Hso

the results company

From firewall to zero trust

HSO Security Assessment identifies risks and advises recommendations

With the arrival of Cloud Technology and mobile computing, the IT landscape of most companies has changed dramatically. This new world calls for a different vision on security. Whereas companies used to secure their on-premise environment with a firewall, in other words a solid fence around all systems, we now see the rise of the zero-trust architecture: a security approach in which every part of your IT platform is secured separately.

In the HSO Security Assessment, we map out the weaknesses in your digital environment and provide a clear step-by-step plan on how you can optimise the security of your hybrid or cloud platform. You can read more about this in this factsheet zero trust approach and the security assessment.

Getting started?
Our Cloud & Security team is ready to help you.

Contact us:
Lucas Köhler
lkohler@hso.com
+31 (0)6 825 79 667

01

The weaknesses *in your IT platform*

The risks of cybercrime are high. Sooner or later almost all companies will have to deal with it. You will not be the first organisation to fall victim to a crypto hack, where criminals encrypt your data and demand a ‘ransom’ for its release. Other major risks are loss of data, for example, stolen customer data, and the damage to company reputation. Cybercrime should always be high on the agenda, and if it happens to you, you want to be able to limit the damage as quickly and as much as possible.

We see that most hackers enter systems via stolen login data, via malware contained in e-mails or via stolen devices. That is why a complete security approach should include:

1. Identities, logins, and access management
2. Devices, laptops, phones, and tablets
3. Dates
4. Applications
5. Infrastructure
6. Network

02 Why a *zero-trust security approach?*

An on-premise environment is usually protected by a firewall. In other words, a solid fence around all systems. Not only are cyber criminals getting smarter at penetrating firewalls, but there is also the risk that if a hacker does somehow gain access, he will soon get hold of all data and applications. It is also very important to note that a hack is not always immediately detected, with all the dangers that this entails. **In addition to these risks, cloud technology and mobile working come with new threats.** More and more employees have access to applications and data outside the 'traditional' company network boundaries.

As a result, security via firewalls and virtual private networks (VPN) is no longer sufficient.

To meet these challenges, Microsoft has developed the Zero Trust Architecture. The three principles of Zero Trust are:

1. Demand explicit verification
2. Give employees only access to the data and applications they need
3. Assume that you will be hacked

When setting up your security, Microsoft recommend that you continuously apply these principles. Does the last principle sound rather disturbing to you? Well, Microsoft call this realistic. However, you can prepare yourself as much as possible to make sure any damage is kept to a minimum.

A Zero-Trust model requires that all the components – user identity, device, network, and the applications - are continuously validated and tested for reliability.

The security strength of Microsoft

We are convinced that it is almost impossible to achieve the same level of on-premise security as you can reach with cloud security. Microsoft invests billions every year in the security of the Microsoft Cloud platform, and some 3,000 people contribute to this every day on a full-time basis. The strength of the Microsoft platform lies mainly in the enormous amounts of data, applications and information flows that are continuously being searched for, deviating signals, data flows or other disruptions using advanced algorithms. As a result, the level of security is becoming ever higher and increasingly automated, from which you, as a user of the Microsoft platform, can benefit from directly.

The four pillars of *Intelligent Security according to Microsoft*

Identity management and access control	Threat protection	Information protection	Cloud security
A universal platform that allows you to manage and secure users (identities).	Integrated and automated security detects and stops cyber-attacks.	Protect your business-sensitive information - wherever this data is stored or transmitted.	Protect your cloud applications.

03

This is how the *HSO Security Assessment* works

Step 1

Determine as-is and to-be

Take stock of the ‘as-is’ status of your security and determine the requirements and preconditions of the ‘to-be’ situation. We draw up the requirements and pre-conditions based on legislation and regulations, standards in the market and, for example, expectations of customers and partners.

Step 2

Inventory of your current IT landscape

We review what your current IT landscape looks like, including users, devices, applications, network, locations, and data.

Step 3

Inventory of potential threats

We analyse the security risks and potential threats to your current environment and map them out for you.

Step 4

Assessment report and roadmap

The final step is a presentation of the report and our findings, plus a compact step-by-step plan to achieve a zero-trust security architecture.

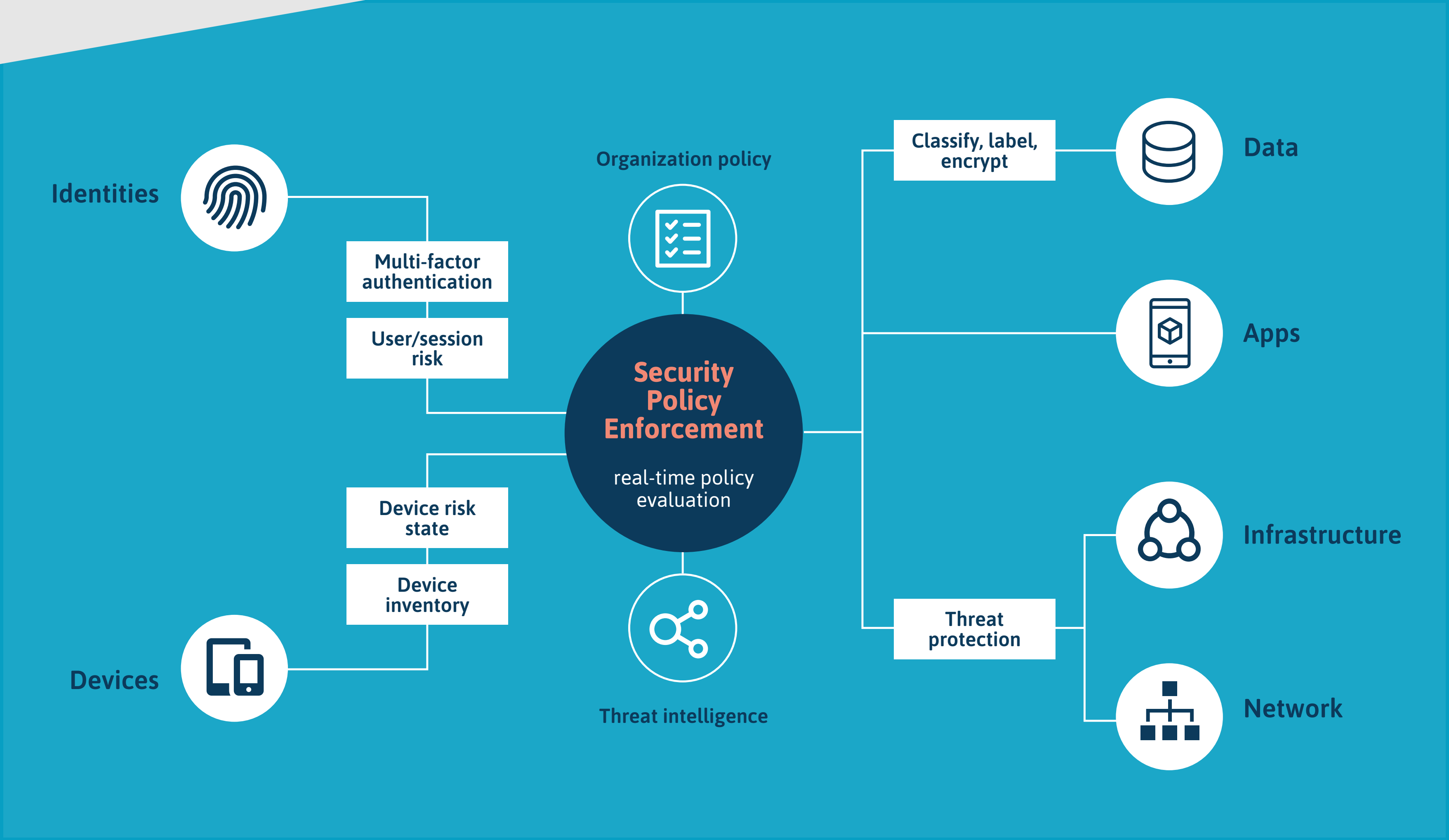
Required time

In general, a turnaround time of 3-4 weeks is a sufficient timeline for the Security Assessment.

What do we ask of you?

For step 1, setting the frameworks and objectives, and step 4, the presentation, we ask for availability of the management and the IT team. For steps 2 and 3, we also ask for commitment from the IT team, with which we jointly map out the current platform and the possible weaknesses and risks.

Zero Trust Architecture



Identities

Multi-factor authentication

User/session risk

Device risk state

Device inventory

Devices

Organization policy

Security Policy Enforcement

real-time policy evaluation

Threat intelligence

Classify, label, encrypt

Threat protection

Data

Apps

Infrastructure

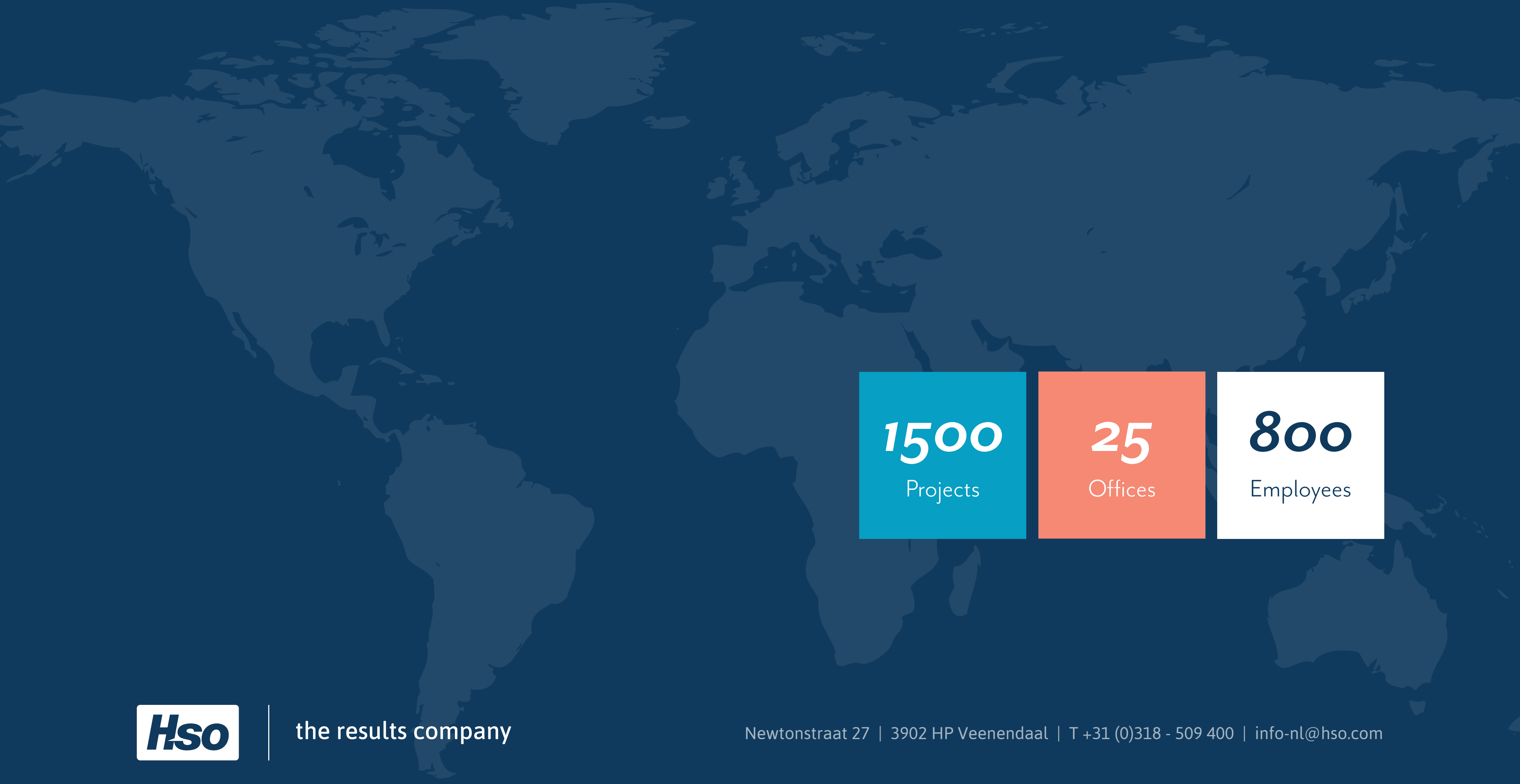
Network

Hso the results company

Keen to know more about the HSO Security Assessment?

Would you like to find out how you can benefit by taking the security of your hybrid or cloud platform to a higher level? Our experts are ready to assist you. Feel free to contact us!

Contact:
Lucas Köhler
lkohler@hso.com
+31 (0)6 825 79 667



1500
Projects

25
Offices

800
Employees

the results company

Newtonstraat 27 | 3902 HP Veenendaal | T +31 (0)318 - 509 400 | info-nl@hso.com

HSO has been active as a Microsoft Solution Integrator since 1989 and has grown into a successful ICT company with more than 800 employees and offices in Europe, North America and Asia. HSO supports local and international companies in retail, wholesale, industry and (technical) services to make a difference with digital technology. The foundation for this is Microsoft Dynamics 365 (CRM & ERP), Microsoft 365 and Data & AI. HSO takes care of the implementation, optimisation and 24/7 management of these cloud solutions, worldwide. HSO belongs to the Microsoft Dynamics Inner Circle and is proud to have been awarded the title 'Microsoft's most customer-oriented partner'. You can find more information on HSO at www.hso.com/nl