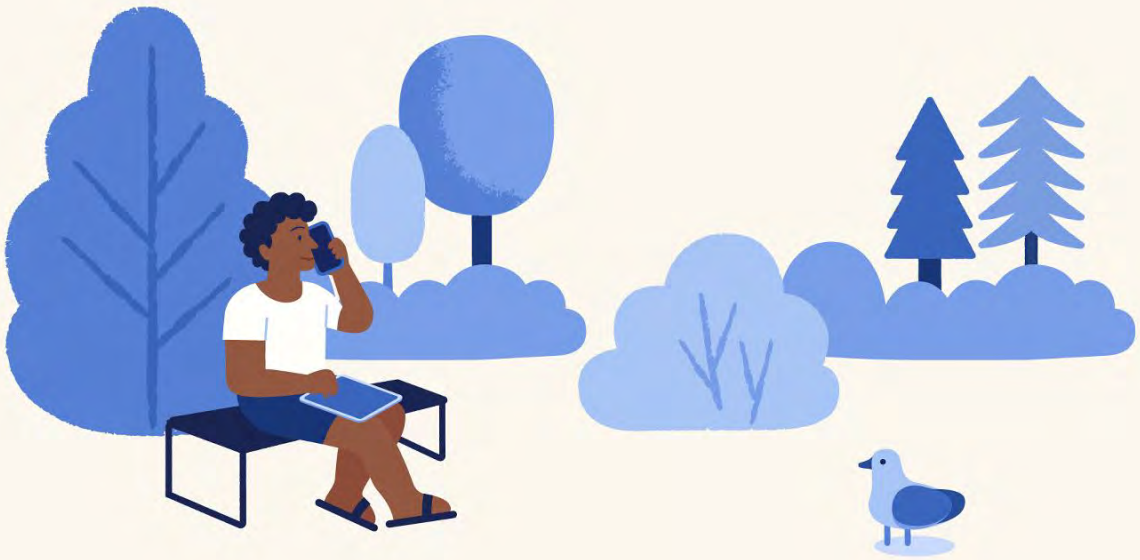
The Access Trust Gap measures the percentage of all sign-ins in a business that are untrusted sign-ins – either because they are sign-ins to unmanaged applications or sign-ins from untrusted devices. The larger the Access Trust Gap, the greater the risk of a data breach.

Modern approaches to security, such as Zero Trust, require that you trust nothing, verify everything. However, the access trust gap clearly shows how traditional IAM falls short of meeting the fundamental tenets of zero trust in a variety of ways:

- Unsanctioned apps and websites outside of the purview of IT and security aren't secured.
- Unmanaged devices or those that may be wounded or compromised are trusted.
- Verifying identity is more than a login and password.

In many cases, organizations can address some of the challenges above, but the ability to address all of these challenges comprehensively remains elusive. So much so that 70% of financially impactful data breaches are the result of compromised credentials.

Let's break down each of these challenges.



Applications: Living on the Edge

A huge portion of this evolution has been driven by the SaaS takeover of business applications. And employees want in. They're increasingly bringing in their own applications from the edge to augment how they work. In fact, according to 1Password's State of Enterprise Security Report:

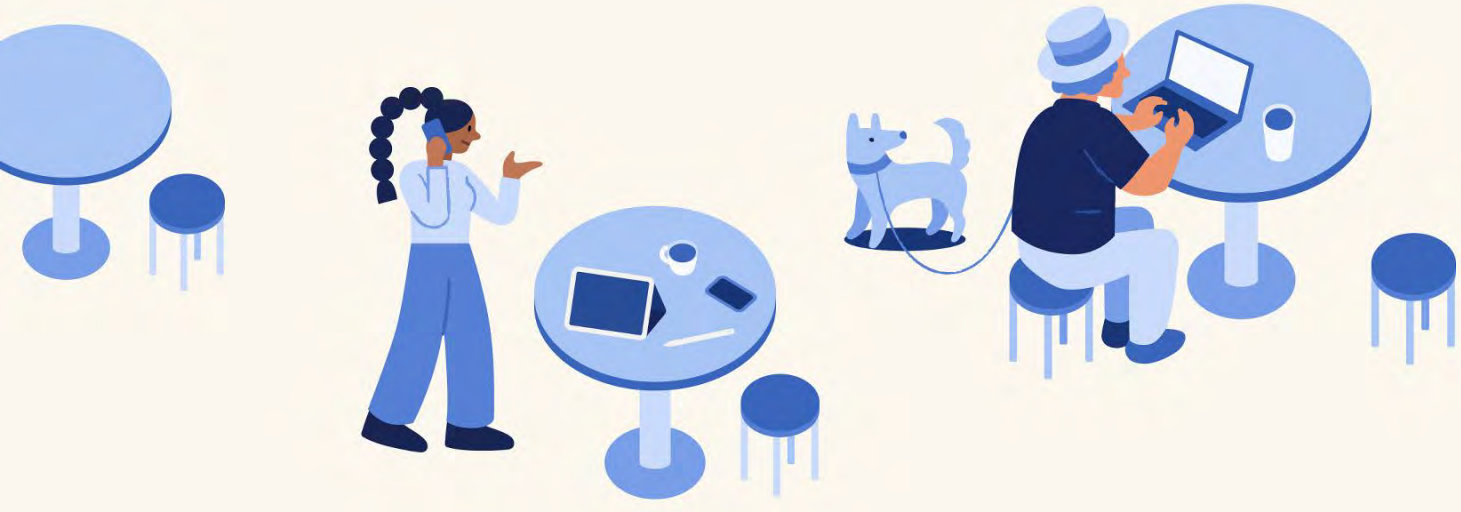
- Despite years of employee education and the deployment of security management software, one in three workers (34%) use unapproved apps or tools – otherwise known as shadow IT.
- 64% of security pros say shadow IT makes navigating employee convenience and security challenging.
- Those who do rely on shadow IT use an average of five unapproved apps or tools.

These challenges extend beyond shadow IT. Single sign-on (SSO) tools are often used to address access to applications, however they are plagued by complexity, high costs, and the "SSO tax" – a practice that requires organizations to pay more money for every application they want to secure.

BYOD

It's not just new expectations driving this trend. It's also a function of how employees want to work. While organizations continue to issue corporate devices, employees are using personal devices for work whether or not they're approved.

- **Nearly two in three security pros (65%)** say that personal devices have made complete visibility into employee security habits much more elusive.
- **84% of security pros** say their company asks that employees only use work-provided devices.
- But **17% of employees** admit to never working on their work-provided devices – opting solely for personal or public computers.
- **More than half of employees (56%)** have worked on a personal device in the last year.
- **One in five employees (20%)** have worked on public computers or from a friend's or family member's device.



Device Trust

It's not just that employees bring their own devices. Businesses can only ensure that the devices they provide to employees are kept up to date with operating system and application patches, have endpoint protection turned on, and are properly configured. And that's only for devices enrolled with a mobile device management (MDM) tool. What about personal devices that employees are using for business purposes?

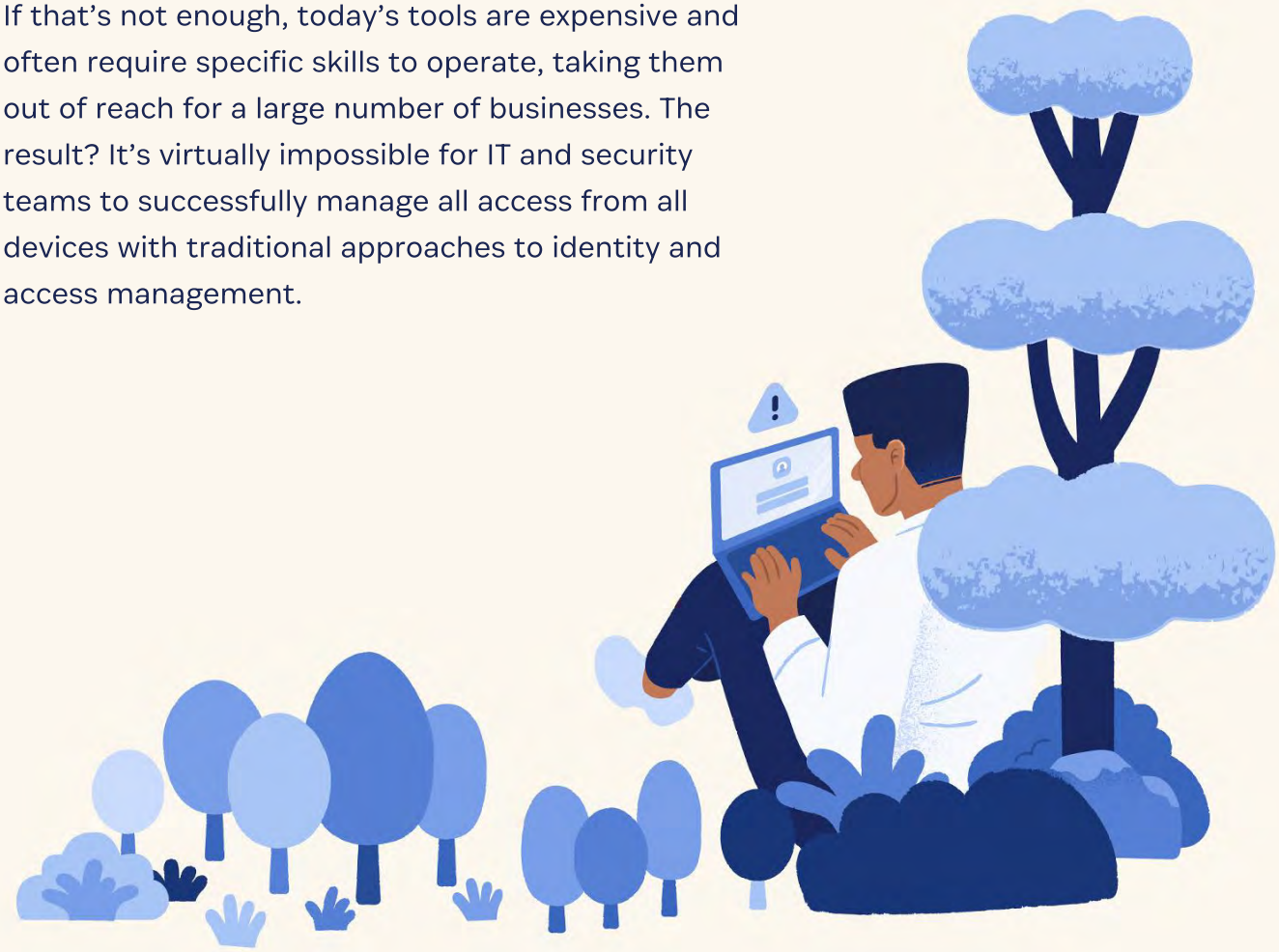
Unfortunately, security and IT are not resourced to remotely manage every single business device. Not to mention that these teams don't have access to employee-owned personal devices used for business. As a result, there is no way to gauge–much less block–access to corporate systems that come from an unhealthy device.

Security teams left powerless

The inability to meet those needs means one thing: risk. And unfortunately, security and IT teams often feel poorly equipped to meet these challenges.

- 92% of security pros say their company policy requires IT approval to download and use software and apps for work.
- But 59% of security pros say they don't control whether employees follow these policies.
- Security teams cannot remotely manage all devices, or control personal devices access business applications.

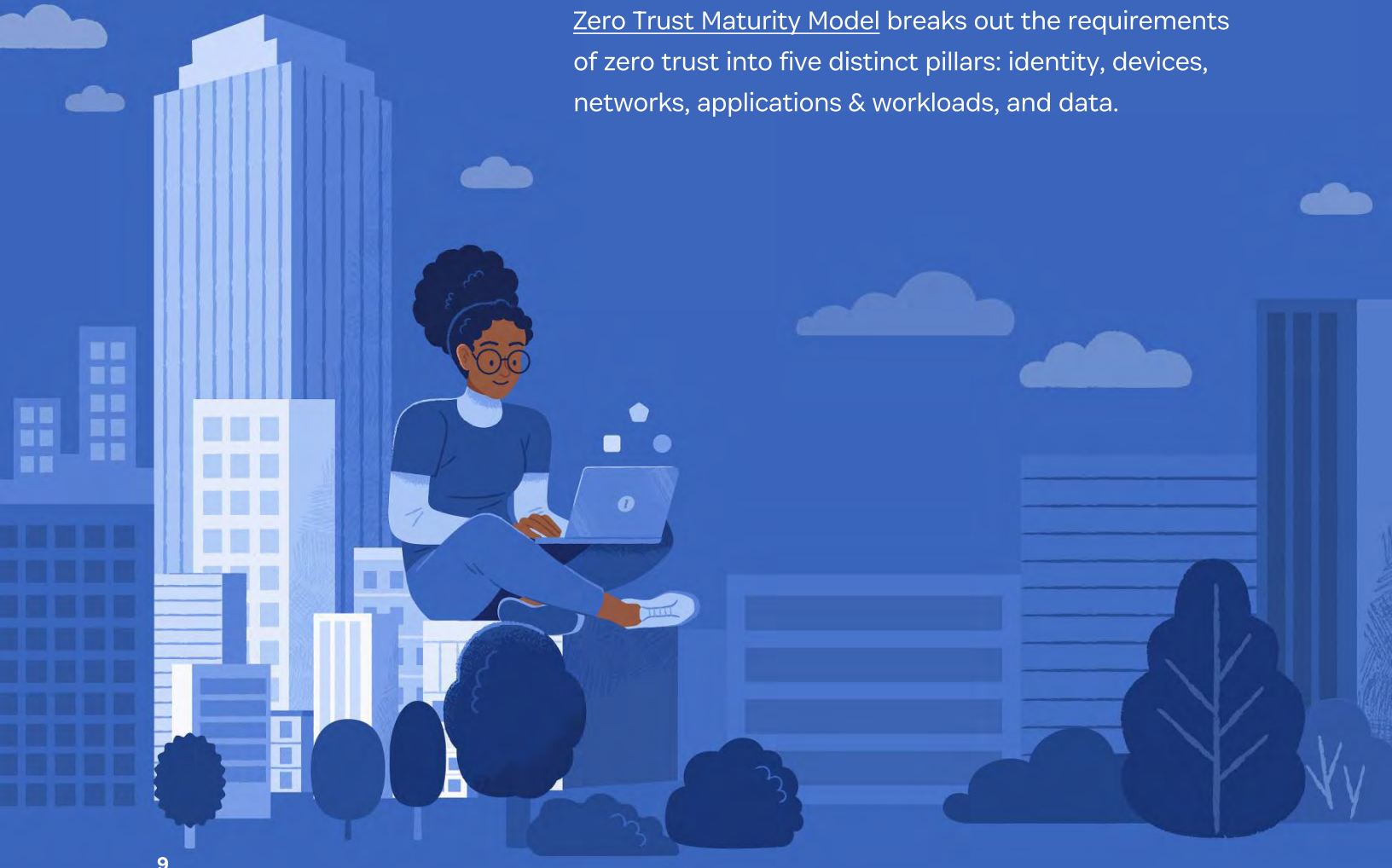
If that's not enough, today's tools are expensive and often require specific skills to operate, taking them out of reach for a large number of businesses. The result? It's virtually impossible for IT and security teams to successfully manage all access from all devices with traditional approaches to identity and access management.



2

Modern Access Management has Modern Requirements

New cybersecurity frameworks have been developed to help meet these challenges. For example, the CISA Zero Trust Maturity Model breaks out the requirements of zero trust into five distinct pillars: identity, devices, networks, applications & workloads, and data.



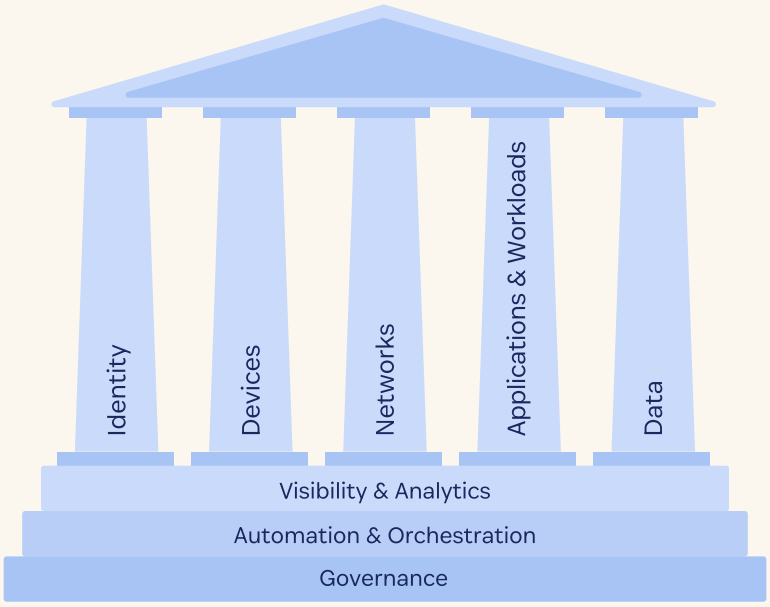


Fig. 1: Zero Trust Maturity Model Pillars

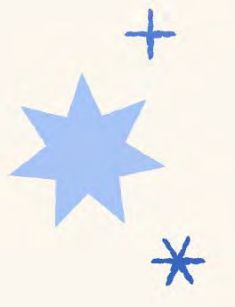
For the purposes of access management, identity, devices, and applications & workloads stand out as the critical pillars to be addressed. Taken in the context of the access trust gap, it's clear where the challenges arise. Requirements as stated in the CISA zero trust maturity model:

- **Identity:** integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities.
- **Devices:** secure all agency devices, manage the risks of authorized devices that are not agency-controlled, and prevent unauthorized devices from accessing resources.
- **Application & Workloads:** manage and secure their deployed applications and should ensure secure application delivery.

Based on the maturity model, we can further break down the pillars above into specific requirements that are needed to close the access trust gap:

Requirement	Definition
User Identity	Ability to manage the identities of your entire workforce and their related access.
Universal Sign-on	Streamlined sign-on that goes beyond SSO to include websites, such as bank accounts and social media, and unmanaged SaaS apps.
Device Trust	Visibility into the health status of all devices used to access business applications – both company-owned and personal – with the ability to guide the device user to keep the device OS and applications patched and in a trusted state.
Contextual Access Management	Dynamic policies that take context – such as time, location, and device health, credential health – into consideration before allowing access.
Application Visibility	Visibility into all managed, legacy, and unmanaged / shadow apps used for business, with the ability to see the strength of authentication, breadth of use, and frequency of use.
Enterprise Password Management	Secure management of credentials across all managed and unmanaged applications and websites.

Meeting the above requirements is virtually impossible with existing workforce identity solutions. In most cases, existing solutions enable organizations to manage the identities but fall significantly short of enabling access, securing devices, and supporting applications brought from the edge.



Existing workforce identity solutions fall short of zero trust

Requirement	Existing Workforce Identity Solutions
User Identity	✓
Universal Sign-on	x
Device Trust	x
Contextual Access Management	x
Application Visibility	x
Enterprise Password Management	x

3

Welcome to the era of Extended Access Management

Zero Trust has become a critical framework for modern security, and meeting the requirements of the modern workplace has only accelerated the need to adopt it. Trust nothing, verify everything, has made one thing clear: the ways we approach access management must be extended to secure all devices, all applications, and all identities.

We call this **Extended Access Management (XAM).**

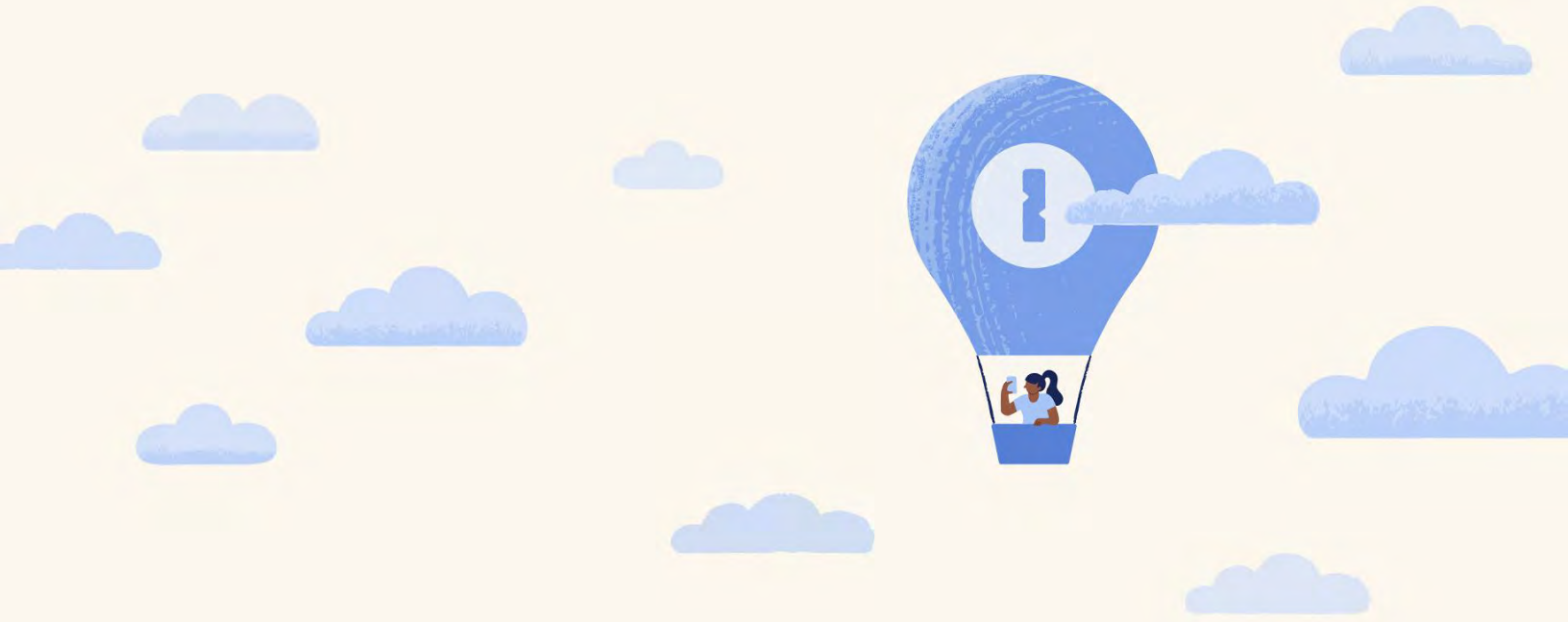
Extended Access Management is an approach to access management that accepts BYOD and shadow IT as the normal course of business, rather than something that IT and security teams need to actively pursue and eliminate. This creates a work environment where:

- Employees are enlisted to play an active role in strengthening security – especially when it comes to ensuring devices are healthy and credentials are secure.
- Security tools that employees will actually use are deployed – in contrast to tools that create so much friction that employees work around them.
- Employee privacy is respected – providing transparency into what data is collected and how it is used to build trust and earn buy-in to the presence of security tools.
- Employee productivity is ensured – giving employees security tools that make the easiest way to get a job done the most secure way to get the job done.

What separates extended access management from existing workforce identity solutions is that XAM supports all applications (including unmanaged and shadow IT), websites, and devices that employees use in their day-to-day operations. Furthermore, XAM does this in a way that enables employees to use the devices and applications they need to be most productive on an ongoing basis.

XAM represents a new category of security software to:

- **Secure all applications** – managed, shadow IT, and legacy applications.
- **Provide a single universal sign-on to all applications** – making it simple for employees to use the most secure credential possible for each application.
- **Ensure the health of all devices** – company-managed, company owned but unmanaged, and employees' personal laptops and mobile devices – and block or limit access attempts from untrusted devices.
- **Allow only healthy devices to access applications** – unlike IAM tools that cannot limit access from unhealthy devices.
- **Deliver an elegantly simple user experience** – works equally well on business and personal devices, encouraging employees to secure their personal devices with XAM because that is the easiest way to access applications.



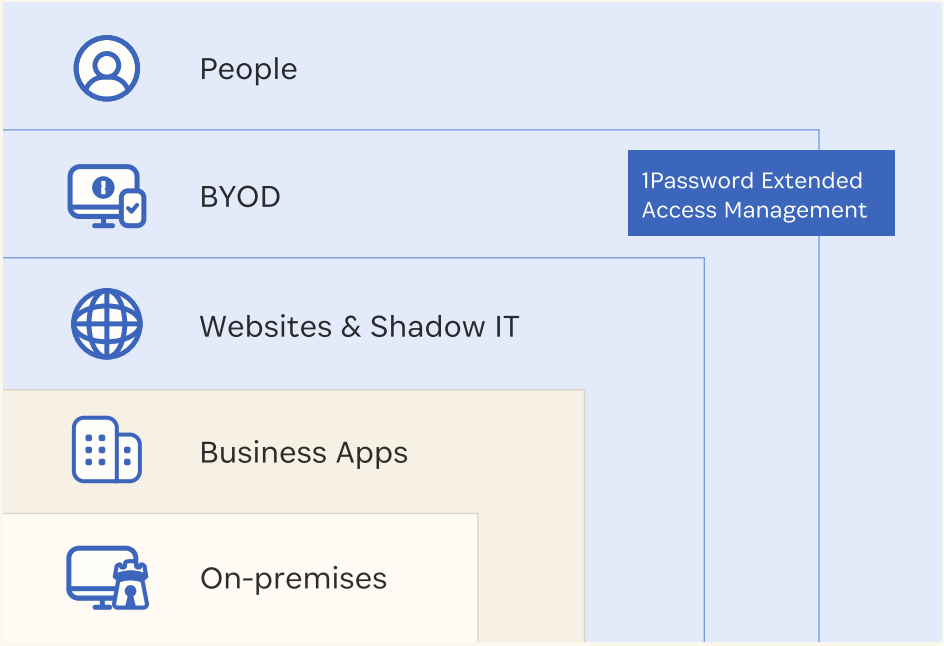
Comparison of traditional workforce identity solutions with Extended Access Management

Requirements	Existing Workforce Identity Solutions	Extended Access Management (XAM)
User Identity	✓	✓
Universal Sign-on	x	✓
Device Trust	x	✓
Contextual Access Management	x	✓
Application Visibility	x	✓
Enterprise Password Management	x	✓

1Password® Extended Access Management and the future of zero trust

1Password Extended Access Management closes the access trust gap that lies between identity and access management (IAM), privileged access management (PAM), mobile device management (MDM), and that extended detection and response (XDR) cannot address. 1Password Extended Access Management:

- Secures all applications
- Provides a single universal sign-on to all applications
- Ensures the health of all devices
- Ensures only healthy devices can access applications
- Delivers an elegantly simple user experience



5

ENABLE AND SECURE

Conclusion

Extended Access Management represents a sea change in how organizations approach identity and access management–one that takes a comprehensive approach to securing identity, devices, and applications. Where once it only required companies to secure employees accessing systems from a controlled, physical environment, the modern work era has fundamentally different needs. XAM is a new approach to cybersecurity that enables organizations to meet these needs in a user-friendly and easy-to-use way.

Learn more about extended access management and 1Password Extended Access Management

1Password

Trusted by over 150,000 businesses and millions of consumers, 1Password offers identity security and access management solutions built for the way people work and live today. 1Password is on a mission to eliminate the conflict between security and productivity while securing every sign-in for every app on every device. As the provider of the most-used enterprise password manager, 1Password continues to innovate on its strong foundation to offer security solutions relied upon by companies of all sizes, including Associated Press, Salesforce, GitLab, Under Armour, and Intercom.

Learn more about 1Password.