Stay connected.
Stay safe.

Skyleaf Annual Report 2025

CYBERWOLF
your digital bodyguard

spotit
YOUR SECURITY & NETWORK LAYER

The year of lasting trust and long-term partnerships

2025 once again confirmed what matters most to us: trust. More than ever, customers see spotit as their preferred partner for cybersecurity and networking. That is the result of strong, sustainable relationships that we build every day, based on reliability, expertise, and true collaboration.

What continues to set us apart is our integrated approach. Networking and security cannot be viewed separately. IT and OT environments are increasingly converging. Only by approaching them together can an organization be sure that its security vision is sound and future-proof. That holistic perspective remains a cornerstone of our strategy.

That many others share this view is reflected in our results. We achieved solid growth, with a 21% increase in revenue. An important milestone in 2025 was the renewal of our partnership with Fluvius after a new public tender. Being selected again, and this for a long term and with a broader scope, is a strong signal of mutual trust. But growth in itself is never the ultimate goal. What truly matters is what lies behind those numbers: the commitment of our people, the quality of our services, and the impact we make by guiding organizations through increasingly complex security and connectivity challenges.

Another important observation in 2025 is the growing value of our 100% Belgian roots. In today's geopolitical context, digital sovereignty is more important than ever. From day one, we deliberately chose to work exclusively with Belgian professionals and to organize our core NOC and SOC activities entirely locally. That guarantees availability, continuity, and peace of mind, 24 hours a day, 7 days a week. You cannot simply 'switch off' spotit.

In 2025, we once again organized a successful edition of our Academy, our training program for new employees. In doing so, we are not only investing in knowledge sharing, but also in strengthening our local expertise. That is how we guarantee our customers the Belgian continuity and hands-on support they expect.

Cyberwolf also took another step in its international growth in 2025. We further expanded our partnerships in the United States and today we work with three of the ten largest banks in the US to protect their wealth clients. Since its launch, Cyberwolf has grown by 300%. That proves that highly specialized protection services developed in Belgium are also receiving recognition at the highest international level.

This Skyleaf Annual Report brings together the highlights of 2025 and showcases the combined expertise of spotit and Cyberwolf. It provides a clear picture of how we think, how we work, and how we support our customers.

Thank you for your continued trust. We look forward to writing the next chapters together in a world where connectivity continues to increase and security only becomes more important.

Steven Vynckier and Frederik Rasschaert,
Founders of spotit and Cyberwolf

About Skyleaf

Our company operates with a holding structure, meaning there is a parent company that oversees various entities. The holding is called Skyleaf, with spotit and Cyberwolf as its entities. The mission is clear: to make the world a safe online place for people, machines, and businesses.

Who is **Cyberwolf**?

Cyberwolf is a 24/7 digital bodyguard for the private lives of executives, board members, entrepreneurs, diplomats, and wealthy families worldwide. Where spotit protects organizations, Cyberwolf protects the people behind those organizations. We secure devices, email, accounts and home networks, monitor threats and dark web activity, and intervene in incidents.

Our goal is simple: to give people the freedom to move through the digital world with confidence. Cyberwolf brings peace of mind in an environment where invisible risks often create uncertainty.

Who is **spotit**?

Spotit creates peace of mind for everything related to security and connectivity. As a strategic partner, we place a strong emphasis on vision, expertise, and trust. We make the difference with a high-level, long-term approach to security and networking, starting from an action plan with concrete objectives.

Locally rooted in Belgium, more than 120 highly trained experts support organizations in making their digital infrastructure secure, high-performing, and resilient. This applies to both IT and OT environments.

What are our **values**?

Human to Human
At Skyleaf, everything revolves around genuine human connections. We place colleagues, customers, and partners at the center and believe that open communication and mutual respect form the basis for strong collaborations.

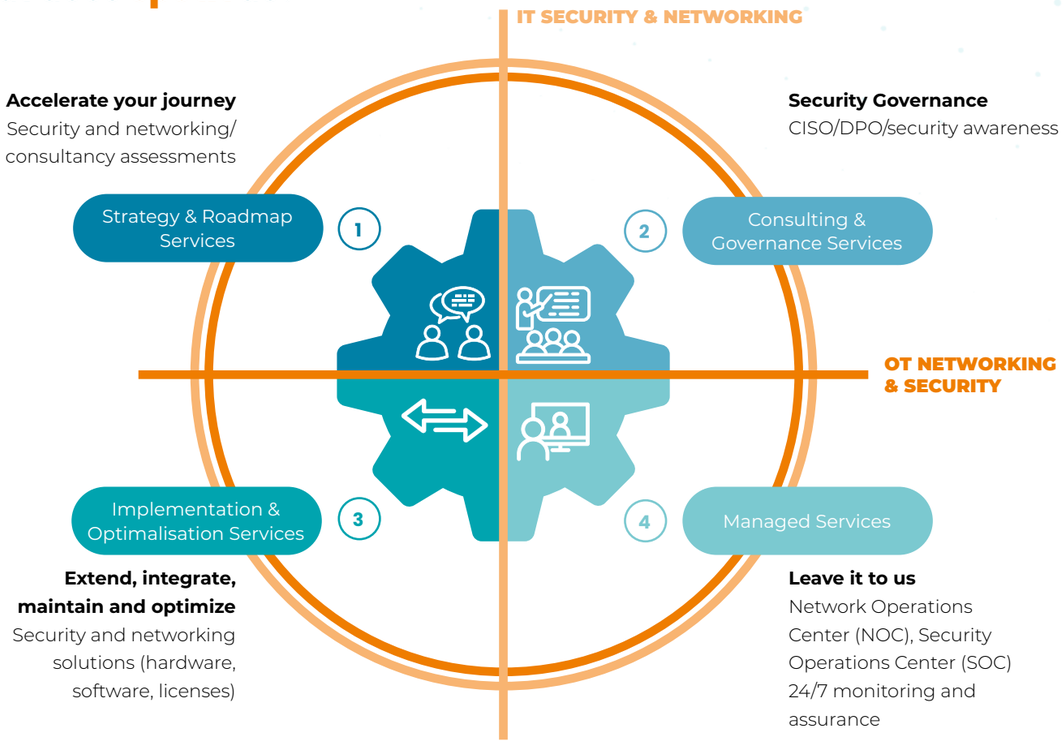
Excel
We strive for excellence and do not settle for mediocrity. Excelling is part of our mindset: continuing to challenge one another, constantly improving, and wanting to do better every day for our customers.

Entrepreneurship
Entrepreneurship is in the DNA of our team. We take responsibility, show initiative, and go the extra mile together to deliver solutions, even outside our comfort zone.

Trust
Trust is crucial, especially in cybersecurity. We handle sensitive information with the utmost care and stand for reliability, integrity, and keeping our promises.

Corporate Social Responsibility
Sustainable business practices are a conscious and integrated choice for us. We actively reduce our ecological footprint, pursue transparent and ethical governance with an eye on long-term value creation, and invest in people by focusing on well-being, development, and collaboration with external partners. In this way, we create a positive impact both within our organization and beyond it, and we take responsibility for today and tomorrow.

What does **spotit** do?



We joined forces with SHIELD

Hospitals and higher education institutions carry a major social responsibility. When digital systems fail, the impact on patients, students, and staff is immediate. That is why spotit is joining forces with SHIELD vzw and Cisco to structurally strengthen cyber resilience in these sectors. This positions us as a focused partner for healthcare and education.

Watch the testimonial!

2025

Cyberwolf gained traction at Skyleaf

In 2025, Cyberwolf deliberately stepped into the spotlight. Through targeted articles and interviews, we made it clear what we do: provide digital protection for executives and their families. We also explicitly positioned Cyberwolf as an employee benefit, allowing organizations to structurally support their executives in the area of personal cybersecurity.

The United States became an important growth market. Our approach gained traction there, including through partnerships with three of the ten largest American banks. With new investments, a strengthened team, and increasing demand, we closed the year with a clear foundation for further expansion in the US. In addition, we took our first steps into sports and entertainment, onboarding our first well-known athlete.

3

During the Cisco Partner Summit 2025, spotit received three awards: Security Partner of the Year – Belgium, Security Partner of the Year – North Theater and Public Sector Partner of the Year – Belgium. These awards are the result of a strong and sustainable partnership with Cisco that has now lasted more than ten years and has deepened year after year.

We continue to grow

In 2025, spotit welcomed 18 new colleagues. The team continues to grow, with talent ranging from 24 to 61 years old. Turnover remained limited to 14%, which is low for our industry. In this way, we continue to build continuity, experience, and fresh expertise, with one clear focus: supporting our customers better every day.

Partnership with XONA

In the context of NIS2, we strengthened our offering around secure remote access through a partnership with XONA, which specializes in OT and ICS environments. Together, we help organizations replace traditional VPN solutions with zero-trust access, with role- and time-based permissions and full logging of all sessions.

White paper: IT Cybersecurity Maturity: Your Roadmap Towards Excellence

Many organizations overestimate their cybersecurity maturity and only discover their vulnerabilities when things go wrong. Based on more than fifty fundamental security assessments, it appears that basic measures are often not sufficiently embedded in a structural way. At the end of 2025, we launched a white paper that bundles our insights from those assessments.

Read it here

An NPS score of 53 shows customers' trust in spotit

For more than five years in a row, spotit has commissioned an extensive Net Promoter Score survey through an external party. The goal is to gain deeper insight into what customers really think of our services and to identify areas for improvement. The 2025 survey showed that we achieved an impressive score of 53.

With spotit's sustainable growth ambitions clearly in focus, customer satisfaction is central. To measure this, each year we survey a selection of customers. Through NPS research, we gain a holistic view of how they experience the collaboration and what their expectations are for the future. The Net Promoter Score, a clear indicator of customer satisfaction and customer loyalty, serves as our compass.

The NPS can range from -100 to 100. Any score above 0 is considered positive, as it means there are more promoters than detractors. In general, a score above 30 is considered good and above 50 excellent, while a score above 70 is exceptional. Such high scores are quite rare.

In many industries, an NPS between 30 and 50 is a realistic goal and an indication of solid customer satisfaction.

With an impressive NPS score of 53, spotit can confidently position itself as a leading and strong service provider in the IT sector. In addition to expertise and reliability, customers this year also emphasize 'partner in cybersecurity' as a core strength. The feedback reflects deep trust in spotit's ability to act as a reliable partner and expert, with a human approach as a distinguishing factor and always with a great deal of expertise in IT/OT cybersecurity and networking. This makes us extremely satisfied, because it is fully aligned with the position we want to hold in the market: not as a pure supplier, but as a trusted partner.

NEXT STEPS

It goes without saying: we do not make progress with good news alone. Listening carefully to what can be improved and remaining critical of ourselves continues to be essential. The research therefore also identified several areas for improvement. More proactive communication, such as keeping the customer informed that we are working on a ticket, and greater emphasis on knowledge sharing and knowledge retention between spotit and the customer were both mentioned. We will, of course, act on this and see these as valuable opportunities to further increase overall customer satisfaction.

CYBERWOLF RESEARCH

CEOs of BEL20 companies are attractive targets for hackers

A large majority of CEOs of BEL20 companies are vulnerable to cyberattacks through their private devices and personal accounts. This is the conclusion of an analysis carried out by Cyberwolf. Over a period of three months, Cyberwolf monitored the digital exposure of these CEOs. The findings show that 70% of them can easily be approached through publicly visible vulnerabilities in their own organization or through other mandates they hold.

Hackers are increasingly exploiting the hybrid work environments of top executives. A personal smartphone, email account, or home network can provide easy access to valuable company information or accounts. "Top executives are a strategic and deliberate target for both cybercrime and advanced corporate espionage by competitors or foreign intelligence services. But it can also happen by accident, as automated scans search 24/7 for any possible security gap, ready to strike the moment they find an opening," says Daan Gheysens, CEO of Cyberwolf.

"The boardroom often applies double standards: while cybersecurity is labeled a top priority, board members not infrequently ask for personal exceptions to security protocols."

Alarming figures

The ambition to better protect top executives should be higher, because vulnerabilities are everywhere. Research conducted by Cyberwolf across all BEL20 top executives shows that there should be no illusions about the current security context.

- 70% of all BEL20 CEOs can easily be targeted through publicly visible vulnerabilities in their own company or through mandates they hold in other organizations.
- That figure rises to 95% when vulnerabilities in affiliated charities or specialized trade media are included.
- For 80% of BEL20 CEOs, a credible deepfake of their voice can be created within five minutes.

The research and findings were shared with the impacted organizations and with the Center for Cybersecurity Belgium. The results were also covered by the newspaper De Tijd.

“This is much more than a customer-supplier relationship.”

Fluvius manages infrastructure that is essential to daily life in Belgium. The company provides the distribution of electricity, natural gas, sewage, and heating. The societal shift towards electrification is increasing the pressure on those networks and making robust digital infrastructure more important than ever. For years, Fluvius has relied in part on spotit for that. Kurt Ceulemans, Head of Systems and Operations, and Wouter De Clercq, Head of Central Infrastructure, sat down with Steven Vynckier and Frederik Rasschaert, founders of spotit.

“Outsourcing, with the right partner, is not a weakness, but a strength.”

Wouter De Clercq
(Head of Central Infrastructure at Fluvius)

Fluvius is a large organization managing critical infrastructure. That creates specific challenges in the area of network management.
Kurt Ceulemans: “Absolutely. Society is clearly in the middle of a major shift. Electrification is everywhere today, and Fluvius plays a key role in that. The electricity grids as they were known in the past are no longer sufficient. Of course, they are being expanded and more cables are being added, but that alone will not be enough. Electrification also needs to be supported in another way: by making the IT network smarter. We need to be able to capture, analyze, and respond in real time to large quantities of information coming from the electricity grid. As a result, the networks that transport that information and control are becoming increasingly important. Flexibility is a key concept here.”
Wouter De Clercq: “Our infrastructure is becoming more and more crucial, and our IT network must evolve along with it. Especially in a highly automated environment, it is essential that the organization is already ready today for what tomorrow will require.”

What fundamentally makes Fluvius’s IT and OT environment different from that of a traditional organization?
Wouter De Clercq: “First and foremost, I’m thinking about the importance of continuity: the availability of electricity and gas is crucial for society. That is exactly why it is so important that digital components are under control and can be actively steered. It is a fundamental evolution the company is going through today and whose importance will only continue to increase.”
Kurt Ceulemans: “That availability and continuity are now closely tied to convergence. Whereas in the past, clear walls could be built between IT and OT systems, those boundaries now have to be deliberately dismantled. That evolution is necessary to enable flexibility and also to commercialize it. Think of battery parks or companies willing to temporarily reduce production. For that, the link between IT and OT is crucial. Information must be able to flow safely, reliably, and quickly from one domain to the other so that it can be acted upon immediately. Only then can the electricity grid be kept continuously in balance. A temporary outage of the IT network used to be inconvenient, but the impact remained limited, whereas today a disruption can have direct consequences for the electricity grid and end users.”
Frederik Rasschaert: “An additional challenge is that more and more availability is needed while at the same time more security has to be added. That means the network has to be maintained continuously. And to avoid shutting it down, the network needs to become increasingly redundant.”
Kurt Ceulemans: “Redundant and smarter. In the past, it might have been enough to add an extra component to the network, but today that is no longer sufficient. Now careful thought has to go into the right architecture. That is exactly where the big challenge lies. To support Fluvius in that, strong partners are needed, including spotit.”

The ideal moment to briefly look back at the beginning of your collaboration, in 2017. Why did Fluvius decide at that time to work together with spotit?
Kurt Ceulemans: “For that, I will go even further back in time, to the liberalization of the energy sector, about 20 years ago. At that time, electricity and gas production and distribution were gradually separated from one another, and different organizations emerged, which also meant the IT services had to be separated. It was then decided to outsource a number of IT elements, including parts of server management and parts of digital network management. In an iteration of the tender in 2017, spotit applied for that latter lot.”
Wouter De Clercq: “We were looking for deep technical expertise and operational maturity. Reliability within those specific domains was crucial. At the time, spotit was still a relatively small company. That represented a certain risk, but we saw that the company had the right expertise and a strong operational model. We very consciously took that leap and chose spotit.”
Kurt Ceulemans: “Although spotit was still relatively

young at the time, it fully embraced the challenge and grew along with Fluvius. Over those eight years, a strong track record was built, and the collaboration worked well."

Last year, after a new tender, the partnership was renewed. Why?
Kurt Ceulemans: "Spotit emerged as the best candidate from the tender. Apart from that, trust is a key element for me. Knowing that we can truly rely on each other."
Steven Vynckier: "We can truly speak of a partnership here, in good times but also in bad. In IT, problems arise from time to time. It is the way you deal with them that makes the difference. By resolving issues quickly and with as little impact as possible, you demonstrate real collaboration, even in difficult periods."

Can you consider the collaboration with spotit as a true partnership?
Kurt Ceulemans: "Absolutely. Recently, for example, we were dealing with an organizational challenge and asked spotit how they could support us in that. We greatly appreciate that openness and willingness to think along with us. That is the extra step that makes one plus one equal three."
Wouter De Clercq: "We work together on a daily basis as one integrated team and communicate openly. Of course, we make the final decisions, but spotit actively thinks along, looks for solutions and opportunities together with us. So this is much more than a standard customer-supplier relationship."

How are you preparing for the future today? Which projects are on the roadmap?
Wouter De Clercq: "There are quite a lot of projects underway. We are strongly focusing on further automation of network management and on continuous lifecycle renewal within data and telecom communication. That connectivity with new systems and devices is essential to keep everything online and operational. The challenges do not stop, so we must continue to invest in digitalization and in the maturity of our organization."
Kurt Ceulemans: "In the electricity grid alone, we will invest more than ten billion euros over the next ten years. That is a massive operation. Our switching stations are becoming digital, just like other parts of the network. Many people do not know that we also manage a large part of the sewer network. There too, we are fully investing in digitalization, with measurement points in the sewers and digital monitoring of buffers and basins. The same applies to heat, for example in the distribution of residual heat from incineration plants. Everywhere, we are taking steps towards a data-driven organization. Our IT/OT network is the foundation for that."

Nice to be able to work on that as an IT professional, right?
Wouter De Clercq: "Absolutely. Fluvius is a large organization with a great deal of IT. That is very rewarding, because you can work both broadly and in depth. The new evolutions are an additional challenge that naturally also brings pressure. That requires strong partners to make the right decisions and to continue to grow in maturity."
Steven Vynckier: "The people who work with us want to continue challenging themselves. And Fluvius offers that challenging environment where they can continue to develop technically and technologically. They also contribute to building various utility services. In addition, there is the one-team feeling, with a symbiosis between two teams, and a partnership in which people truly listen to one another."
Frederik Rasschaert: "One of the strong points in our relationship is that Fluvius has many challenges within our area of expertise. That is exactly what we deal with on a daily basis. As a result, there is strong involvement within our organization, from senior management to the people on the work floor. That engagement is what helps define our partnership."

"We need to be able to capture large volumes of information from the electricity network, analyze it, and respond to it in real time. The networks that transport that information are therefore becoming increasingly important."

Kurt Ceulemans (Head of Systems and Operations at Fluvius)

What should readers especially take away from this?
Wouter De Clercq: "For companies that are also considering outsourcing IT, I want to emphasize that outsourcing with the right partner is not a weakness, but a strength. You bring in someone who thinks along with you, invests alongside you, and takes responsibility."
Kurt Ceulemans: "When choosing the right partner, trust is essential, as well as the certainty that in case of a problem or an opportunity you can rely on that partner. That you can pick up the phone, call each other, and sit down together at the table, with the necessary seriousness and commitment. That is key. Ultimately, you want the network to keep functioning and to be ready for the future as well. And in that, today we have found a strong partner."
Steven Vynckier: "In any case, we are grateful to Fluvius for the trust. At the time, it was a courageous decision to work with a smaller party. Thanks to that trust, we have been able to grow. That is a real win-win situation."
Kurt Ceulemans: "On our side, we are also proud that we have contributed to the growth of a strong Belgian company. That is certainly something worth mentioning."

And how do you look ahead?
Kurt Ceulemans: "Expectations remain high. The challenges continue to evolve; our network will never be 'finished.' It is a continuous collaboration in which we take the next steps together. And in that, we continue to rely on spotit."
Wouter De Clercq: "Spotit has by now clearly positioned itself as an expert and as a driving force behind innovation. We count on them to continue to take the lead in the future within their domains and to keep deepening that expertise."
Steven Vynckier and Frederik Rasschaert: "Challenge accepted!"

Who is Fluvius?

Fluvius is the utility company responsible for building, managing, and maintaining distribution networks for electricity, natural gas, sewer systems, and heating. Fluvius also manages the municipal public lighting infrastructure. In total, the company manages 230,000 kilometers of utility lines and 7 million connections. Fluvius is active in all Flemish cities and municipalities.

FACTS &STATS

€32.000.000
Spotit revenue

5 SECTORS IN WHICH WE ARE MOST ACTIVE

1. Utilities & energy sector
2. Manufacturing & process industry
3. Logistics & ports
4. Pharmatech & life sciences
5. Healthcare & education

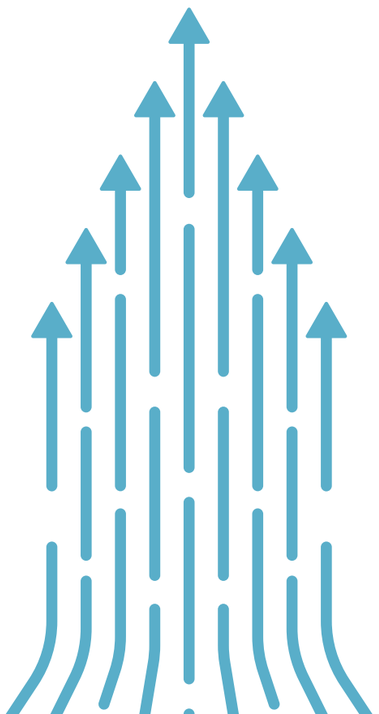
MOST POPULAR ASSESSMENTS IN 2025

- Pentest
- Fundamental security assessment
- NIS2 assessment

+21%
growth

X3
growth Cyberwolf

+19%
growth managed services



230
active customers (in portfolio)

CASE

Fednot supports notaries safely and smoothly in the digital world

Fednot, the federation of the notarial profession in Belgium, plays a crucial role in supporting notary offices in legal, administrative, and technological areas. With more than 1,100 offices, 1,754 notaries, and nearly 10,000 employees, **digitization is indispensable to improve efficiency and optimize service delivery** IT is the foundation.

Standardization is one of the core pillars of Fednot's IT strategy. "In concrete terms, this means using fewer IT tools, but making optimal use of the tools that are used. Over time, the goal is to reduce the number of applications and integrate them better. Fewer tools, but more coherence," says Program Manager Vincent Arijs.

That approach also applies to collaborations with partners. "Fednot deliberately chose fewer suppliers, but partners who truly understand the organization and genuinely help move it forward. With spotit, it has such a relationship. The teams can have in-depth technological conversations and receive precisely the support that is needed," stresses Arijs. **Automation is also a key element in the modernization** of IT processes, just like robust security.

One of the biggest recent challenges was the network renewal of the SDN data center, a crucial part of Fednot's IT infrastructure. Since Fednot manages the **critical applications for all notaries in Belgium**, it was essential to create a watertight migration plan that minimized downtime as much as possible.

The entire migration went extremely smoothly, to Arijs's great satisfaction: "The migration of the data center network was no simple task. The project was technically complex and had to be aligned with many other ongoing interventions. In addition, the rollout largely had to take place outside business hours to guarantee operational continuity. I would like to emphasize the tremendous flexibility of the spotit team."

"The spotit team not only brought strong technical expertise, but also exceptional flexibility. They adjusted seamlessly to Fednot's schedule and ensured that the impact on operations was kept to a minimum."

Vincent Arijs (Program Manager at Fednot)

KEY FINDINGS IN 2025 (SOURCE: CCB)

- INCREASE IN UNPATCHED VULNERABILITIES
- INCREASE IN MALVERTISING AND FAKE SOFTWARE
- INCREASE IN CEO FRAUD

BIGGEST CYBER THREATS IN BELGIUM (SOURCE: CCB)

- OPERATIONAL DISRUPTION
- DATA THEFT

TOP 3 ATTACKS BY VOLUME IN THE SPOTIT SOC

- PHISHING
- MALICIOUS CODE
- INTRUSION (ATTEMPTS)

Insights into cyber threats in 2025

HOW DO THEY GET IN? MOST COMMON METHODS (SOURCE: SPOTIT CSIRT)

- EXPLOIT
- EXPOSED SECURITY INFRA
- ACCOUNT COMPROMISE

TOP 4 ATTACKS IN BELGIUM (SOURCE: CCB)

- ACCOUNT COMPROMISE
- RANSOMWARE
- DDOS-ATTACKS
- PHISHING

MOST COMMON ATTACK TYPES BY MOTIVATION IN EUROPE (SOURCE: ENISA)

- RANSOMWARE – FINANCIAL GAIN
- DDOS – IDEOLOGY
- EXPLOITS AND ADVANCED PERSISTENT THREATS – ESPIONAGE

In addition to data from the Centre for Cybersecurity Belgium, the following reports are recommended for further reading:
Unit 42 Incident Response Report 2025, Threat Exposure Brucon 2025, ENISA Threat Landscape 2025, 2025 Report on the State of Cybersecurity in the Union, Internet Organised Crime Threat Assessment (IOCTA) 2025, Unit42 Attack Surface Threat Report, Verizon Data Breach Report 2025.

NIS 2 – ONE YEAR LATER

“An important step for companies’ cyber resilience”

2025 was the first full year in which the NIS2 directive was effectively in force. The European legislation, which was already transposed into national law in Belgium in October 2024, has a major impact on thousands of companies. Dries Wouters, Strategic Architect at spotit, looks back on the first year of NIS2 and outlines where companies stand today.

“Many organizations have already invested in essential security measures and basic protection. Where things often go wrong is in the area of documentation and policy.”

Dries Wouters (Strategic Architect at spotit)

What exactly is NIS2?
“NIS2 stands for Network and Information Security Directive 2, an EU directive that strengthens cybersecurity for essential and important organizations in Europe. In Belgium, this currently concerns around 3,500 companies that have registered as subject to NIS2, of which approximately 1,500 are classified as essential and 2,000 as important. These are companies in sectors that play a crucial role for our society and economy, such as energy, transport, healthcare, water, digital infrastructure, government, and manufacturing. In these sectors, little or nothing can go wrong in terms of cybersecurity, because incidents can immediately have a major impact on the economy and the continuity of essential services. With NIS2, Europe therefore obliges companies to structurally increase their cyber resilience: not only to prevent attacks, but above all to be better prepared when things do go wrong and to limit the impact as much as possible. The legislation does take into account the size of organizations: companies with at least 50 employees or an annual turnover of 10 million euros or more fall within scope, while smaller SMEs remain outside it. In other words: the larger and more critical the organization, the heavier the obligations and expectations in terms of cybersecurity and governance.”

Belgium is often cited as an example. Why?
“Belgium is the only country that has transposed the NIS2 directive on time and quite comprehensively into national legislation. In addition, the CyberFundamentals framework (CyFun) has been developed as a concrete and usable framework to help companies with the implementation. In many other European countries, this is still lacking, which means that NIS2 is less prominent there. That is striking, because Europe’s ambition is precisely to increase the cyber resilience of the entire economy.”

What did Belgian companies have to do concretely over the past year?
“The first step was to register with the Centre for Cybersecurity, so that the government knows which organizations fall under NIS2. After that, companies must take measures to limit their risks and report serious incidents within 24 hours. There is also a strong focus on supply chain risks and on the responsibility of management. Directors are personally responsible for compliance and must even follow mandatory training.”

Where do we stand today in the overall process?
“We are still very much in the transition period. By April 2026, the most critical group must demonstrate that it is actively working on improvements, and by April 2027, organizations must achieve the required maturity level. After the heavy wave of information and registrations at the beginning of 2025, most companies are now in the implementation phase.”

How should they approach this? And how does spotit help them with that?
“We develop a NIS2 roadmap for them. A three-part assessment forms the starting point. First, we organize a risk workshop with different profiles within the organization, from IT and security to management, finance, and marketing. In this way, we map risks from multiple perspectives. Then a self-assessment follows, based on concrete themes, which results in a maturity score per domain. Based on that, we translate everything into a concrete action plan and a feasible cybersecurity roadmap, usually over a period of one to one and a half years.”

What are the biggest challenges in this?
“Many organizations have already invested in essential security measures and basic protection. Where things often go wrong, however, is in the area of documentation and policy. That is why, in a NIS2 assessment, we always look at two aspects. On the one hand, there is the policy side: is there a formal and documented framework that describes what must happen, when, and why? On the other hand, we look at the implementation: how well are those measures set up in practice, are they complete, and are there no gaps? Especially in organizations with lower maturity, we see that the technical implementation is often reasonably okay, while the documentation lags. Backup and recovery are a typical example of this. Many companies make a backup every night, but have never explicitly determined which data are most critical to them and how quickly they need to be operational again. If you cannot afford a full day of data loss, a nightly backup is not sufficient. You also need to think about frequency, recovery procedures, and available reserve capacity. Making backups is, of course, necessary, but without a well-thought-out strategy around recovery and continuity, it is insufficient.”

Is NIS2 the end point?
“Absolutely not. NIS2 fits into a broader European movement; the Cyber Resilience Act and the AI Act are also on their way. Cybersecurity is increasingly becoming a fixed component of legislation. The mindset is shifting from purely protecting and avoiding to being prepared for incidents and being able to recover quickly. That is what cyber resilience is really about. To support organizations in this, we at spotit offer different forms of services. We help companies strategically with consultants who work with them to develop policies around information security, network security, and business continuity. In addition, our managed services take over part of the operational burden. If, for example, a firewall detects something, we follow that up 24/7 for the customer. This can be complemented with technological support and implementation services, where our engineers set up or fine-tune systems correctly. Through that combination, organizations gradually grow towards a higher level of cyber resilience.”

“Cybersecurity is increasingly becoming a fixed component of legislation. The mindset is shifting from purely protecting and avoiding to being prepared for incidents and being able to recover quickly. That is what cyber resilience is really about.”

Dries Wouters (Strategic Architect at spotit)

ZUIDNATIE WORKED WITH SPOTIT ON A FEASIBLE NIS2 ROADMAP

“From assessment to a concrete roadmap”

Logistics service provider Zuidnatie has been investing very actively in cybersecurity for years. The company has already been working with spotit for quite some time, both in security and networking. So when NIS2 appeared on the agenda, it was logical to involve that same partner. “To be honest, the whole NIS2 story caught the company a bit off guard, with more than a hundred requirements that an organization has to comply with. That simply cannot be achieved overnight,” says Floris Verswijvel, IT manager at Zuidnatie. “Many fellow IT managers, even outside the sector, were struggling with the same questions. The technology is often already present within organizations, but the formal documentation of all policies and procedures is much less so.”

Spotit started the process with a thorough NIS2 assessment. The results were translated into a roadmap that was discussed with senior management. “In one go, that made it clear which direction had to be taken in order to achieve the NIS2 objectives. What are the priorities? How can the process be divided into manageable phases? What are the quick wins and what are more like nice-to-haves? That approach ensured that, with a realistic effort, value could still be created quickly.”

What Zuidnatie particularly appreciates is the pragmatic way in which spotit approaches this. “The team not only has the expertise to provide direction, but also takes into account who the company is as an organization. It looks at what is already present in the IT environment and how existing solutions can be incorporated into the process,” adds Verswijfel.

Today, Zuidnatie is actively working on around fifty action points within the NIS2 framework. The goal is first to comply with the ‘important’ level and then continue to grow towards the essential level, which the company is legally required to meet. “The end result is not just a paper exercise. It is an approach that not only helps the organization become compliant, but also truly contributes to its day-to-day operations,” Verswijvel concludes.

CASE

At Roger & Roger, crunchy chips, rock-solid security

Roger & Roger is a dynamic Belgian company best known for Croky, but its activities go far beyond chips alone. Today, the group combines two key pillars: chips and snacks, and frozen vegetables. **With five factories operating 24/7, IT is vital.**

The strong growth of Roger & Roger also brought new challenges. Its existing infrastructure, built around an MPLS network and one central firewall, was no longer sufficient. **There were multiple challenges.** The company had to find a balance between synergy and risk and make choices about the focus of the internal IT team. On top of that, there was the distinction between the office environment and the factory.

In March 2022, the collaboration with spotit began with a whiteboard session in which the segmentation of the network was mapped out. From that session, a roadmap emerged, broken down into manageable work packages. That made the migration controllable and the costs predictable. **The approach went beyond firewalls alone.** Dedicated management zones were introduced, along with vendor and supplier access, a revision of URL filtering, and new policies to clearly separate IT and OT.

In 2023, all sites were connected to the spotit Network Operations Center and Security Operations Center, which brought 24/7 monitoring and operational support. **The migrations took place in a production context where every minute counts.** During the firewall migration in Mouscron, spotit was given exactly ten minutes of downtime. In the end, the team succeeded in carrying out the intervention without anyone noticing. “Trust is extremely important,” says Group IT Director Koen Van Ceulebroeck. “We tested spotit, and spotit proved its value. That trust is the basis of the collaboration.”

Over the coming years, the focus will be on **further strengthening and standardizing the group’s digital foundations** so that all sites operate according to the same best practices. At the same time, the company continues to build towards an even higher level of IT and OT visibility in order to detect risks even faster.

“We had to perform factory resets, replace certificates, and rebuild tunnels. Those are the kinds of things that keep an IT director awake at night. But thanks to the collaboration with spotit, everything could be done without impacting production.”

Koen Van Ceulebroeck (Group IT Director at Roger & Roger)

EMPLOYEE PERSPECTIVE

Peter Vanagtmael
Presales Architect

“We listen carefully to the needs of the customer and match them with the best possible solution within budget. We strive for perfection and always go the extra mile.”

OUR SPECIALISTS PUT IT TO THE TEST

Can your company withstand a cyberattack?

Ethical hacking, pentesting, penetration testing: these are terms you hear more and more often in the world of cybersecurity. In essence, it all comes down to one thing: proactively testing how strong your digital defenses really are. Ethical hackers simulate realistic attacks, uncover vulnerabilities, and help organizations adjust their security in time. How does this work in practice? Keanu Nys, Ethical Hacker and Offensive Security Lead at spotit, explains.

Read the frequently asked questions about pentesting here

"A penetration test is essentially a controlled, realistic cyberattack in which ethical hackers look for weak spots within a predefined scope. We simulate what real attackers would attempt, but in a safe and controlled way, and with one objective: to make your security stronger. All findings and recommendations are included in a clear pentest report, which organizations can use to make targeted improvements."

The benefits are clear: a pentest increases your security maturity, provides insight into your resilience, and shows which vulnerabilities an attacker could exploit. By testing proactively, for example before a new application goes live, you avoid surprises and keep your security structurally at the required level.

Different types of tests

Spotit offers a wide range of penetration tests, each tailored to the specific needs of an organization.

1. For an **external infrastructure test**, our specialists map the public attack surface and investigate whether someone from the Internet can gain access to systems or data.
2. In an **internal infrastructure test**, we examine what is possible once an attacker has already gained access: from lateral movements to privilege escalations. What can someone do with a lost laptop? How far can an employee with limited rights get? And how secure are the 'crown jewels' in the event of an internal attack?
3. In a **physical penetration test**, we investigate whether an unauthorized person can gain physical access to secured areas, ranging from office buildings to server or production sites. Depending on the scope, we simulate techniques such as tailgating, impersonation, badge cloning, or lockpicking to assess how far an attacker could get.
4. In addition, we carry out **web application penetration tests** on, among others, customer portals, e-commerce platforms, APIs, and SaaS solutions.
5. Finally, in cloud migrations it is crucial to verify whether the environment has been configured correctly and securely. **Spotit analyzes Azure and Entra ID environments** for vulnerabilities such as unprotected storage, exposed services, and overly broad access rights.

What many people do not know is that operational technology (OT) can also be a candidate for penetration testing. "In industrial environments where IT and OT come together, outdated systems often remain vulnerable. We test segmentation, industrial networks, wireless systems, and even physical access security to uncover risks at an early stage," concludes Nys.

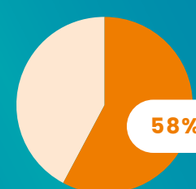
RESEARCH

6 out of 10 corporate passwords can be cracked within an hour

6 out of 10 Belgian employees (58%) have a password that cybercriminals can crack within an hour. This is shown by a study conducted by our team of hacking experts. They carried out the password strength study among 67,557 employees from various small and medium-sized enterprises and multinationals. Very short passwords, in which the company name is combined with a year, are particularly popular.

"People use a password that is very easy to remember, but that comes with considerable risks," says Keanu Nys. "They often rely on predictable patterns, especially in a work context, which makes it very easy for attackers to guess a password. The combination of the company name with a year or seasonal combinations is therefore frequently used.

We especially see the latter when passwords have to be changed every three months. We also advise against setting a short expiration period for passwords. Instead, choose a strong and long password that remains valid much longer, to prevent users from falling back on a simple variant that is easy to remember."



AS MANY AS 58% HAVE A PASSWORD THAT CYBERCRIMINALS CAN HACK IN THE BLINK OF AN EYE.

SOME CUSTOMERS SHARE THEIR EXPERIENCE

"The pentester came across as very knowledgeable and explained the different cases in a clear and structured way. Everything was also supported with clear screenshots."

Steve Detremmerie (Technical IT Manager at Grandeco Wallfashion Group)

"The results of the pentest were particularly valuable: several critical vulnerabilities were uncovered, and their report contained clear advice on how these could be remediated. We therefore highly recommend spotit for testing your IT infrastructure."

Sam Vandevelde (Head of IT at Verhelst Group)

“People management and coaching are not side issues here”

People management has a prominent place at spotit, not as a supporting process in the background, but as an essential part of how people collaborate, grow, and feel good in their jobs. Sanne Vinck, Head of HR, explains.

What, in your view, characterizes the culture at spotit?
“For me, it is mainly the balance between clarity and care. Expectations are clear, feedback is not a one-time moment but an ongoing conversation, and support is always close at hand. That creates a safe working environment in which people dare to speak up, take responsibility, and help shape their own development. It also ensures that everyone feels treated fairly and equally.”

How do you view growth, both for people and for the organization?
“For us, growth is not a checklist or a trend. It is about sustainable relationships, about moving forward together in a way that remains achievable. Careers rarely follow a straight line, and they do not have to. It is a journey with different phases. At spotit, we try to go through that journey together, with attention to the work, but also to the person behind the role.”

For you, people management is not a side issue. Why is individual coaching so important?
“Because good work starts with people who feel supported and understood. For us, people management is not separate from day-to-day reality. It is embedded in how we collaborate, how we define expectations, and how we engage in conversation with one another. When people know where they stand and feel there is room to grow, that naturally also benefits the work.”

How do you put that into practice?
“We try to create an environment in which expectations are clear and conversations can take place openly. That requires structure, but also closeness. People need to know what is expected of them, but also feel that they are supported along the way. That combination makes the difference. That is why, over the past year, we have strongly focused on the role of middle management. From HR, we worked closely with them to develop a clear approach in which they actively and proactively follow up with their team members, at least on a quarterly basis. This does not only cover performance, but also how someone is feeling, the goals they want to set, and where they want to grow. We support this process and have streamlined it so that everyone in the organization works according to the same principles. In this way, we create consistency without losing the personal aspect.”

You apply one approach, but with room for individual paths. How do you reconcile the two?
“No two careers are the same, and they do not have to be. We work with a shared framework that provides clarity and equality within the organization. At the same time, we leave room for personal ambitions, team dynamics, and individual needs. It is not a rigid straitjacket. We want to provide direction without limiting, and support without controlling. I personally take on the role of a confidential advisor in this, particularly regarding psychosocial matters. People need to know that they have somewhere to turn, even when things are more difficult. That is part of the same vision: taking care of people, in all aspects of their work.”

OT SECURITY REQUIRES ITS OWN APPROACH

One year of spotit OT in practice

At the beginning of 2025, spotit strengthened its activities in Operational Technology (OT) with a specialized team. “Of course, before that we were already working at spotit on connectivity and security in industrial environments. But 2025 was the year in which we set up a separate business unit for this,” says Erik De Nert, Head of Operational Technology at spotit. A look back at the first year.

“Many companies do not realize how much OT is actually present in their organization,” says De Nert. “Machines, PLCs, sensors, but also wireless networks, HVAC installations, warehouses and logistics systems: everything is connected today, often historically grown and not always well secured. And all of this while the number of cyberattacks on industrial environments continues to increase.”

Cybersecurity in OT also is about much more than data. “If something goes wrong in IT, perhaps a server goes down or no one can send emails. In OT, the consequences are much bigger: production coming to a standstill, impact on product quality and risks for the safety of people or for the environment, for example in industries such as shipping, energy or nuclear power.”

These risks are further increased by the nature of OT systems. “We often work with environments that are decades old, with protocols that were never designed to communicate with IT or the cloud. At the same time, we see a strong drive towards digitalization: companies collect more data, use AI and connect systems. That exposes vulnerabilities, while you cannot simply patch or shut down those systems for updates.”

A traditional IT approach is therefore not sufficient for production environments; they require a different mindset and different technology. At spotit, we work around three pillars: we focus on cyber-secure, manageable and compliant production environments.

Awareness as a first step

“We notice that our OT focus resonates with customers that have production environments,” he reflects on the first year. “On the one hand, we received questions from companies that are still at the very beginning and wonder how to start such an OT project, and, on the other hand, also from organizations that are already further along and come to us for an OT SOC. As a result, we are now working on OT projects across our entire portfolio. The customer base is very broad, from food and pharma to energy, ports and logistics.”

The starting point of an OT trajectory? Awareness. “That works in two directions: IT teams must understand what is happening in production environments, and at the same time people in production must be aware of potential risks. After that, we map all systems. Which ones are connected to what? What vulnerabilities are there? And how do networks communicate with each other, towards IT and towards the outside world? In addition to that technical aspect, there is also an organizational aspect, because external suppliers also play an important role. Through a scan, we map the systems in the production environment, draw up a report and, based on that, develop a concrete action plan and roadmap. The next crucial step is usually separating IT and OT networks through firewalls. By segmenting those environments correctly, you already cover a large part of the risks.”

Mathieu Millecam (Head of OT Architecture) and Erik De Nert (Head of OT)

2026: remote access and OT monitoring

Remote access is a hot topic for many companies, they notice at spotit. “In almost every conversation, it comes up. Remote access is one of the main ways attackers get in. About 50 percent of cybersecurity incidents occur through some form of uncontrolled external access, often without multifactor authentication. Moreover, production environments work with many different suppliers who need access. That access must be controlled, but it must also not become so complex that people start bypassing it. Traditional IT solutions often fall short in this regard. That is why at spotit we work with OT-specific remote access solutions from Xona and Cisco. We deploy their solution for third-party and remote access, specifically tailored to OT and cyber-physical environments.”

“In addition, the demand for active monitoring of industrial networks and early detection of vulnerabilities, threats and abnormal behavior is increasing. In an environment where continuity and reliability are crucial, continuous visibility in the OT network is becoming increasingly important. Together with our well-known partners Palo Alto, Cisco and Nozomi Networks, we develop the most suitable solution that offers both visibility and control,” he concludes.

How to do it in practice

“Start with awareness: do you have sufficient knowledge of your production environment and are the right people around the table? Then map your assets, suppliers and vulnerabilities. And start with segmentation from top to bottom: first separate IT from OT and ensure secure and controlled OT remote access. That already covers a large part of the risks.” A solid network foundation is indispensable in this. “Security and network go hand in hand. If the foundation is in place, you can move on to anomaly detection and targeted monitoring. It is therefore logical that companies where we started with the right steps are now already evolving towards permanent monitoring via NOC and SOC.”

CASE

Pemco International strengthens its cyber resilience

For Pemco International, a producer of industrial coatings and enameled glass, **cybersecurity became a strategic priority**. Due to stricter regulations and an increasing threat landscape, the company engaged spotit to strengthen its security. With the Cortex XDR solution from Palo Alto Networks and spotit's 24/7 SOC, Pemco built greater peace of mind and cyber resilience.

"Our furnaces run 24/7. If a critical IT component fails, we cannot simply stop or restart production," says Voicu Potrovita, Global IT Manager at Pemco International. **"IT not only supports our administrative processes, but also directly supports production."**

As a chemical manufacturing company, Pemco falls under European NIS2 legislation, which requires companies in critical sectors to strengthen their cybersecurity. In addition, the American investment firm behind Pemco took out cyber insurance with a number of conditions attached. "It was not a sudden crisis, but rather the next logical step in our evolution. We knew we needed professional support," says Potrovita.

He was already familiar with spotit from a previous collaboration at an earlier employer. When Pemco began looking for a reliable security partner, the choice was quickly made. "We did compare several suppliers, but **spotit clearly offered the right expertise as well as the proximity we were looking for**. They are Belgian, understand our context, and have an excellent reputation in cybersecurity." Spotit proposed not only strengthening the basic security, but also having Pemco's IT network monitored by the spotit Security Operations Center (SOC).

Since implementing Cortex XDR and connecting to the SOC, Pemco has gained greater visibility into what is happening in its IT environment. Alerts are generated for suspicious files or unusual data flows, allowing the company to respond more quickly. More importantly, **the IT department can operate with peace of mind**.

"Cybersecurity is a continuous game of cat and mouse. Today we are better protected than yesterday, and tomorrow we will be even stronger. With spotit, we know we are not alone in that evolution."

Voicu Potrovita (Global IT Manager at Pemco International)

"Figures are important for trust"

They mainly work behind the scenes, but the finance team plays a crucial role in keeping everything running smoothly. The team of six is responsible for everything related to orders and finance. "In this way, we form an important link in the journey toward a strong customer experience," says Martine Theunis, Head of Finance.

A large part of our work revolves around orders. Everything that sales sell to a customer, we correctly convert into an order. We prepare the purchase order, follow up on the delivery, and ensure that the necessary materials are available on time. We also take care of license renewals.

In addition, the finance side also falls under our responsibility. Purchase invoices come in via Peppol, are checked by us, and placed in an approval flow. Every Thursday, we carry out payments so that suppliers are paid on time. We prepare sales invoices, answer customer questions about them, and follow up on payments. In addition, we, of course, also take on all statutory tasks, such as VAT returns, corporate income tax, and other administrative obligations.

To keep everything running smoothly, we regularly collaborate with other teams within spotit. For example, when there are questions about an invoice, we consult with sales or with the service managers. For registered and invoiced hours, we are in contact with the people from planning and operations. In addition, every month I prepare a report for the executive committee, so that they can make the right decisions and, if necessary, adjust.

One of the biggest challenges is to present the right figures as quickly as possible each month. This already starts with the sales invoices, which must be sent out correctly and on time as soon as we have closed the month. As the company grows, the number of purchase invoices also increases, and these must be processed quickly so that our analyses remain accurate.

The beginning of the year is always particularly intense. In January, we close the financial year, and in the last week of that month the auditor already comes by. By then, all figures and details must be available and everything must be reconciled. It is checked whether everything has been recorded correctly, and revenue is also verified based on the hours registered by employees. In February, we start a new financial year.

An important milestone each year is submitting the annual accounts on time. Reporting correct figures on time remains essential, so that customers can see that we are performing well and trust in our company continues to grow.

Outstanding performance thanks to a strong team

Every day, our employees help build the future of our organization and of our customers. Get to know our different teams:

MANAGED SERVICES

- **SOC team:** our Security Operations Center monitors and protects customers' IT environments 24/7 against threats, with real-time detection and response.
- **CSIRT:** a dedicated team that responds quickly and expertly to security incidents to minimize impact.
- **NOC team:** manages and optimizes network performance and uptime through a proactive, problem-solving approach.

DOMAIN EXPERTS

- **OT-team:** focuses on the security and connectivity of industrial systems, with expertise in the unique challenges of OT environments.
- **Offensive team:** performs ethical hacking tests and vulnerability assessments to strengthen systems against potential attacks.
- **Consulting team:** helps organizations manage risks, ensure compliance, and develop a robust security strategy.

TECHNOLOGY

- **Internal IT Operations team:** ensures our employees have access to top-tier tools to deliver productive, high-quality work.
- **Service Excellence team:** combines development and operational expertise to deliver fast, reliable, and scalable solutions. The team includes **DevOps** (automating repetitive processes and tasks for the benefit of customers and spotit colleagues), **Data Science** (analyzing existing data from customers and spotit and translating it into actionable reporting) and **Platformation** (configuring the IT ticketing system and continuously improving ticket handling processes).

OPERATIONS

- **Architect team:** translates networking and security challenges into tailored technological solutions.
- **Projects & Service Management team:** implements customized solutions for complex IT projects, from start to finish, with a strong focus on quality.

SALES & MARKETING

- **Presales, Sales & Marketing, Service Development team:** connects customer needs with spotit solutions through a customer-focused approach and persuasive communication.

STAFF

- **HR team:** is committed to attracting, developing, and supporting talent, with a focus on a stimulating and positive work culture.
- **Finance & Orders team:** ensures financial stability and growth through accurate planning, analysis, and strategic management.
- **Legal:** clear agreements (on paper) make for strong relationships.
- **Facilities & Reception:** ensures a high-quality office environment and a warm welcome at all times.

Interested in joining our team?
jobs.spotit.be

Our partner ecosystem

Our strategic technology partners

We believe in the power of collaboration. That is why we deliberately choose technology partners that are among the top in their field. Each of them combines innovation and quality and, like us, is committed to sustainable solutions. Through these strategic alliances, we build long-term relationships that benefit our customers—today and tomorrow.

Our academic partners, industry associations, and network organizations

As a specialist in cybersecurity and networking, we take our role within the broader ecosystem seriously. Through our memberships, we not only stay up to date on technological and regulatory developments, but also actively contribute to the future of the industry. In this way, we help build a strong, innovative, and resilient business environment.

Our valued customers

Many organizations in Belgium rely on us. And we are proud of that.
Below is a selection:

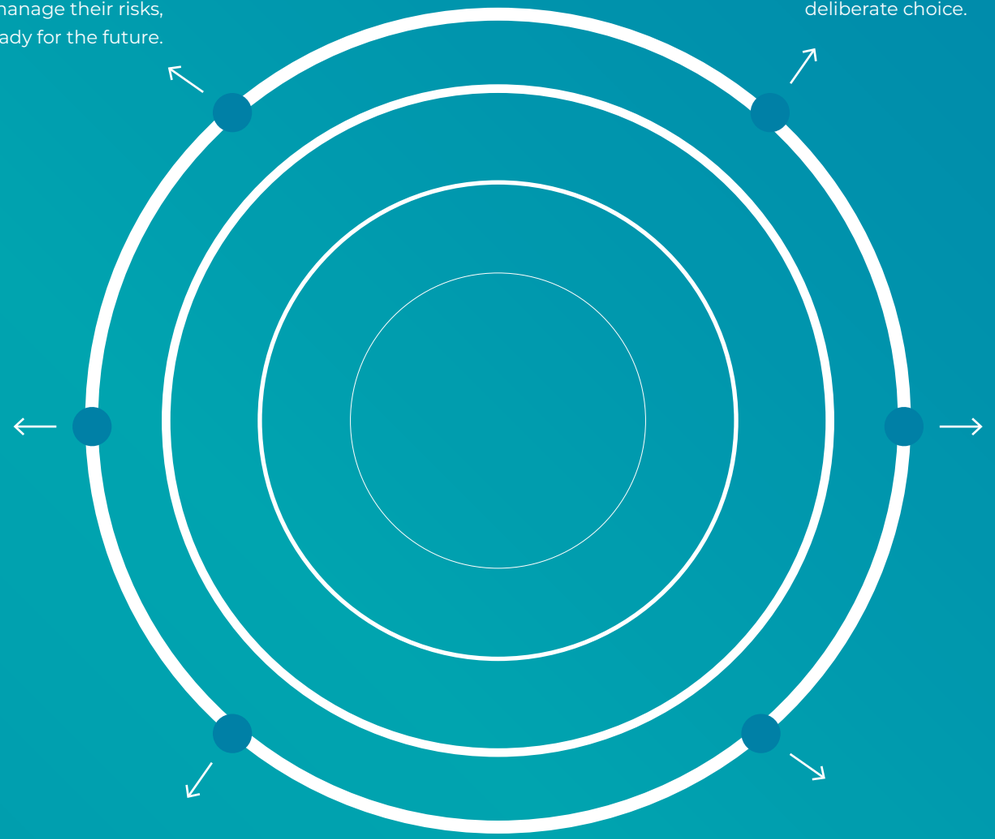
Discover more of our customer references on our website:

EMPLOYEE PERSPECTIVE

Priorities for the future

Stronger focus on governance, risk & compliance
Governance, risk management, and compliance (GRC) have been a core part of our services for years. With an **experienced team of specialists**, we support customers across a wide range of sectors. Today, GRC is becoming increasingly important, especially with the introduction of NIS2 and ever stricter regulations. That is why we are making targeted investments in further expanding our GRC activities. This allows us to remain a trusted partner for companies that want to manage their risks, strengthen their compliance, and be ready for the future.

Peace of mind thanks to our 100% Belgian SOC and NOC
For ten years, we have distinguished ourselves with a **unique combination of SOC (Security Operations Center) and NOC (Network Operations Center)**. While many providers focus solely on cybersecurity, we also offer the underlying network expertise that is essential for a strong security approach. Because real security starts with a stable, high-performing network. Moreover, all our services are **100% Belgian**. In times of geopolitical uncertainty, this provides many customers with peace of mind and is a deliberate choice.



Stepping up OT Security & Networking
Operational technology is the beating heart of industries such as logistics, manufacturing, utilities, and pharma/life sciences. Yet OT networks often do not receive the attention they deserve. To address this, **we are strongly investing in OT Security & Networking** through a dedicated business unit. In doing so, we provide our customers with the specialized knowledge, approach, and technology needed to make their operational systems both future-proof and cyber-secure.

Strong growth in the public sector
Until recently, we were less visible in the public sector, but that is changing rapidly. We are strongly focusing on **collaboration with governments and organizations in healthcare and education**. An important milestone in this is our partnership with Shield vzw, a collaborative initiative that supports institutions in healthcare and higher education in setting up and managing a high-performing and secure cybersecurity architecture. With our solutions and expertise, we are actively contributing to a digital and resilient public sector.

Fast and effective support during cyber crises
With our CSIRT team (Cyber Security Incident Response Team), we are ready to support companies during digital incidents and crisis situations. But we go one step further. **We are expanding our offering with offensive security**, in which—always in consultation with the customer—we simulate targeted attacks. This allows us to identify vulnerabilities before real hackers do. For this new business unit, we have appointed an experienced expert, enabling us to proactively strengthen our customers' defenses against cyber threats.

Cyberwolf accelerates internationally
Over the past years, Cyberwolf has built a strong customer portfolio in both North America and Europe. We now want to further accelerate that **international growth**. Until now, we have deliberately operated under the radar. But the next step is clear: increasing our visibility, without losing our characteristic discretion. Cyberwolf remains a quiet force – but one that is making an ever-greater impact.

10 TIPS

for greater peace of mind in cybersecurity and networking

Gain a clear overview of your IT landscape.
Start with a complete and up-to-date overview of your assets: devices, applications, data, and users. Identify where the biggest risks are and address those first.

01

Build a strong security foundation.
Conduct a thorough security audit and immediately resolve critical vulnerabilities. A solid foundation prevents small problems from becoming major incidents.

02

Limit access according to the zero trust principle.
Trust no one automatically, not even within your own network. Only grant access based on need, role, and context.

03

Implement multi-factor authentication.
Protect all critical accounts and externally accessible systems with MFA. It is a simple measure with a major impact on your security.

04

Segment your network and actively protect zones.
Ensure a clear separation between IT and OT environments and inspect traffic between zones using next-generation firewalls.

05

Keep systems up to date with patch management.
Inventory vulnerabilities, automate updates, and ensure a structured patch management process to close gaps in your security quickly.

06

Protect data with strong encryption and backups.
Encrypt sensitive data, both in transit and at rest. Combine this with a well-thought-out backup strategy and a tested recovery plan.

07

Invest in monitoring and detection.
Build operational capacity to monitor your environment continuously. With 24/7 oversight through a SOC or automated tools, you detect incidents faster and limit the impact.

08

Make people co-responsible.
Raise awareness and train employees on phishing, social engineering, and safe online behavior. Human awareness remains a crucial layer of defense.

09

Embed cybersecurity in your operations.
Work on clear security governance, incident response procedures, and continuous follow-up. Integrate risk management into your daily operations and improve step by step.

10

More information? Contact us!

Ready to discuss your networking and security needs?

We are always available. Do not hesitate to contact us for a no-obligation conversation and a good cup of coffee. Visit us at one of our offices, or schedule a meeting with an expert.

www.spotit.be
+32 (0)9 322 04 44
info@spotit.be


spotit
YOUR SECURITY & NETWORK LAYER