Zero Trust: the new standard in the world of cybersecurity explained

inetum realdolmen
Positive digital flow

The world is changing. Has your security kept up?

There was a time when a strong password, antivirus software and a firewall with VPN were enough to protect your organization against cyberattacks. Sadly, those days are long gone.

Today, we're no longer tied to one fixed workplace – or even to one fixed device. We work remotely, on different devices, even on private devices, and increasingly in the cloud.

With this **growing complexity** of our work environment, cyber risks and threats have also increased significantly. After all, a single fixed target is easier to secure than lots of moving targets.

It is clear that we need to adapt our security tools to this new workplace reality. But just expanding the security team alone won't do. We need a fundamentally different view of security in order to arrive at a completely new approach. This **security shift** also requires a shift in our organization culture and the mindset of our employees.

"In 2022, cyberattacks have risen again, by 32 percent. Almost one in eight Flemish companies fell victim to a cyberattack in the past year."

Zero Trust security: new security principles for a new reality

Zero Trust security. In short: Zero Trust. Maybe you've already heard about it? Under this heading is a new, **proactive approach** to security that allows you to respond to threats faster and more efficiently, effectively repelling and even preventing attacks.

To do this, Zero Trust relies on a wide array of **adaptive controls and mechanisms** and a process of **continuous verification**. Consequently, bringing in a single product, service, solution, or technology is not enough, just as you can't rid yourself of such attacks and threats once and for all with a single project or implementation. Zero Trust requires sustained long-term effort and constant vigilance against new risks and hazards.

THE CONCEPT OF ZERO TRUST IS BASED ON THREE IMPORTANT BASIC MEASURES:

1. **Verifying comprehensively and thoroughly:**
   The most important principle behind the Zero Trust security model is "never trust, always verify". This means, for example, that you should not automatically trust devices, even if they are connected to an authorized network and even if you have verified them before.

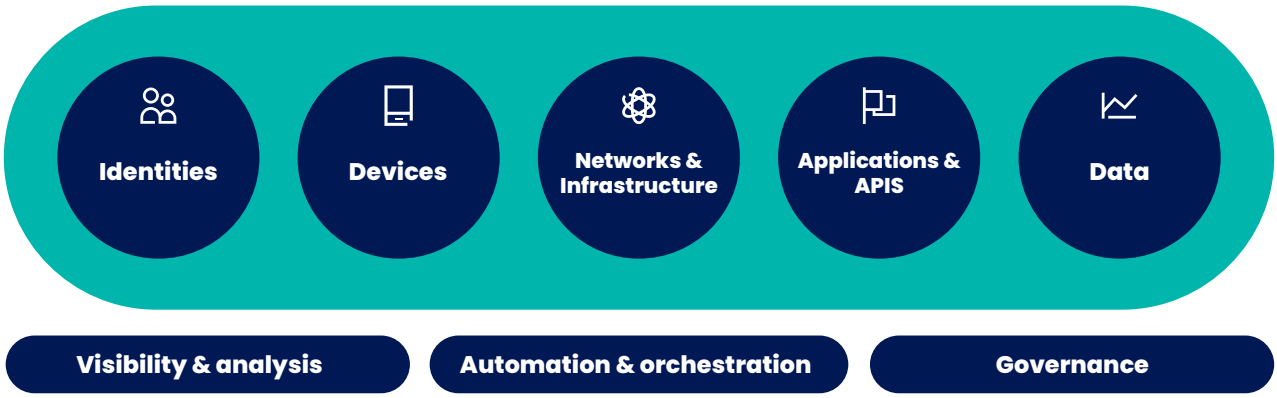
2. **Providing access by giving as few privileges as possible:**
   The principle of least privileged access (LPA) means that you restrict access to your work environment to the minimum (JEA, Just Enough Access) and that you only grant access at the moment and for the time it's needed (JIT, Just In Time).

3. **Assuming that breaches will occur:**
   As a precaution, create an infrastructure designed to minimize the impact of a breach.

The architecture behind Zero Trust Security is based on five essential pillars

WE BRIEFLY LIST THEM FOR YOU:

Basic components of Zero Trust



Pillar 1: secure your IDENTITIES

Everything starts with the user. This person may have one or more identities. Each identity has a number of specific user rights and sometimes administrative rights as well. It is therefore of the utmost importance that you always thoroughly verify this identity and always authenticate the user before granting the user access to your work environment (Identity & Access Management, IAM).

A password alone, no matter how strong, is no longer good enough. When we talk about **strong authentication** today, we're generally talking about **multiple authentication or MFA (Multi-Factor Authentication)**, which adds an extra layer of security to your access control.

What is important is not only that the access provided is "compliant" (in line with your access control rules), but that the access is **typical** of the identity you verify.
If a user tries to log in from India while physically in Belgium, something is probably wrong. In this context, it is also positive that you can now base the authentication on a **risk assessment** that takes the user's location and behavior into account, in addition to the user and device.

While the use of **single sign-on (SSO)** ensures that a user only needs to log in once to gain access to your work environment, the principle of **least privileged access (LPA)** ensures that the same user does not just get access to everything.

FOCUS ON MULTIFACTOR AUTHENTICATION, SINGLE SIGN-ON, IDENTITY AND ACCESS MANAGEMENT, PRIVILEGED IDENTITY MANAGEMENT AND RISK-BASED AUTHENTICATION

Pillar 2: secure your DEVICES

Once the user's authentication is complete and the identity is sufficiently verified, the user can access the resources in your working environment, including your data. To retrieve this data, an "endpoint" or user device such as a PC or smartphone. is usually necessary. This creates a **new attack surface** which we must of course also monitor and protect.

First of all, we are going to impose rules to prevent an insecure device from ever gaining access to our work environment (**device compliance**). For example, you can enforce that a device has been purchased and/or is managed by your organization in order to qualify for access. You can also demand that the device be equipped with an antivirus program that continuously monitors its behavior and condition and automatically maintains its security (**endpoint protection**).

Basically, it comes down to actively managing your users' devices, including the security aspect (**mobile device management, MDM**). This has become all the more necessary as users are increasingly bringing their own private devices to work (**bring your own device, BYOD**). What's more, business applications such as email often run on these devices. So, to limit the security risks, you must also manage these devices. Among other things, this management may include the option of deleting data remotely in the event the device is lost (**data loss prevention, DLP**).

"In addition to the corporate network, the user's home network is now increasingly being targeted. One easy way to reach many people at once is through the smartphone."

FOCUS ON MOBILE DEVICE MANAGEMENT, DEVICE COMPLIANCE AND ENDPOINT PROTECTION

Pillar 3: secure your NETWORKS and INFRASTRUCTURE

Once past the access control, the user is on your network. This infrastructure will ultimately give them access to the data on the servers, databases and storage systems in your data center.

To reduce that immense potential attack surface, it's important to divide or **segment** your network into smaller units. You may have done this before, for example, by using VLAN technology to virtually separate the clients from the servers on your network, but that's no longer sufficient. From now on, **microsegmentation** is recommended, at the level of the individual equipment or even its components, such as a network port. By dividing your infrastructure into even smaller, more protected areas, you avoid a virus, for example, from deeply infecting and paralyzing large parts of your infrastructure.

In addition, it's important that you invest in resources to monitor your infrastructure in real time and protect it against threats (**real-time threat protection**). A firewall can be used to detect suspicious network traffic, for example. Abnormal, risky behavior can be automatically flagged and signaled, after which you can block it or take other protective measures.

Last but not least, you can also encrypt your network traffic itself (**end-to-end encryption**) to avoid it being captured or compromised.

FOCUS ON SEGMENTATION, THREAT PROTECTION AND ENCRYPTION

Pillar 4: secure your APPLICATIONS & APIs

Applications and APIs provide the interface that allows a user to access and use your data. It is therefore important that you get the best possible control over the use of these applications and APIs.

A first major security challenge for IT administrators with regard to applications is the phenomenon of **shadow IT**: solutions that your employees buy and use outside the field of vision of your IT organization. Having no view of these treacherous solutions in the shadow of your regular IT environment is a very big risk. Therefore, invest in resources that allow you to clearly identify which **unauthorized applications** are in use within your organization.

However, you should be aware that **authorized applications** can also pose a security risk. Just because the use of an application is accepted and allowed within your organization does not mean that every employee can and should just use it. In particular, employees must be authorized to access financial or other sensitive information in an application (**in-app permissions**). There are now solutions available for allocating and managing these authorizations.

Moreover, again, you need to **screen your applications for abnormal behavior**. Thanks to the growing use of APIs, applications can now retrieve data from anywhere and communicate with virtually anything. The flip side of that coin is that applications are more exposed than ever to risks and dangers. That's why it's better to set up and maintain strict **access control**, especially for your critical applications.

Finally, it's important to **patch** correctly and on time to close vulnerabilities in a software package or suite. The longer you wait to install the required patch, the greater the chance of a cyber incident. It's not incidental that the vulnerabilities or errors in a program are one of the main causes of breaches today. That's why it's important to have an overview of your software vulnerabilities at all times.

FOCUS ON ACCESS AUTHORIZATION, ACCESSIBILITY, MONITORING, PATCH MANAGEMENT

Pillar 5: secure your DATA

This is what it's all about in the end: securing your data. The four previous pillars support this ultimate goal. Without those supporting pillars, your data would not be nearly as secure. That said, it's in your best interest to also protect that data yourself. That way, you ensure that it's safe at all times, even if it leaves (e.g., via email or file sharing), the applications, devices, infrastructure and networks that you yourself so carefully manage.

A first step in that security process is to **classify and label** your data. This allows you to separate your public data, to which everyone may have access, from your private or secret data, which you do not wish to share with the outside world under any circumstances, and maybe not even with anyone within your organization.

"Of the companies impacted, **23.5%** had to contend with the destruction of company data; **13.3%** were hit by theft of company data."

Based on this classification and labeling, you can also set up and maintain a certain **access control** for your data. In doing so, by again adopting the principle of **least privileged access (LPA)**, you only give each user access to data needed to perform his or her job properly, and nothing more.
You may also have sensitive, personal data, such as medical records, which you need to handle very carefully pursuant to European GDPR legislation. This means that you need to **anonymize or pseudonymize** the data if you still want to use it in big data applications, for example.

Finally, as we've mentioned before: **encrypt**. Encrypting your critical data prevents it from being read in the event of loss or theft. **Data loss prevention (DLP)** solutions also enable you to intervene in your data and delete it after it has been lost or stolen. If everything goes wrong, it's a good idea to be able to resort to a **back-up** or copy of your data as a last resort.

FOCUS ON CLASSIFICATION, LABELING, ENCRYPTION, ACCESS AND DATA LOSS PREVENTION, BACKUP & RECOVERY.

Additional foundations

The five outlined pillars underpinning Zero Trust Security are in turn supported by three important layers that guarantee you an extra-solid foundation. So it pays to invest in this substructure as well.

VISIBILITY AND ANALYSIS
Without a clear view of your work and IT environment and the risks and dangers they may pose, there is no way you can successfully set up the complex security architecture of Zero Trust Security.

Fortunately, the investments you make in setting up the same architecture, particularly through the five pillars, also already provide better visibility, for example of your shadow IT, or of all the user devices you manage (endpoint management).

The same investments also provide a lot of data that you can analyze to further refine your security approach.

AUTOMATION AND ORCHESTRATION
It goes without saying that you can't implement every access control yourself. The same goes for most of the other security tasks we mentioned here: micro-segmentation, encryption, back-up, etc. That's why a truly efficient security approach requires you to automate as many tasks as possible and orchestrate software.

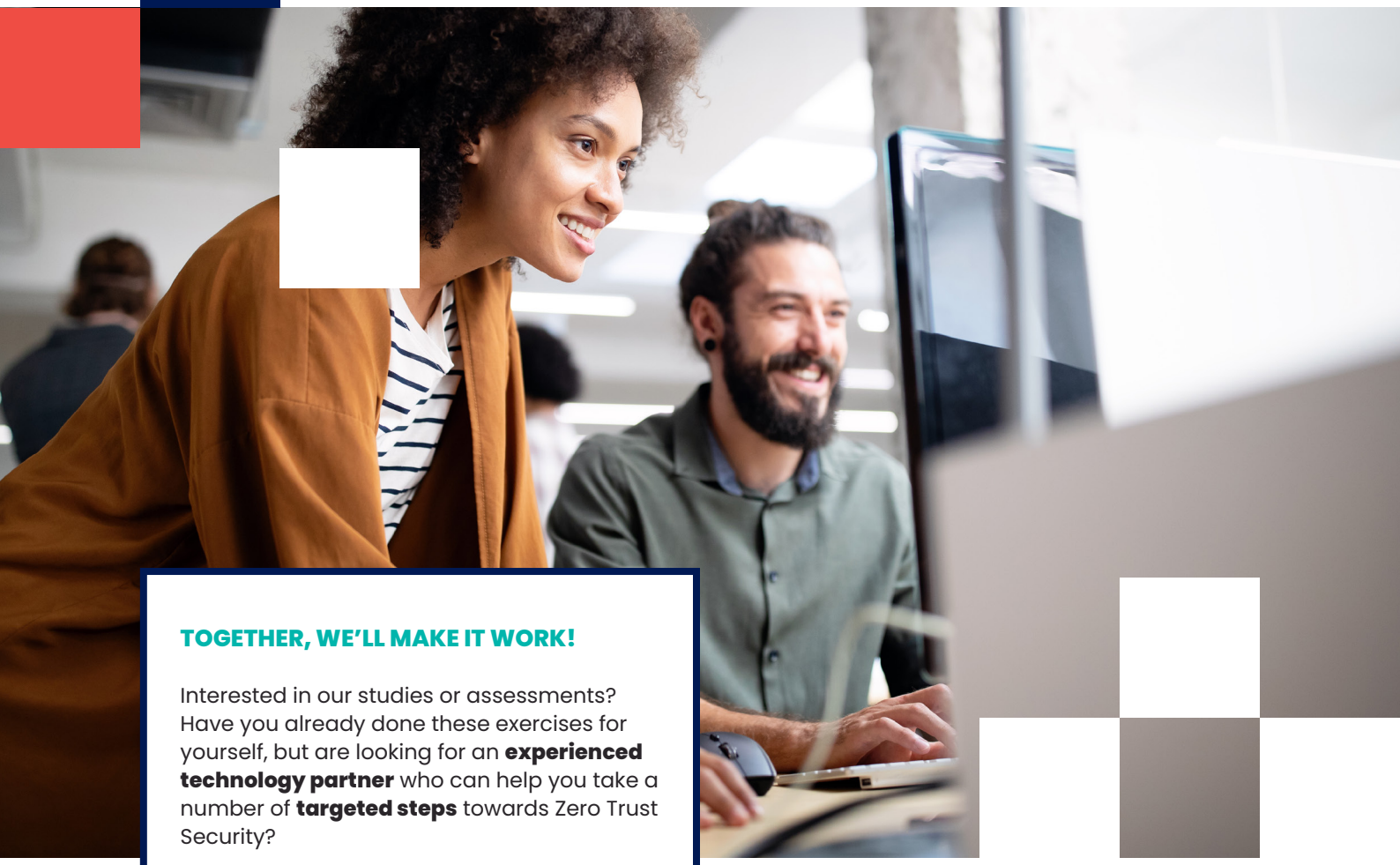
GOVERNANCE
Zero Trust Security is not a simple, well-defined implementation project that you can quickly take care of during your downtime. It's a complex long-term strategic journey of change that you must continuously monitor and adjust. That is why it is important that you also provide good governance, so that you can take the necessary ownership of that process and maintain an overview at all times.

Zero Trust Security: are you ready for it?

Are you already convinced of the concept of Zero Trust Security, but not sure how best to get started? Maybe you've even taken your first steps on the path to Zero Trust Security, but are still unsure about exactly how to proceed?

In either case, you will undoubtedly benefit from a brief study or **security assessment**. In it, we will take stock of your current situation and map your **maturity** or **Zero Trust readiness**. That way, at least you will know where you really stand.

If you then combine this entry-level exercise with the creation of a **security roadmap**, including a step-by-step plan, **priority assessment** and **specific technology advice**, you will also immediately have a clear view of where you are headed next on your journey. This not only lets you know exactly where you need to go, but also how to get there.



TOGETHER, WE'LL MAKE IT WORK!

Interested in our studies or assessments? Have you already done these exercises for yourself, but are looking for an **experienced technology partner** who can help you take a number of **targeted steps** towards Zero Trust Security?

In either case, you can turn to us. We have the necessary in-house expertise for all the technological pillars and foundations covered in this document.

Together we can create a safer working environment!

CONTACT US

Inetum-Realdolmen
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum realdolmen
Positive digital flow