ezeep by ThinPrint®

eBook

Zero Trust – How To Securely Integrate Printers?

Contents

Introduction

Ever-increasing attacks on IT systems require a rethink. The zero-trust principle offers a hopeful security concept for additional protection. Within this structure, however, problems often arise with printers. In this eBook, you will learn how to solve these problems and how to make printing in your environment easier yet more secure.

eBook contents

- What is a zero-trust environment?
- Why should security concepts be enhanced with a zero-trust architecture?
- How do you easily integrate printers into a zero-trust environment?
- How to simplify printing processes?
- What is pull printing and how is it implemented?

Zero Trust – Trending for a Good Reason

IT systems are being attacked with increasing frequency. A result reflected in a Bitkom publication in August 2021. According to that study, 59% of companies with home-office employees have been affected by such attacks since the beginning of the pandemic. In 52% of cases, damage was caused as a result. Internal IT teams are therefore faced with the challenge of creating an even more secure environment.

Previous security concepts were largely based on VPN (Virtual Private Network). This is virtual and self-contained, but no longer offers sufficient protection in today's world since criminals easily overcome this obstacle.

These VPNs, which in theory are protected, have one big problem. As soon as someone has gained access, that person has access to all the resources behind them.

For this reason, it is necessary to supplement the existing VPN system with a more modern security concept. For example, the zero-trust concept has become increasingly popular in recent years, especially among government agencies and highly regulated organizations in the financial, medical, and judicial sectors. Recently, even U.S. President Joe Biden prompted public institutions to create such environments with his **executive order 14028**.

Image 1: The White House: Devices and users are not automatically trusted here.

What is Zero Trust?

In simple terms, zero trust is a security model that requires the user to log in not only to a network but to each individual application. This makes it possible to regularly check the rights of the person accessing the network. If an attacker manages to infiltrate the network, they will fail when attempting to access zero-trust applications. The prerequisite for this is that, when rights are assigned, each user is granted only those rights that are necessary to perform their tasks.

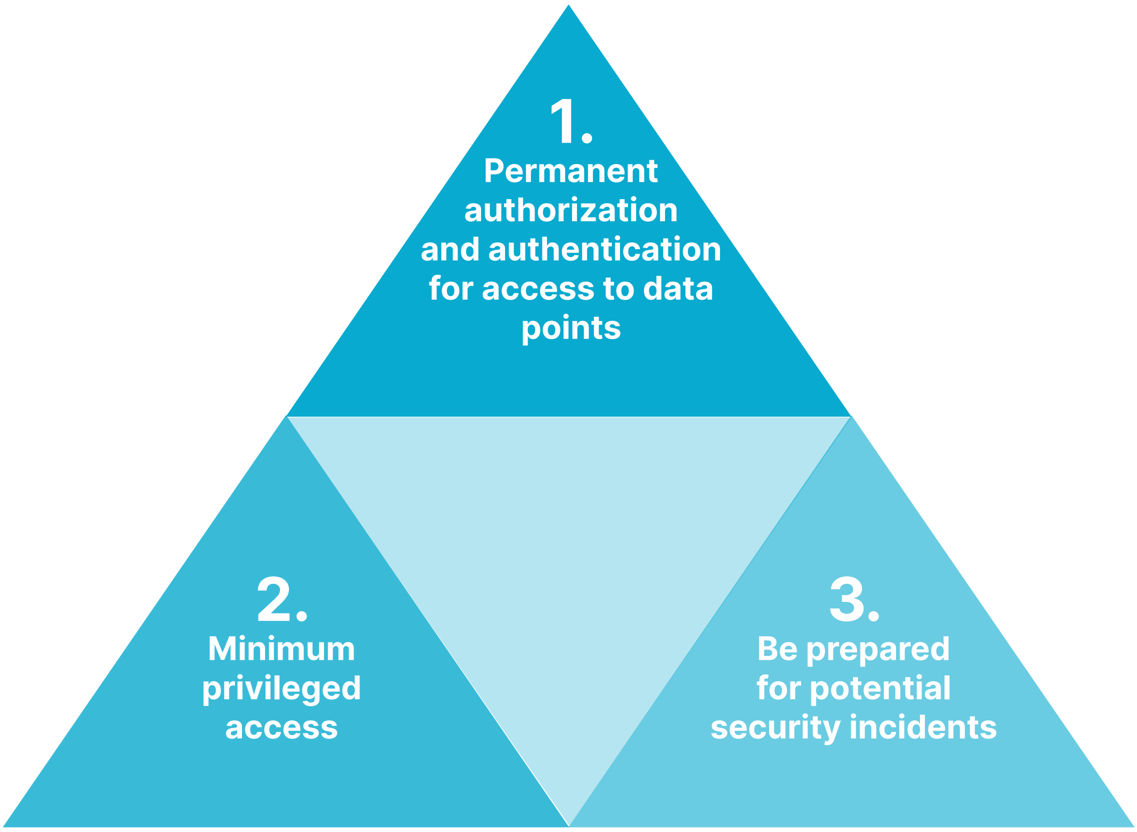
1.
Permanent authorization and authentication for access to data points
2.
Minimum privileged access
3.
Be prepared for potential security incidents

Image 2: The three cornerstones of the zero-trust concept

If you want to optimize a network using the zero-trust concept, you need to implement network segmentation. This special case is also referred to as zero-trust segmentation or micro-segmentation. In such cases, the network is subdivided so that it is possible to allow user-targeted access to network resources without making the entire network available to all users. If this security concept is used, it is important that user computers and application servers are located in separate segments of the zero-trust environment.

When it comes to home office scenarios, there is one more aspect to consider. Since no administrator should vouch for the security of private networks, it is important to strictly separate employees' local home networks from the corporate applications they use. To do so, it is advisable to use a shared VPN with a remote desktop approach. The number of scenarios in which a combination of VPN and web applications is sufficient is increasing. This means that users are free to make their own choice of end device, with Chromebooks being used, for example.

As we can see from this initial sketch, implementing zero trust does involve some effort. There is a lot to consider, and one particular aspect we will focus on in the next chapter is printers.

How Do Printers Function in Zero-Trust Environments?

People who set up a zero-trust environment can recognize printers as problems at an early stage. This is because printers can be addressed via a large number of protocols, and these are usually all activated in the delivery state. For this reason, all unnecessary print or network protocols should be deactivated immediately after switching on the device.

Printers: Obstacles in Zero-Trust Environments

Here are common problems that arise when printers are used in zero-trust environments:

1. With clear network segmentation, printers and application computers are in separate segments. This makes setting up a direct connection for printing more complex and not instantly possible.

2. It is often not possible to connect printers directly to the home network, external ports, or local interfaces because they do not have access to the zero-trust environment at secure home office workstations.

3. Due to the prohibited access to the local hard disk, it is also not possible to print from a web application without first creating a PDF.

Other zero-trust principles must be considered:

- Permanent authorization and authentication for access to printers should be ensured
- Full encryption of communication channels

How to Securely Integrate Printers into Zero-Trust Environments?

An enterprise-wide printing solution that can connect to all applications, devices, and printers without compromising the security measures put in place to protect the business and its data is what is needed. The example of the cloud printing solution ezeep Blue can be used to show how each of the above obstacles can be removed.

Connect Directly to Printers on Segmented Networks

First, a secure connection must be established between the cloud and the printer. To be able to block other incoming connections, it must be ensured that the printer is not directly addressable from the internet.

Cloud printing solutions offer connector software or hardware for this purpose. For example, ezeep Blue uses the ezeep Hub, which independently establishes the connection between the cloud and printer and is then the only point of contact for the printer.

The ezeep Hub, which is small enough to fit in your pocket, is simply connected to the same network where the printer is located. The ezeep Hub is then registered in the ezeep Admin Portal via its Mac address and automatically connects the printer to the ezeep Cloud.

Image 3: Large, expensive print servers can be eliminated with appliances like the ezeep Hub. All print data is encrypted with ezeep Blue.

Local Printing from a Secure Home Office

The ezeep Hub is also ideal for the home office, as it requires no maintenance, is small, and contributes only slightly to power consumption. Small and straightforward, it enables zero-trust printing without the need for the PC and printer to access each other.

This solution is a secure and easy way for businesses to manage the difficult home office printer scenario without having to deal with VPN settings or connecting printers via USB. Since the ezeep Hub can be configured via the cloud and only needs to be plugged into the network, IT administrators can also send it directly to anyone in a home office. Local printers can then be used without any issues. Native printing is also possible when using a remote desktop solution such as Azure Virtual Desktop. Once an ezeep account has been created in the Azure Marketplace, all that is necessary is to install an additional agent on the machine.

Printing from Web Applications

To enable web applications to print without storing files locally, ezeep Blue is equipped with an API that can trigger print jobs from the backend of the web application. Furthermore, you can simplify the usage by embedding ezeep via the ezeep.js JavaScript module.

Printing is also made easier for apps. By connecting ezeep and Zapier, automatic printing is possible in countless apps. Zaps are automated workflows. If a Zap is triggered by an event, it starts the predefined steps. If you integrate ezeep into a Zap, you can then easily print automatically from apps.

Authorized Access to Printers

To maintain the security of the zero-trust environment, it is important to allow the use of a printer only with authorized access. Cloud printing solutions that require the user to authorize themselves with the cloud printing service are recommended. Here, two-factor authentication is particularly secure. These solutions do not allow direct access to the printer at any time. One example of this is ezeep Blue. As a cloud printing solution, ezeep Blue sets up two-factor authentication via Active Directory or Google.

The Connector software/hardware also ensures that continuous authorization with OAuth 2 is guaranteed. For example, the ezeep Hub independently scans the network and enables the selection of the desired printer. This means that the printer can only be controlled by authorized persons, thus closing an often-forgotten security gap. After all, printers store and output a wide variety of documents, including those containing sensitive data. Authorized use of the printer prevents malware from spreading to the corporate network or infecting employees’ computers.

Pull Printing

To maintain the zero-trust concept even when printing, many cloud printing solutions, such as ezeep Blue, use the pull printing method. This lets the user print securely and waste-efficiently to any printer. The pull printing function is activated for the desired groups and users with a simple click in the ezeep Admin Portal.

Image 4: Various authentication methods are possible, such as NFC or card readers.

To print the selected documents, the user scans a QR code on the printer to use two-factor authentication to ensure that the documents are not removed by an unauthorized person. Thus, the secure zero-trust environment is maintained even when printers are shared. It also conserves resources such as toner and paper, because only items that are actually needed are outputted.

Another advantage of pull printing, as offered by ezeep Blue, is that a convenient "flex desk" solution can be activated instantly. This is perfect for employees who change their location frequently. Thanks to a non-printer-specific printer queue, there is no need to select a specific printer and they can go to their preferred printer whenever they are ready.

Conclusion

The zero-trust concept is indispensable in today's world. Conventional solutions often neglect printing. Cloud printing services, such as ezeep Blue, solve this problem and enable the secure use of the printer. Administrators also benefit from ezeep Blue compared to the traditional printing environment, as ezeep Blue is easier and more resource-efficient to manage. With ezeep Blue, you protect printers from attackers and unauthorized access to confidential documents. A free trial of ezeep Blue can be found **on our website**.