9 Steps to securing your workplace devices

How to enable digital identities on enterprise devices

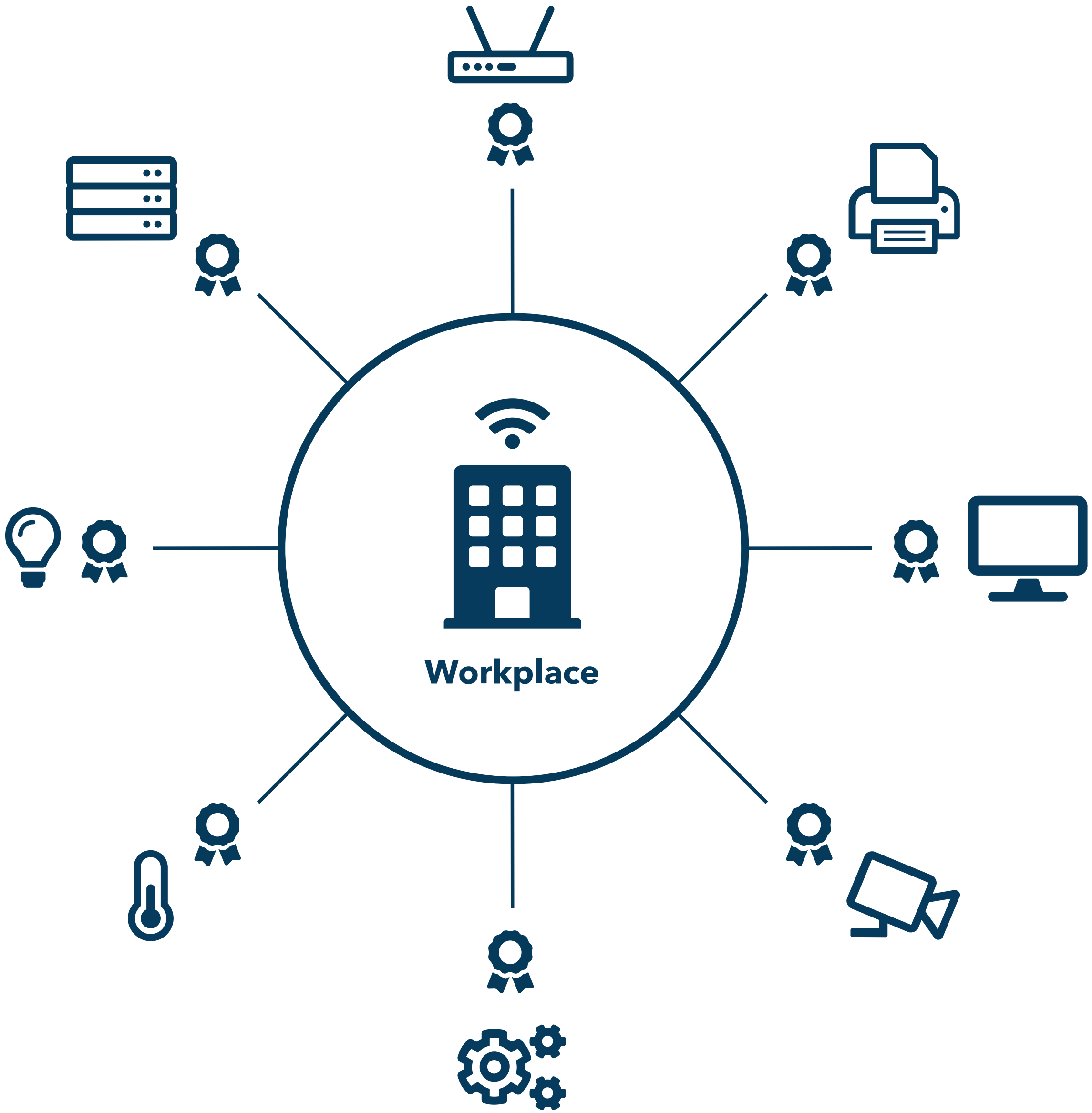
nexusgroup.com

nexus IN GROUPE

In these days of digital transformation, when most organizations need to give employees access to company applications and data from anywhere and at any time, a new approach to security is needed instead of the conventional perimeter-based model. Security mechanisms need to be applied based on trusted identities of people and things. This so called Zero Trust model helps mitigating risks such as unauthorized access, cyber espionage, theft of confidential data, disturbance in applications and denial-of-service attacks.

As part of this strategy, trusted identities must be issued to all connected workplace devices, for example mobile devices, laptops, network equipment, routers, printers, conference devices, domain controllers, web servers and internal servers.

In this guide, you will learn how to secure the workplace devices in your organization while avoiding the pitfalls, and how to set up a scalable and flexible solution that works today and in the future.



Use trusted identities to authenticate all devices

Identities that are based on public key infrastructure (PKI) enable strong authentication of people and things as well as other use cases, such as email encryption, digital signing and Windows logon.

In a Zero Trust security model, all devices are given PKI certificates to identify them in the company network. Strong authentication with the PKI certificates is enforced for the device to communicate with any other devices or applications or get access to data over the network.

This approach provides complete end-to-end security covering all domain and non-domain endpoints.

nexus
INGROUPE

Do an inventory of devices

To start the transition into a Zero Trust strategy for your workplace devices, an inventory is needed, to check if your current devices support PKI, what certificate enrollment protocols they support, and who are owners and administrators of the different devices.

Considering that this is a long-term strategy that is not implemented in a day, you will need to set a priority order. Which devices are prioritized to get PKI certificates?

Now is also the time to decide what you want for the future. Can you reduce the spectrum of devices, to make them easier to administrate? What requirements do you want to put on future devices that you invest in?

For sure, any devices you buy must support PKI. Support for simple certificate enrollment protocol (SCEP) or automated certificate management environment (ACME) is also recommended to help you automate managing the PKI certificates.

nexus INGROUPE

Enable a single point of management

The IT infrastructure in a typical organization is a heterogeneous landscape. Due to company merges and multiple locations and departments, several different systems might be available for managing devices and PKI certificates.

By enabling a single point of management, you can simplify the administration and minimize the manual work and risk of errors. This is important, considering that the number of connected devices will only keep increasing.

A central PKI provides high assurance certificates for connected devices and - via a wide range of integration capabilities - link their issuing, renewal and revocation to the asset management of the IT. With one central system, it is much easier to ensure compliance to security policies and manage the complete lifecycle of devices and certificates.

Use a flexible PKI platform

A PKI platform must be flexible to adapt to the needs of an organization, to make sure you can consolidate the certificate management; cover multiple certificate policies, algorithms and validity periods; manage complex PKI setups, and support certificates for different bearers, such as smart cards, virtual smart cards for laptops and phones, IoT devices and code signing.

Depending on the devices and use cases, specific certificate enrollment protocols might be needed. These interfaces are typically relevant when it comes for workplace devices:

SCEP (simple certificate enrollment protocol) – supported by many existing devices to enroll and provision certificates

ACME (automated certificate management environment) – supported by more and more devices and needed to automate certificate issuing, management and revocation. A certificate management client of some kind must be available on the device

REST API (RESTful application programming interface) – needed to integrate with third party management tools, for example to issue, manage and revoke certificates

If there are already certificate authorities in place, then make sure you can either integrate with them to enable consolidated management or migrate data to one single certificate authority.

Many industries, such as banks, military, telecommunications and car industry, have strict local or international regulations they must follow. Make sure to choose a PKI solution that can support any applicable standards and regulations, for example by building them into the certificate policy.

Choose how to deploy

Depending on the use cases and needs of an organization, there may also be specific requirements on the deployment. Consider if you want the PKI platform to be hosted by a trusted PKI service provider or deployed on-premises.

If you choose to use a trust service provider to host your PKI, then there is no need for you to have PKI competence in-house. Trust service providers use hardware security modules (HSMs) to store certificate authority (CA) keys, so that you can ensure high security without having to buy your own HSMs. With PKI as a service, you also do not need to depend on your internal IT infrastructure.

Automate processes

There are many examples of when a forgotten certificate expiry has caused downtime of critical services and problems for millions of users. This has happened when certificate renewal is dependent on manual processes.

To avoid this issue, make sure to automate certificate provisioning for both domain endpoints, such as machines and servers, and non-domain endpoints, such as devops servers, mobile devices and networking devices.

Many services and devices are already equipped with certificates proving their identity in a secure way but lack the automation, for example to renew certificates when the existing ones are expiring.

By using devices that support the SCEP or ACME protocol and come with a certificate management client, you can allow automatic renewal of certificates when they expire. This helps minimize manual processes and minimize issues, which is especially important in large organizations.

Consider preregistration of devices

To prove that they belong to the company network, devices must be registered in some way before they can request certificates. Registration can take place before or after they are distributed to the organization.

Preregistration means an extra security measure and is also a way to implement segregation of duties between an asset owner and a system administrator.

If done manually, preregistration means more time and effort before a device can come into use. Consider what suits your organization and how flexible it should be.

The process of preregistration differs between use cases and protocols. For example, with ACME, preregistration can be applied by using DNS names. It is a good idea to get help from a trusted vendor on how to implement it in your environment.

Integrate with related systems

In a complex environment of multiple CAs, use cases and systems, consolidation is crucial. Ensure that the important related systems in your organization can be integrated to enable a single point of management.

Make sure you can integrate the PKI solution with your main user management system, for example your Active Directory via the LDAP protocol.

To manage devices, it might be relevant to integrate with device and IT asset management systems, such as Intune, MobileIron, AirWatch or ServiceNow, with the available interfaces. A programmer-friendly API, such as a REST API, also allows easy integration into third party IT management systems with little effort.

See the big picture

Now you know the most important steps to secure your workplace devices. But a successful Zero Trust strategy is only as good as its weakest point. Apart from securing the actual devices, ensure that device owners and administrators do not authenticate using passwords, but use strong authentication.

Make sure you can easily combine the solution for workplace devices with other security solutions for issuing trusted identities for your employees, secure access to all digital resources and self-service for common user tasks, to mention some examples.

Only when all areas are secured, you have a Zero Trust strategy in place.

nexusgroup.com