Zero Trust

– Don’t trust anyone or anything

Checklist: Do you cover all aspects?

nexusgroup.com

nexus INGROUPE

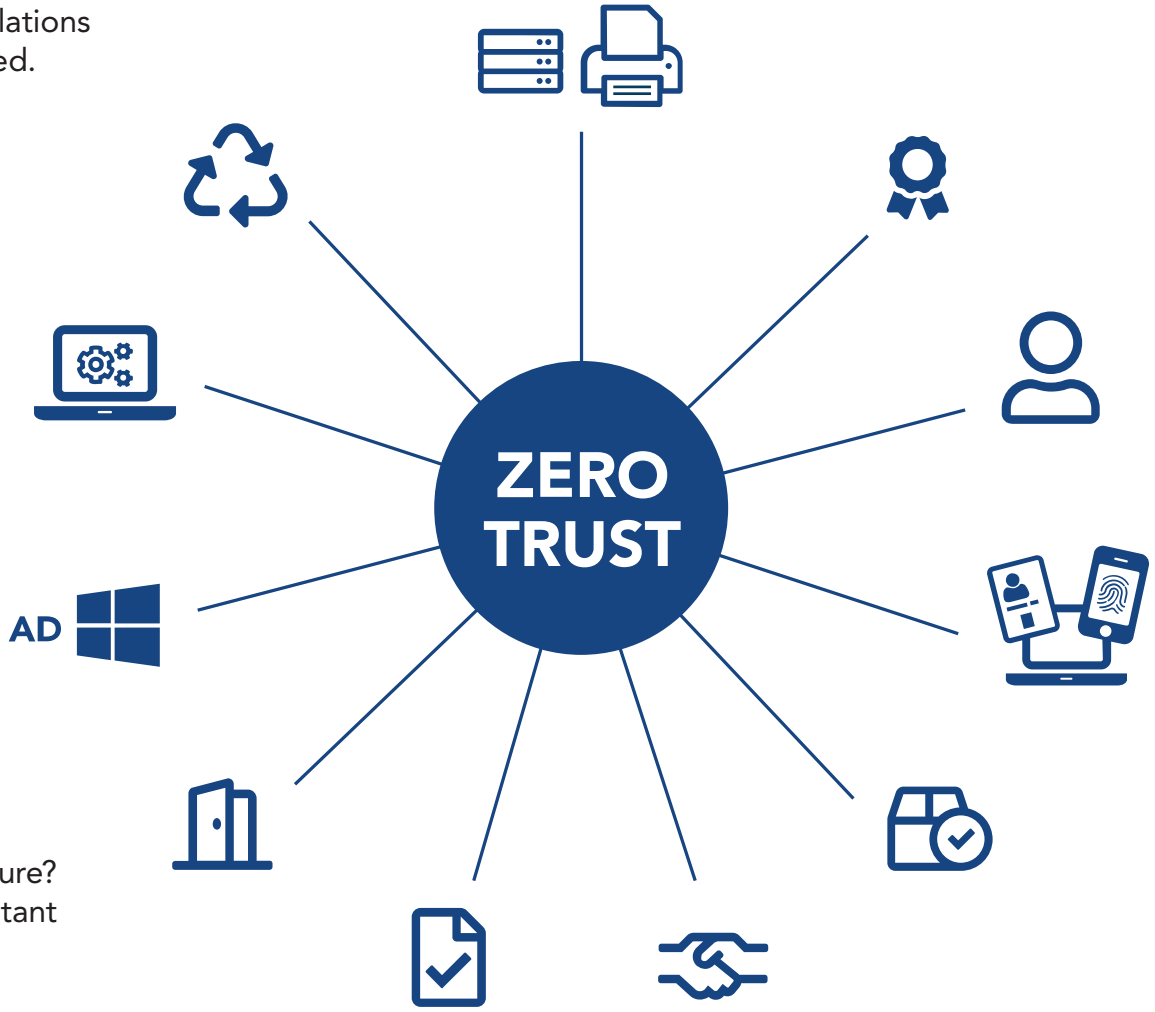
Enforce zero trust with trusted identities for people and things

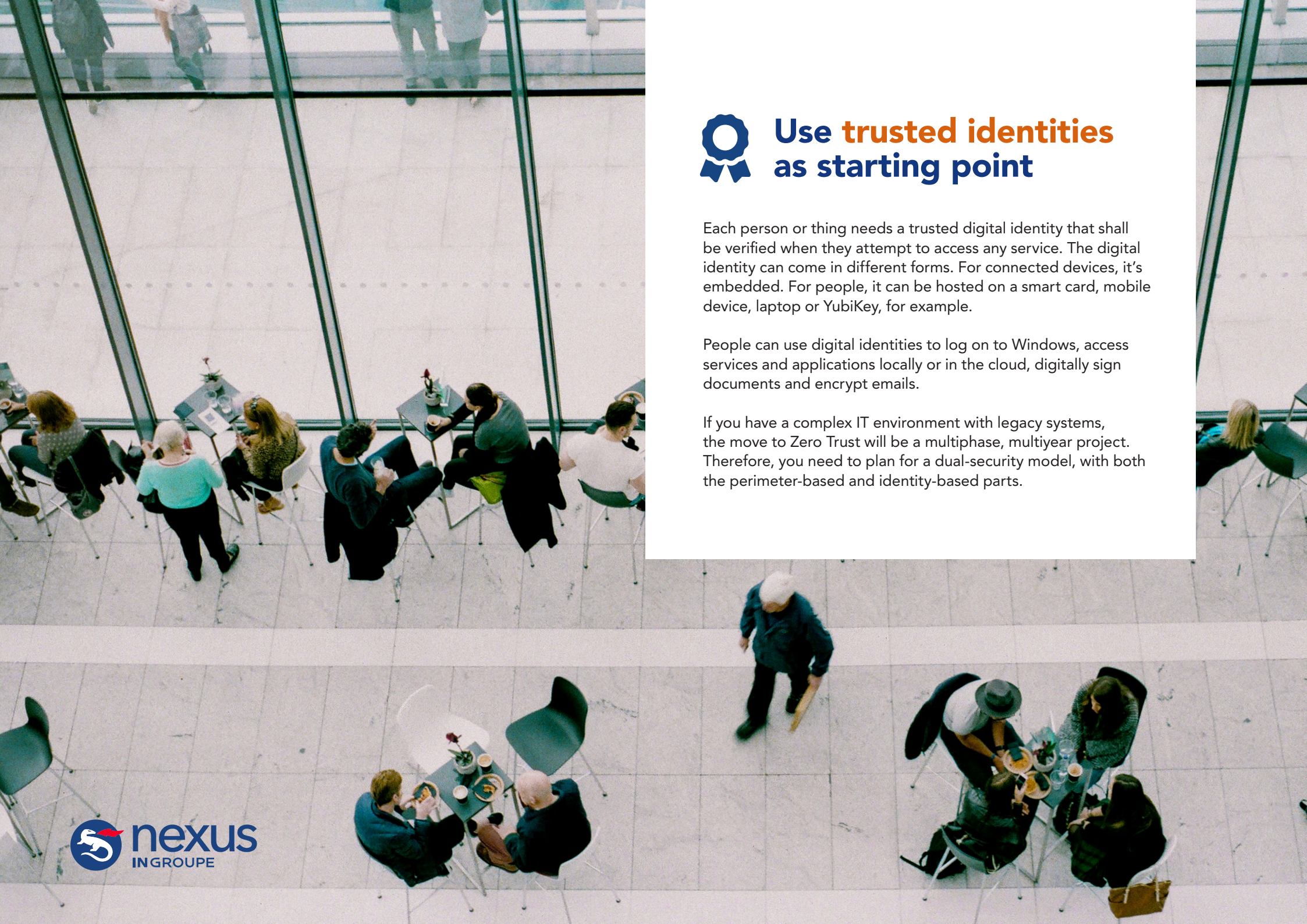
As many organizations today replace on-premises installations with cloud services, a new approach to security is needed. Instead of the conventional perimeter-based security model, a more dynamic and active security architecture is needed to protect the new hybrid environment with applications and data both in- and outside of the traditional firewall.

With a zero-trust or identity-based security approach, you apply security mechanisms based on the identity of the user.

"Most experts agree that it's imperative you don't trust anyone or anything before verifying their identity. Make sure to always authenticate and authorize every user, device, and network flow before you grant them access to any digital resources. Passwords are no longer sufficient; every user or device needs a digital identity that can be trusted," says Magnus Malmström, CEO of identity company Nexus Group.

So, how do you create and enforce a Zero Trust architecture? Use this checklist to make sure you cover the most important aspects to achieve a successful security solution for your organization.





Use trusted identities as starting point

Each person or thing needs a trusted digital identity that shall be verified when they attempt to access any service. The digital identity can come in different forms. For connected devices, it's embedded. For people, it can be hosted on a smart card, mobile device, laptop or YubiKey, for example.

People can use digital identities to log on to Windows, access services and applications locally or in the cloud, digitally sign documents and encrypt emails.

If you have a complex IT environment with legacy systems, the move to Zero Trust will be a multiphase, multiyear project. Therefore, you need to plan for a dual-security model, with both the perimeter-based and identity-based parts.

nexus INGROUPE

Do an inventory of your identity management – Are you in control?

To get in control of your organization's security, the first thing you must do is to analyze the current state of the identity management. Enterprises often have several legacy systems for identity and access management (IAM) and mobile device management (MDM). They also usually have many locations and rely on outsourcing to various degrees.

To find the gaps in your current IAM environment, evaluate its maturity, and incorporate the findings into your security strategy, you can use the Forrester Identity Management Maturity Model. The model defines five maturity levels, ranging from non-existent identity management (level 1) to optimized identity management (level 5).

"Our experience at Nexus is that many enterprises are on level 2, which means that the identity management process is intuitive and undocumented. On level 2, the process usually looks like this: when a new employee joins the organization, they meet with an IT admin who sets up their email and other applications. The IT admin knows exactly what needs to be done, without following any formalized process," says Malmström.

Make sure to consolidate and choose systems that can easily integrate. For example, in a Microsoft environment, the cloud-based identity and access management service Azure AD, can be used for multiple purposes in communication with related services.

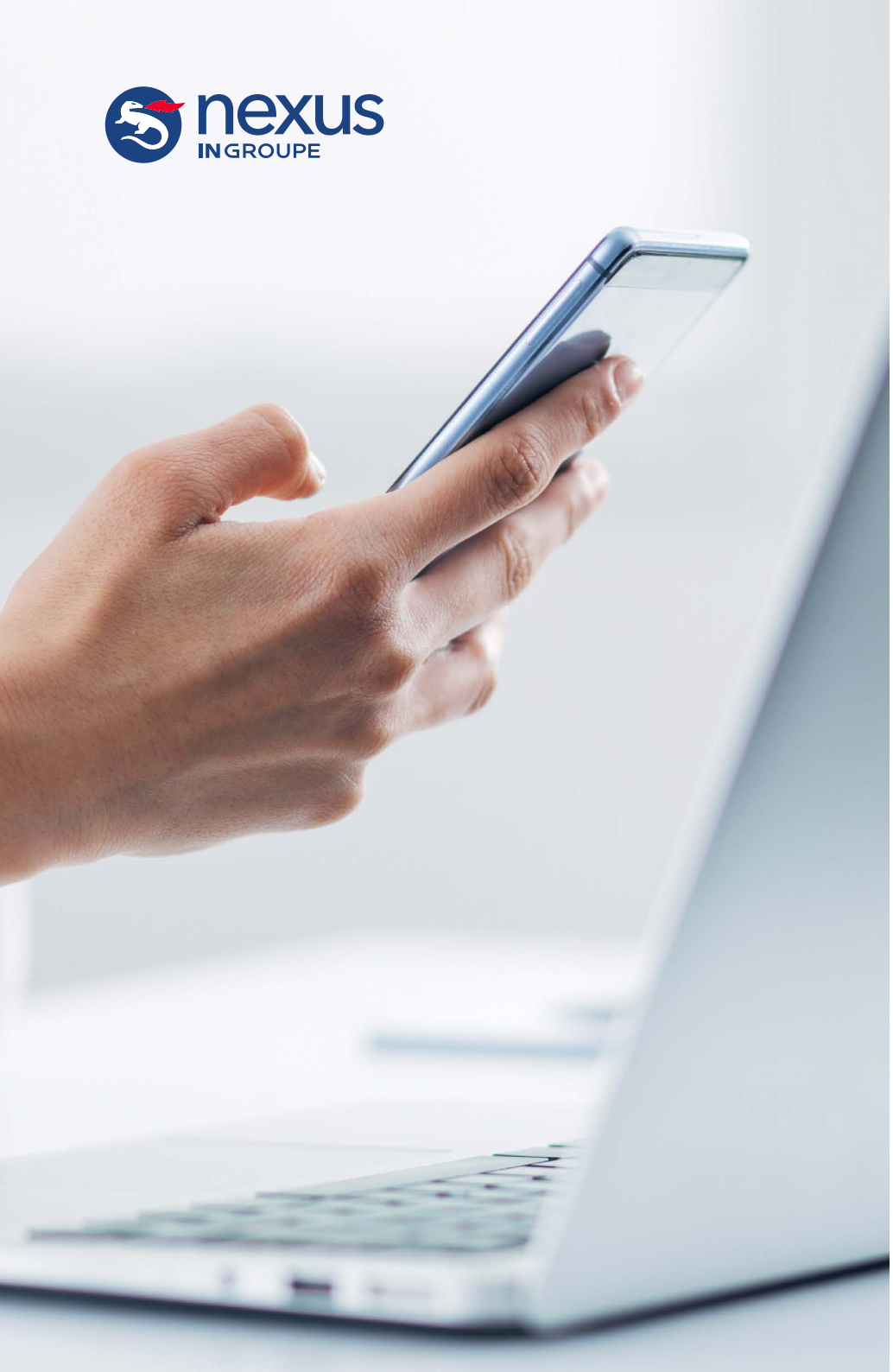
Consider the people – Company security is only as good as people's behavior

Usability is a key issue for security. If it is not easy for employees to follow your policies, they are not going to do it. Good usability also means fewer helpdesk issues, and therefore more time for other tasks. Simplifying for your users will pay off.

Here are some examples of how to ensure security and usability:

- Use the same secure login method for all purposes, instead of forcing them to remember multiple insecure passwords.
- Allow for single sign-on to all systems.
- Let your users log in with their mobile phones, instead of having to carry around an additional hardware token.

All employees need to be aware and work in line with the security policies. Company security is never better than people's behavior. So how can you get all employees onboard? As discussed already, enforcing policies with easy-to-use tools is one way. You also need to keep reminding employees of what they can contribute to security. Accessible and comprehensible documentation, for example a security checklist, can be of help.



Provide smooth and secure credentials to your users

If you haven't replaced passwords yet, it is time to do so! As most of us know today, passwords aren't secure enough and a hassle to remember.

With two-factor authentication (2FA), you make it much harder for the attackers. When choosing 2FA methods, consider the required level of security for your different applications and the convenience for your users. Methods need to be flexible to support the mobile workforce accessing resources from different parts of the world. If possible, use devices that users already have, such as smartphones or laptops, to avoid extra hardware costs.

At least one backup method is needed, to not risk users being locked out of systems, if they would lose their phone or smart card.

Some choose to use the smart card as the root of trust but allow controlled derivation to a strong digital identity that allow greater user convenience, and support smart phones, tablets and laptops. At this point you have laid the foundation for always verifying the digital identity against all resources.

Here are some recommended 2FA methods:

- Mobile Virtual Smart Card
- Virtual Smart Card
- Smart Card
- One-time passwords
- Hardware tokens
- External Identities

AD

Set up conditional access rules

For today's mobile workforce that can access resources from anywhere at any time, it is no longer enough to check if a user is inside or outside the corporate network. Rather, security depends on multiple factors such as user roles, group belongings in the corporate directory, IP addresses, geographic location, network, and so on. Therefore, these factors should be used as conditions in the access rules you set up.

Depending on who and where the user is, they can access different resources. Some security-critical resources might only be accessible from within the company network, while others have lower security requirements.

Using conditional access rules makes management much easier than managing access rights per user. When a user changes role or group in the corporate directory, new access rights can be applied immediately.

If you use federation-based access that is based on SAML (Security Assertion Markup Language) or OpenID Connect, you can support access to all kinds of resources and enable single sign-on.

nexus
INGROUPE

Integrate physical access in the security solution

Security isn't just one area, but all aspects must be covered. As an example, physical and digital security are intertwined and can't be separated from each other. For example, breaking into a building means access to computers, and thereby access to digital resources.

Make sure to integrate physical access control with identity management and digital access. Again, use automation to ensure on- and offboarding is made easy. When a new employee starts with a certain role and in a certain department, they should automatically get access to the needed facilities and office spaces.

By including physical access control in the authorization processes, you ensure full control.

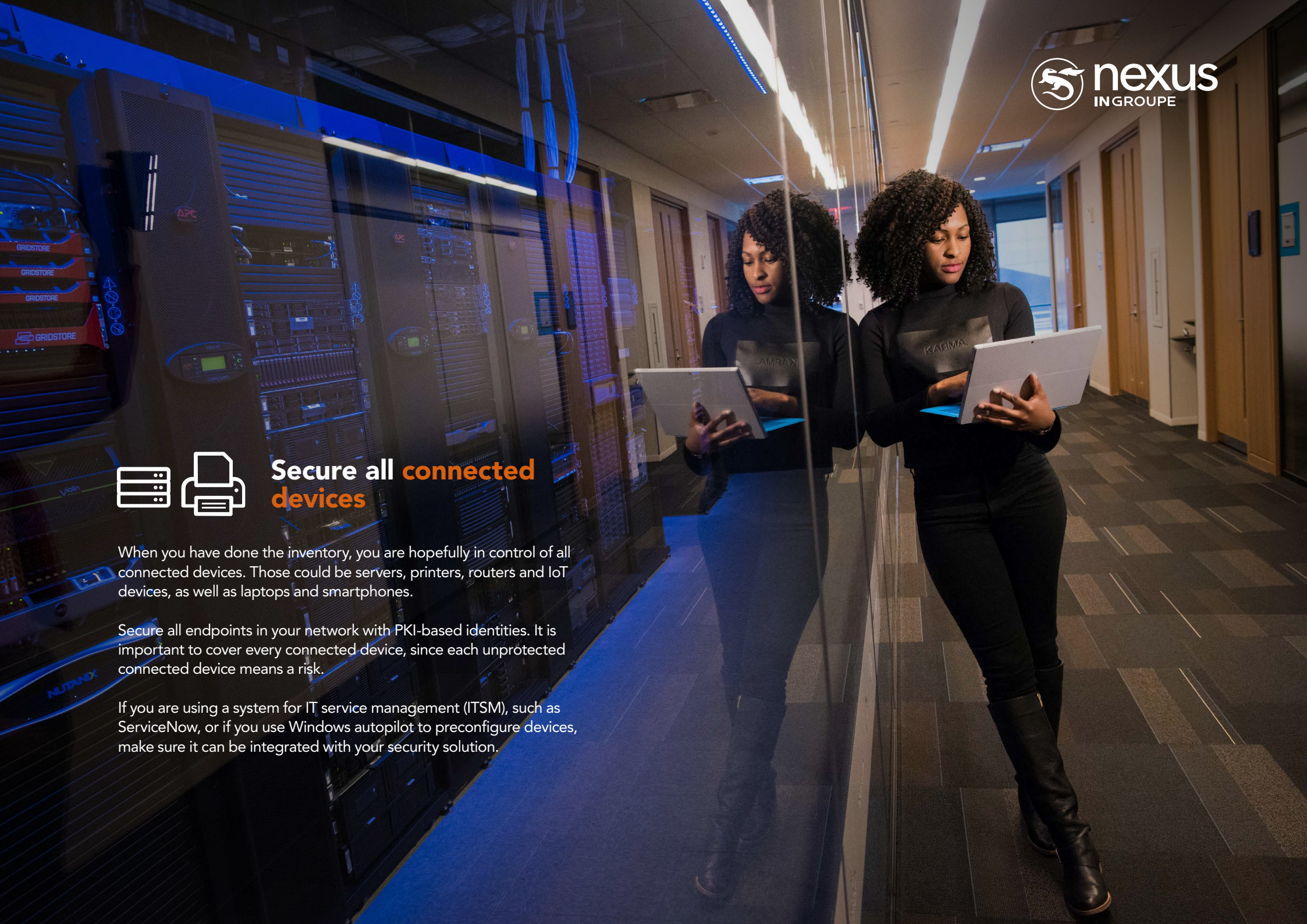
Work smarter with self-service solutions

Self-service solutions increase usability and minimize administrative work.

By using self-service tools, you can delegate some tasks to the employees, such as reporting a lost access card or getting a new card PIN.

Self-service solutions let your users be in charge. They can change their PIN or order a mobile identity whenever they want to and without being dependent on an administrator to help them.

nexus INGROUPE



Secure all connected devices

When you have done the inventory, you are hopefully in control of all connected devices. Those could be servers, printers, routers and IoT devices, as well as laptops and smartphones.

Secure all endpoints in your network with PKI-based identities. It is important to cover every connected device, since each unprotected connected device means a risk.

If you are using a system for IT service management (ITSM), such as ServiceNow, or if you use Windows autopilot to preconfigure devices, make sure it can be integrated with your security solution.

Automate as much as possible

Manual processes are both costly and insecure and opens up for human error. Automation helps bringing down costs and simplifying work, for example with lifecycle management of identities and credentials.

With automation, you keep manual work and helpdesk issues to a minimum, and gain time to move from IT maintenance to IT development.

Specifically, consider automated processes to manage identities for devices. You don't want to risk having services go down, due to forgotten renewal of certificates.

A good advice is to explore the automatic certificate management environment (ACME) protocol as the communications protocol for automating certificate management to web server endpoints, allowing automated deployment of public key infrastructure at very low cost. There are several open source ACME clients available like acme.sh, WinCertes, dehydrated, Certbot.

nexus INGROUPE

Security by design – Enforce your company policies

If you want your users to work securely, make them do so. Build in the security measures into your organization's services and processes. This must be done with usability in mind, so that it is not a hinder to your employees.

Consider the policies you have in the following areas:

- Physical security: access control, secure areas
- Information security: classification of information, incident handling, cryptography
- Behavior and culture: employees need to be aware of how they can contribute

Attempt to enforce the policies into your company processes, for example on-and offboarding of employees and contractors, physical and digital access rules and lifecycle management of identities.

nexus INGROUPE

Team up to make it happen

The IT department shouldn't manage the Zero Trust security transformation alone – the HR department has the potential to play a key role, being the first to say hello and the last to say goodbye to employees and contractors.

"This means that your HR system is the natural start and end point of your IAM process for people. A single click in the HR system can grant the right access at the right time to the right person – and one click can take away all access rights to all your digital and physical resources. One click in, and one click out," says Malmström.

Other parts of the organization need to be involved, for example, facility managers that manage buildings and access. It is important that the management stands behind the security investments and allocate a reasonable budget.

The basis of the Zero Trust model is to create a trusted digital identity for each person and thing your organization interacts with.

"Partnering with an identity company such as Nexus lets you do this. It also lets you create a self-service driven and audit-friendly process that protects all your resources with multi-factor authentication," says Malmström.

nexus
INGROUPE

nexusgroup.com