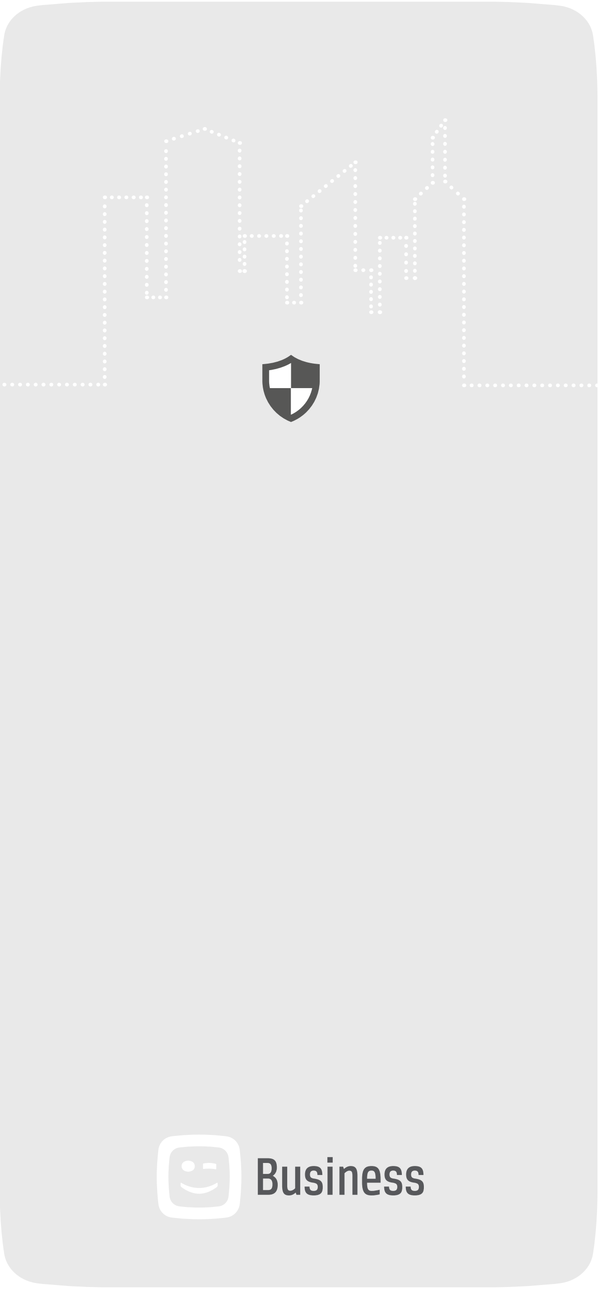
Business

IT-SECURITY IN 2016

More than ever at the heart of every company


Business

FOREWORD

“IT security is like insurance. You don’t need it. Until something bad happens”

Fire, theft, industrial accidents ... Every company is well aware of the need for good insurance. And, admittedly, you’re not always happy when it comes to paying the premiums. But the moment you’re up against it, you’re certainly glad you’re insured.

It’s no different with IT security. It may sometimes seem hard to justify the investment, but if you fall victim to things like hacking, a DDoS attack or ransomware, the consequences can be very serious. For your business operations, your financial situation and your image.

Even though we all know that prevention is better than cure, IT security is all too often resorted to as a reaction to a problem or situation. Companies often hold off too long before investing in proper security.

We hope that this brochure will convince you that acting proactively can save you a lot of expense and problems. That IT security is no longer an IT matter, but is above all a business issue. Our specialists set out the context and threats of today’s world and give you insight into our security approach.

Enjoy.

Martine Tempels
Senior Vice President – Telenet Business

1. From reactive to proactive
2. Threats are getting more advanced
3. Technology's getting better
4. Numbers of DDoS attacks on the up
5. The useful life of hardware is getting shorter
6. Perimeter security is no longer enough
7. IT security is becoming a priority for everyone

EXECUTIVE SUMMARY

7 trends in the field of IT security

1

From reactive to **proactive**

When we look at the trends in IT security, the most salient is probably the rise of proactivity. In the past, reaction often only came after an incident, but that kind of reasoning no longer holds water. The proactivity of both the technology and the approach of integrators is increasing as time passes. In the context of business continuity, more and more companies are adopting this proactive approach.

2

Threats are getting **more advanced**

The threats facing your company are increasing not only in number but also in complexity. Did you know that 27% of all malware was developed in 2015 alone? And that malware adapts, so that traditional anti-malware systems can't detect it? Just as worrying is the fact that SSL traffic – till recently a cradle of safety – is increasingly misused and that hackers are getting smarter in devising social engineering techniques and clever tools.

3

Technology's getting better

Fortunately, it's not just the threats that are advancing, but the product developers' technology and solutions are also keeping pace. Although the latest malware is assuming countless forms, it always relies on around 20 'exploitation techniques'. Today's security technologies therefore no longer recognise malware based on signatures, but look much more at its behaviour.

4

Numbers of **DDoS attacks** on the up

Another, very perceptible, trend is the rise in DDoS attacks. They're more frequent, getting more intense and are being launched with greater stealth. In the most virulent DDoS attack measured to date, no less than 602 Gb of data a second was transmitted. DDoS attacks often comprise different types of assault, are used simply as a decoy for other forms of attack, or both.

5

The **useful life** of hardware is getting shorter

New threats mean that security hardware is getting outdated faster. Firewalls, for instance, are expected to perform much more than, say, five years ago. They include new features like sandboxing, antivirus or Intrusion Prevention Systems (IPS) and process more traffic because they now also have to scrutinise SSL traffic. Firewalls used to be sold with around a 10 to 20% annual growth margin, a figure that's much too small nowadays.

6

Perimeter security is no longer enough

It used to be enough to secure the IT outer wall, setting a 'bulwark around the company'. Increasingly, threats are spreading from the inside, which means that internal infrastructures have to be thoroughly secure. Not just north-south traffic (between clients and servers), but also east-west traffic (between servers themselves) has to be scrutinised and secured. Like an onion, the best security is made up of a series of layers.

7

IT security is becoming **a priority** for everyone

Because business-critical assets are generally becoming digital, governance, risk management and compliance are assuming huge importance. The famous 'CIA' of business continuity (confidentiality, integrity and availability) has to figure high on companies' priority lists. Especially if you realise that the law is also getting stricter on that score. For instance, the end of 2015 saw the first steps being made towards an unequivocal, harmonised IT security policy in Europe.

Learn how today's business context creates challenges for every company.

CHAPTER 1

> *“Shadow IT is certainly not new, but the arrival of the millennials and the cloud means it has increased exponentially.”*

Lore Mattelaer
Security Business Development Manager at Telenet

CHAPTER 01

- As time passes, more assets and companies are becoming digital
- The new workforce generation
- Shadow IT, IT's paths of least resistance
- Towards a clear, harmonised legal framework

The challenge posed by the new corporate context

As time passes, more assets and companies are becoming digital

Business-critical data is increasingly digital in form. Every company collects and processes documents and data digitally, from customer details via payroll information to R&D results. This new context entails a whole raft of risks, making companies more vulnerable than ever. The impact that a single IT incident can have is vast: reputation damage, customers switching to the competition, data loss or loss of sales, all because operations and availability are laid flat for a period of time.

The new workforce generation

Millennials (those born between 1980 and 2000) increasingly determine the pace of the market and the shop floor. They're changing the game rules. They're the first generation of digital natives and that is having a big impact on the world of business. "The influx of the millennials has changed the role of the IT manager and upped its importance," says Andrew Turner, Product Manager at Telenet. "IT managers are increasingly expected to keep pace with the way the business thinks and come up with proactive solutions – their task is no long a reactive one."

Millennials are always connected, are equipped to the eyeballs with the latest technology, use the latest apps and expect their work environment to be at least at a comparable level.

These moves mean that the ways in which companies can potentially be attacked are multiplying. Andrew Turner: "It's true, there are more and more 'gateways' that can get left open. Not just because there are more tools being used in the workplace but, mainly, because millennials pay little or no attention to security. What they want are devices and applications that they can work with fast."

Shadow IT, IT's paths of least resistance

With the cloud there is now an alternative for just about every business application. "And that's not the least of it," says Lore Mattelaer, Security Business Development Manager at Telenet. "In a couple of mouse clicks they're also installed, up and running. Dropbox is less laborious for sharing files than SharePoint, Yammer messages are answered quicker than e-mail. And why use the company's sluggish CRM system when Salesforce is so much easier?"

"Shadow IT is certainly not new, but the arrival of the millennials together with the cloud means it has increased exponentially," says Lore. Shadow IT is all the soft- and hardware that's used within the company but that falls outside the IT department. "And, so, isn't officially approved," continues Lore. "They're the paths of least resistance in the corporate IT infrastructure: staff prefer to cut across the grass if that seems more practical and efficient than taking the secure, but often lumbering, official routes."

The well-worn tracks between the firmly tarmacked roads pose great challenges for IT managers. Of that, Lore's only too conscious: "because it's my job to make sure that all devices and business data are secure. But how do you do that if programs and hardware are being used that you're not even aware of?"

"Today's workers are 'always connected' and that creates a lot of challenges, especially for IT security."

Andrew Turner
Product Manager at Telenet

Towards a clear, harmonised legal framework

What if you're attacked? What if one of your staff leaks data? Who's responsible? Do you have a duty to tell? Could you be fined? Isabelle Ghislain, Legal Counsel at Telenet, looks at what the law has to say.

"There are widely differing approaches to cyber security within Europe," Isabelle starts off. "Though member states realise that it's a priority, they're conspicuously inconsistent in how they approach it. They regard cyber security as a national issue, which leads to great differences in policy, statutory set-up and operational capacities."

IN BRIEF

The law in Belgium

- Critical Infrastructures Act
- Cyber Security Strategy
- Privacy Act

The law in Europe

- Network and Information Security Directive *(NISD)*
- General Data Protection Regulation *(GDPR)*

BELGIUM

Critical Infrastructures Act

Belgium operates on the basic principle that each 'professional market player' can and may be expected to have an adequate security policy. Isabelle: "The general rules of the law of liability can indeed imply a 'general duty of security'. For certain sectors, like energy, transport, financials and telecoms, we also have the Act of 1 July 2011 on the security and protection of critical infrastructures. Because they operate what's called a critical infrastructure, the law obliges them to name a security contract person and develop a minimum security plan with internal material and organisational measures."

Cyber Security Strategy

In 2012, the Belgian government also enacted a national Cyber Security Strategy. "It's the government's bid to achieve an internal approach to digital safety," says Isabelle, "but, even in 2016, little information is available on how the strategy has to be implemented in its detail."

Privacy Act

The moment companies process personal details, additional legislation clicks in. Isabelle: "Consumers are not always aware of this but, nearly every day, they reveal their personal details: when they apply for a loyalty card, sign up for a course or take part in a competition. Because consumers generally have no control over what happens to that data, there has been a law since 1992 that sets out how companies have to deal with that information: the Privacy Act."

The Privacy Act says that additional (security) measures have to be taken to provide adequate protection for personal data. Isabelle: "The list of privacy requirements is long, but do-able. For instance, data processing has to be registered with the Privacy Commission and you continually have to respect the rights of the individual in question. The data always has to be correct and up to date, has to be deleted in time, only processed for the pre-defined legal purpose, and access to it has to be limited to authorised persons."

EUROPE

Network and Information Security Directive *(NISD)*

For companies that do not process personal data, data security is often based on 'goodwill': they protect themselves to avoid untoward consequences like reputation damage and loss of sales.

Isabelle expects a certain increase in awareness, nonetheless. "At European level, a lot is happening. At the end of 2015, we had the Network and Information Security Directive (NISD), which attempts to close the gap between EU member states with a harmonised, firmly defined approach to security measures. Belgium is currently working on its transposition into national law."

General Data Protection Regulation *(GDPR)*

On top of this, the spring of 2018 will see enactment of the General Data Protection Regulation. As Isabelle knows, "The new GDPR will bring in a large number of changes. Every company that processes data on European citizens will be obliged to notify privacy incidents to their national authorities. This will extend to other sectors a duty that only exists in the telecom sector in Belgium at the moment. The coming of the GDPR will also bring in new penalties for the first time, which could be substantial in amount, depending on the nature of the incident. Nor can it be overlooked that the GDPR will also mean that companies are expected to conduct a documented privacy and security policy."

ROUND UP

TO INVEST IN SECURITY IS TO INVEST IN CONTINUITY

With the beefing-up of the legal framework, it is more than clear that the importance of IT security is increasing. In the context of business continuity, it's better to know where the threats could come from and what levels your company needs to be protected at. Learn more in the next chapter.

> *"The arrival of the General Data Protection Regulation gives the Privacy Commission power to impose what could be substantial fines."*
>
> Isabelle Ghislain
> Legal Counsel at Telenet

CHAPTER 2

“The key to good security is a clear design in which you take full account of your security policy.”

Glyn Jones
Service Manager at Telenet

CHAPTER 02

- Threats are increasing in number and complexity
- Security is evolving to deal with that complexity

New threats – new forms of security

Threats
are increasing in number and complexity

Threats and attacks come from everywhere. Many companies think that they aren't interesting as targets, but nothing could be farther from the truth. Nowadays, every company's a potential target. First, because attacks are not always aimed at a given company but are a random phenomenon. For instance, hackers are able to detect weaknesses with blunderbuss scans and intrude into your company because you're not properly protected. Second, the victim company is often but a stepping stone to the ultimate target. Hackers are not always interested in your data but in that of your customers or other firms that you do business with. It's nevertheless you that's the victim of the attack.

Here are a few common threats companies need to be prepared for.

Malware

Malware, short for malicious software, is software that's used to disrupt computer systems, steal sensitive information or gain access to private computer systems. It often has the appearance of regular programs or files, but they contain hidden functions that allow access to the infected computer from the outside. Remarkable, but true – no less than 27% of all today's malware was created in 2015, and it constantly adapts. That means that traditional malware protection, which detects malware on the basis of known signatures, will be unable to identify new forms of malware.

Ransomware

Ransomware is a method of blackmail that uses malware. Ransomware blocks the infected computer or the data stored on it and then requires the user to pay a ransom to free the computer or data. Much ransomware works with a deadline and uses powerful encryption to block the system or data. If the company doesn't pay up within the stipulated period – usually via an untraceable payment method such as BitCoin – the decryption key isn't released and the data or system is rendered useless. Regular back-ups of (valuable) data can save companies a lot of anguish.

DDoS attacks

A DDoS attack (distributed denial of service) disables a company's web infrastructure – websites, mail servers and so on. Ten per cent of Belgian companies have suffered a DDoS attack at some time or another. They come in different forms. In volumetric attacks, your infrastructure is inundated with huge quantities of data, thus occupying your full available bandwidth. Applicative attacks are more subtle and target a specific application or server, which is then unable to process the quantity of data and crashes. Protocol attacks hijack network protocols. By sending network packages that don't meet web standards, servers will slow down and even stop functioning altogether.

The clear, inexorable increase in DDoS attacks continued unabated in 2015 in terms of both numbers and complexity. Whereas previous attacks usually stemmed from activists or vandals, the aim is now more to blackmail the target company. At present, more than a quarter of reported attacks involve a scope exceeding 100 Gbps. In the most brutal DDoS attack measured to date, as much as 602 Gbps was transmitted. And complexity is on the up as well: companies have to cope with a combination of attacks in which volumetric, applicative and protocol strategies alternate tag-team-style.

DID YOU KNOW THAT

27%

of all malware was developed in 2015?
And that malware adapts, so that traditional anti-malware detection can't identify it?

10%

of Belgian companies have fallen victim to a DDoS attack at some point?
And the scope of the attacks is on an inexorable rise?

Botnets

All over the world there are computers that are infected unbeknown to their users. Many of these computers combine to form a botnet, a network that can be steered from a single command centre. Botnets are often used to launch DDoS attacks. Botnet computers cause businesses harm because they use up bandwidth and can significantly slow down a network.

Bugs in software and systems

Vulnerabilities are constantly discovered in software. If these weak spots are found, software suppliers quickly develop and distribute patches to stop the gaps. If companies don't install the patches – at all or straight away – they're vulnerable. Because anyone who's aware of the vulnerability can easily exploit it to their advantage.

SSL traffic

Applications and websites often use SSL encryption to prevent their data flows being 'eavesdropped' on by others. SSL certificates change the URL in the address bar to an https protocol, giving web users the impression that the connection to the site is secure. Because increasing numbers of web applications are based on SSL traffic, its share of corporate bandwidth is constantly on the increase, from 20 or 30% to even 40 or 50%.

The problem is that hackers are getting smarter at circumventing SSL security. One way they do so is by means of the 'man-in-the-middle' principle. Web users entering a website address usually first go to the http address before switching through to the https site. It's at that moment, just as the secure connection is supposed to be established, that the hackers intervene and connect the user with the server that's under their control. User and server alike think the connection is secure, whilst the hacker can now easily eavesdrop on the traffic.

In addition, SSL traffic is increasingly used to conceal malware, meaning the malware can be sent and received unseen because very few companies decrypt their SSL transmissions and scrutinise it in the SSL tunnel. The great danger with SSL traffic is that companies all too often assume it's secure, and only apply their policies to non-SSL traffic.

Shadow IT

Although for the most part innocent and, in many cases, just what's needed to promote productivity and innovation, shadow IT can also be the source of a host of disadvantages. Continuity and, above all, security are hard to guarantee. Data leaks are often the result of initiatives that IT managers never gave approval for and never even had any knowledge of. The damage stems mainly from failure to adhere to requirements and because new processes are created that don't abide by existing rules. Shadow IT is therefore something that most IT managers would prefer not to see within their organisation.

DID YOU KNOW THAT

HTTPS

companies all too often assume that SSL traffic is secure? And therefore only apply their policies to non-SSL traffic?

The human factor in your business

People are the weakest link when it comes to IT security, and that even applies at a variety of levels. At level C, there are threats because IT security frequently isn't a priority. Setting funds aside for security is certainly not without its returns. The outlay may not raise new income for companies, but it can staunch a leakage of resources. Even when money is set aside, there's often no uniform policy identifying which data is sensitive and there are no policies setting down what the company allows, and what not.

Plus, there's more to it than policies. The real difficulty lies in turning them into practice. Even the staff can, unwittingly, create security gaffes for the company. They can invite malware in by visiting the wrong websites or using an infected flash stick. Phishing is very much on the rise, for the very reason that people click on links without stopping to think. Passwords can also be an easy port of entry for hackers. Even when staff use a secure network, stealing passwords is not all that hard. Hackers lure workers to a copy of a web page and, without even using malware, get to know their passwords. Awareness is the only way to make staff attentive to these kinds of risks.

Social engineering

Social engineering, or social hacking, is a collective name for the techniques by which hackers dupe people into carrying out acts or divulging information. The best-known form of social engineering is without a doubt phishing. Even though phishing e-mails are often so badly made that it's clear they're phony, they still bear fruit for fraudsters simply because they're sent to so many millions of people.

More worrying for companies is the sharply increasing craftiness that criminals are able to muster. Spear phishing is the targeted form of phishing: perfect fakes targeted at specific people. They're so well done that they can hardly be recognised as fakes. Perhaps an e-mail that appears to come from a colleague or a company you work with. Much preparation has often gone into such e-mails, such as researching the company's organisational chart.

On top of that, it can just as easily involve e-mails from people we don't know. HR departments are frequently sent CVs, which it's their job to open and examine. Hackers therefore just need to pick a vacancy, prepare a CV that looks perfectly normal (easy using a public LinkedIn profile) and, when HR staff open the file, malware gets installed and the hackers are into the network, financial data, R&D info and so on.

DID YOU KNOW THAT

.pdf is the prime means for a perfectly camouflaged attack?
.pdf files are ubiquitous and seem innocent, but have a great deal of potential for harbouring concealed code.

Security
is evolving to deal with that complexity

IT security is sometimes likened to a boiled sweet: hard on the outside, but with a soft centre. The outside, or perimeter, is well protected with things like firewalls and monitoring but, on the inside – the internal infrastructures – security measures are limited to the minimum that's absolutely necessary.

"Today's security goes far beyond the perimeter," says Patrick Lecluyse, Manager, Professional Services, at Telenet. "You can have perfect protection for your front door but still have the back door standing wide open. The best security is structured like an onion, in numerous layers. By securing the network, the data centre, the cloud and the endpoints, all the doors are closed, not just the front door. That approach ensures that the centre of the sweet is also a hard nut to crack."

"The key to good security lies in a clear design in which you take account of your security policy," adds Glyn Jones, Service Manager at Telenet. "Sometimes, the client's focus homes in on replacing the hardware, not improving security. The choice of solutions of course depends on the type and size of the business: SMEs, for instance, can make do with just a firewall; companies that do a lot of online operations also have to ensure security for endpoints and applications in addition to their network, and must also arm themselves against DDoS attacks. Our consultants help clients by thinking proactively about what angles they need to cover."

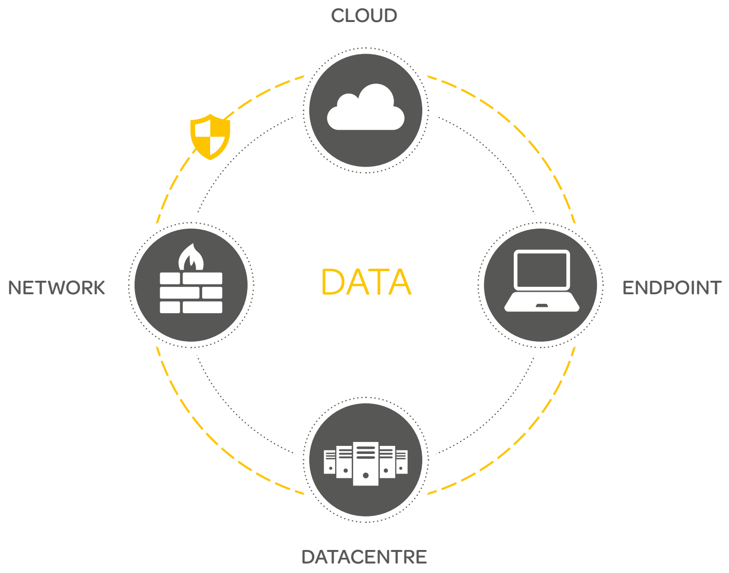
Below, we graphically compare the old way of approaching IT security to the new-school vision.

"The best security is structured like an onion, in numerous layers. The perimeter can't be the only form of security."

Patrick Lecluyse
Manager, Professional Services, Telenet Business

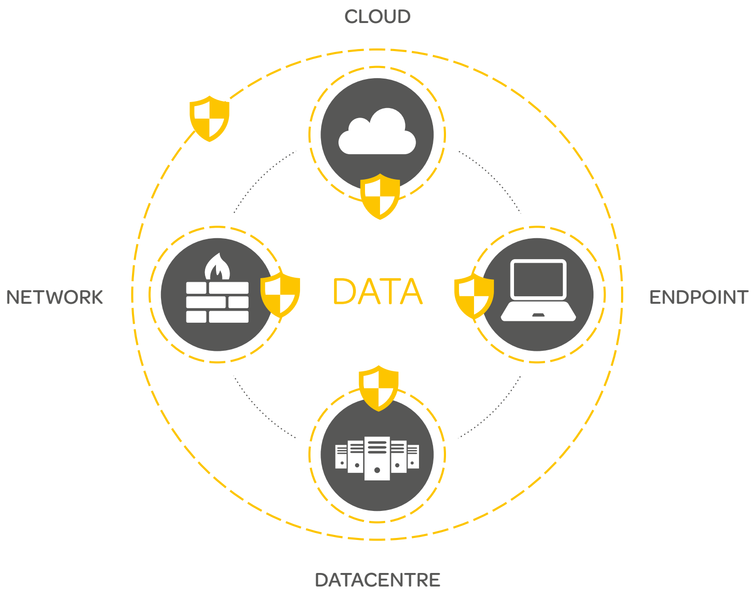
OLD SCHOOL I IT SECURITY LIKE A BOILED SWEET

Hard on the outside, with a soft centret



NEW SCHOOL I IT SECURITY LIKE AN ONION

Built with a multi-layered structure



Learn how the technologies are evolving at different levels to offer a defence against today's threats.

Network

In recent years, networks have become much more vulnerable because of their increased complexity, the rise in personal and business applications, user behaviour and the new threats. “Network segmentation offers a defence to these challenges,” says Nico Vandevoort, Security Presales Consultant at Telenet. “With network segmentation, the network is divided into a number of sections with connections between the different sections being controlled by a firewall. This restricts the risks and the effects of an attack on the network to a single section, and so prevents the entire network being jeopardised.”

“In addition, next-generation firewalls can also save a great deal of tears,” continues Nico. “Features are constantly being added to protect the network better. Sandboxing and intrusion-prevention systems (IPS) are two examples. Sandboxing allows you to scan suspect files for malevolent behaviour in a separate (cloud) environment. The file is sent to the sandbox and its behaviour simulated. If suspicious operations occur, you know something’s not right. Intrusion-prevention systems, on the other hand, monitor the network traffic for malevolent activity and ensure that known vulnerabilities are not exploited.”

Datacentres & cloud

New datacentre technologies such as cloud computing have radically changed the typical IT infrastructure. Nico Vandevoort: “This has also changed the security aspect. Until recently, it was important in datacentres to scrutinise and secure the north-south traffic, between clients and the server. We’re now seeing an increase in the traffic between servers themselves, which demands enforcement of a policy between servers: in what we here call east-west traffic, it has to be explicitly defined what’s allowed and what’s not. Whereas a physical firewall used to be enough to enforce policies between clients and the datacentre, that falls short of the mark nowadays. To enforce a policy between servers, you now also need firewalls within the virtualised environment.”

> *“Features are constantly being added to next-generation firewalls to protect the network better, such as sandboxing and intrusion-prevention systems (IPS).”*
>
> Nico Vandevoort
> Security Presales Consultant at Telenet

Endpoints

To protect themselves against modern cyber attacks, companies also have to adopt a new approach to securing endpoints. Kris Bogaerts, Security Consultant at Telenet: "This is a trend that hasn't escaped the attention of the big vendors, either. For instance, Palo Alto Networks and Check Point have brought two systems onto the market, Palo Alto Traps and Check Point SandBlast Agent, to protect endpoints better than ever."

Both of these technologies put companies in a position to react appropriately to both current and future threats. Kris explains: "Palo Alto Traps offers advanced endpoint protection against the most sophisticated threats. No longer by using a signature database – like traditional antivirus – but by seeking out a number of core techniques that attackers might deploy. Traps identifies the techniques used as a means of attack and then puts a stop to them. Check Point SandBlast Agent takes a different approach, implementing existing gateway functionality to the endpoints. It focuses on the strong integration between the protection by the gateway and the endpoint. Alongside proactive protection that uses sandboxing and threat-extraction technology, SandBlast Agent also offers forensic analysis of security incidents."

Combination of levels

DDoS attacks can deliver a knock-out blow to companies at a number of levels: by sending vast swathes of data to their infrastructure, targeting specific applications or transmitting false network packages. Plus, a DDoS attack can be just a decoy for another attack. Whilst a DDoS attack is disabling your mail server – thus drawing your attention – hackers can, for instance, be off with client details. Of course, the best thing is to protect yourself against all three types of attack, since, in a worst-case scenario, you'll be having to cope with a combination of attacks and so a combination of anti-DDoS solutions is no excessive luxury.

"Palo Alto Networks and Check Point have brought two systems onto the market, Palo Alto Traps and Check Point SandBlast Agent, to protect endpoints better."

Kris Bogaerts
Security Consultant at Telenet

Security is not an exact science

Your company may well implement the right protection at every level, but easily foul things up when setting the policies.

Glyn Jones: "Here, companies have to weigh up the risks against the opportunities. You can configure a firewall to be very strict, but that could cost you productivity. Or your policy can be so wide open that you reduce your firewall's function to that of a router."

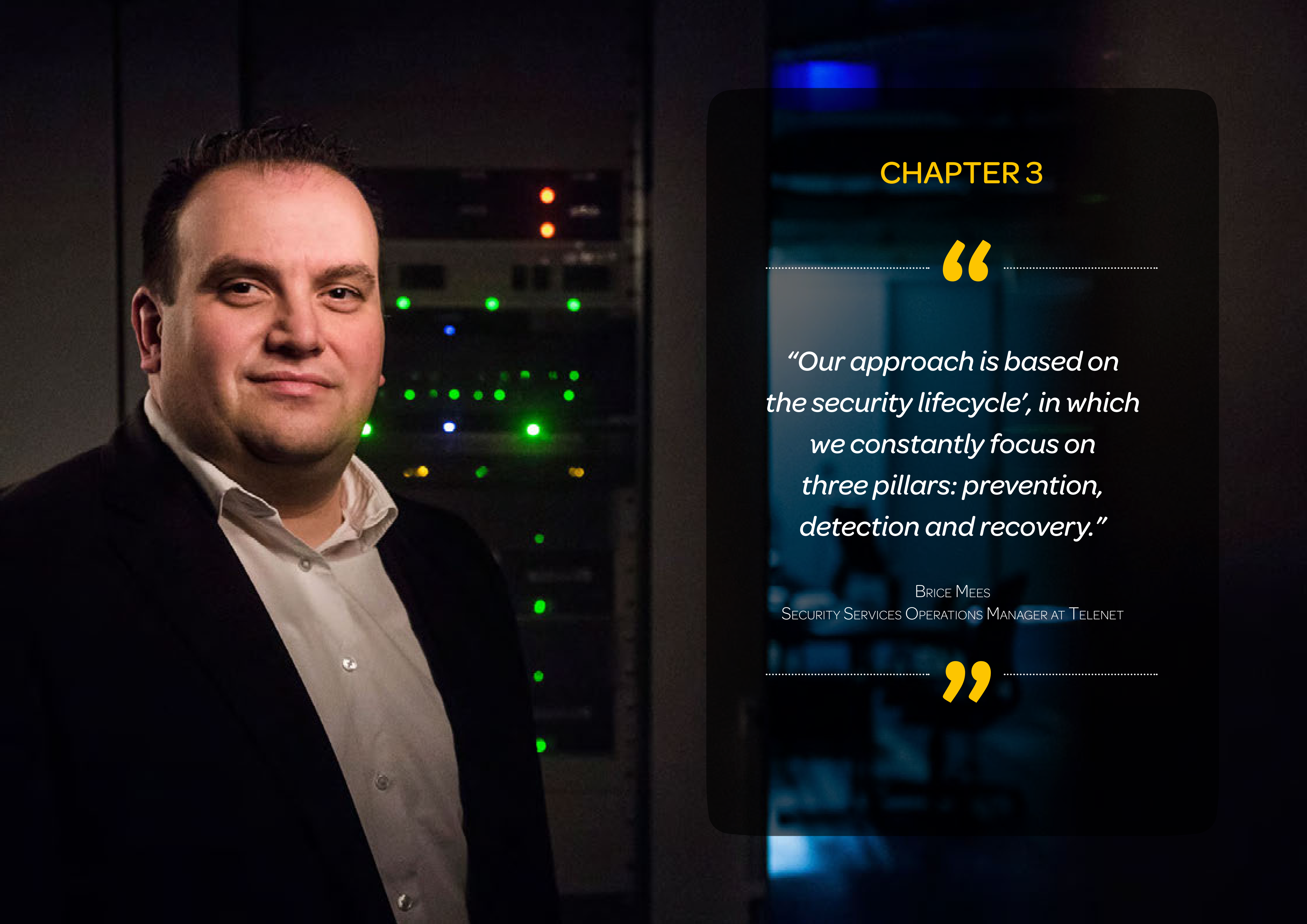
Companies have to look at their security policy and decide what risks they're prepared to take and which ones they want covered. Glyn: "Based on that, they can develop the required security infrastructure. Telenet can help define and optimise the firewall rules, but it's the client that bears ultimate responsibility. We're the locksmiths: the client decides which lock he wants on his door and how many copies there should be of the key."

ROUND UP

IT SECURITY DEMANDS A CLEAR VISION AND APPROACH

A new context, new threats and new solutions need a clear global vision of security. In the next chapter, learn how Telenet Security's approach has evolved.

> *"Telenet is the locksmith. The client decides what lock to put on their door and how many copies there should be of the key."*
>
> GLYN JONES
> SERVICE MANAGER AT TELENET



CHAPTER 3

“Our approach is based on the security lifecycle’, in which we constantly focus on three pillars: prevention, detection and recovery.”

Brice Mees
Security Services Operations Manager at Telenet

CHAPTER 03

- Everything begins with awareness
- A limited number of vendors for the best knowledge
- Architecture approach with client-bespoke components
- Flexibility in terms of support
- Strong focus on the proactive, advisory role
- DDoS security starts with the telecom supplier

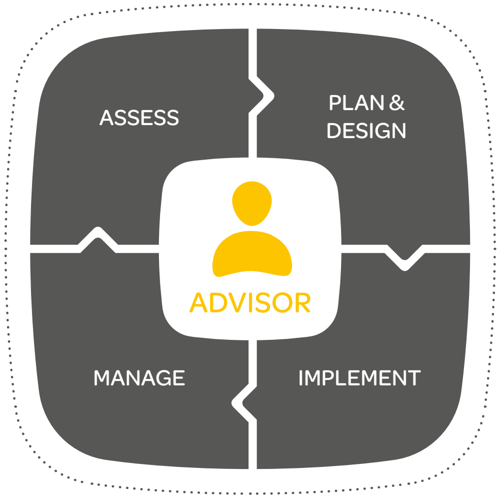
Telenet Security's approach

Security lifecycle

as a starting point for constant security

Telenet Security sees security as a continual process. A process that begins with an assessment or audit of your present situation and analysis of your needs. Based on that audit, we sketch out the best architecture and implement it. Monitoring and fine-tuning are essential components for keeping security up to scratch.

Our approach is based on the 'security lifecycle', in which we constantly focus on three pillars: prevention (avoiding threats), detection (finding the threats) and recovery (repairing damage done by a threat).



Everything begins with awareness

Everything begins with awareness – that's our mantra. "Creating awareness in the client's mind is important," says Bart Van den Branden, Product Manager Security at Telenet. "In terms of products, until a few years ago Telenet was a classic security integrator. We put the classic components in the network: firewalls, proxies, etc. What we've really been focusing on in the last two years is our advisory role. And that advice starts with making our clients aware."

Pentesting is the ideal starting point for more efficient security. Bart: "This is why we're teaming up with Toreon. Toreon is a Belgian leader in ethical hacking. The biggest benefits lie in their expertise and independence. They don't tie themselves to certain products, suppliers or telecom providers. They tell it like it is, warts and all." Dieter Sarrazyn, Toreon's Security Consultant & Managing Partner, briefly explains their approach. "We always use a standard work plan. We determine the scope of the project and, on that basis, put together a team of ethical hackers. These are certified experts with minimum 15 years' experience who've specialised in hacking a given area, like networks or web applications. After the pentest – 20% of which is done using tools and 80% manually – we produce a report containing recommendations, which we discuss with Telenet and the client."

Whereas pentesting in mostly used as a one-off benchmark, vulnerability management is a more constant, automated means of assessment. Bart: "The difficulty in vulnerability management is not in the monitoring but in its constant, active follow-up – patching. For this, we rely on Davinsi Labs, who possess all the competences to give exactly the right interpretation to the report and, above all, to develop it into concrete governance, risk management and compliancy (GRC). Vulnerability management is therefore the ideal and most proactive step-up to a clear and improved security policy."

"Our partnerships with Toreon and Davinsi Labs have greatly bolstered our product portfolio in terms of awareness. In the past, we mainly implemented solutions, but now we can really get into the client's business mindset," concludes Bart.

***Assessment** in practice*

"Our partnerships with Toreon and Davinsi Labs have greatly bolstered our product portfolio in terms of awareness."

Bart Van den Branden
Product Manager Security at Telenet

IN PRACTICE | SECURITY CONSULTANCY

Security Consultancy is the collective name for our specialised services aimed at achieving awareness.

Security Check-up

A Security Check-up maps out your network utilisation and security status.

- A clear view of your network traffic
- Extensive report on your security status, with points for action
- No prior knowledge of your infrastructure required

Security Policy Optimisation

Security Policy Optimisation looks at how your policy can perform better.

- Structured analyses, no manual actions
- Detection of unused, duplicated, contradictory and dangerous rules within your policy
- The same tool as for ISO, SOX and other certificates

Security Assessment

We analyse your current infrastructure and offer you recommendations for optimum protection.

- Guaranteed quality backed by CISA certification (Certified Information Systems Auditor)
- Extensive report on the status of your security infrastructure, accompanied by specific recommendations
- Ideal starting point for an improved security environment

Security Pentesting

– *in conjunction with Toreon* –

We get an ethical hacker to test your infrastructure. The aim is to point out to you the weaknesses in your security and improve it.

- Guaranteed quality backed by CEH certification (Certified Ethical Hacker)
- A clear view of the vulnerabilities in your security
- The same techniques and tools as dishonest hackers, but without endangering your data

Vulnerability Management

– *in conjunction with Davinsi Labs* –

A form of assessment in which your IT infrastructure is systematically scrutinised to detect vulnerabilities at an early stage

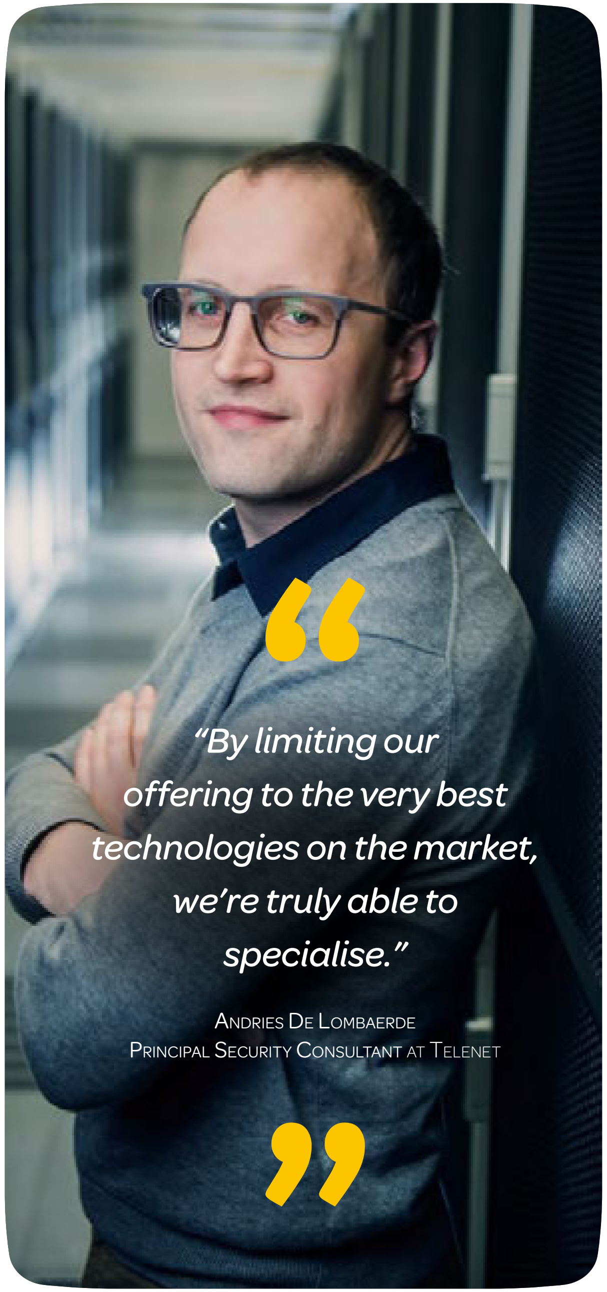
- Rapid 7's Nexpose as vulnerability scanner
- User-friendly dashboards and clear reports give good insight into your current state
- Guidance in interpreting the reports and carrying out action points

A limited number of vendors for the best knowledge

Telenet Security doesn't promote products but enters into partnerships according to what clients need. Andries De Lombaerde, Principal Security Consultant at Telenet: "By limiting our offering to the very best technologies on the market, we're truly able to specialise. Our knowledge is therefore our real value-added over other integrators."

The ranking of partnerships is the living proof of this: Four-star Partner of Check Point, Platinum Partner of Palo Alto Networks, and Gold Partner of F5. Andries: "Partnerships of this calibre allow us to truly challenge the vendors. To work together on further developing the technology, so that it's better directed at what our clients need. We have regular meetings with them where they tell us about new functionalities they're planning to implement or new tools they're bringing out, and we tell them of our experience in the field. We discuss outstanding issues, problems we've encountered with our clients, the limitations of a given product. They really take our remarks and feedback on board. There's true interaction: they use our input to further fine-tune their products, and even to develop new features."

***Plan & design** in practice*



"By limiting our offering to the very best technologies on the market, we're truly able to specialise."

Andries De Lombaerde
Principal Security Consultant at Telenet

IN PRACTICE | FOCUS ON PARTNERSHIPS

The three top vendors we work with are Check Point, Palo Alto Networks and F5. Year after year, technology consultant Gartner again places Check Point and Palo Alto Networks among the leaders in its 'Magic Quadrant for Enterprise Firewalls'.

Gold Partner of F5

Telenet is a Gold Partner of F5, renowned as a specialist in improving the speed and availability of applications, particularly via load balancing. F5 is nowadays also a major player in security. With its BIG-IP Application Delivery Controllers (ADCs), you can now optimise the speed, the security and the availability of applications.

4-Star Partner of Check Point

Telenet is a 4-Star Partner of Check Point Software Technologies, one of the market leaders in next generation firewalling. In addition to advanced identity and application control, Check Point's solutions offer a host of virtualisation possibilities. In 2015, Telenet was acclaimed as Check Point's Best Performing Partner.

Platinum Partner with ASC elite status of Palo Alto Networks

Palo Alto Networks developed the very first next generation firewall with a high-performance single-pass engine. Today, the company still continues to offer very progressive and integrated security solutions.

Telenet is a Platinum Partner with 'ASC Elite Status' (Authorised Support Centre). This status brings extra benefits for our clients, like direct escalation to senior support experts at Palo Alto Networks.

Our guaranteed Palo Alto Networks expertise, fast response times and continuity of service have already garnered us the prestigious 'Excellence in Support EMEA Award' in the past.

Xavier Duyck,
Country Manager Belux
at Check Point

"With its fast, smooth adaptation to our latest technologies and attendant certification, Telenet time and time again proves its knowledge and professionalism."

Luc Vervoort,
Director EMEA Strategic Alliances
at Palo Alto Networks

"In terms of security support, Telenet is the only partner in Belgium with ASC Elite Status."

Architecture approach with client-bespoke components

We believe that security has to go much farther than just products. Our resolute choice lies in an architecture approach and not technical ad hoc solutions that, in the best of cases, offer companies only temporary solace to their problems.

Bart Van den Branden: "Because information security is such a complex matter nowadays, no single security supplier is able to offer a global solution any longer. To be able to give you the fully integrated security you need, we work together with a range of technology partners. Our experts sit down with you and sketch out the best architecture, look at the most suitable security components, and implement them. In all of this, we don't just look at the perimeter, but consider the security of things like endpoints, web servers and datacentres, plus anti-DDoS solutions."

***Implement** in practice*

"Our experts sit down with you and sketch out the best architecture, look at the most suitable security components, and implement them."

Bart Van den Branden
Product Manager Security at Telenet

IN PRACTICE | SECURITY IMPLEMENTATION

We design an architecture, choose the hard- and software and implement the security architecture in your company. And we include advice on use and raising staff awareness.

We only use the services of the best technology partners and install the best-suited security components based on our experts' experience.

Depending on your situation, your security infrastructure might be made up of these components and technologies:

COMPONENTS	TECHNOLOGY PARTNERS
Firewalls	Check Point – Palo Alto Networks
Web Application Firewalls	F5
Remote Access	Check Point – Palo Alto Networks – Pulse Secure – F5
Link/Loadbalancers	F5
Strong Authentication	Vasco
Network Automation	Infoblox
Firewall Optimalisation	Algosec
Proxy Servers	BlueCoat – F5
Mail AntiVirus/AntiSpam	Cisco Ironport – Barracuda Networks
Threat Prevention	Check Point – Palo Alto Networks – FireEye
Anti-DDoS	Akamai – Telenet – Check Point
Mobile Security	MobileIron
Endpoint protection	Check Point – Palo Alto Networks – Trend Micro
Vulnerability scanning	Rapid7

Flexibility in terms of support

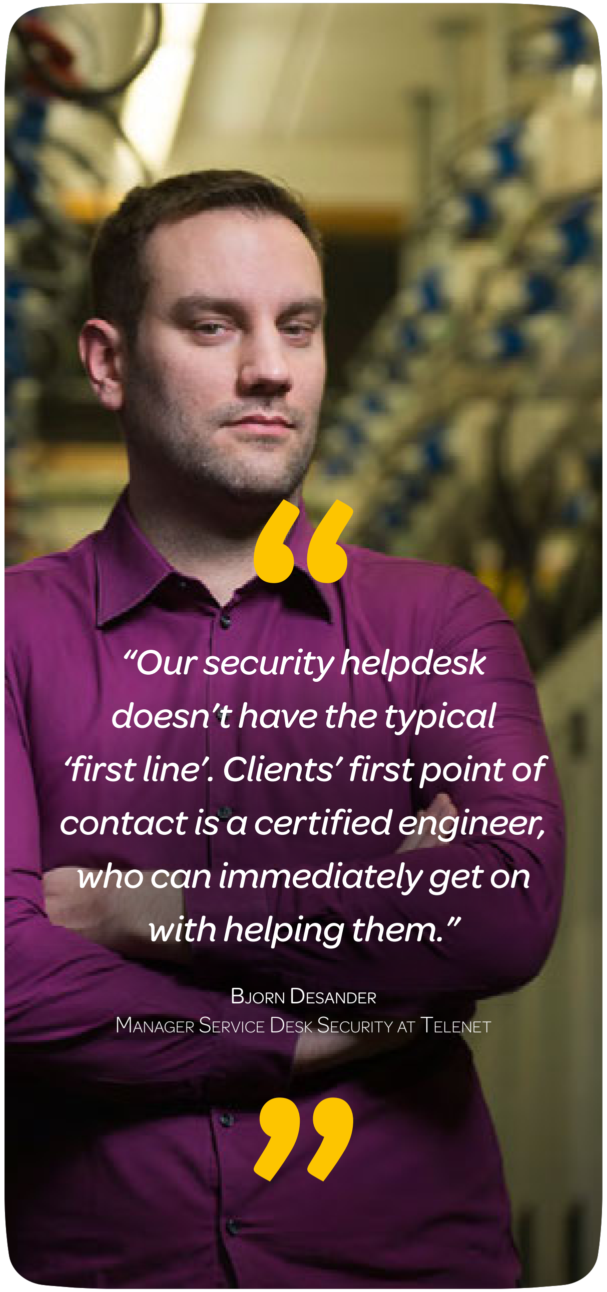
In terms of support, there is a great deal of flexibility for Telenet Security clients. From a do-it-yourself approach to getting support from us, at various levels up to full management outsourcing.

Brice Mees, Security Services Operations Manager at Telenet: "Many of our clients manage their solutions themselves. We provide training, give advice and share our expertise at regular meetings. Where adjustment is needed in certain regards, we tell them what action needs to be taken. In this preventive maintenance, we may for instance advise them that a technology has reached the end of its life or that a patch or update is imminent. The client can then carry out the changes themselves. If they wish, we can also do that for them."

Clients that want to go a step further go for Security Support, either during office hours or 24/7. If they have questions or problems, they can contact our specialists direct. Bjorn Desander, Manager Service Desk Security at Telenet: "We set ourselves apart, because our security helpdesk doesn't have the typical 'first line'. Clients' first point of contact is a certified engineer, who can immediately get on with helping them. It's not just our clients who appreciate that, our partners do as well. We're more than just a post box, because, for our top vendors, we even provide their first and second-line support. That means we resolve most incidents ourselves, without having to involve the vendor at all."

For clients that want to leave full management of their security architecture up to us, we have Managed Security. Brice: "Under Managed Security, our specialists take care of managing the infrastructure and the monitoring and optimisation of security, with clients able to choose from a number of SLAs (service level agreements), from a Basic package to a Premium package."

Manage *in practice*



> *"Our security helpdesk doesn't have the typical 'first line'. Clients' first point of contact is a certified engineer, who can immediately get on with helping them."*
>
> Bjorn Desander
> Manager Service Desk Security at Telenet

IN PRACTICE | SECURITY SUPPORT AND MANAGED SECURITY

Security Support

Sound technical support by certificated security specialists and proper licence management as a guarantee of continual security.

BUSINESS HOURS SUPPORT

- Telenet Security Desk as Point of Contact
- Weekdays from 8.30 a.m. to 5.30 p.m.

24/7 SUPPORT

- Extension on top of Business Hours Support
- 24/7

Managed Security

Outsourcing to our security specialists of management of your infrastructure and monitoring and optimisation of your security.

BASIC | Basic package for maintenance of your ICT security

- Day-to-day management of your infrastructure by our specialists
- Monitoring of availability
- Personal Service Manager
- Annual meeting to discuss functioning and results

STANDARD | Extension on top of Basic Managed Security, with complete monitoring of availability and performance

- Complete monitoring of availability and performance
- Larger number of configuration changes and software updates
- Three-monthly, detailed reporting by your Service Manager

PREMIUM | Extension on top of Standard Managed Security, with continual analysis of the status and evolution of your security

- Continuous analysis of the status and evolution of your security
- Larger number of configuration changes and software updates
- Monthly, detailed reporting by your Service Manager

Strong focus on the proactive, advisory role

IT security is highly critical and complex, and evolutive in the extreme. For your organisation to keep pace with this evolution, it can periodically call in the know-how of Telenet Security's senior security experts.

Brice Mees: "All our experts have at least five years' experience in the field, giving them the ability to attune perfectly with the mindset of the client's business and guide them towards an optimum security environment. We place great importance on expertise, which is why, within the Security team, we invest a great deal in training. This means that our experts are always up to date in terms of know-how and certification. This incidentally means that our team's turn-over rate is also very low, which of course benefits continuity in our client service."

Brice sees the Trusted Security Advisor as the lynchpin in the client's security lifecycle: "For instance, they will proactively alert the client to new versions and functionalities and advise on current performance, manageability and security. They can also help in coaching specific profiles and change management, and help in the validation of major changes."

"All our experts are able to attune perfectly with the mindset of the client's business and guide them towards an optimum security environment."

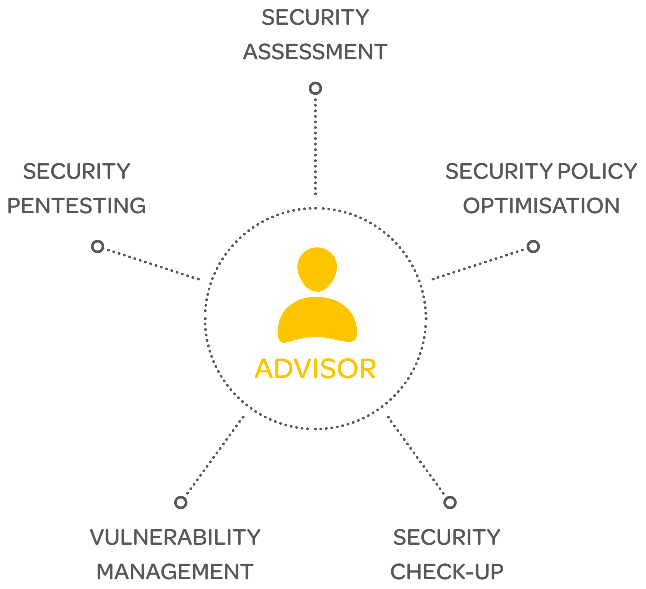
Brice Mees
Security Services Operations Manager at Telenet

***Advice** in practice*

IN PRACTICE | TRUSTED SECURITY ADVISOR

You can call in security experts,
even occasionally as and when you wish.

- Your security environment better attuned to your business's needs
- Faster, better adapted reaction to quick-changing security challenges
- Better guidance and support of your own IT security team



DDoS security starts with the telecom supplier

There are a range of solutions for repelling DDoS attacks: from solutions 'on site' to 'in the cloud'. At Telenet Security, we also believe that the telecom supplier has to play its part.

Lore Mattelaer: "Because of the rapid surge in DDoS attacks, at the beginning of 2016, we launched Anti-DDoS on our own connectivity. This allows us , in conjunction with technology partners, to offer our connectivity clients a unique combination of three anti-DDoS technologies. Whereas an on-site solution will typically protect you from applicative and protocol attacks, anti-DDoS on our connectivity and in the cloud will specifically protect you against volumetric attacks."

ANTI-DDOS ON OWN CONNECTIVITY

The anti-DDoS solution is available on Corporate Fibernet and iFiber, and shields you against the following attacks:

- Invalid packets: packets that do not comply with the internet standards
- Fragments that cannot be reassembled correctly
- Large NTP and DNS packets, which are typically used in DDoS amplification attacks
- All batches and SSDP reply packets
- Traffic from equipment forming part of a botnet

Anti-DDoS *in practice*

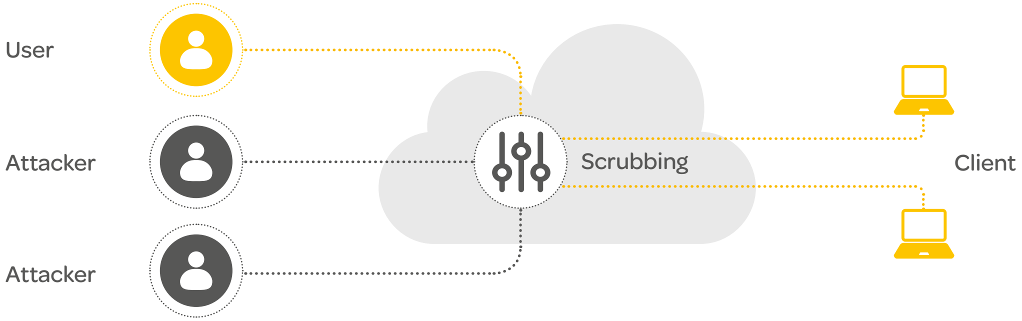
"Because of the rapid surge in DDoS attacks, at the beginning of 2016, we launched Anti-DDoS on our own connectivity."

Lore Mattelaer
Security Business Development Manager at Telenet

IN PRACTICE | ANTI-DDOS ON OWN CONNECTIVITY

To give you maximum protection against volumetric attacks, we are now launching our own anti-DDoS solution. A prime feature is that attacks are repelled on our network before they're even able to reach you. Your bandwidth is never in jeopardy, therefore.

The anti-DDoS solution operates in two stages:



STAGE 01

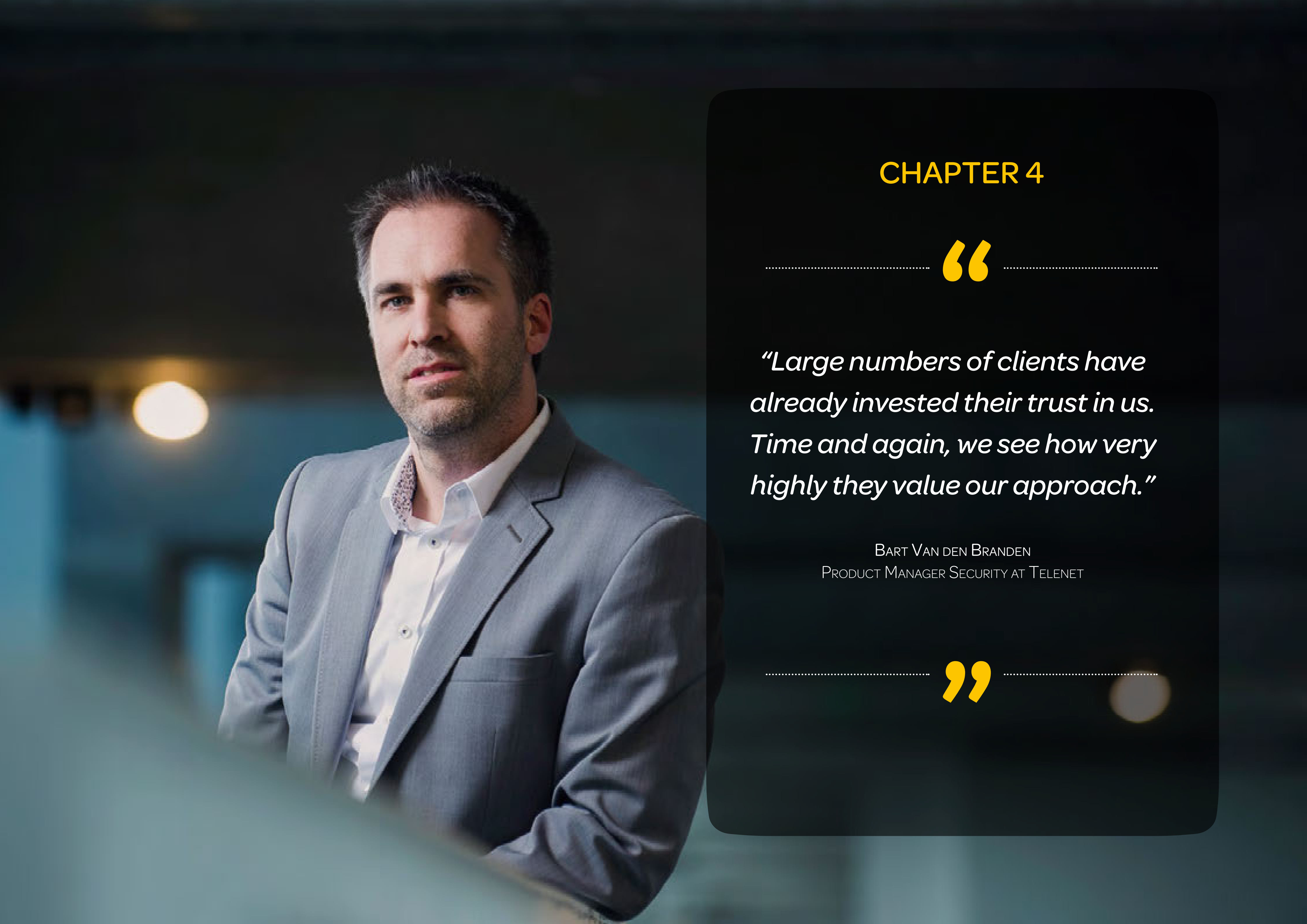
We continuously monitor and analyse your network traffic

Telenet will continuously monitor and analyse your network traffic using an anti-DDoS management system that detects typical volumetric DDoS attacks based on a DDoS intelligence feed with current fingerprints of attacks and a list of botnets.

STAGE 02

Our scrubbing infrastructure filters out the malevolent traffic automatically

If there's an attack, all your network traffic is diverted to a scrubbing infrastructure. The scrubbing process filters out the DDoS attack and forwards only the good network traffic back to your network. And you don't notice a thing: the attack never reaches your network, and so your bandwidth is never in danger.



CHAPTER 4

“Large numbers of clients have already invested their trust in us. Time and again, we see how very highly they value our approach.”

Bart Van den Branden
Product Manager Security at Telenet

PARTENA

Partena opts for two-layer security from Telenet

"We now have a fully up-to-par solution that guarantees the security of our data."

Franky Goethals
Manager, Infrastructure & Security, at Partena

CHALLENGES

- Outdated IT-infrastructure updates
- Optimal protection of confidential client data
- Keeping costs under control

SOLUTIONS

- Security Check-up
- Security Implementation: F5 and Check Point
- Managed Security

BENEFITS

- Reliable security that's up to date all the time
- 24/7 Business Support
- Cost-saving by outsourcing management

Read Partena's client story ››

KEYTRADE BANK

Telenet helps Keytrade Bank with watertight security and connectivity

> *"The combination of two technologies enables us to achieve a higher level of security."*

Arnaud de Prelle
Head of IT Infrastructure at Keytrade Bank

CHALLENGES

- Extreme security and reliability needed
- Rising global issue of cyber attacks and malware
- Partner with comprehensive security knowledge

SOLUTIONS

- Check Point
- FireEye
- Advice on implementation, maintenance and evaluation

BENEFITS

- End-to-end security
- Fast 24/7 business support
- Personal service provision with a high degree of involvement

Read Keytrade Bank's client story >>

New firewall at Sint-Blasius Hospital

"Telenet helps us with regular reviews and makes sure that our firewall rules stay consistent."

Rik Van Oost
ICT Manager at Sint-Blasius Hospital

CHALLENGES

- Getting security up to date
- A single, uniform security for all traffic
- Small IT team

SOLUTIONS

- Global approach, from hardware to support
- Two new firewalls: Check Point
- Management by Telenet

BENEFITS

- Permanent monitoring with regulare reviews
- Increased response time
- Full redundancy

Read Sint-Blasius Hospital's client story >>

Business

LEARN MORE

telenet.be/security 0800 66 066