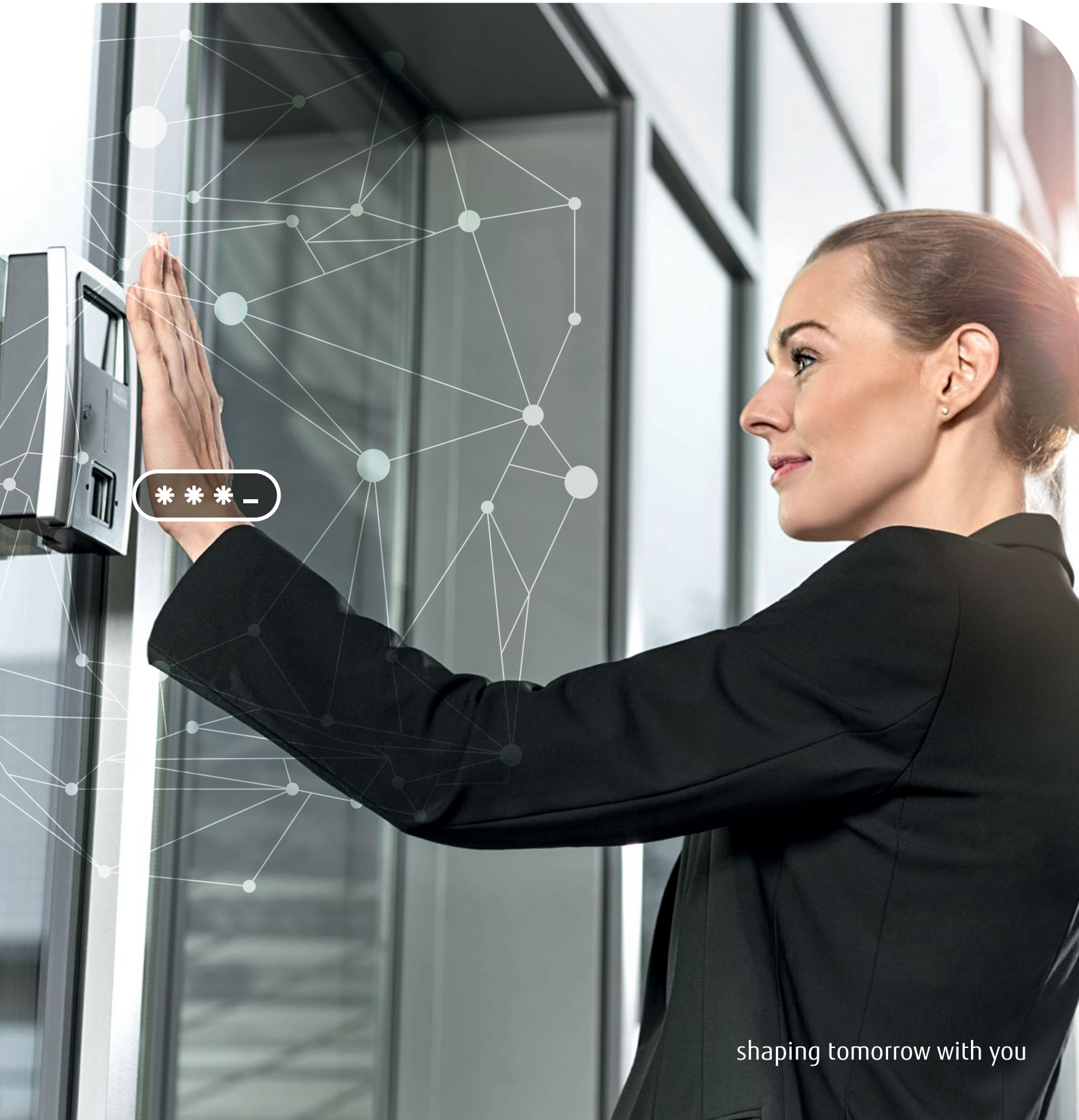
FUJITSU

Passwords are dead.
Long live data protection.



shaping tomorrow with you

We're all guilty.
Every time we register for something online we ought to create a new password. Websites even ask us sometimes if our choice is indeed unique.

But is it?

No. We tend to key in words or character strings we've used before. It's fast, it's easy, and it reduces the chances that we'll forget the magic word. That's why most of us tend to use at best a small handful of passwords we'll remember, and at worst just the one. For everything.

You are the key to your devices

And that's not all. We use these passwords across several devices – not just our office desktop, but our notebook, our tablet, our smartphone. We may even ask our devices to remember them so we don't have to re-key them every time.

That's not a problem, right? We say, "It's OK. Really. I use a four-digit access key for all my kit (OK, it's the same four digits for every device, but whatever). And I never, ever leave my stuff lying around anyway."

Hmm. But just suppose our notebook were lost or stolen anyway. How good would we feel about our four-digit access key then? If criminals could beat or bypass it they would then have full access to our data – and even if we hadn't saved our passwords to the device, they would have the time, patience and probably the tech knowledge to figure them out. Result: disaster for us and for our employers too.

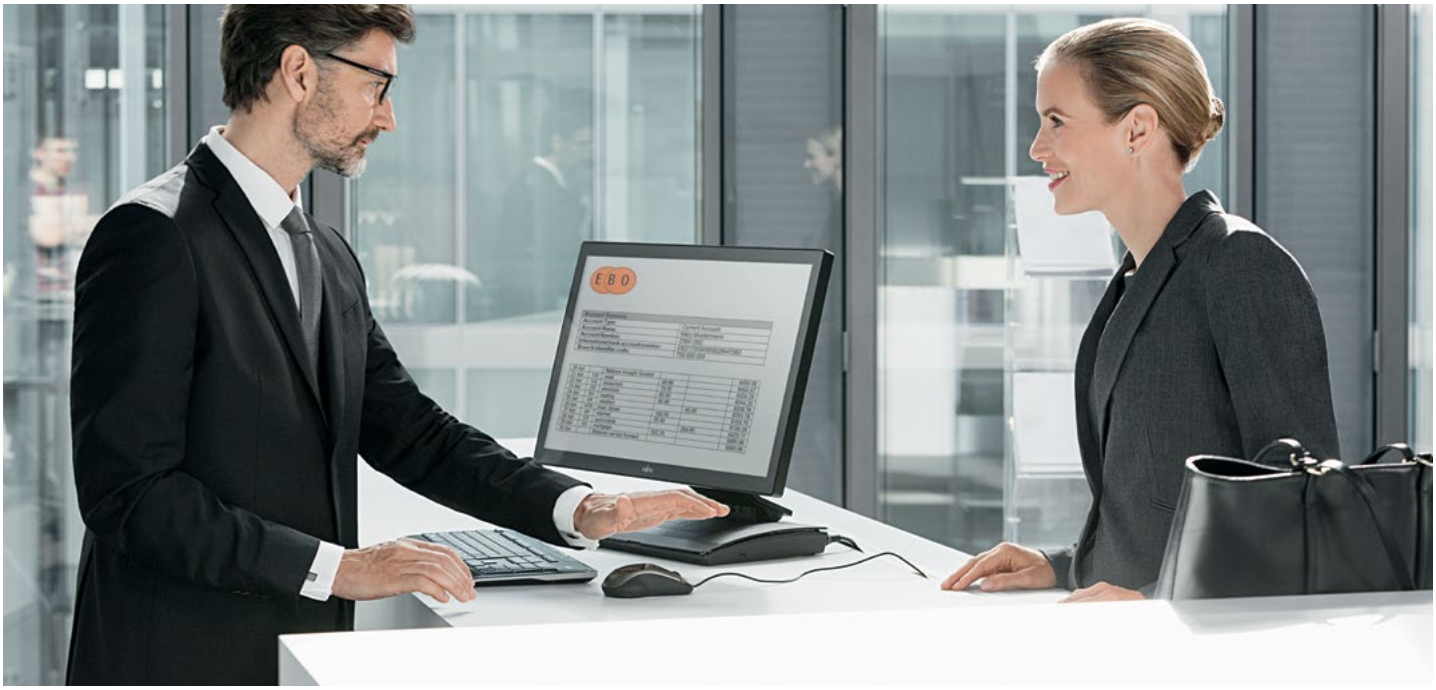
It's little wonder, then, that the information security industry is so worried about the fragility of the username/password system. Last year, McAfee estimated that information theft worldwide might be costing **as much as $160 billion annually.** And it's no surprise either that password management is becoming a major problem at enterprise level.

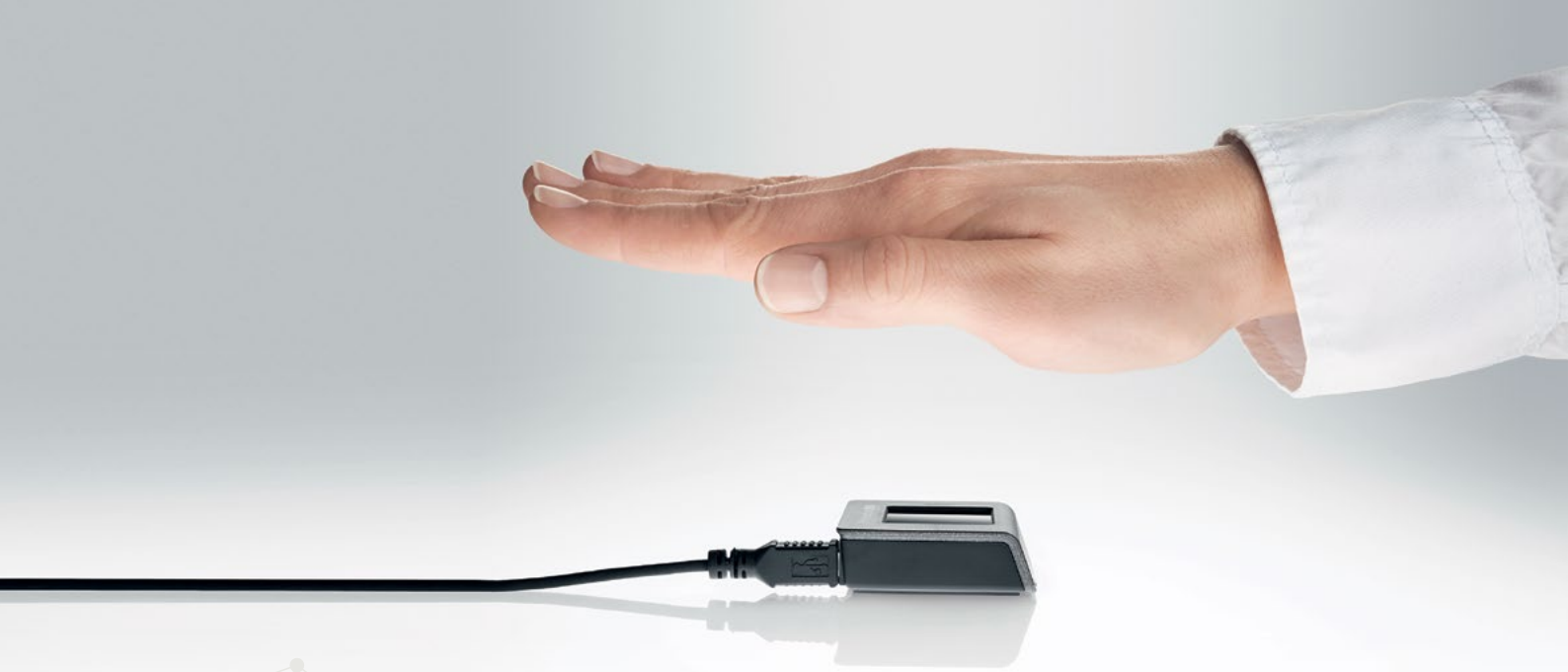
Major organizations are now exploring combinations of several different authentication methods. They include computer recognition software – sending one-time passwords by email or SMS; out-of-band verification; peripheral device recognition; and scratch-off cards.

Getting personal

With so many devices on the move, what we need as organizations and as individuals are forms of security that are as robust as the most uncrackable string of random characters but that are also as easy as our date of birth or our favorite color. Even if you find this balance, you need a different password for each application, site or service. And, then, you need to change them regularly to maintain their strength. Hence the growing use of biometric methods of personal identification, each of them appropriate to different circumstances. They can be used in isolation or in combination with other authentication methods such as ID cards.

Common biometric identification methods include fingerprints, voiceprints, facial recognition and palm veins. Each of these takes advantage of physical attributes that are unique to each of us as individuals – but what distinguishes palm veins from the others and makes it more secure is that the patterns it checks exist inside the body, and so can't be stolen by means, for instance, of photography or voice recording. This is just one reason why Fujitsu has invested in its PalmSecure™ technology.





PalmSecure gives peace of mind to people and service providers alike. Each individual's palm scan has more than five million reference points, making it 100 times more exact than fingerprint identification. What's more, the vein pattern is hidden. It's visible only to light in the near-infrared waveband, and only when blood is flowing through it (so-called 'life detection') – so, for example, a photocopy of someone's hand simply won't do.

The scan can be stored on a server, in the cloud or on a card owned by the individual. It all depends on the law in your country and on your specific company requirements and policies. Either way, it's highly secure. Instead of – or perhaps as well as – requiring an access code, PalmSecure-enabled devices ask for a palm vein scan. As users, we provide this by holding our hand over the device. The cross-match is fast and convenient.

It's a contactless technology: we only have to hover our hand over the surface. In other applications, such as identity verification in hospitals using fixed scanners, hygiene issues are of course of even greater importance.

Let's say our notebook is stolen and it's protected by PalmSecure. The biometric password is saved on the card we hold and not on the notebook itself. Thanks to Workplace Protect software, the device's inbuilt pre-boot authentication routine asks for a palm scan, which of course the thief is unable to provide. Without it, access is close to impossible.

Organizations, such as The Bank of Tokyo-Mitsubishi, The Hiroshima Bank and The Bank of Iked, have been using PalmSecure technology for more than a decade. It was demonstrated at Mobile World Congress in Barcelona in March 2015. And Banco Bradesco, one of the largest banks in Brazil, uses PalmSecure in its ATMs. Douglas Francisco, CTO, Banco Bradesco, says: "Since the biometric system, fraud declined. Other ATMs don't show the same improvement since they don't have that system."

With biometric technology this robust and this simple to use, it's perhaps time to stop kidding ourselves that our password choices are that clever, or that we never even for an instant take our eyes off our devices. But instead of being honest about these things, we can perhaps look forward to a time when we no longer have to rely on them so heavily.

CONTACT US
choosepeopleoverpasswords.global.fujitsu.com