



How Extended Access Management (XAM) closes the gaps in security



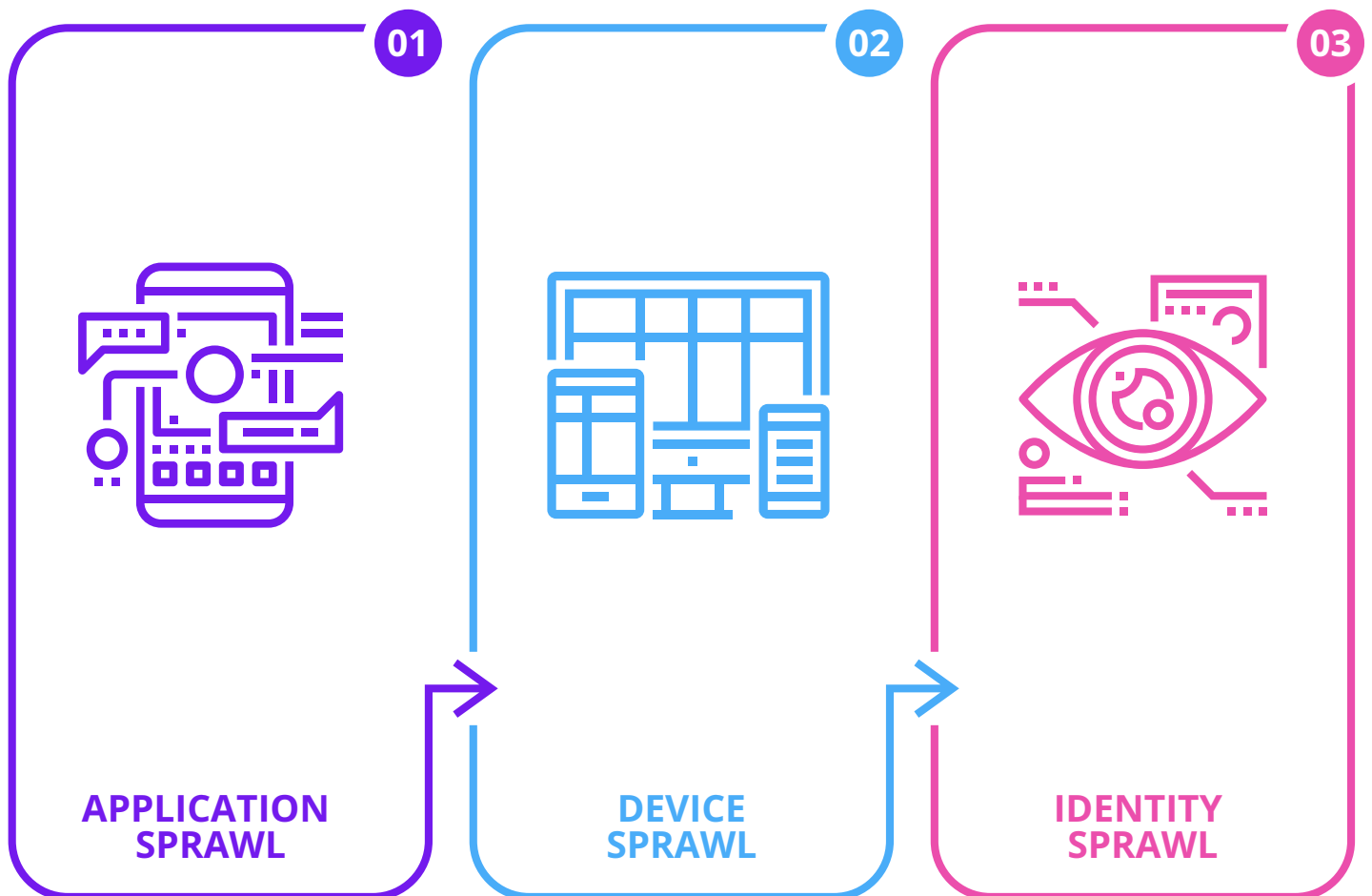
Brought to you by Informa Tech

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Introduction

There are three distinct challenge areas of access management (see Figure 1): **application sprawl**, **device sprawl**, and **identity sprawl**. This section explores why these are significant challenges for security and IT teams.

Figure 1: Three distinct challenges of access management



Source: Omdia

Application sprawl

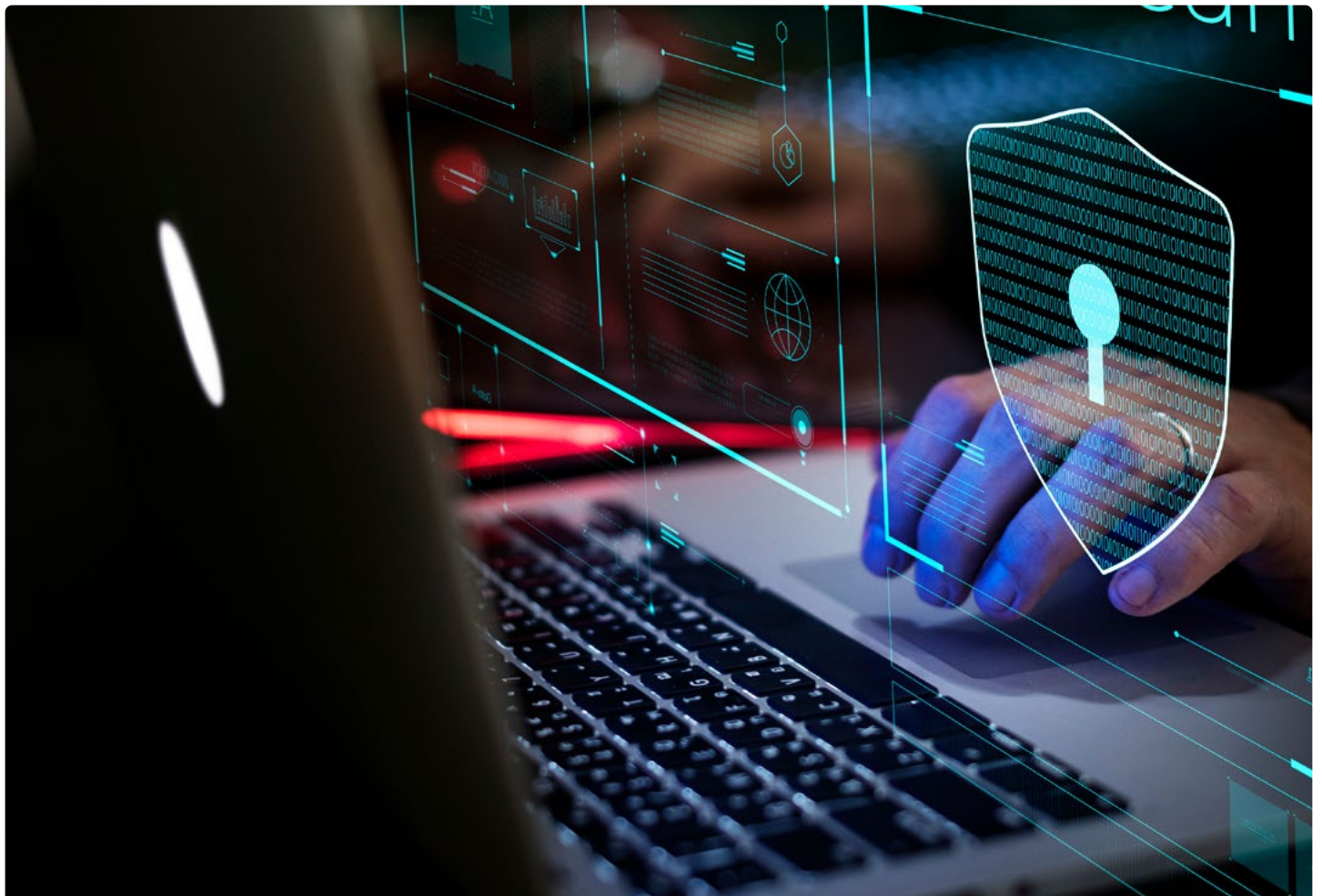
First, there is application sprawl, which refers to the uncontrolled proliferation of applications within an organization. With the rise of SaaS and cloud-based solutions, departments often adopt their own tools without centralized oversight. This results in a fragmented SaaS environment where IT and security teams struggle to maintain visibility and control over who has access to what applications. A study in February 2024 from Canva and Harris titled *How CIOs are planning for an AI-first future* supports this; it found that 72% of chief information officers (CIOs) are concerned about application sprawl.

Device sprawl

Secondly, there is device sprawl, which refers to the explosion of devices accessing corporate resources, including personal phones, IoT devices, and remote work setups. Each device is a new access point that needs to be managed and secured but IT and security teams struggle to ensure consistent security policies across a diverse range of devices, especially given the limitations of the management tools they are accustomed to using.

Fundamentally, security and IT teams have a mandate to ensure that only trusted devices can access their resources. But while MDMs are a popular solution for company-owned devices, they weren't built to provide real-time device posture verification during authentication, and they are often incompatible with personal or BYO-devices.

Likewise, while IAM solutions manage known identities and simplify access to SaaS, they weren't built to provide real-time device posture verification during access. Thus, unknown and untrusted devices frequently circumvent these tools and access sensitive company data.



Identity sprawl

Finally, there is identity sprawl, which refers to the uncontrolled growth of user identities within an organization, including employees, AI agents, contractors, and third-party vendors, each requiring access to various systems. Without proper governance, identities can accumulate unnecessary permissions, leading to security risks and compliance issues. CrowdStrike's 2025 Global Threat Report stated that "adversaries increasingly target identities using credential theft, MFA bypass, and social engineering while covertly moving laterally between on-premises, cloud, and SaaS environments via trusted relationships." The report goes on to say that these are interactive attacks, often bypassing static controls, and they are up 35% year over year.

Now, AI agents are transforming the access management landscape and creating a new type of identity sprawl. Agentic AI systems can perform complex tasks autonomously, but this capability requires expansive access, which introduces complexity and risk. AI agents need to integrate with numerous applications, requiring access to API keys, passwords, and sensitive business data – often without proper governance. Agents can create dozens of "non-human identities" whenever authentication is needed, and existing IAM tools were not designed to safely provision, deprovision, and govern them.

In response to these threats, 1Password launched a new category in May 2024: Extended Access Management (XAM). XAM is designed to address the complexities of modern access management by:



Centralizing access control across all applications, devices, and identities



Enhancing visibility into who has access to what, reducing security gaps and operational inefficiencies



Automating lifecycle management to ensure timely provisioning and deprovisioning of access

In this white paper, Omdia explores the drivers behind XAM, the Access-Trust Gap it addresses, and how it can help organizations modernize their security posture without compromising productivity.

The problem: Existing access management approaches have failed

Legacy identity access management (IAM) and mobile device management (MDM) tools have fallen short of providing security while enabling a productivity-driven and innovative workforce. These tools were designed for a world where IT controlled every application, device, and tool in use, and employees had no digital free will or choice in how they did their work. In today's world, employees freely adopt the tools and devices they need to be the most productive, regardless of whether they are provisioned or managed by their organization. As a result, untrusted and unmanaged forms of access proliferate across these devices and apps. Omdia believes that this problem is only getting worse with the continued rise of BYOD, SaaS apps, and AI-powered tools.

Traditional approaches to cybersecurity were predicated on the centralized control of devices and applications. With this approach, it was easy for IT and security to use the “rule of no” to maintain a secure and manageable environment. The “rule of no” is the practice of denying employees access to tools, devices, and applications in the name of security.

This has created a dangerous mismatch between security expectations and operational realities. Employees, often unknowingly, circumvent security policies in order to get work done, leading to a proliferation of shadow IT, shadow AI, and ungoverned credentials. As this trend accelerates, credential, device, and application risks continue to spiral beyond the reach of legacy controls.

“

The “**rule of no**” is the traditional practice of denying employees access to tools, devices, and applications in the name of “**being secure,**” regardless of the impact on the employee or business.

The Access-Trust Gap

This confluence of unmanaged access points—spanning users, devices, and applications—has created a critical security blind spot that organizations can no longer afford to ignore. It's what 1Password defines as the Access-Trust Gap: the security risks posed by unfederated identities, unmanaged devices, applications, and AI-powered tools accessing company data without proper governance controls.

The gap widens every time an employee uses a personal device to log into a SaaS application that is not sanctioned by IT. It widens further when contractors access systems with insufficient oversight or when former employees retain credentials that are not promptly deactivated. Ultimately, the Access-Trust Gap is the outcome of empowered and technically savvy employees circumventing traditional cybersecurity measures to increase their productivity. This gap has widened even more with the advent of AI agents. Indeed, CrowdStrike's 2025 Global Threat Report stated that access broker activity is also surging, with a 50% rise in advertisements selling access to compromised accounts. The proliferation of unmanaged access points gives attackers more opportunities to walk right through the front door. The larger the Access-Trust Gap, the greater the risk of a data breach.

Modern approaches to security, such as Zero Trust, require that people trust nothing and verify everything. However, the Access-Trust Gap clearly shows how traditional IAM, SSO, and MDM solutions fall short of meeting the fundamental tenets of Zero Trust:



Employees regularly use unsanctioned and unsecured apps and websites outside the visibility of IT



Users access company resources on unknown, unmanaged, and compromised devices



Despite the availability of SSO and MFA, identity verification often relies on weak, phishable forms of authentication, such as passwords

The solution: 1Password Extended Access Management

To address this growing gap, 1Password launched 1Password Extended Access Management, a comprehensive solution designed to modernize access control for today's hybrid and decentralized work environments. Extended Access Management expands the security perimeter to include unmanaged endpoints, unsanctioned apps, and identities previously invisible to IT.

1PASSWORD EXTENDED ACCESS MANAGEMENT AIMS TO CLOSE THE ACCESS-TRUST GAP IN THE FOLLOWING WAYS:



- Discover unmanaged SaaS, shadow IT, and shadow AI apps employees use



- Guide IT to implement SSO for high-risk apps, and effectively ban unsanctioned shadow IT



- Ensure compliance for every device used for work tasks, whether or not it is managed by MDM



- Block access to sensitive apps from untrusted devices and empower employees to self-remediate device issues to reduce IT overhead



- Eliminate password risks by securing compromised credentials and accelerate the journey to passwordless authentication

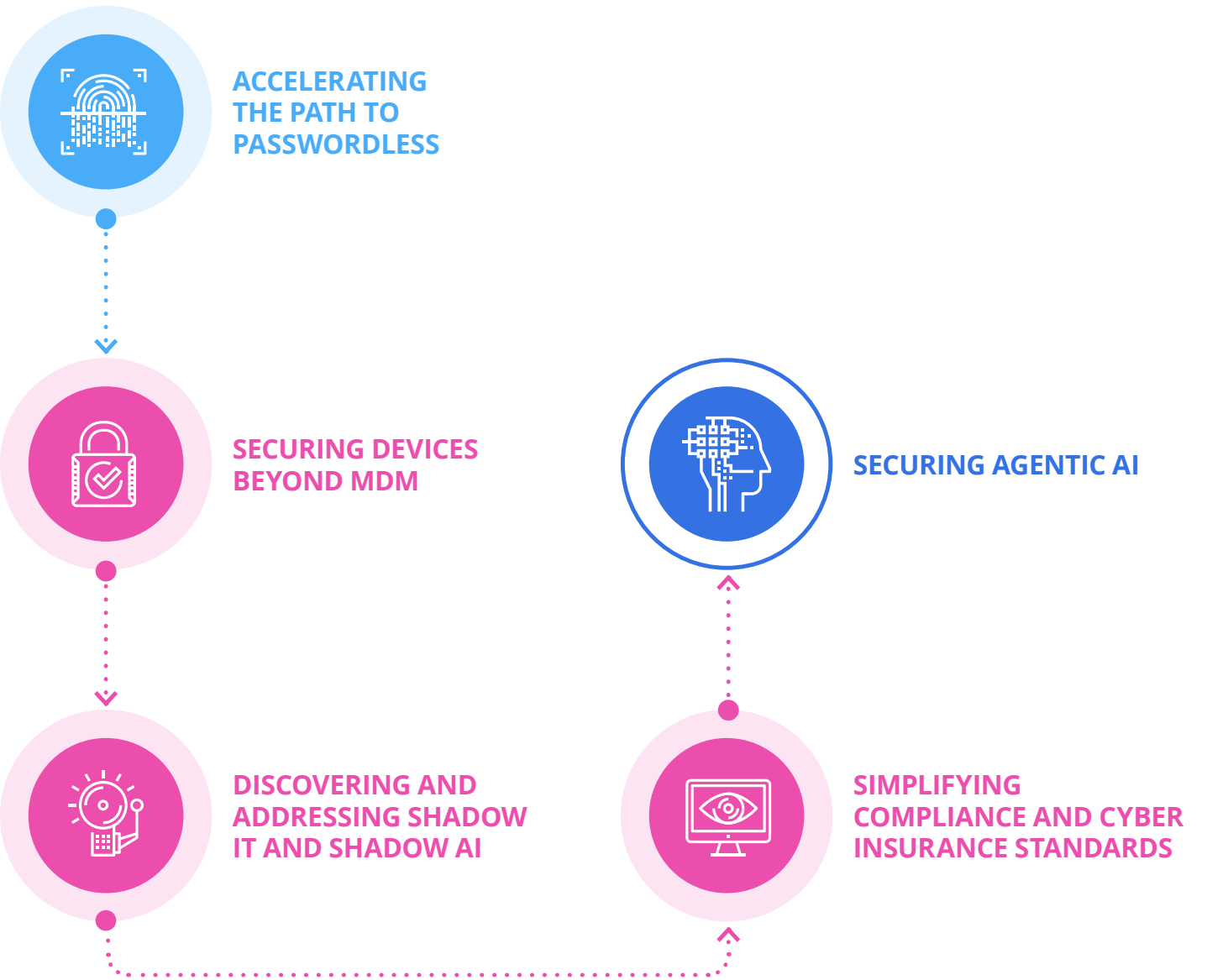


- Secure access for all identities, including AI agents

Five critical activities to strengthen identity security

The following section highlights five critical security goals that XAM aims to address (see Figure 2), which will help CISOs and organizations respond to today and tomorrow's security risks.

Figure 2: Five critical activities to strengthen identity security

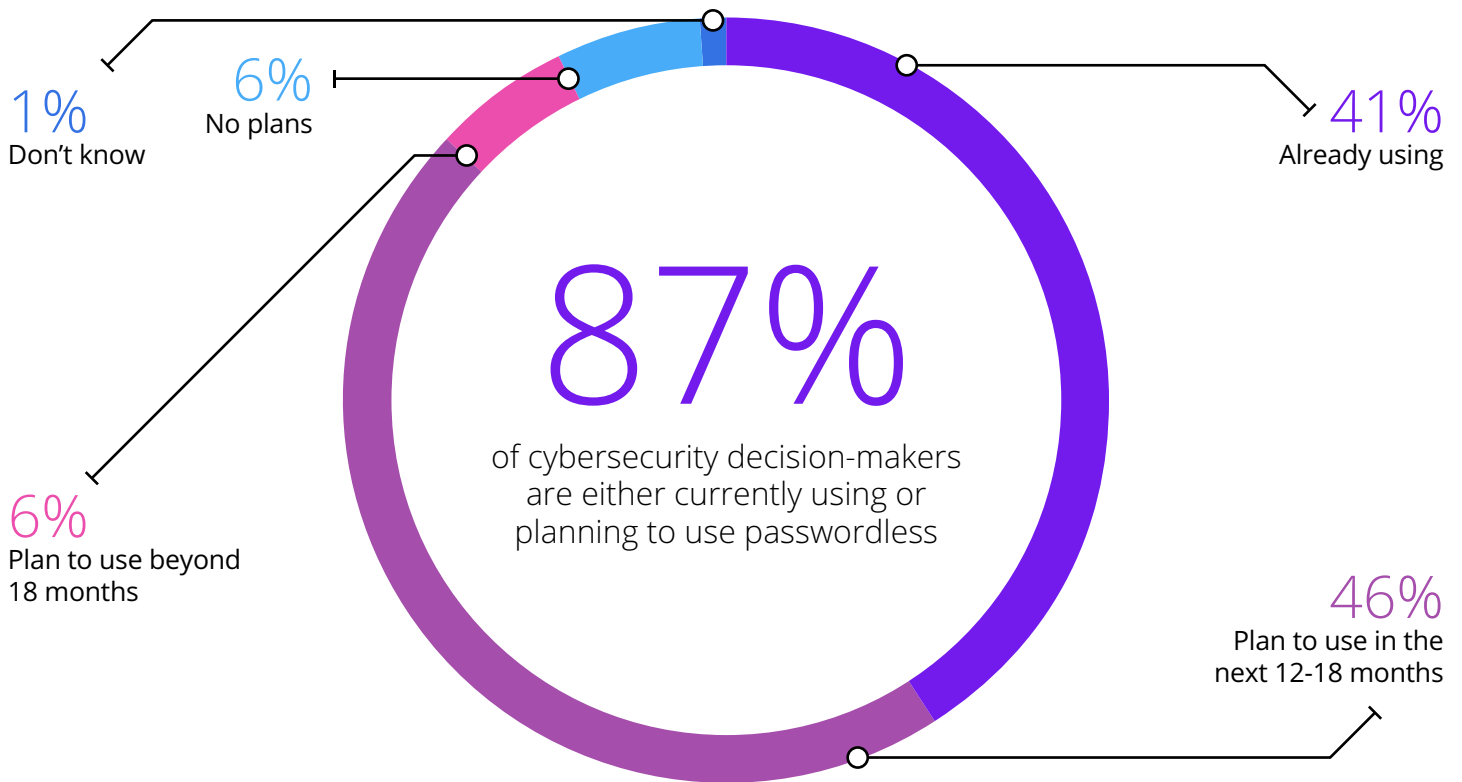


Source: Omdia

1 ACCELERATE THE PATH TO PASSWORDLESS

A truly passwordless environment has long been the dream of security leaders. In fact, 87% of cybersecurity decision-makers are either currently using or planning to use passwordless authentication technologies in the near future (see Figure 3). However, fully eliminating passwords is a years-long undertaking, and authentication must be as secure as possible at every step along the way.

Figure 3: What is the status of passwordless authentication technologies in your organization?



Source: Omdia

Eliminating password risk requires taking a methodical approach to discovering passwords everywhere they are used—even in previously unknown shadow IT apps—and replacing them with stronger credentials and passwordless authentication.

1Password Extended Access Management aims to accelerate the path to passwordless by:

- Giving administrators visibility and risk oversight into what applications are in use, what devices they're accessed from, and by whom—therefore ensuring appropriate authentication security is in place
- Identifying every compromised or weak credential and every sign-in that does not use available multi-factor authentication or passkeys
- Enforcing security policies to ensure employees replace every at-risk sign-in with a stronger credential before accessing the application
- Evaluating application risks across the company and identifying high-use unmanaged apps that are likely to hold sensitive data, so they can prioritize SSO integration or migrate users to managed apps

2 SECURE DEVICES BEYOND MDM

Most enterprises rely on mobile device management (MDM) solutions to secure corporate hardware. However, MDM coverage often stops short of the full picture, leaving personal devices, contractor laptops, and unmanaged endpoints outside the purview of IT. According to Microsoft's Digital Defense Report, published in December 2024, 92% of successful ransomware attacks involve unmanaged devices. There is a clear need to discover and secure all the devices used for work, not just the IT-managed and company-provided devices that are secured by today's typical cyber tech stack.

1Password Extended Access Management addresses this through device trust. Before access is granted to a SaaS application, 1Password Device Trust can validate a device's encryption status, ensure that security software is installed and running, and verify compliance with organizational security standards. This ensures that any device trying to connect to an organization's apps is healthy and belongs to a known user. Devices that fail these checks are prevented from authenticating until the issue is remediated via step-by-step user guidance.

A hand holding a smartphone is shown against a dark background with a network of glowing nodes and lines. A white padlock icon is overlaid on the network, and a series of asterisks represents a password field.

“

Omdia believes that this approach transforms the endpoint from a weak link into a controlled and trusted access point, reducing the risk of malware, ransomware, and unauthorized data access.

3 DISCOVER AND ADDRESS SHADOW IT AND SHADOW AI

As organizations adopt more cloud-based applications and platforms, IT teams are finding it increasingly difficult to maintain visibility into all the tools employees are using. SaaS sprawl has led to a dramatic rise in shadow IT: apps and tools used without the approval or knowledge of security teams. This risk is compounded by the rapid adoption of generative AI tools, often accessed without oversight and used to process sensitive or proprietary data.

Protecting organizations means securing all the apps used by employees, not just the managed apps.

Figure 4: More than one-third of employees use shadow IT



Source: Omdia

1Password Extended Access Management helps organizations discover these unsanctioned tools and understand how they are accessed. It highlights high-risk applications so they can be integrated with SSO. But it is not reliant on SSO and enables automated and secure provisioning and deprovisioning for all apps, even those not protected by SSO. This is an essential capability, given that technical limitations and the "SSO Tax" make it unfeasible for organizations to extend SSO to every app. Additionally, 1Password provides a full audit trail of access events, which is essential for responding to incidents quickly and efficiently. Further, it provides deep visibility, automation, and actionable insights, helping businesses reduce risk, streamline operations, and optimize SaaS investments.

4 SIMPLIFY COMPLIANCE AND CYBER INSURANCE STANDARDS

Navigating the complexities of compliance and cyber insurance standards can be daunting for any CISO or organization. Increasingly, compliance requires security leaders to control risks associated with app sprawl, secure access to sensitive data, and enforce device governance standards – even on apps and devices previously considered low-risk or out of scope. Indeed, an article by RF Investment Partners in November 2024 noted that “with 70% of corporate risk and compliance professionals saying that they’ve noticed a shift from check-the-box compliance to a more strategic approach over the last few years, the compliance tech sector will continue to benefit from increased adoption and continued capital investment.”

XAM addresses these evolving compliance requirements by unifying access governance under a single platform. It simplifies compliance reporting and audit readiness by enforcing policies aligned with standards like SOC 2, ISO 27001, and GDPR.

Moreover, with insurers increasingly requiring proof of robust identity security and risk mitigation measures, 1Password Extended Access Management’s capabilities in automated policy enforcement, risk identification, and remediation provide a clear path toward meeting these expectations and securing favorable cyber insurance terms.

“

Omdia believes that compliance and cyber insurance standards don't have to be overwhelming. The key is to approach compliance as a journey, not a destination. With a clear plan, proper documentation, and solutions that simplify the process, CISOs and organizations can navigate even the most complex regulatory environments with confidence.

The rapid evolution of AI agents and AI-powered applications is fundamentally reshaping the software landscape, signaling a paradigm shift in SaaS and enterprise applications. Unlike conventional static applications, AI-driven software operates autonomously, adapting to user needs, automating workflows, and interacting with other applications without constant human intervention. In many ways, AI agents mimic human interactions with enterprise applications: making decisions, requesting data, and triggering workflows, just as an employee would. This also means AI agents face many of the same security and access challenges as humans, requiring identity verification, permissions management, and secure credential storage to prevent unauthorized access or data leaks. Yet AI agents also have distinct needs that make them difficult to manage using traditional approaches to access management: they can operate continuously, require broad-based permissions to function, and are not capable of certain forms of authentication, like biometrics. Without proper governance, AI-driven processes can become a security liability, creating an invisible layer of shadow IT that circumvents traditional access controls.

A real-world example is the increasing use of AI-driven financial automation bots in enterprises. An AI-powered expense management system may need access to corporate banking data, payroll records, and approval workflows, just as a finance employee would. If these AI agents are not properly secured, they could inadvertently leak sensitive financial data, approve fraudulent transactions, or expose high-value credentials to cyber threats. For an economic buyer, this represents a direct financial risk; an unsecured AI agent managing critical business functions could mean millions of dollars in fraud, regulatory fines, and reputational damage. As these AI-driven solutions continue to proliferate, they will replace legacy enterprise applications that rely on manual user input and static authentication models. Traditional SaaS applications will no longer be the primary interface for employees and consumers. AI-powered agents will dynamically access data and services across multiple systems, raising profound implications for identity, security, and access management. Securely managing access for this army of agents will require new tools, explicitly designed to manage the unique needs of non-human identities.

**Omdia believes that
1Password Extended Access
Management provides AI
agent security to accelerate the
development, adoption, and
management of AI agents and
apps in the modern enterprise.**

Integrations and strategic alliances

Omdia believes that integrations and strategic alliances are fundamental to the growth and acceptance of cybersecurity products and solutions. They help to naturally drive synergies and growth for both vendors and customers. 1Password Extended Access Management has integrations and alliances with vendors such as CrowdStrike, Microsoft, and AWS.

For example, in September 2024, CrowdStrike announced an expanded Tier 1 partnership with 1Password to simplify security for customers. Through an easy-to-use bundle, 1Password Extended Access Management customers can now access the enterprise-grade protection they need to stop ransomware and data breaches with CrowdStrike Falcon® Go. This integration with CrowdStrike spans multiple fronts and includes:

- **1Password Extended Access Management Device Trust Falcon Check:** Enables 1Password Device Trust to check whether CrowdStrike's Falcon product was installed correctly on devices.
- **1Password Extended Access Management Device Trust ZTA Score:** Enables 1Password Device Trust to block device authentication if it fails to meet a specific CrowdStrike ZTA score.
- **Mutual customers can stream security events to CrowdStrike's SIEM from 1Password's enterprise password manager (EPM) and Device Trust products.**

In 2024, 1Password also deepened their partnership and product integrations with AWS. In order to streamline procurement and billing, AWS customers can buy 1Password Enterprise Password Manager and 1Password Extended Access Management products via the AWS marketplace. Deepening product integrations with AWS include:



- **1Password Device Trust health Checks:** Device Trust uses health Checks to ensure every device accessing an organization's sensitive data is known and secure. For AWS customers, 1Password offers a pre-built check that scans devices for unencrypted AWS credential files and prompts users to secure them.



- **Log pipeline:** Device Trust's Log Pipeline also integrates with AWS S3 (cloud storage service), exporting authentication and audit logs directly into the AWS ecosystem. This gives organizations the power to analyze security data using AWS's extensive analytics tools, providing a more comprehensive understanding of their security posture and helping identify potential risks.



- **Passkeys for Amazon Cognito:** Passage by 1Password offers a secure, passwordless authentication solution for apps and websites that simplifies the login experience using passkeys. Passage allows businesses relying on Cognito for authentication to adopt passkey technology without the complexities of in-house development.



- **AWS Nitro Enclaves:** By leveraging AWS Nitro Enclaves, 1Password enables administrators to gain insight into application usage across the organization, all while maintaining data privacy. This technology lets admins securely view app usage metrics without exposing sensitive information.



- **AWS AppFabric integration:** AWS AppFabric integrates with 1Password Business to improve security management by centralizing log data, allowing Security and IT teams to monitor and secure user access across multiple apps more effectively.

Omdia believes that deepening partnerships and product integrations can significantly enhance the overall security posture of organizations and help them stay ahead of evolving threats.

In addition, 1Password's integration with Microsoft Sentinel enables customers to seamlessly monitor access and activity events with data and credentials stored within 1Password Extended Access Management and 1Password Enterprise Password Manager. Furthermore, in November 2024, 1Password joined the Microsoft Intelligent Security Association (MISA), an ecosystem of independent software vendors (ISVs) and managed security service providers (MSSPs) that have integrated their solutions with Microsoft Security technology to better defend mutual customers against a world of increasing cyber threats. Now, as part of Microsoft's security ecosystem, 1Password's Extended Access Management platform offers Microsoft users real-time threat visibility, device health enforcement, and robust access management through its integrations with Microsoft Sentinel and Microsoft Entra ID. 1Password is the only password management solution included.

Omdia believes that one of the key benefits of 1Password being part of the MISA program is access. If a product issue arises, 1Password has privileged access to lobby Entra product leadership to advocate unblocking or facilitating changes to the product roadmap.

Other integrations

OTHER NOTABLE INTEGRATIONS INCLUDE:



- **Governance risk compliance (GRC):** 1Password partners with key players like Drata to strategically position 1Password Extended Access Management as a remediation mechanism to help small businesses and middle market companies accelerate and reach compliance.



- **Zero Trust:** 1Password has partnerships with Tailscale and Twingate. Customers can input signals from Device Trust into Tailscale and Twingate, which will let them block access to the network for users whose devices aren't in policy.



- **SIEM integrations:** The basis of all these partnerships is 1Password's Event API, which allows customers to share data from 1Password (item usage and sign-in attempts) into customers' SIEMs. The ultimate aim is to be able to make this data share bi-directional.



- **1Password Marketplace:** Finally, 1Password is also investing in an integration ecosystem called 1Password Marketplace. This initiative is building on strategic alliances with key partners to extend 1Password Extended Access Management capabilities and ensure the company operates seamlessly within a customer's existing security stack.

Customer feedback on 1Password Extended Access Management

"Before 1Password Extended Access Management, we didn't really have a way to enforce policies and vulnerability checks on personal devices. This completely solved that issue without much friction for the end users."



"Using 1Password Extended Access Management is an important part of us being SOC 2 compliant, which is important in keeping our customers' trust. They can check we are compliant and that we take security seriously."



"We see using 1Password Extended Access Management as part of the journey to being passwordless. It's like a bridge between the password and passwordless worlds."



"1Password has done a terrific job supporting passkeys. Passwordless is a core objective we're committed to making a reality for our employees."



"1Password helped us achieve our enterprise security and compliance goals."



Conclusions and Omdia view

This paper explored the shortcomings of existing access management approaches and highlighted the growing Access-Trust Gap. Omdia believes that, if left unaddressed, these challenges will only intensify – particularly as the number of AI agents and tools continues to grow exponentially.

Key findings from this analysis include:



1Password's introduction of the Extended Access Management (XAM) category marks an important shift in how the industry addresses identity and access security.



Omdia believes that 1Password Extended Access Management is certainly worth considering for organizations who are looking to go beyond legacy IAM and PAM tools to deliver universal visibility, real-time risk response, and a frictionless user experience, all of which are essential for scaling secure operations in today's hybrid and fast-moving environment.



For CISOs, security architects, and IT leaders, the imperative is clear: evolve or fall behind. 1Password Extended Access Management is not just a security upgrade; it is an enabler of business agility, resilience, and compliance. It bridges the widening Access-Trust Gap and brings the vision of a passwordless future within reach.



The advent of AI agents and AI-powered applications is turbocharging change and is fundamentally reshaping the software landscape, signalling a paradigm shift in SaaS and enterprise applications.



No company is an island when it comes to providing end-to-end cybersecurity products and solutions, and having strategic alliances and integration can only help security postures.



Omdia believes organizations that act now by investing in technologies like XAM will be best positioned to manage risk, unlock productivity, and build lasting digital trust.

About 1Password

Trusted by over 165,000 businesses and millions of consumers, 1Password pioneered Extended Access Management, a new cybersecurity category built for the way people and AI agents work today. Our mission is to unleash productivity without compromising security. The 1Password Extended Access Management platform secures every sign-in to every app from every device, including the managed and unmanaged ones that legacy IAM, IGA, and MDM tools can't reach. Leading companies such as Asana, Associated Press, Aldo Group, Canva, IBM, MongoDB, MediaComm Communications, Octopus Energy, Slack, Salesforce, Stripe, Under Armour, and Wish rely on 1Password to close the Access-Trust Gap: the security risks posed by unfederated identities, unmanaged apps, devices, and AI agents accessing sensitive company data without proper governance controls.

Learn more at [1Password.com](https://1password.com)



About Omdia

Omdia is a global technology research powerhouse, established following the merger of the research division of Informa TechTarget (Ovum, Heavy Reading, and Tractica) and the acquired IHS Markit technology research portfolio*.

We combine the expertise of more than 400 analysts across the entire technology spectrum, covering 150 markets. We publish over 3,000 research reports annually, reaching more than 14,000 subscribers, and cover thousands of technology, media, and telecommunications companies.

Our exhaustive intelligence and deep technology expertise enable us to uncover actionable insights that help our customers connect the dots in today's constantly evolving technology environment and empower them to improve their businesses – today and tomorrow.

*The majority of IHS Markit technology research products and solutions were acquired by Informa in August 2019 and are now part of Omdia.



The Omdia team of 400+ analysts and consultants are located across the globe

Americas	Asia-Pacific	Europe, Middle East, Africa	
Argentina	Australia	Denmark	Sweden
Brazil	China	France	United Arab Emirates
Canada	India	Germany	
United States	Japan	Italy	United Kingdom
	Malaysia	Kenya	
	Singapore	Netherlands	
	South Korea	South Africa	
	Taiwan	Spain	

Contact Omdia

- E insights@omdia.com
- E consulting@omdia.com
- W omdia.com
-  OmdiaHQ
-  Omdia

Contact 1Password

- W 1password.com
-  1Password
-  1Password

COPYRIGHT NOTICE AND DISCLAIMER

Omdia is a registered trademark of Informa PLC and/or its affiliates. All other company and product names may be trademarks of their respective owners. Informa PLC registered in England & Wales with number 8860726, registered office and head office 5 Howick Place, London, SW1P 1WG, UK. Copyright © 2025 Omdia. All rights reserved. The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa TechTarget and its subsidiaries or affiliates (together "Informa TechTarget") and represent data, research, opinions or viewpoints published by Informa TechTarget, and are not representations of fact. The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result. Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials. To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.