Enabling the Future of Work with EPM, Identity and Access Controls

January 2022

Authors:

Mark Child
Research Manager, European Security, IDC

Jay Bretzmann
Program Director, Security Products, IDC

IDC #EUR148370521

An IDC InfoBrief, sponsored by

LastPass

Troubled Waters

- The COVID-19 pandemic has been one of the biggest challenges ever for enterprises, and we're not out of the storm yet.
- There is hope, however. Vaccines and innovative safeguards are enabling a return to some kind of normal, and business, commerce, and travel are bouncing back.

AN UNEVEN RECOVERY

Tourist arrivals to Europe rose 75% from December 2020 to May 2021, according to the UNWTO. In the Americas, however, they rose only 14% and 8.5% in Asia/Pacific. In Africa they dropped 35%.

SUPPLY CHAIN WOES DELAY RECOVERY

European retailers are struggling with higher freight and labor costs and supply chain disruption, impacting their sales, according to the Economist. In the U.S., FedEx, UPS, Walmart, and two large ports have switched to 24 x 7 schedules to alleviate supply chain bottlenecks, according to the Financial Times*.

CHIP CRISIS HITS HOME

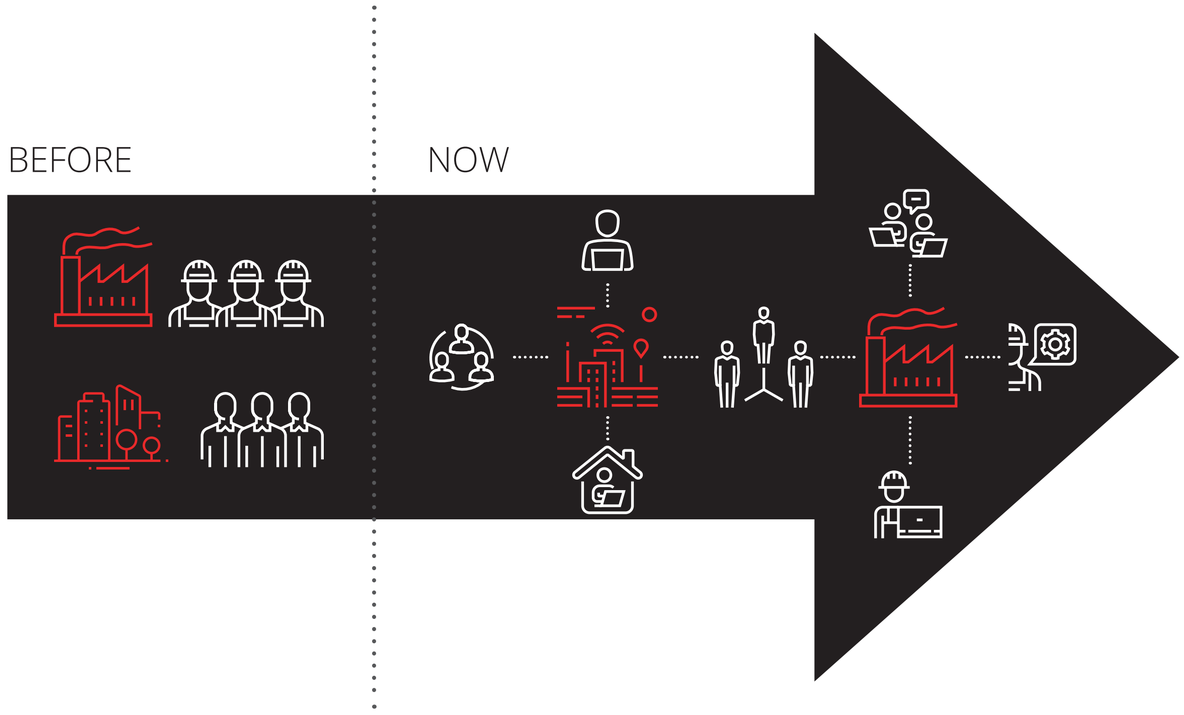
Semiconductor shortages will cause global vehicle production to fall by up to 5 million units in 2021, according to consultancy AlixPartners**. Apple expected a drop of $6 billion in its FYQ4, while Samsung reported potentially having to delay the launch of its new Galaxy Note smartphone.

BUDGET IMPACT

30% of organizations worldwide reported reduced security budgets for 2021, due to COVID-19***. The figure is even higher in France (41%), Singapore (38%), and the U.K. and Ireland (37%).

*Source: https://www.ft.com/content/8055d806-3166-48c9-9786-9bdea0e2d806
**Source: https://eandt.theiet.org/content/articles/2021/10/apple-results-hit-by-chip-and-supply-chain-woes-warns-that-impact-will-get-worse/
***Source: IDC-LastPass Custom Survey 2021 (n = 700)

The Days of Workers Tied to an Office Desk Are Over



FUTURE-OF-WORK IMPERATIVES

- Work from anywhere
- Hybrid work models
- Flexibility
- Hot desking
- User experience (UX)
- Productivity
- Mobility
- Invisible security
- B2E, B2P, and B2C identity management

Very few organizations have a return to old working norms on their agenda. Mindsets have shifted from office work to working from home to working from anywhere, and from traditional offices and cubes to hybrid and hot desking.

Employers have realized that their workforces can be remote and still be productive. They've seen the other side and are fighting to get there. **But collaboration and security challenges remain**.

According to a joint survey conducted by IDC and LastPass, **one in three organizations worldwide** is striving to balance user experience, productivity, and security in the face of operating restrictions caused by COVID-19.

Identity and access controls are core components for addressing many future-of-work imperatives.

Identity Compromises Are Far Too Common

Among organizations that have suffered data loss following a network security breach,

83%

say the breach was the result of an identity compromise such as **phishing**

In Germany, this stands at **82%**, in the US it rises to **87%**, and in India it hits **90%**.

"Balancing security requirements and user experience for employees" is the

#1

identity challenge (38%), followed by **"employees struggling with too many passwords"** (32%)

"Too many passwords" is a key challenge for **36%** of large organizations, and for **40%** of public sector organizations.

45%

of organizations have deployed an **enterprise password management solution** to address these challenges.

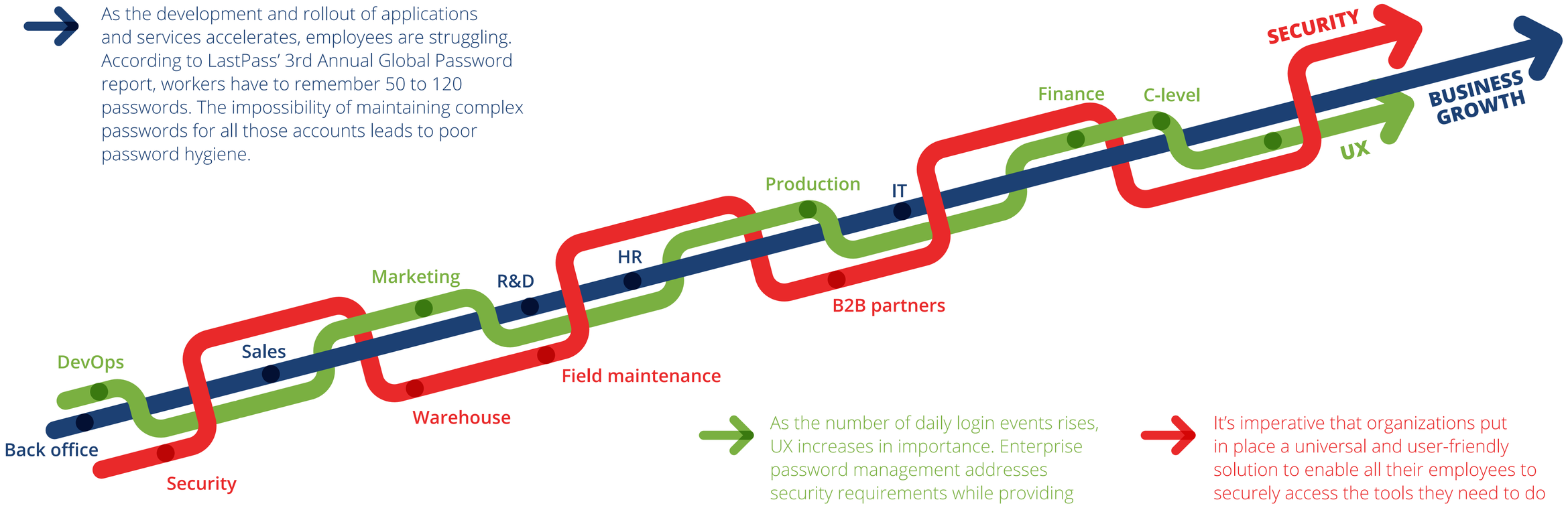
These include both **large enterprises** that wish to provide an extra layer of protection and user convenience and **SMBs** with limited security budgets.

EPM penetration is even higher in Asia/Pacific **(52%)** and highest in vertical markets such as manufacturing **(60%)** and retail **(50%)**.

Source: IDC-LastPass Custom Survey 2021 (n = 700)

Accelerating Business Requires Ubiquitous Security … and Convenience

As the development and rollout of applications and services accelerates, employees are struggling. According to LastPass' 3rd Annual Global Password report, workers have to remember 50 to 120 passwords. The impossibility of maintaining complex passwords for all those accounts leads to poor password hygiene.



As the number of daily login events rises, UX increases in importance. Enterprise password management addresses security requirements while providing a consistent and comfortable user experience.

It's imperative that organizations put in place a universal and user-friendly solution to enable all their employees to securely access the tools they need to do their jobs. **Security controls need to be transparent and manageable for all users.**

Facing the Adversary

Are cybercriminals just too good at what they do?

- According to IDC research, 60% of European organizations are either implementing or extending digital-first strategies to deliver business outcomes. Leveraging new partners and suppliers brings business benefits but increases exposure.
- How can organizations provide secure access to requisite systems to a supplier without potentially exposing themselves to compromise? Passwords and authentication can be a weak link if those mechanisms are not protected.
- Moreover, ransomware attacks and supply chain attacks continue to threaten our organizations. Supply chain risk will only increase as we move beyond the pandemic and globalization accelerates.

According to Verizon's Data Breach Investigation Report 2021

93% of attacks come from financially motivated organized crime actors. The most frequent data compromised is credentials (44%), while threat actors are 57% external and 44% internal (some have multiple actors).

Breach patterns for small organizations (<1,000 employees) match those for large, with around one in four confirming a data disclosure. Note, however, that large organizations are typically able to discover breaches more quickly (within hours/days) compared to small organizations.

In 2020, login data for over 500,000 gamer accounts at US video game publisher Activision were targeted in a credential stuffing attack and published online, giving hackers access to the Call of Duty accounts.

According to LastPass' 2021 Psychology of Passwords report, 65% of people always or mostly reuse the same password or a variation, and 45% didn't change their password even after a breach had occurred. This behavior results in a higher volume of breaches putting businesses and consumers at greater risk.

Attacks Span All Geographies and Industries

Nintendo — Gaming

- Japan
- 2020
- Credential stuffing
- A credential stuffing attack using previously exposed user IDs and passwords from video game company Nintendo gave hackers access to over 300,000 player accounts.

HSBC — Banking

- U.K.
- 2018
- Credential stuffing
- An estimated 14,000 customers had names, addresses, phone numbers, email addresses, dates of birth, account numbers, account balances, and transaction history exposed.

UniCredit — Banking

- Italy
- 2019
- Email phishing
- A security incident leaked 3 million customer records, including customers' names, cities, telephone numbers, and emails.

EyeMed, Aetna — Healthcare

- U.S.
- 2020
- Email phishing
- A phishing attack on EyeMed exposed the personal and medical information of 484,000 Aetna members, 60,500 members of Tufts Health Plan, and 1,300 members of Blue Cross Blue Shield.

HSE.ie — Healthcare

- Ireland
- 2021
- Conti ransomware
- Nationwide IT system shutdown impacted hospitals across the country, preventing access to electronic records, knocking radiology systems offline, and forcing appointment cancellations. Patient data was also leaked online. The estimated cost of the attack was more than €100 million.

Multiple public figures

- Germany
- 2018
- A lone hacker leaked private data of almost 1,000 German politicians and celebrities. Investigators reported that most of the accounts hacked had simple passwords such as 'ILoveYou' or '1,2,3', making it relatively easy for the hacker to gain access to email accounts, cloud services, and social networks.

How can security solutions shift the needle?

Where Identity Controls Intersect with Risk Management

Verizon also mapped the findings of its Data Breach Investigation Report against the recommended controls proposed by the Center for Internet Security (CIS). The core set of controls that every organization should consider implementing, regardless of size and budget, include **account management, access control, and security awareness and skills training.**

Key questions to ask include:

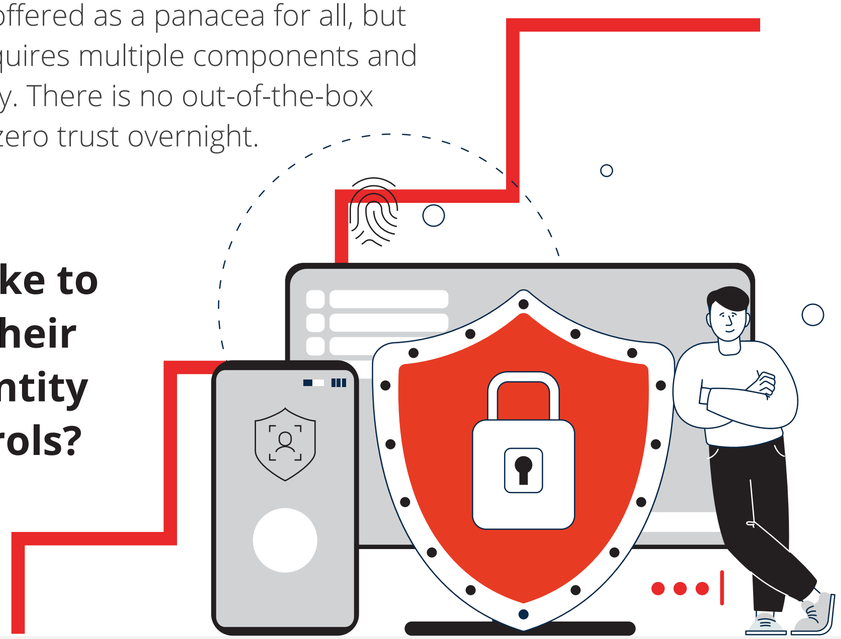
What tools are available to safely authenticate and grant secure and appropriate access to remote workers?

How can organizations tackle the persistent problems of weak passwords and poor password hygiene that are a hacker's best friend?

What safeguards can be put in place to prevent major threats like ransomware from penetrating and spreading within the organization?

Concepts like passwordless authentication and zero-trust access control are offered as a panacea for all, but achieving these goals requires multiple components and a comprehensive strategy. There is no out-of-the-box solution that will deliver zero trust overnight.

What steps can organizations take to begin reducing their risk through identity and access controls?

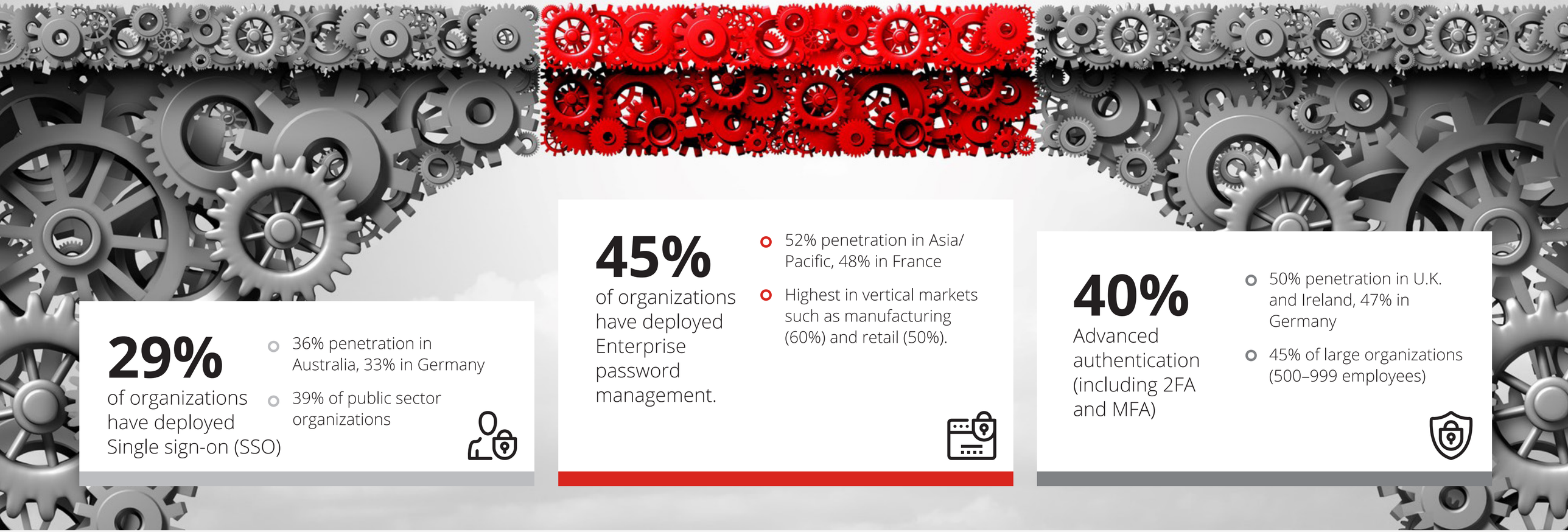


Bridging Infrastructure and Process Gaps with a Single Deployment Is Not Always an Option

- Every organization wants to leap ahead when it identifies a market opportunity.
- Dev teams are suffused with messages about speed to market, failing fast, or failing forward.
- Business wants to expand as rapidly as possible.

- Employee access delays and outright inability to use applications designed to support productivity and business goals should not occur due to missing SAML (SSO) support.
- B2C solutions must appeal to perhaps the most fickle group of prospects and customers where the competition is a click away.
- For many organizations, it takes a combination of security tools to address the identity needs of all users.

Deploying the Solutions to Bridge the Gap



29%
of organizations have deployed Single sign-on (SSO)

- 36% penetration in Australia, 33% in Germany
- 39% of public sector organizations

45%
of organizations have deployed Enterprise password management.

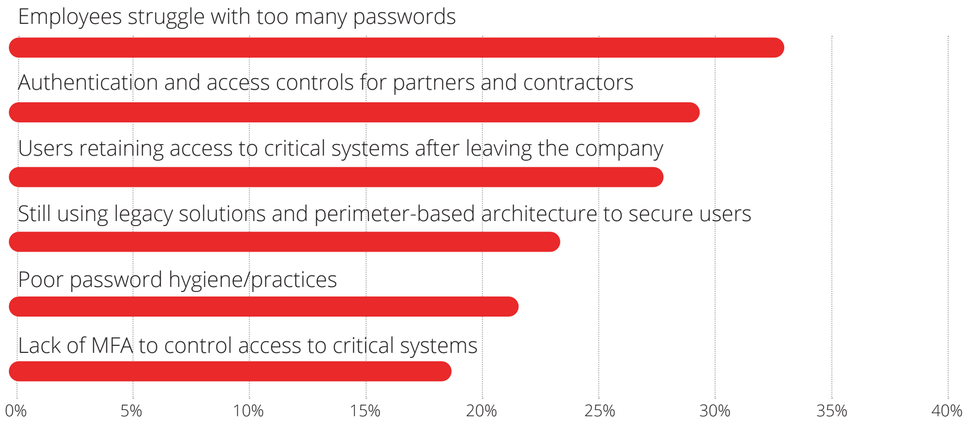
- 52% penetration in Asia/ Pacific, 48% in France
- Highest in vertical markets such as manufacturing (60%) and retail (50%).

40%
Advanced authentication (including 2FA and MFA)

- 50% penetration in U.K. and Ireland, 47% in Germany
- 45% of large organizations (500–999 employees)

Enterprises Continue to Grapple with What Should Be Fundamental Identity and Access Controls …

Which of the following challenges does your organization face in terms of identity and access?



… such as rescinding users' access when they leave the company.

Organizations remain overdependent on legacy solutions and perimeter-based architecture **and are exposed to unnecessary risk due to poor password hygiene**.

There is considerable scope for improvement in the identity and access area.

- 42% of Australian companies struggle to balance security and UX for employees.
- 32% of French firms find authentication and access controls for partners and contractors challenging.

- 43% of large organizations (500–999 employees) struggle to balance security and UX for employees.
- **32% of small businesses (10–99 employees) say their employees struggle with too many passwords.**

- 33% of services companies struggle with users retaining system access after leaving the company.
- 42% of transportation firms say their employees struggle with too many passwords.

Source: IDC-LastPass Custom Survey 2021 (n = 700)

EPM Adoption Is Characterized by Multiple Drivers and Configurations

EPM as a standalone solution:

45% say more complex identity solutions such as SSO and MFA are nice to have, but they don't have the budget (this is true for 55% in Asia/Pacific and 48% in North America).

34% say complex solutions such as SSO and MFA are nice to have, **but they don't have the resources to deploy and run them** (this is true for 41% of European organizations).

27% say their organization is too small to need solutions such as SSO and MFA.

EPM combined with SSO but not MFA:

48% say SSO reduces password fatigue, but few of their apps require additional MFA controls which would restore fatigue.

46% say **password management provides additional protection with regards to shadow IT usage**.

40% say SSO is not universal for all the apps they use, so they also need password management.

EPM combined with SSO and MFA:

91% say EPM provides a usability convenience that employees appreciate for **frequently visited external websites**.

77% say **the more layers of controls and safeguards they have, the better**.

75% say SSO is not universal for all the apps they use, so they also need password management.

Source: IDC-LastPass Custom Survey 2021 (n = 700)

A Solution for Everyone in the Room

An ideal identity and access management tool should:

- Be deployed and effective across every team
- Behave like a security tool but not look like one
- Be user friendly for everyone from the most IT savvy to the most IT phobic

Features of an ideal tool should include:

- Easy deployment and integration with all key applications your organization uses
- User transparency and a frictionless experience
- A price tag that midmarket and enterprise accounts can afford

Enterprise password management delivers:

- A **secure repository for every login of every employee that nobody else can access**, not even administrators or LastPass itself
- Additional security controls such as validating the authenticity of a site before credentials are entered
- Added value like complementary family member accounts for work-from-home employees

About LastPass

LastPass

Simply and securely connect employees to their work.

IT is challenged to keep the business secure, without impacting productivity.

From authentication to access to passwords, LastPass manages every entry point to your business so you can mitigate risk while improving employee productivity.

Comprehensive security controls

Plug-and-play integrations

Adaptive authentication

Easy user management and reporting

Convenient password sharing

Frictionless user experience

Dark web monitoring

Designed for security first

Seamless deployment, management and experience

Over 85,000 businesses use LastPass

30M+ users

A free Families account for employees

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Corporate Headquarters
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
508.872.8200
www.idc.com