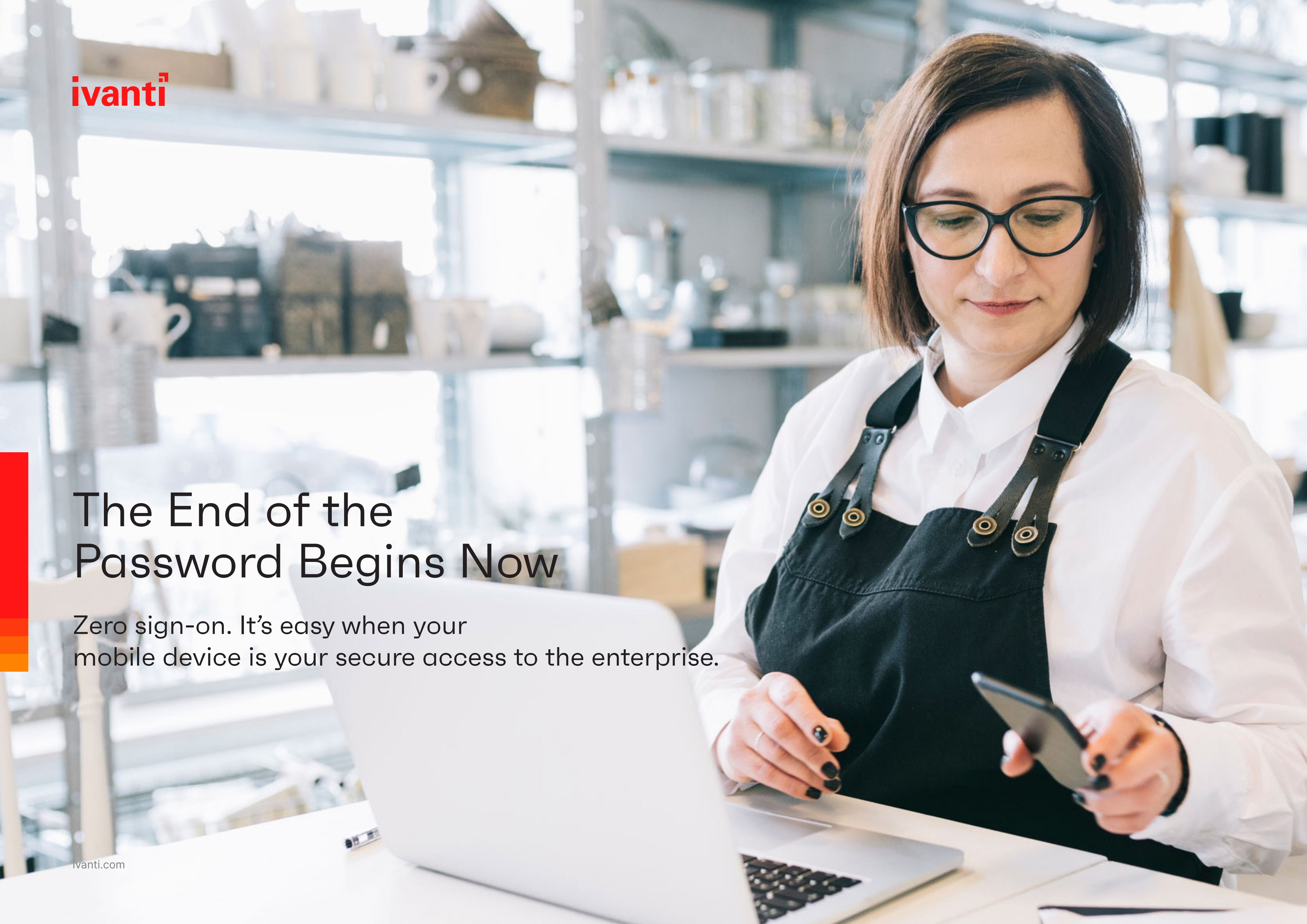


The End of the Password Begins Now

Zero sign-on. It’s easy when your mobile device is your secure access to the enterprise.

Introduction

Passwords. They’re the top security risk and a notorious end user pain point. And they’re about to become a memory. Ivanti is eliminating passwords by making the mobile device your identity and your secure access to the enterprise.

We’re also making it simple, because your existing Ivanti Unified Endpoint Management (UEM) is at the center of this breakthrough, creating the foundation of our end-to-end, zero trust security approach. That means you’ve already got what it takes to make your organization a password-free zone for smoother experiences and greater productivity.

This ebook explains how Ivanti Zero Sign-On (ZSO) ends the pain of passwords, and how your organization can benefit from this groundbreaking shift in security by leveraging your investment in your Ivanti UEM.

The problem with passwords

Passwords have become more of a security liability than a security solution. They represent headaches for IT and hassles for end users. Efforts to improve the situation have failed because passwords were minimized, not entirely removed from the equation.

Security challenges for IT

As a top cause of breaches, passwords represent tremendous risk for organizations, creating an ongoing security challenge for IT. And for hackers, they represent a potential payday as automated brute force programs make it relatively easy to crack them.

A wide variety of social engineering tactics are also used for credential theft, including phishing attacks, which use email or malicious websites to solicit passwords. Other exploits, such as “vishing” (voice phishing) and “smishing” (SMS/text phishing), are also becoming more prevalent. But this isn’t a scary story. It’s a chance for change.

Poor user experience

A universal truth: users can’t stand passwords. This growing frustration only contributes to their risk. To strengthen them, passwords have become more complex, which makes remembering them even more difficult. Users are now expected to memorize passwords of at least eight characters, with uppercase and lowercase letters, a number, and a special character – and it must be unique within the last three months. Trying to type these strings of characters into mobile devices is a whole new level of frustration.

The sheer volume of passwords employees need to remember exacerbates the problem. Variations of this frustrating password experience are repeated for all cloud services and other applications within the organization. The result is forgetting, resetting, lockouts and a repeating pattern of non-productivity.

61% of breaches involved credentials.[1]

Use of stolen credentials was second most frequent tactic in data breaches.[1]

Credentials compromised faster than any other data type.[1]

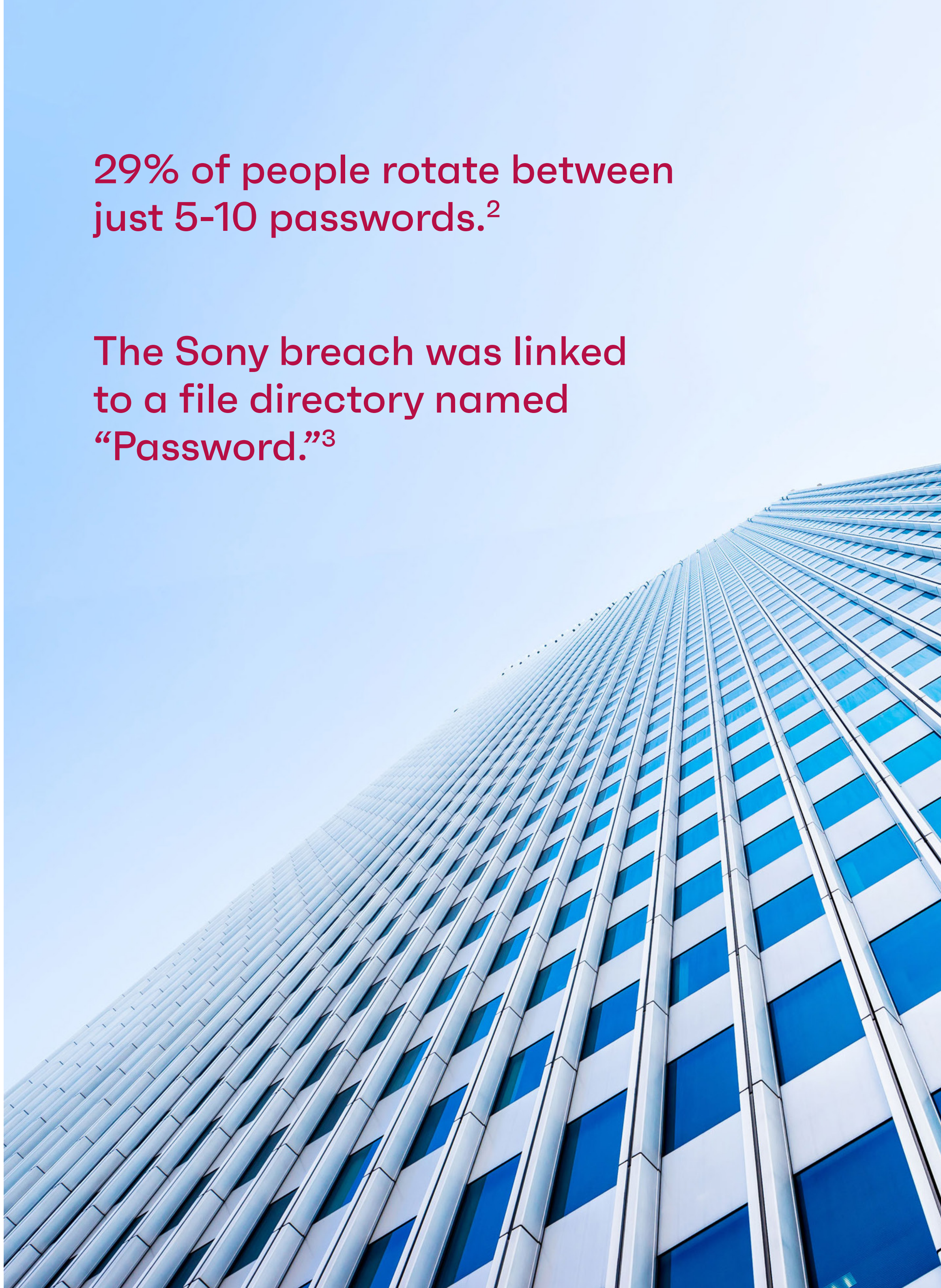
23% of organizations had security events related to brute force and credential stuffing attacks.[1]

Risky workarounds

The trickier password requirements become, the more people are driven to risky behavior to deal with them. To avoid the hassle of resetting or getting locked out from failed attempts, users resort to:

- Using the same password across multiple accounts.
- Handwritten passwords stuck right on devices.
- Storing all their passwords in one obviously named file.

ZSO provides both SSO and MFA functionality, thus we should avoid denigrating SSO and MFA in our own materials.



29% of people rotate between just 5-10 passwords.[2]

The Sony breach was linked to a file directory named "Password."[3]

Zero sign-on

We said this wasn't just a scary story, right? Here's the happy ending. It took the leader in mobile security to figure out how to replace the password and create a zero sign-on experience.

With mobile as your ID and secure access, seamless authentication experience is possible from anywhere. Users can securely access any business app, device or resource with a glance or a tap of their finger. No passwords required. Just simple passwordless access to any service, from any device, on any OS – anywhere. With the rise of the Everywhere Workplace, this has never been more important.

Consumer-like security ease

Providing this consumer-like security ease is a natural extension of what we've already come to expect from our mobile devices. The most widespread example of this is mobile payment systems, such as Apple Pay and Google Pay, which let you enroll a credit or debit card. When you pay using that card, the systems authorize the transaction based on something you have (your phone, watch, or tablet) and something you are (a biometric confirmation via a technology such as Apple's Face ID or Touch ID). We're bringing this type of seamless security experience to the workplace.

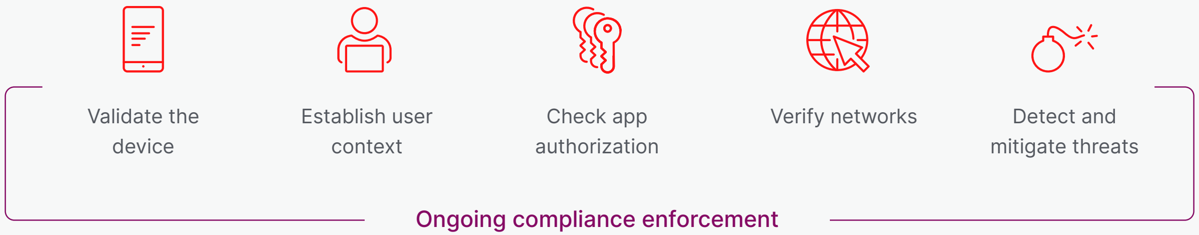
End-to-end, zero trust approach

It's all a part of how we're redefining enterprise security with an end-to-end, zero trust approach – which starts with the UEM foundation you already have. This grants access only after correlating user, device, app, network and threats – all without requiring a password.

Any cloud service.
This same passwordless process also allows secure access to any cloud service your company needs, such as Microsoft 365, Salesforce or Dropbox.

Any device.
This seamless security extends to devices that your organization doesn't manage, such as contractors and partners who need access to certain company apps.

Never trust, always verify.



Validate the device

Establish user context

Check app authorization

Verify networks

Detect and mitigate threats

Ongoing compliance enforcement

Passwordless access to any service from any device on any OS from anywhere.

Our devices already use biometrics for secure access.

Zero Sign-On.
Ivanti delivered.

By turning your mobile device into your secure ID with end-to-end, zero trust security, Ivanti has created a world in which you can:

- Reduce security risk from credential theft.
- Avoid users' risky password workarounds.
- Protect against growing mobile threats.
- End the frustrating cycle of forgetting and resetting passwords.

It's all possible because of end-to-end, zero trust security that starts with the UEM framework you already have. Put it to work to end passwords in your organization. Users and IT will thank you.

Learn more

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Verizon, "2021 Data Breach Investigations Report", 13 May 2021. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/
2. Verizon, "2021 Mobile Security Index", 6 April 2021. https://www.verizon.com/business/resources/reports/mobile-security-index/2021/foreword/
3. Insider, "Thousands Of Leaked Sony Passwords Were Reportedly Kept In A Folder Marked 'Password'", 4 December 2014. https://www.businessinsider.com/sony-leak-reveals-thousands-of-passwords-in-obvious-password-folder-2014-12