Orange
Cyberdefense

Manage your remote workforce securely:

Authentication and access controls

Working from home: the next standard?

The COVID-19 health crisis showed that remote working was key to business continuity. It made it clear that companies weren't on the same page to cope with the brutal, immediate upheaval induced by new and generalized operating modes.

Even if remote access solutions – once meant for restricted uses, like VPNs – are available, they are internal applications, key to companies' activities that had to be made accessible from the Internet, overnight. Likewise, many organizations hastily shifted to cloud services, such as video conferencing tools, the impact of which is obvious security-wise.

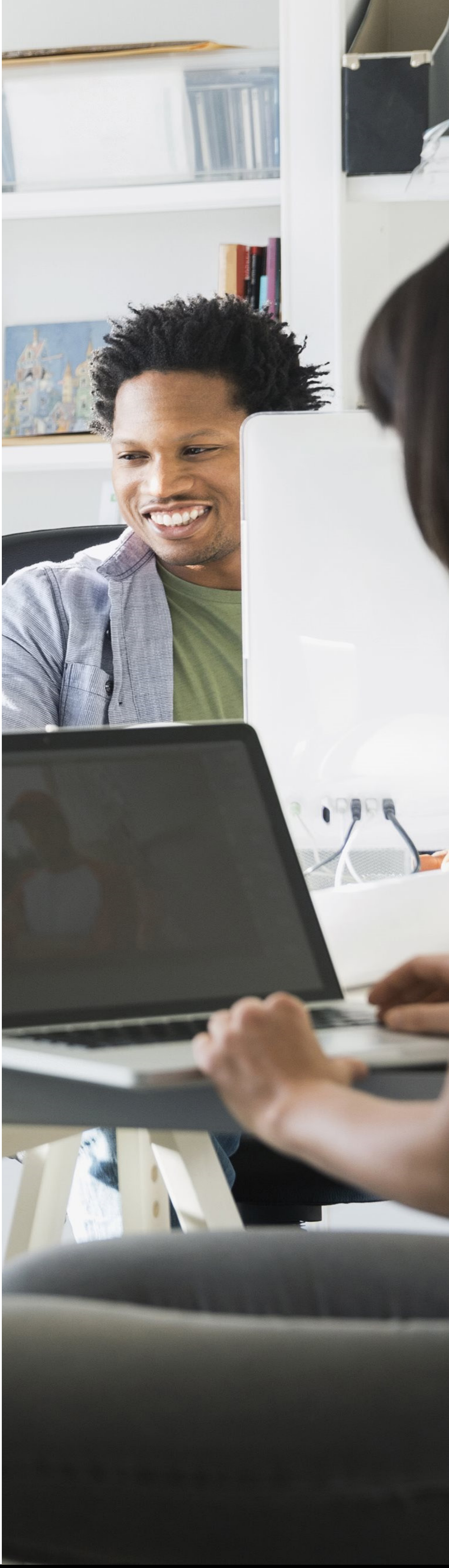
Cloud and VPN services have, indeed, been adopted massively within a brief timeframe. They bring about challenges for IT and security managers. First, a large number of businesses had no choice but urgently rush and subscribe services directly, outside of any framework; second, during the crisis, all cloud-focused industry players made their services available free of charge. Albeit commendable, this approach caused many companies to adopt sets of solutions that didn't always prove relevant to their needs and, above all things, which got out of hand. These implications fostered the concept of shadow IT.

> **Now, 40% of working people would rather be working from home.** [1]

What's next?

The post-lockdown era is the right time to inventory new use cases for shadow IT. The crisis often caused remote working to stand at the heart of strategic decisions. Besides, a number of solutions that proved worthwhile in organizations in times of crisis are likely to be maintained.

Now that the emergency is starting to wind down, they must reflect upon the impact of these use cases when it comes to corporate data exposure, and on the means that should be implemented to sustain and secure the telework environment. In this respect, access management is a key asset to bring these uses back under control.



(In)secure passwords

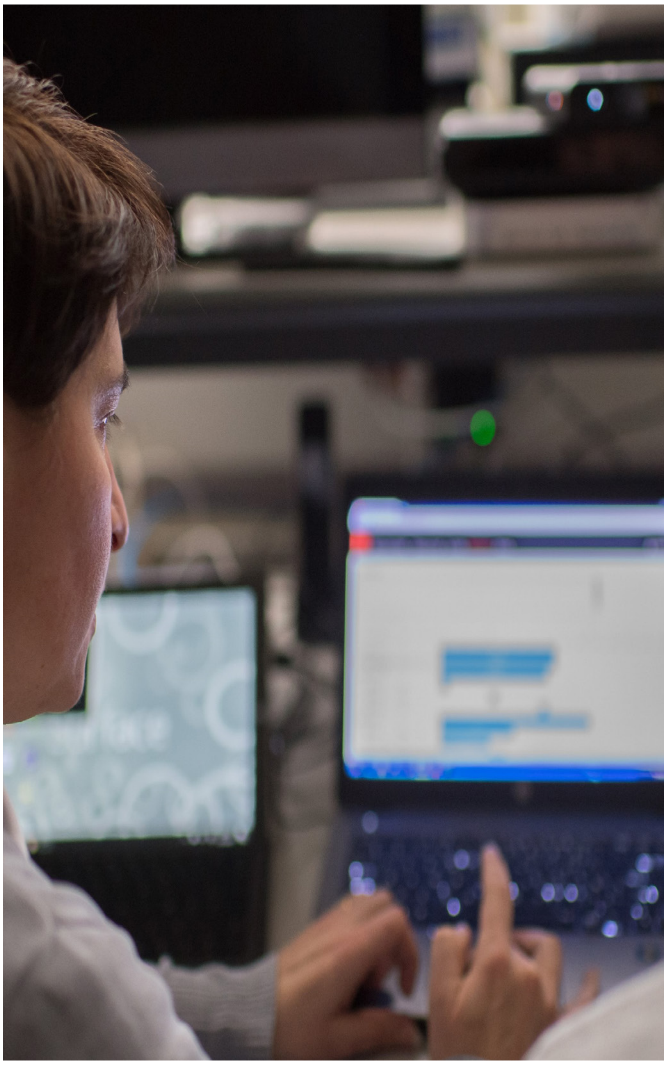
40 passwords for people to remember, on average

83% use the same password for different sites [2]

40% of data leaks relate to fraudulent password use [3]

Passwords are often viewed as the basic level in a security policy. Coupled with an identifier, they allow access to applications in the information system, or in the cloud.

Passwords have been around since the birth of information technology, and they remain the most widely used solution seeing how easy they are to implement. However, even if these tools have proven their worth, they are no longer enough. As the number of passwords to be remembered increases, as well as their complexity (required by companies), users began seeing them as a constraint. Most of them even use the same password for several sites. This bad practice exacerbates the risks of both ID thefts and data leaks.



An expensive and risk-inducing way to connect

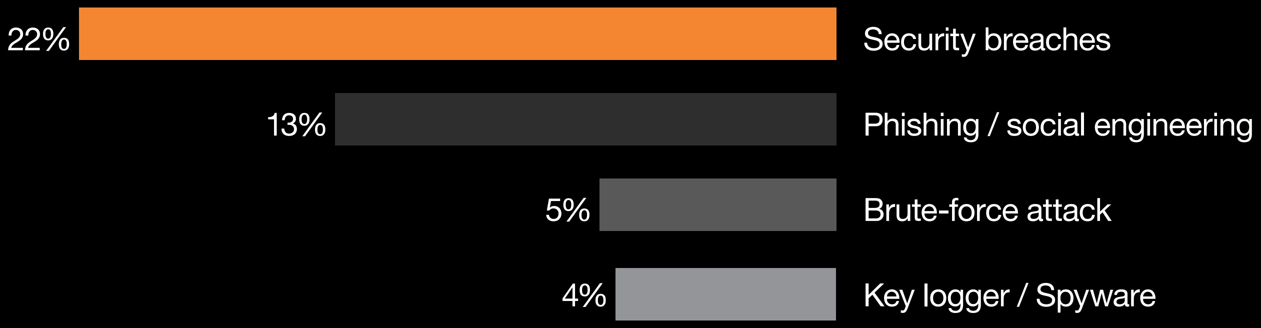
20–50%

of support calls regard password resets [5].

€60

Average cost of a support call

Attacks targeting passwords: [4]

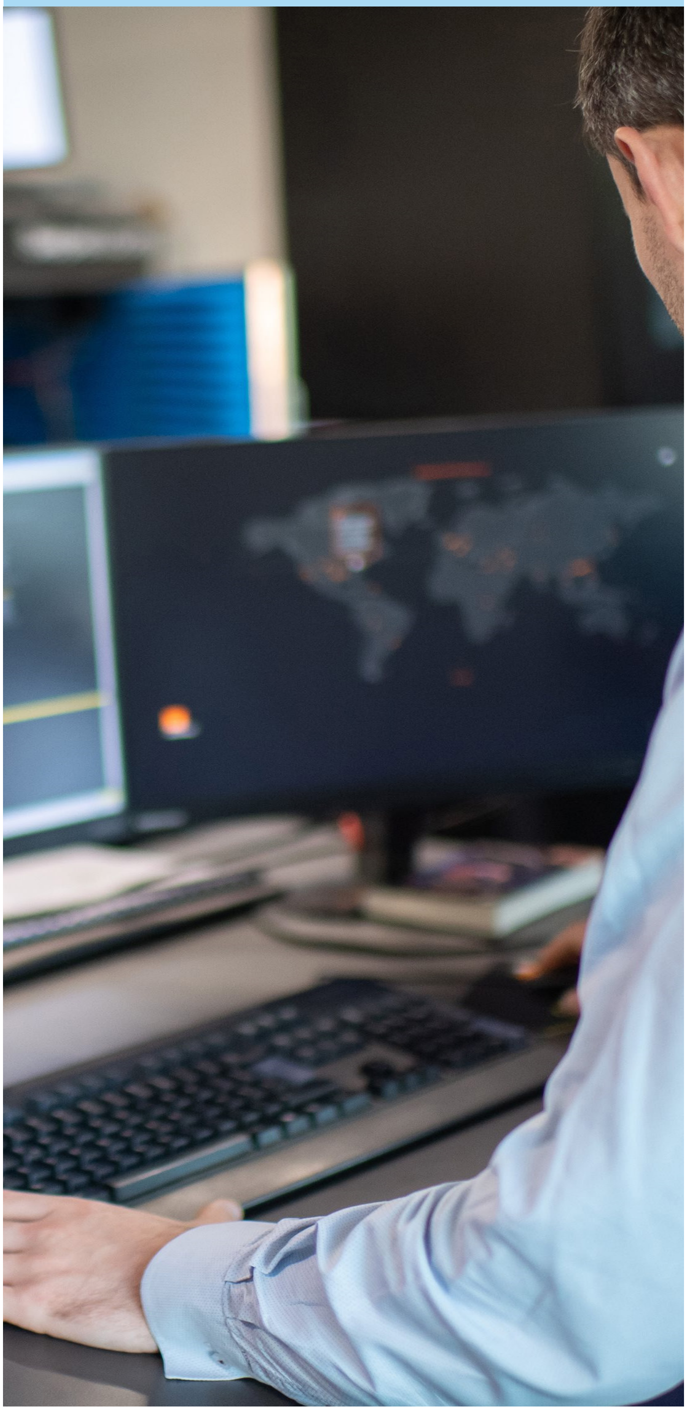


Strong authentication: a keystone in digital trust

Today's massive adoption of Cloud services and the explosion of VPN access for remote working, call for reconsidering how users access their services. The growing consumption of data from mobile devices introduces another issue. Different authentication contexts emerge with different risks. For example, connecting from a personal mobile device to a Wi-Fi network in a railway station won't allow for the same control level as logging on from a professional workstation connected to the corporate network from a remote location. Therefore, authentication mechanisms have to be adapted to simplify connection processes when acceptable from a security standpoint, while strengthening accesses where necessary.

Regarding access reinforcement, strong authentication obviously guarantees the user's identity. This identity is certified through combining several authentication factors. It is deemed that nearly 99% of fraudulent access attempts can be avoided by using strong authentication [6].

> **45% of organizations already experienced at least one compromised cloud account** [7]



Avoiding the trap of identity silos?

Not so long ago, identity management was limited to the corporate perimeter, with known users and mastered applications. The reliance on VPNs was a first approach and still widely applies. However, with cloud adoption, today's users get access to SaaS applications directly, without going through the corporate network. The risk would be to create a multitude of identity silos that might become entry points for attackers. The paradigm shift brought about by the Increasing number of applications outside the corporate perimeter leads to an overhaul of the security perimeter: it is being extended way beyond traditional boundaries.

However, most in place identity management systems aren't designed to address these new uses. Therefore, there are two approaches to managing identities: on the one hand, managing identities directly from the cloud application and, on the other hand, using a synchronization agent. While the first approach presents operational limitations, the second only solves part of the issue. Beyond the benefits of identity synchronization, each cloud application imposes its own authentication methods. This results in a very heterogeneous user experience, and could ultimately be detrimental to security. Identity federation then appears as a much more efficient solution to meet corporate needs.

Identity federation:
simplifying access controls

When a company subscribes a cloud service, it stays liable for the security of their facility, including user management. With the concept of identity federation, the company is responsible for the authentication process.

In other words, the cloud application no longer manages passwords: someone else is entrusted with their management. The point is to apply a single, unified access policy to all federated applications, to ensuring better access control and security. For the user, identity federation is a means to simplify and streamline accesses, based on Single-Sign-On (SSO): a single connection process for access to all their cloud-based apps.

Ending password: the next step?

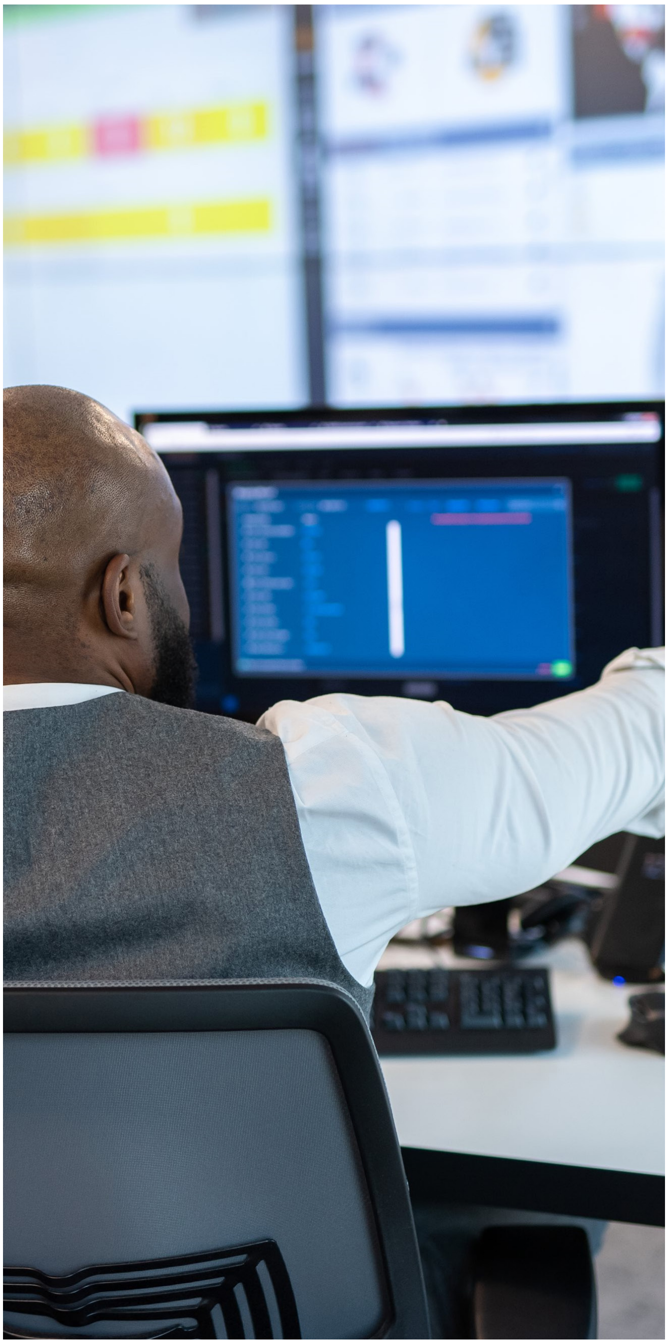
Identity federation simplifies user experience, but the primary authentication step sometimes remains complex, hence the following question: why not just give up passwords or any other form of complex connection mechanism that repels users? This question is of even more interest seeing that two in five helpdesk requests are regarding passwords, and incur substantial costs for the company.

Putting an end to passwords, or the notion of "passwordless" authentication, may seem to contradict security concepts. However, today's technological advances offer modern solutions that drastically reduce user friction, while offering the highest security guarantees. Concepts such as Zero Trust allow for the establishment of specific models, where all elements that make up a connection are viewed globally, and systematically verified.

A user connection can then be considered within an authentication context. By verifying the terminal, IP address, the target app and other control points, the method used to provide access can be adapted in a transparent manner. This is referred to as contextual authentication and smart sessions (or "Smart SSO"), with the ability to add granularity to app access based on their criticality and the connection environment.

These solutions not only meet an ever-increasing user demand for seamless authentication, but they also meet IT and security managers' expectations given the ease with which apps can be added, their centralized administration and unified access security management.

The benefits of “smart” identity federation



Standardizing and Simplifying Accesses

Access management solutions heavily contribute to simplifying employees’ daily tasks. Different passwords used to be required, with varying degrees of complexity and different resetting frequencies, but users can now rely on a single access. They may browse through their cloud apps or applications hosted on the corporate network enjoying the same user experience.

Enhancing Traceability and Access Control

Another advantage: all application accesses can be traced to better comply with corporate policies or regulatory requirements. The users’ access control security level is homogenized, and companies enjoy guarantees as to the conditions in which corporate were accessed. Uses are under control for the sake of sustaining their activity.

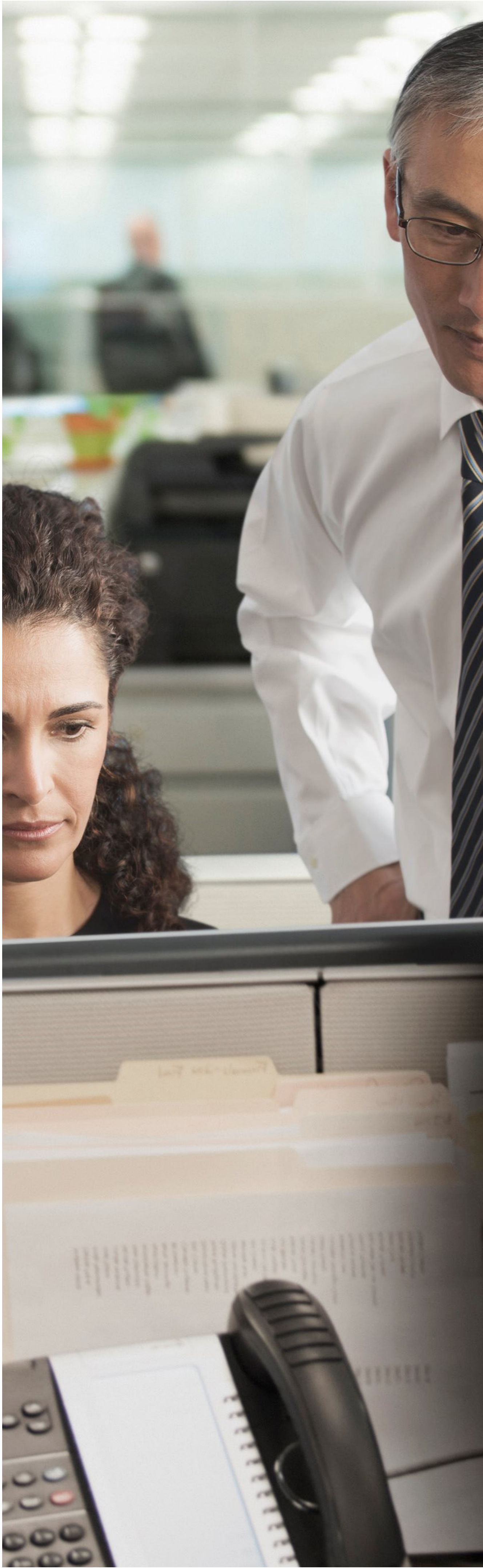
Applying Access Controls to Match Users’ Needs

Smart session management consists in understanding users’ authentication contexts and applying the relevant level of control. Depending on the environment and security policy, active (requiring user interaction) or passive (running a number of automated tests that are transparent to the user) login information let access control strategies be fine-tuned to match environmental needs and security policies in the best possible manner.

Speeding Up Cloud Transformation Plans

The cloud stands at the heart of business transformation plans. These projects require high agility levels and speed when it comes to adopting new services and applications. The ability to integrate these new uses fast, while offering the ease of use that an identity federation solution brings, is an asset and a productivity booster for businesses. Fewer questions when logging in, means more time for key activities!

5 key points when implementing an access management solution



1. Effectiveness and Deployment

A flexible and scalable solution to facilitate rapid implementation: when evaluating your solution, we recommend that you check how many on-site components will need to be installed, how many servers will be required, and how much effort will be required to manage them. In general, SaaS solutions adjust better to unexpected use-related peaks.

2. Automation

In times of crisis, fast enlistment is required and help-desk calls must be kept to a minimum. An automated, one-click enrollment and installation service lets your organization enable users to self-enroll. IT teams would then avoid heavy and time-consuming manual deployments.

3. Flexible Authentication Mechanisms

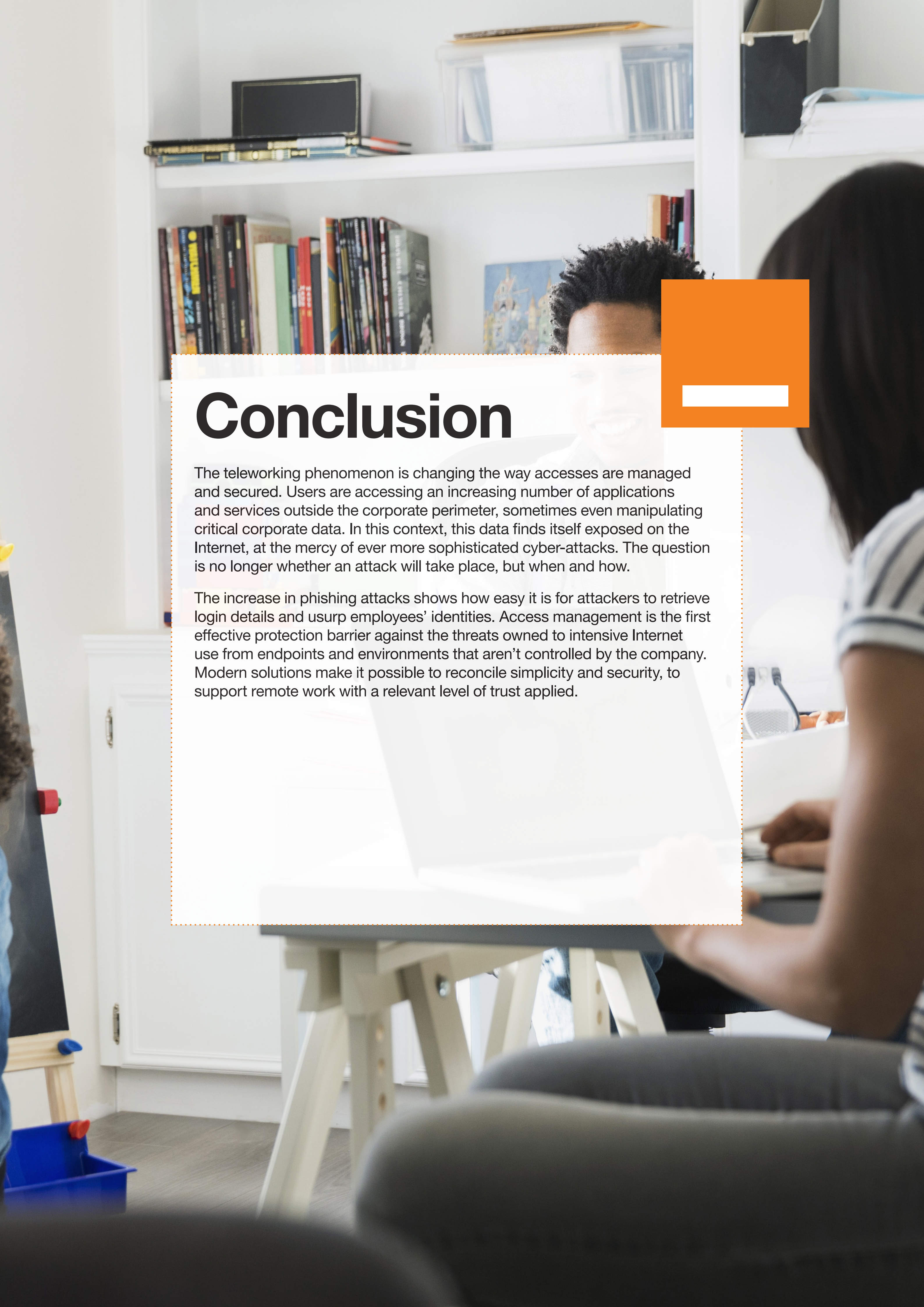
Software-based authentication methods are ideal for teleworking employees. When combined with automated and simplified enrollment, your users benefit from a seamless login experience. To support the needs of all users, choose a solution that offers a wide range of authentication methods, able to accommodate different needs and security levels.

4. Support for Hybrid Environments

Does the cloud access management service support the applications your company uses regularly? When working from home, you may need access to Salesforce, Dropbox, Confluence, or other services. Consider implementing an access management service able to handle several applications simultaneously on the same platform, and secure your VPN. This way, you may protect all applications with a single, more convenient solution, based on a single connection.

5. Smart SSO for Optimal Security

To offer the most flexible experience possible, without sacrificing security, companies may rely on SSO in the cloud, combined with contextual information and enhanced authentication. This allows users to access all their cloud-based apps with a single identity. You must, therefore, find a solution that offers enhanced conditional access, based on access policies, and avoid solutions that allow generalized SSO access to all apps with the same usernames.



Conclusion

The teleworking phenomenon is changing the way accesses are managed and secured. Users are accessing an increasing number of applications and services outside the corporate perimeter, sometimes even manipulating critical corporate data. In this context, this data finds itself exposed on the Internet, at the mercy of ever more sophisticated cyber-attacks. The question is no longer whether an attack will take place, but when and how.

The increase in phishing attacks shows how easy it is for attackers to retrieve login details and usurp employees' identities. Access management is the first effective protection barrier against the threats owned to intensive Internet use from endpoints and environments that aren't controlled by the company. Modern solutions make it possible to reconcile simplicity and security, to support remote work with a relevant level of trust applied.

Glossary

IDaaS: Identity-as-a-Service, Cloud equivalent of IAM platforms (Identity and Access Management)

Passwordless: authentication method that doesn’t involve a password, where the user connects to a computer system without entering (and memorizing) a password

SaaS: Software-as-a-Service

SSO: Single Sign-On (SSO), single sign-on authentication technology enabling connection to multiple services with just one identifier

VPN: remote access to the corporate network using a secure gateway

Zero Trust: security concept based on the belief that organizations should not trust any of the users or devices that access network data and systems until their legitimacy has been verified

Notes

[1] Les Echos, May 2020

[2] Cycloide Report, 2018.

[3] Verizon Data Breach Investigations Report, 2018

[4] Gartner 2019

[5] Seasoned Cyber Security Professionals (SCSP) 2019

[6] Google, 2019

[7] Proofpoint Report 2019

Orange
Cyberdefense

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 18 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

www.orangecyberdefense.com
Twitter: @OrangeCyberDef