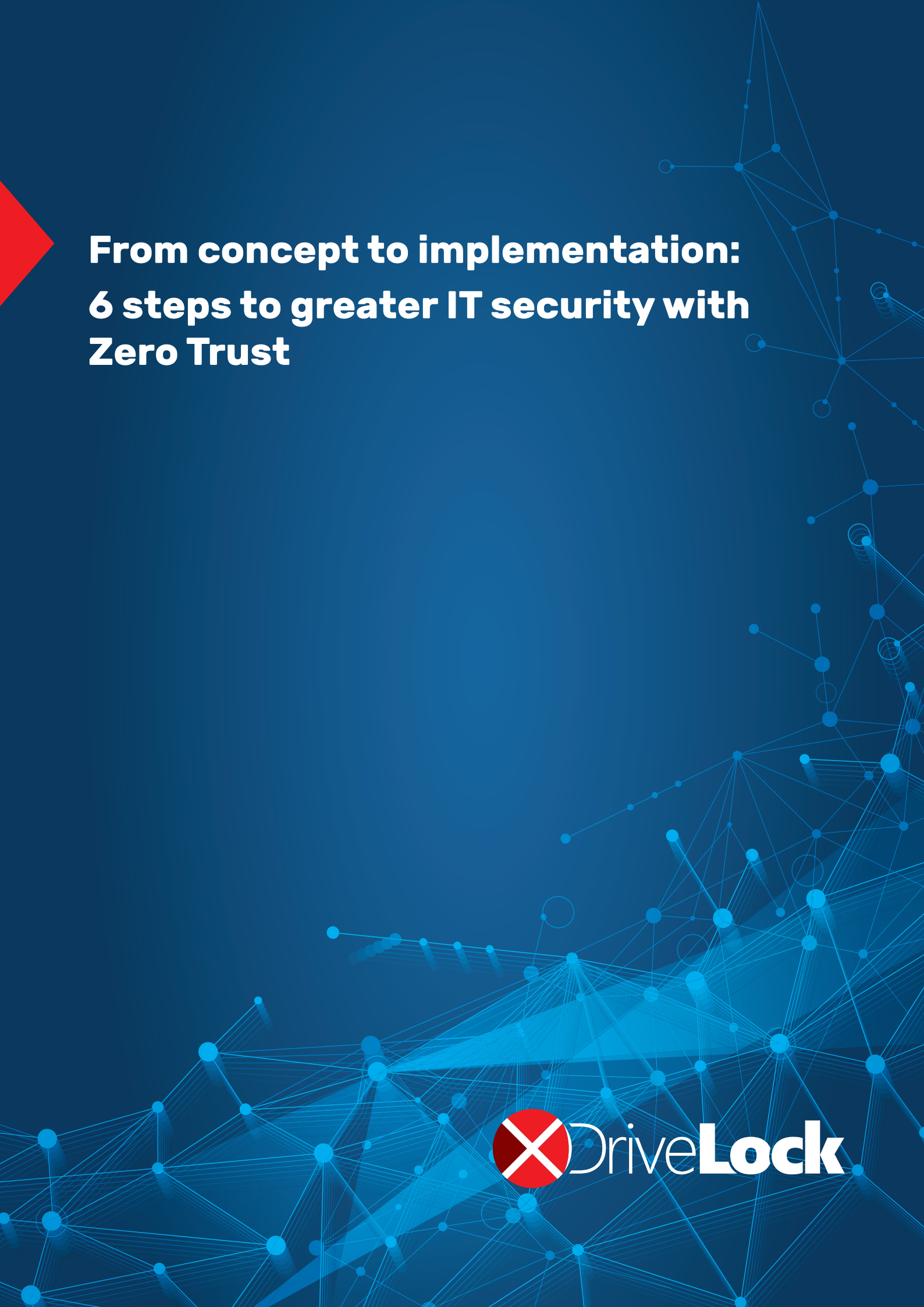
From concept to implementation: 6 steps to greater IT security with Zero Trust



Why are IT (security) experts currently engaging with the concept of “Zero Trust“?

We used to be reliant on firewalls to protect companies from threats. For IT managers, there was a clear line of defence with “inside“ and “outside” borders. In addition to ever increasingly intelligent attacks, social engineering or zero day exploits, hybrid network boundaries are also regarded as a highly complex IT security situation today.

The Zero Trust approach helps CIOs and security officers to meet these challenges effectively. The concept primarily focuses on the protection of sensitive and critical data. Zero Trust takes into account today‘s heterogeneous infrastructures with a large number of devices to be protected, and treats every access, every application, every device with the same level of care - whether it‘s internal or external. In other words: Zero Trust - as the name already indicates - doesn‘t trust anyone and relies on a constant monitoring.

What does that mean in concrete terms? With the following six steps, we will show you how to implement Zero Trust in your own organization and thus ensure a comprehensive protection of business-critical data.

Step 1

An assessment to determine the organisational framework.

Ask yourself the following questions:

- What do you aim to protect and why?
- Are the digital and physical assets hosted on dedicated servers or in the cloud? What data have you classified as public and what data is highly sensitive? Does your company allow the use of your own end devices? (BYOD)
- Do you use external data carriers (e.g. USB sticks)?
- Which touchpoints with employees, partners, suppliers or end customers are there?
- How, from where and via which media is your company network accessed?

Consider this:

Your company network doesn't just consist of desktops and laptops! Mobile devices such as cell phones, virtual environments and virtual desktop infrastructures also extend network boundaries.

TIP 1:

Company policies for security and devices play a significant role

If your company allows „Bring Your Own Device", the security risks are potentially higher. However, if only company-owned equipment is allowed to be used the employees will be more restricted.

TIP 2:

Restrictions may also apply to removable storage devices

You can deny write permissions on USB sticks or even block their use completely. But it is also possible that certain users, e.g. maintenance staff for production plants, can also be given extended rights to connect their own USB sticks and exchange data.

It is fundamental that:

The security officer in your company should know how the processes within your company are structured and which devices, applications, services and workloads are utilized and how they are used.
For a successful implementation of Zero Trust it is absolutely crucial to involve all the people concerned in the company.

Step 2

Take an inventory of your hardware and software.

In the next step, you must visualize all the data in an inventory in order to determine further security-relevant aspects and potential weaknesses. Your inventory should include all connected hardware, software and operating systems.

Questions arising from the inventory are, for example:

- Have you installed all updates and patches?
- Is there still support from the manufacturer or is the system already outdated?

Important: The importance of these points for your IT security is illustrated by the devastating consequences of the Trojan WannaCry, which prompted Microsoft to deliver a patch for the outdated Windows XP.

With a solution for the automated vulnerability and patch management, you will structure this work much easier. An overview of the Security Posture, i.e. the status and current settings of all endpoints, then introduce the next steps.

Step 3

Prevention: These tools should be known to you.

There are many measures in place to eliminate cyber threats and ensure data integrity. Institutions such as the Federal Office for Information Security (BSI) or the Center of Information Security provide the appropriate and comprehensive guidelines.
From our perspective, the following tools should be a decisive factor in your prevention measures.

TIP 1:

Hard disk, file & folder encryption

Always encrypt hard drives and files, whether they are located on mobile storage devices, local servers or in the cloud. Guidelines for data encryption on removable storage devices help protect against loss, theft, and industrial espionage.

TIP 2:

Actively utilize Device Control

Data carrier and data flow control are extremely important, because USB sticks are still a commonly used gateway for malware and data theft. Guidelines must clarify who is allowed to do what with which devices and data carriers.

TIP 3:

Application Control with Whitelisting

Only allow the execution of familiar and permitted applications that are on the „whitelist“. This ensures the best possible protection against zero-day exploits, i.e. unknown or unpatched security vulnerabilities and new malware.

Supplementary information:

www.av-test.org for example, registers 350,000 new malware programs per day. A security network that supplements firewalls and antivirus programs is therefore essential. Thanks to Application Control, malicious software that still makes it into the system will not be executed. In addition, you should not assign local administration rights so that applications cannot be downloaded and installed without verification.

TIP 4:

Identity & Access Management

Access control is another critical security measure, especially where weak passwords are used. With the help of a 2-factor or multi-factor authentication, for example, you can protect yourself from the consequences of social engineering. Despite having captured login data, attackers won‘t be able to gain access to your data and systems.

Step 4

Detection & Response - Detection is the first step to increased IT security

TIP 1:

Detection tools

So-called detection tools are able to recognize certain actions, patterns or applications and put them into context. Through this, they are able to detect anomalies and potentially dangerous behavioural patterns. For example, if a disproportionate number of files are copied to a removable disk, this could indicate industrial espionage.

TIP 2:

File Reputation Services

These will, for example, help you to implement the right response measures for unknown applications, and to blacklist an application. These lists collect all the information about applications and make it publicly available, because not everything unknown fundamentally has to be dangerous. If necessary, devices can be switched off, disconnected from the network or quarantined, and processes can be aborted.

TIP 3:

Analysis and forensics

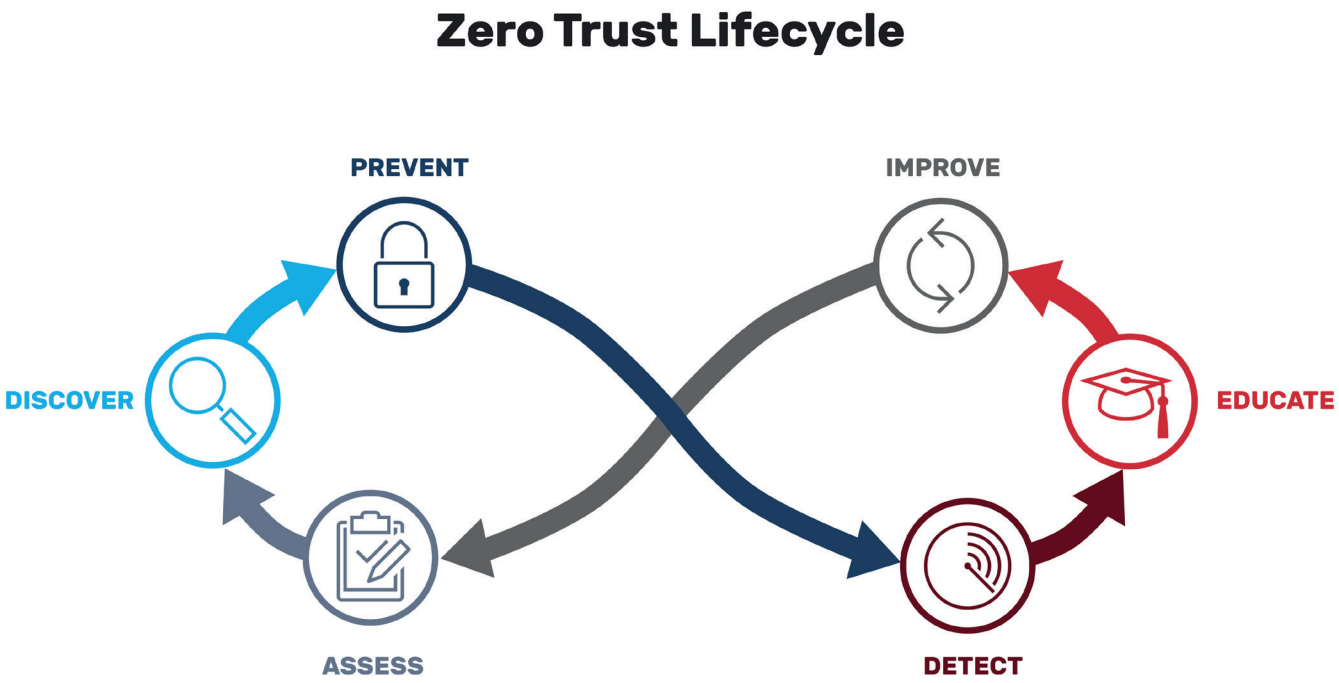
Analysis and forensics capabilities will allow you to determine how the malware entered the system. With the help of this knowledge, further response measures can be derived.

If you also feed the data into a security incident and event management solution such as Splunk or Logrhythm, you can benefit from additional functions such as alerting and automated prioritization.

Step 5

Continuous improvement - After the process is as important as before the process

As with many things in the digital world, IT threats change rapidly, and you should evaluate the risks over and over again, especially after significant events.
The reason may be a restructuring within the company, the introduction of a company-wide software (e.g. SAP) or other larger software and website projects.



Important: You should restart the entire Zero Trust process at regular intervals to keep the security level within the organization at the highest level.

Step 6

Keep your employees up-to-date.

Raising Awareness through Security Education

All the safety measures of the previous steps will only perform effectively the entire workforce contributes to the effort.

Of course, security measures are also associated with restrictions that frustrate employees. In digital times we are used to self-determined work and do not like any form of restrictions. Always keep in mind that ALL employees are an important part of the overall security strategy.

Regular and incident-related training and communication measures, e.g. when an employee connects an external USB stick, create the necessary security awareness and prevent frustration.

CONCLUSION | Designing solutions together.

Zero Trust is a combination of several, complementary security measures with the strategic goal of ensuring data integrity and preventing data breaches.

The Zero Trust concept achieves this maximum level of IT security by creating as many hurdles and restrictions as possible and by checking all assets, users and actions in the system.

In times of digital transformation, the success of companies depends largely on how reliably people, companies and services are protected against cyber attacks and the loss of valuable data.

We have set ourselves the goal of protecting company data, equipment and systems.
Our Zero-Trust platform combines the elements

- **Data Protection**
- **Endpoint Protection**
- **Endpoint Detection & Response**
- **Identity & Access Management**

Our fully integrated, zero-trust platform supports multiple operating systems, endpoint devices, and is offered as an on-premise solution and a managed security service.
The solution is Made in Germany and "without backdoor".

DriveLock