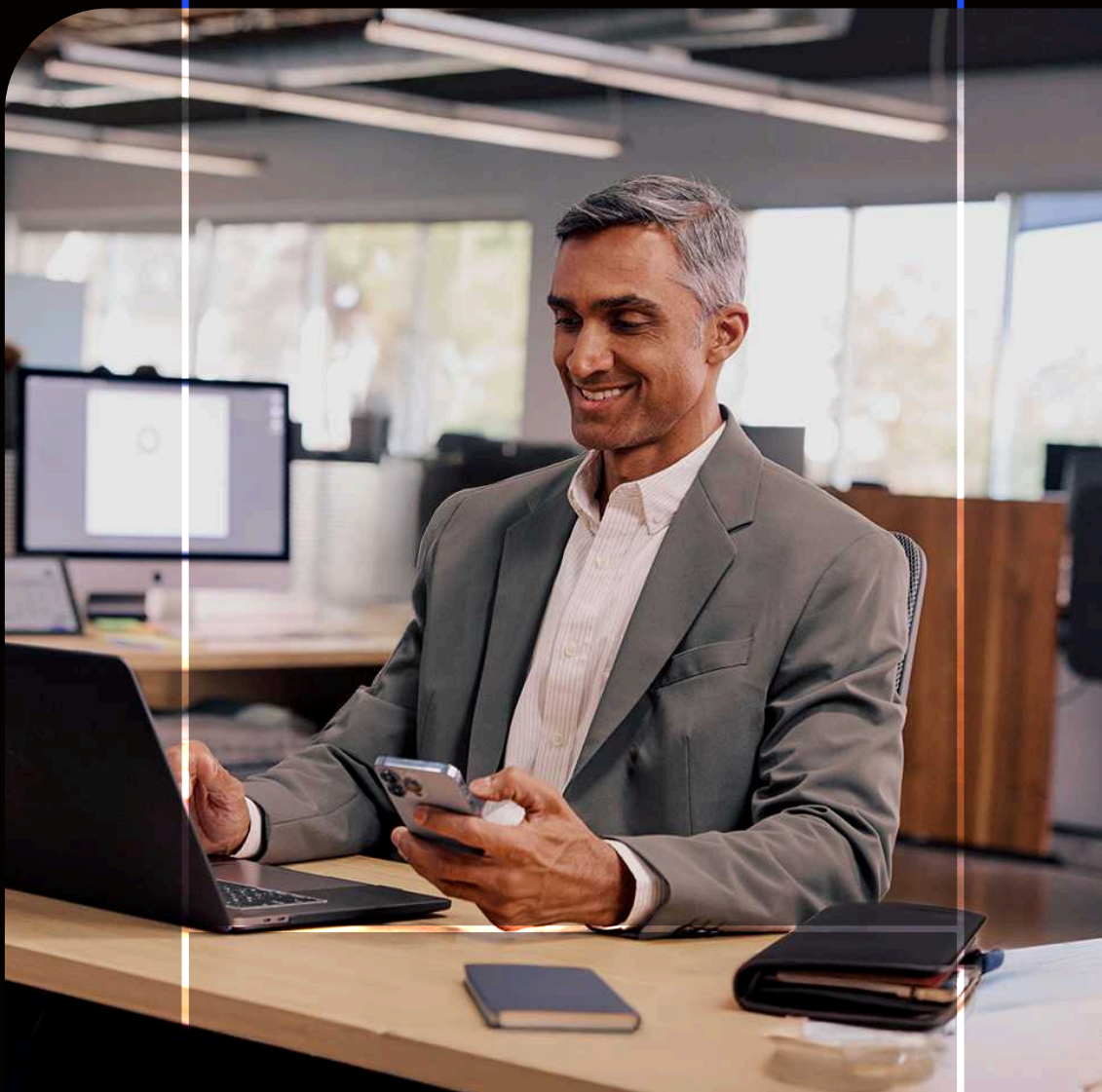
1Password

E-BOOK

Extending Access Management

Warum Zero Trust über traditionelles IAM hinausgehen muss – und wie Sie es umsetzen können



Inhalt

Einführung:

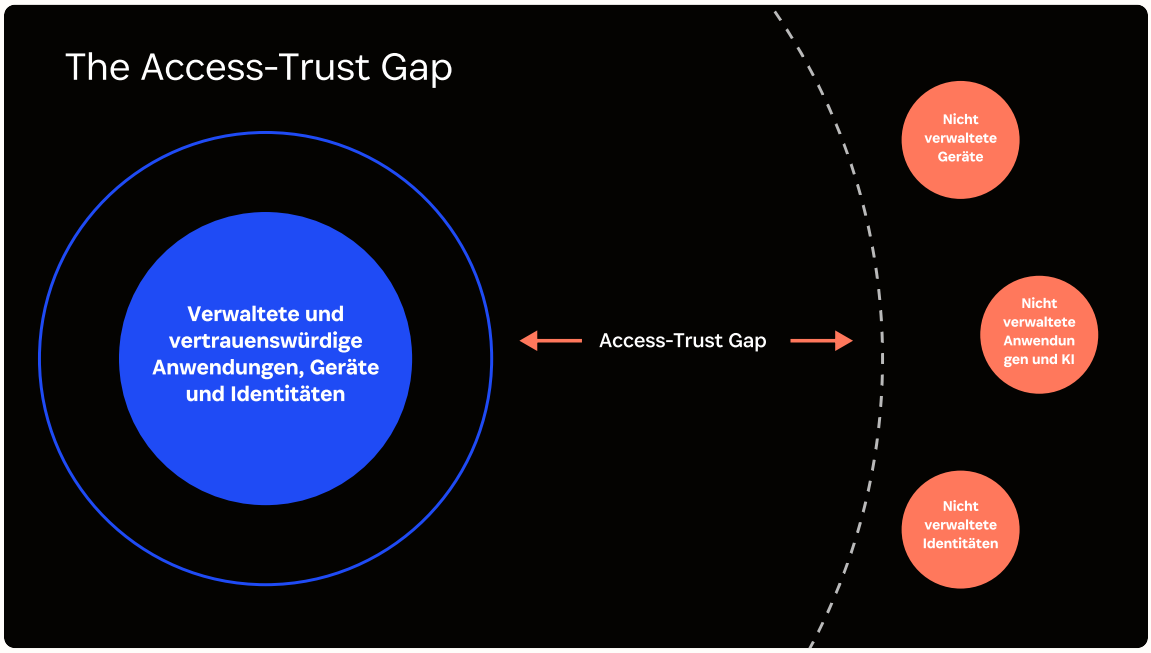
The Access-Trust Gap

Remote- und Hybridarbeit sind zur Norm geworden, nicht zur Ausnahme – und es ist klar, dass Arbeit nie wieder so funktionieren wird, wie früher. Flexibilität wird zunehmend zur Erwartung. Nicht nur hinsichtlich wo und wie wir arbeiten, sondern auch in Bezug auf die täglich genutzten Geräte und Anwendungen.

Traditionelle Ansätze für Identitäts- und Zugriffsmanagement (IAM) stammen aus einer anderen Zeit – als Mitarbeitende im Büro, im Firmennetzwerk und an einem Firmenendgerät arbeiten mussten. Die neue Arbeitsweise macht es nahezu unmöglich, mit diesen bestehenden Werkzeugen die Anforderungen von Remote- und Hybridarbeit, BYOD und der Absicherung von externen Anwendungen zu erfüllen.

Wie unten zu sehen ist, hinterlassen traditionelle IAM-Ansätze kritische Lücken in Ihrer Sicherheitsstrategie. Wir nennen dies die **Access-Trust Gap.**

Das Access Trust Gap ist die Lücke zwischen dem, was aktuelle Sicherheitslösungen bei Geräten, Anwendungen und Anmeldungen abdecken können – und dem, was sie nicht abdecken können.



Was ist die Access-Trust Gap?

In den meisten Unternehmen gibt es einen großen Unterschied zwischen dem Ziel der Sicherung aller Geräte, Anwendungen und Identitäten in einer Organisation und der Realität, dass Sicherheitstools gegenwärtig nur einen Bruchteil davon absichern können.

Dies nennen wir die Access-Trust Gap.

Die Access-Trust Gap misst den Prozentsatz aller Logins in einem Unternehmen, die nicht vertrauenswürdig sind – entweder weil sie auf nicht verwaltete Anwendungen oder von nicht vertrauenswürdigen Geräten erfolgen. Je größer die Access-Trust Gap, desto größer das Risiko eines Datenverstoßes.

Moderne Sicherheitsansätze wie Zero Trust verlangen, dass Sie nichts vertrauen und alles verifizieren. Die Access-Trust Gap zeigt jedoch deutlich, wie traditionelles IAM in vielerlei Hinsicht nicht den grundlegenden Prinzipien von Zero Trust gerecht wird:

- Nicht genehmigte Apps und Websites außerhalb des Zuständigkeitsbereichs von IT und Sicherheit sind nicht abgesichert
- Nicht verwaltete Geräte oder solche, die möglicherweise beschädigt oder kompromittiert sind, gelten als vertrauenswürdig.
- Überprüfung einer Identität ist mehr als nur ein Login und ein Passwort.

In vielen Fällen können Organisationen einige der oben genannten Herausforderungen bewältigen, aber die Fähigkeit, all diese Herausforderungen umfassend anzugehen, bleibt ein schwer erreichbares Ziel. So sehr, dass 70 % der finanziell folgenschweren Datenverstöße das Ergebnis kompromittierter Zugangsdaten sind.

Lassen Sie uns jede dieser Herausforderungen aufschlüsseln.

Anwendungen: Leben am Rande des Abgrunds

Ein großer Teil dieser Entwicklung wurde durch die Übernahme von Geschäftsapplikationen durch SaaS angetrieben. Und Mitarbeitende wollen mitmischen. Sie bringen zunehmend eigene Anwendungen von außen mit, um ihre Arbeitsweise zu verbessern. Laut dem „State of Enterprise Security Report“ von 1Password ist es sogar so:

- Trotz Jahren an Schulungen und dem Einsatz von Sicherheitsmanagementsoftware nutzt jede*r dritte Mitarbeitende (34 %) nicht genehmigte Apps oder Werkzeuge – auch bekannt als Schatten-IT.
- 64 % der Sicherheitsexpert*innen geben an, dass Schatten-IT den Spagat zwischen Nutzerfreundlichkeit und Sicherheit erschwert.
- Diejenigen, die Schatten-IT nutzen, verwenden durchschnittlich fünf nicht genehmigte Apps oder Werkzeuge.

Diese Herausforderungen gehen über Schatten-IT hinaus. Single-Sign-On-(SSO)-Werkzeuge werden oft genutzt, um den Zugriff auf Anwendungen zu verwalten, sind jedoch mit Komplexität, hohen Kosten und der sogenannten „SSO-Steuer“ verbunden – einem Modell, bei dem Organisationen für jede gesicherte Anwendung zusätzliche Gebühren zahlen müssen.

BYOD

Es sind nicht nur neue Erwartungen, die diesen Trend vorantreiben. Es ist auch Ausdruck davon, wie Mitarbeitende arbeiten möchten. Während Organisationen weiterhin Firmengeräte ausgeben, nutzen Mitarbeitende private Geräte für berufliche Zwecke – ob genehmigt oder nicht.

65 % **Fast zwei Drittel der Sicherheitsexpert*innen (65 %)** sagen, dass private Geräte die vollständige Transparenz über das Sicherheitsverhalten der Mitarbeitenden erheblich erschweren.

84 % **84 % der Sicherheitsexpert*innen geben an,** ihr Unternehmen erwarte, dass Mitarbeitende ausschließlich bereitgestellte Arbeitsgeräte nutzen.

17 % **Doch 17 % der Mitarbeitenden geben zu,** nie auf den ihnen bereitgestellten Geräten zu arbeiten – sie nutzen ausschließlich private oder öffentliche Computer.

56 % **Mehr als die Hälfte der Mitarbeitenden (56 %)** hat im vergangenen Jahr von einem privaten Gerät aus gearbeitet.

20 % **Jeder fünfte Mitarbeitende (20 %)** hat an öffentlichen Computern oder dem Gerät eines Freundes oder Familienmitglieds gearbeitet.

Device Trust

Es geht nicht nur darum, dass Mitarbeitende ihre eigenen Geräte nutzen. Unternehmen können nur sicherstellen, dass die von ihnen bereitgestellten Geräte aktuell gehalten, mit Betriebssystem- und Anwendungspatches versehen, mit Endpunktschutz ausgestattet und ordnungsgemäß konfiguriert sind – und das auch nur, wenn sie in ein Mobile Device Management (MDM)-System eingebunden sind. Doch was ist mit den privaten Geräten, die Mitarbeitende für geschäftliche Zwecke nutzen?

Leider verfügen Sicherheits- und IT-Teams nicht über die nötigen Ressourcen, um jedes einzelne Unternehmensgerät aus der Ferne zu verwalten. Ganz zu schweigen davon, dass diese Teams keinen Zugriff auf private, von Mitarbeitenden für geschäftliche Zwecke genutzte Geräte haben. Infolgedessen gibt es keine Möglichkeit, den Zugriff auf Unternehmenssysteme von nicht vertrauenswürdigen Geräten zu erkennen oder zu blockieren.

Sicherheitsteams sind machtlos

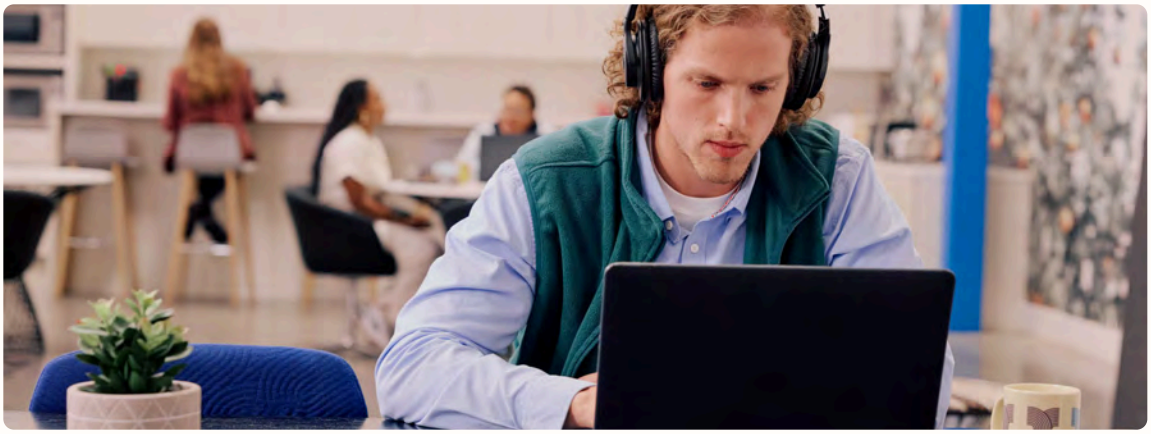
Die Unfähigkeit, diesen Anforderungen gerecht zu werden, bedeutet eines: Risiko. Und leider fühlen sich Sicherheits- und IT-Teams oft unzureichend ausgestattet, um diesen Herausforderungen zu begegnen.

- 92 % der Sicherheitsexpert*innen sagen, dass die Unternehmensrichtlinie eine IT-Freigabe für das Herunterladen und Verwenden von Software und Apps zu Arbeitszwecken vorschreibt
- Aber 59 % der Sicherheitsexpert*innen sagen, dass sie nicht kontrollieren können, ob Mitarbeitende diese Richtlinien einhalten
- Sicherheitsteams können nicht alle Geräte aus der Ferne verwalten oder den Zugriff persönlicher Geräte auf Geschäftsanwendungen kontrollieren.

Als wäre das nicht genug: Heutige Tools sind teuer und erfordern häufig spezielle Kenntnisse, was sie für viele Unternehmen unerschwinglich macht. Das Ergebnis? Es ist nahezu unmöglich für IT- und Sicherheitsteams, mit traditionellen IAM-Ansätzen sämtliche Zugriffe von allen Geräten erfolgreich zu verwalten.

92 %

der Sicherheitsexpert*innen sagen, dass die Unternehmensrichtlinie eine IT-Freigabe für das Herunterladen und Verwenden von Software und Apps zu Arbeitszwecken vorschreibt



Modernes Zugriffsmanagement hat moderne Anforderungen

Neue Cybersicherheits-Frameworks wurden entwickelt, um diesen Herausforderungen zu begegnen. Das „CISA Zero Trust Maturity Model“ beispielsweise unterteilt die Anforderungen von Zero Trust in fünf verschiedene Säulen: Identität, Geräte, Netzwerke, Anwendungen & Workloads und Daten.

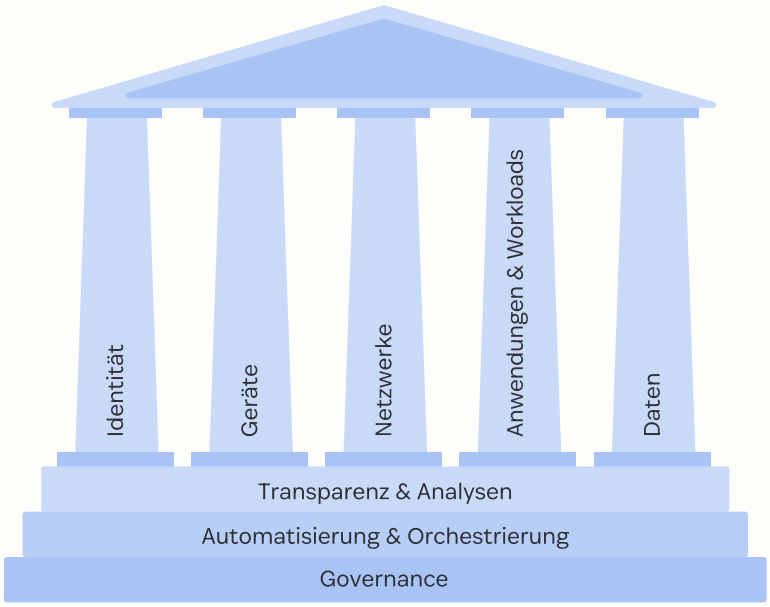


Abb. 1: Säulen des Zero-Trust-Reifegradmodells

Für das Zugriffsmanagement sind die Säulen Identität, Geräte sowie Anwendungen & Workloads besonders relevant. Im Kontext der Access-Trust Gap wird deutlich, wo die Herausforderungen liegen. Laut dem CISA Zero Trust Maturity Model lauten die Anforderungen:

- **Identität:** Integration von Lösungen für Identitäts-, Zugangsdaten- und Zugriffsmanagement im gesamten Unternehmen, um starke Authentifizierung durchzusetzen, kontextbasierte Autorisierung zu erteilen und Identitätsrisiken für Benutzer*innen und Entitäten zu bewerten.
- **Geräte:** Alle Unternehmensgeräte absichern, Risiken autorisierter, aber nicht verwalteter Geräte managen und den Zugriff unautorisierter Geräte auf Ressourcen verhindern.
- **Anwendungen & Workloads:** Bereitgestellte Anwendungen verwalten und absichern sowie eine sichere Bereitstellung gewährleisten.

Basierend auf dem Reifegradmodell lassen sich die oben genannten Säulen in konkrete Anforderungen unterteilen, die zur Schließung der Access-Trust Gap erforderlich sind:

Anforderung	Definition
Benutzeridentität	Fähigkeit, die Identitäten Ihrer gesamten Belegschaft und damit verbundenen Zugriff zu verwalten.
Universal Sign-on	Vereinfachter Anmeldeprozess, der über SSO hinausgeht und auch Websites wie Bankkonten, soziale Netzwerke sowie nicht verwaltete SaaS-Anwendungen einschließt.
Device Trust	Transparenz über den Sicherheitsstatus aller Geräte, die auf Geschäftsapplikationen zugreifen – sowohl firmeneigene als auch private – mit der Möglichkeit, den Nutzenden zur Aktualisierung von Betriebssystem und Anwendungen anzuleiten, um diese in einem vertrauenswürdigen Zustand zu halten.
Kontextbasiertes Zugriffsmanagement	Dynamische Richtlinien, die Kontextfaktoren wie Zeit, Standort, Gerätezustand und Zustand der Zugangsdaten berücksichtigen, bevor Zugriff erteilt wird.
Anwendungssichtbarkeit	Einblick in alle verwalteten, veralteten sowie nicht verwalteten / Schatten-Apps, die geschäftlich genutzt werden, mit der Möglichkeit, Authentifizierungsstärke, Nutzungsbreite und -häufigkeit zu erkennen.
Enterprise-Passwortmanagement	Sichere Verwaltung von Zugangsdaten über alle verwalteten und nicht verwalteten Anwendungen und Websites hinweg.

Die Erfüllung der obigen Anforderungen ist mit bestehenden Workforce-Identity-Lösungen nahezu unmöglich. In den meisten Fällen ermöglichen diese Lösungen zwar die Verwaltung von Identitäten, bleiben aber bei der Gewährung von Zugriff, der Sicherung von Geräten und der Unterstützung von extern eingebrachten Anwendungen deutlich hinter den Erwartungen zurück.

Bestehende Workforce-Identity-Lösungen erfüllen Zero-Trust-Anforderungen nicht

Anforderung	Bestehende Workforce-Identity-Lösungen
Benutzeridentität	✓
Universal Sign-on	✗
Device Trust	✗
Kontextbasiertes Zugriffsmanagement	✗
Anwendungssichtbarkeit	✗
Enterprise -Passwortmanagement	✗

Traditionelle Ansätze und Tools für IAM hinterlassen kritische Lücken bei der Umsetzung von Zero Trust.

Willkommen im Zeitalter von Extended Access Management

Zero Trust ist zu einem unerlässlichen Rahmenwerk für moderne Sicherheit geworden, und die Anforderungen des modernen Arbeitsplatzes haben die Notwendigkeit seiner Einführung nur noch beschleunigt. „Nichts vertrauen, alles überprüfen“ hat eines deutlich gemacht: Unsere Ansätze zur Zugriffsverwaltung müssen erweitert werden, um alle Geräte, alle Anwendungen und alle Identitäten zu sichern.

Wir nennen dies Extended Access Management (XAM).

XAM ist ein Ansatz für Zugriffsmanagement, der BYOD und Schatten-IT als normalen Bestandteil des Geschäftsbetriebs akzeptiert – und nicht als etwas, das IT- und Sicherheitsteams aktiv bekämpfen müssen. Dies schafft ein Arbeitsumfeld, in dem:

Mitarbeiter werden dazu angehalten, eine aktive Rolle bei der Stärkung der Sicherheit zu spielen – insbesondere, wenn es darum geht, die Integrität der Geräte und den Schutz der Zugangsdaten zu gewährleisten.	Die Privatsphäre der Mitarbeiter wird respektiert – Transparenz darüber, welche Daten erfasst und wie sie verwendet werden, schafft Vertrauen und sorgt für die Akzeptanz der vorhandenen Sicherheitstools.
Es werden Sicherheitstools eingesetzt, die von den Mitarbeitern auch wirklich genutzt werden – im Gegensatz zu Tools, die so umständlich sind, dass die Mitarbeiter sie umgehen.	Die Produktivität der Mitarbeiter ist sichergestellt – indem sie Sicherheitstools erhalten, mit denen der einfachste Weg, eine Aufgabe zu erledigen, auch der sicherste ist.

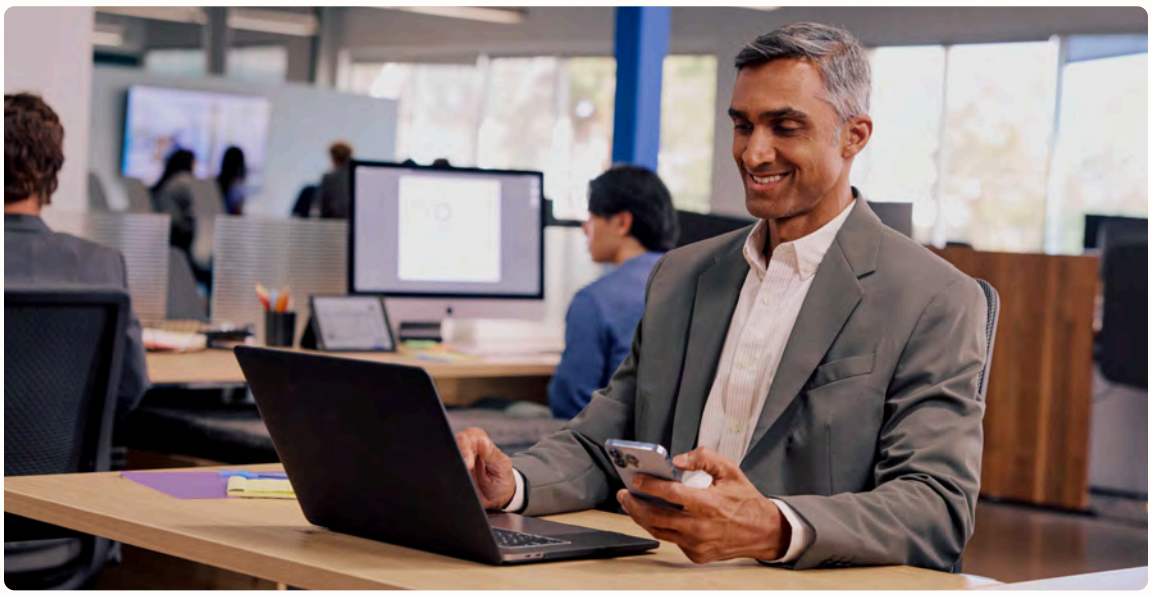
Unsere Ansätze zur Zugriffsverwaltung müssen erweitert werden, um alle Geräte, alle Anwendungen und alle Identitäten zu sichern.

Was Extended Access Management von bestehenden Identitätslösungen unterscheidet, ist, dass XAM alle Anwendungen (einschließlich nicht verwalteter und Schatten-IT), Websites und Geräte unterstützt, die Mitarbeitende im Arbeitsalltag nutzen. Darüber hinaus ermöglicht XAM dies auf eine Weise, die es Mitarbeitende erlaubt dauerhaft maximal produktiv zu arbeiten.

XAM stellt eine neue Kategorie von Sicherheitssoftware dar, mit der Sie Folgendes leisten können:

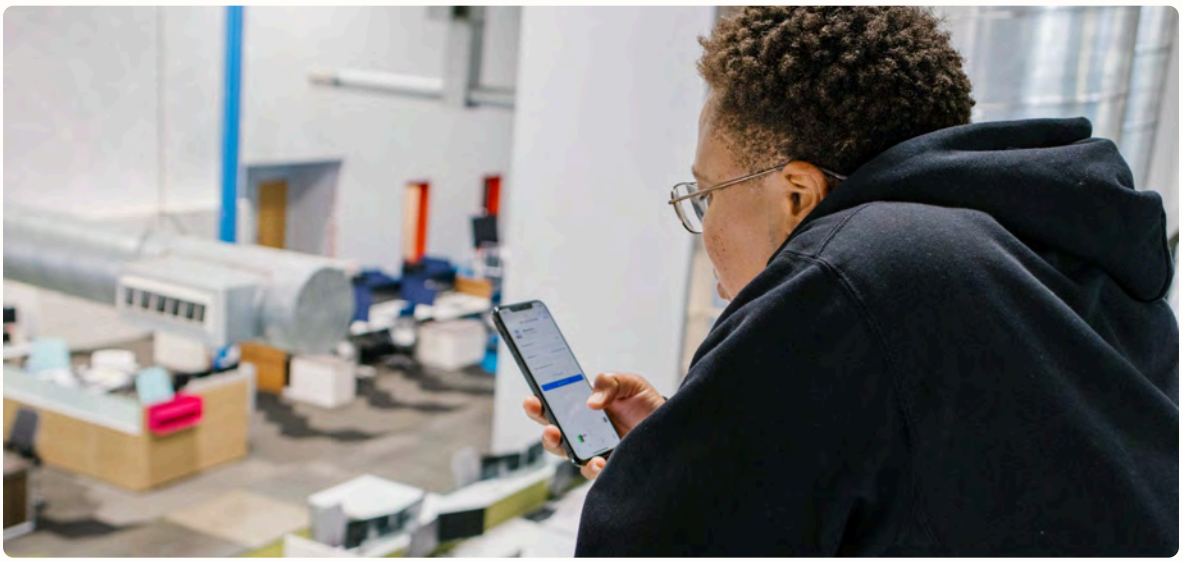
	Alle Anwendungen zu sichern: verwaltete, Schatten-IT- und Legacy-Anwendungen.
	Eine einzige, universelle Anmeldung für alle Anwendungen bereitzustellen. Dies macht es Mitarbeitenden einfach, für jede Anwendung die sichersten Zugangsdaten zu verwenden.
	Sicherstellung des einwandfreien Zustands aller Geräte – vom Unternehmen verwaltete, unternehmenseigene, aber nicht verwaltete und private Laptops und Mobilgeräte der Mitarbeitenden. Blockierung oder Beschränkung von Zugriffsversuchen von nicht vertrauenswürdigen Geräten.
	Ausschließlich gesunden Geräten den Zugriff auf Anwendungen zu gewähren – im Gegensatz zu IAM-Tools, die den Zugriff von nicht vertrauenswürdigen Geräten nicht einschränken können.
	Bereitstellung eines elegant einfachen Nutzererlebnisses, dass gleichermaßen gut auf geschäftlichen wie privaten Geräten funktioniert und Mitarbeitende dazu motiviert, ihre persönlichen Geräte mit XAM abzusichern, da dies der einfachste Weg ist, auf Anwendungen zuzugreifen.

XAM stellt eine neue Kategorie von Sicherheitssoftware dar, um die Gesundheit aller Geräte sicherzustellen.



Vergleich traditioneller Lösungen für Workforce Identity mit XAM

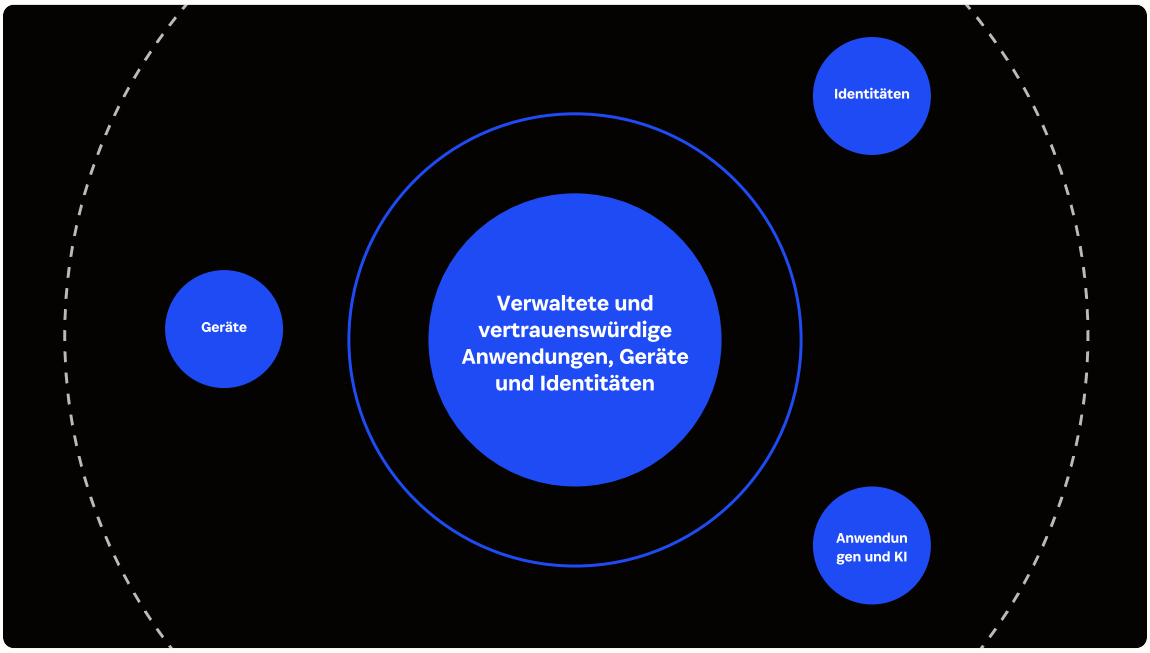
Anforderung	Bestehende Workforce-Identity-Lösungen	Extended Access Management (XAM)
Benutzeridentität	✓	✓
Universal Sign-on	x	✓
Device Trust	x	✓
Kontextbasiertes Zugriffsmanagement	x	✓
Anwendungssichtbarkeit	x	✓
Enterprise -Passwortmanagement	x	✓



1Password® Extended Access Management und die Zukunft von Zero Trust

1Password XAM schließt die Access-Trust Gap zwischen Identity and Access Management (IAM), Privileged Access Management (PAM), Mobile Device Management (MDM) und Bereichen, die selbst Extended Detection and Response (XDR) nicht abdecken kann. 1Password XAM:

- Schützt alle Anwendungen
- Bietet einen einzigen universellen Login für alle Anwendungen
- Stellt die Integrität aller Geräte sicher
- Stellt sicher, dass nur fehlerfreie Geräte Zugriff auf Anwendungen haben
- Bietet eine elegant einfache Benutzererfahrung



Fazit

Aktivieren und sichern

XAM stellt einen grundlegenden Wandel in der Herangehensweise von Unternehmen an Identity and Access Management dar – mit einem umfassenden Ansatz zur Absicherung von Identitäten, Geräten und Anwendungen. Während früher nur der Zugriff von Mitarbeitenden auf Systeme in kontrollierten, physischen Umgebungen abgesichert werden musste, stellt die moderne Arbeitswelt völlig andere Anforderungen. XAM ist ein neuer Ansatz in der Cybersicherheit, der es Organisationen ermöglicht, diesen Anforderungen auf benutzerfreundliche und einfache Weise gerecht zu werden.

Erfahren Sie mehr über Extended Access Management und 1Password Extended Access Management.

Mit über 165.000 Unternehmen und Millionen von Verbrauchern als Kunden bietet 1Password Identitätssicherheits- und Zugriffsmanagement-Lösungen, die für die heutige Arbeits- und Lebensweise entwickelt wurden. Die Mission von 1Password ist es, den Konflikt zwischen Sicherheit und Produktivität zu beseitigen und gleichzeitig jede Anmeldung, in jeder App, auf jedem Gerät abzusichern. Als Anbieter des am häufigsten genutzten Enterprise-Passwortmanagers baut 1Password seine starke Grundlage kontinuierlich aus und bietet Sicherheitslösungen, auf die Unternehmen jeder Größe vertrauen – darunter Associated Press, Salesforce, GitLab, Under Armour und Intercom.

Erfahren Sie mehr über 1Password.