Business

Fully integrated IT security

for companies and governments

Fully integrated IT security

THE SECURITY LIFECYCLE

TRUSTED SECURITY ADVISOR

The starting point for constant security

Telenet Business 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 work out the best architecture and implement it. Monitoring and fine-tuning are essential components for keeping security up to scratch. We constantly focus on three pillars: prevention (avoiding threats), detection (finding the threats) and recovery (repairing damage done by a threat)."

Your lynchpin in the security lifecycle

IT security is highly critical and complex, and evolves very quickly. For your organisation to keep pace with this evolution, it can periodically call on the know-how of Telenet Business' senior security experts. These 'Trusted Security Advisors' will proactively alert you 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 with the validation of major changes.

Why a Trusted Security Advisor?

- 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

Our security portfolio in practice

Security Consultancy

What we've really been focusing on is our advisory role. And that starts with making you aware. Security Consultancy is the collective name for our specialised services aimed at achieving awareness. There are various possibilities.

Security Assessment

We use Security Assessment to analyse your current infrastructure and offer you recommendations for optimum protection.

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

Security Policy Optimisation

Larger networks result in a complex firewall policy. 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 Pentesting

Security Pentesting is where we have an ethical hacker try to penetrate 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 those used by dishonest hackers, but without endangering your data

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

Vulnerability Management

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 situation
- Guidance in interpreting the reports and carrying out action points

Security Implementation

Telenet Business doesn't promote products but enters into partnerships based on what clients need. We believe that security has to go much farther than just products.

A limited number of vendors for the best knowledge

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. Because information security is such a complex matter nowadays, no single security supplier can 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. By limiting our offering to the very best technologies on the market, we're truly able to specialise. Our knowledge is therefore our real added value over other integrators.

Architecture approach with client-bespoke components

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

Security Support & Management

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

Preventive Maintenance

Many of our clients manage their solutions themselves. We provide training, give advice and share our expertise at regular meetings. In this preventive maintenance, we tell them what action needs to be taken and the client can then carry out the changes themselves.

Clients that want to go a step further opt for Security Support or Managed Security.

Two levels of Security Support

If clients have questions or problems, they can contact our specialists directly – either during office hours or 24/7. We stand out, because our security helpdesk doesn't have the typical 'first line'. A client's first point of contact is a certified engineer, who can immediately begin offering assistance.

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

Three levels of Managed Security

For clients who want to leave full management of their security architecture up to us, we have Managed Security. 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 one.

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

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

Premium

Extension on top of Standard Managed 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

Additional products and services

Anti-DDoS on our connectivity

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

To give you maximum protection against volumetric attacks, we are now launching our own anti-DDoS solution. 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.

A prime feature is that attacks are repelled on our network before they're even able to reach you. 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.

User

Attacker

Attacker

Scrubbing

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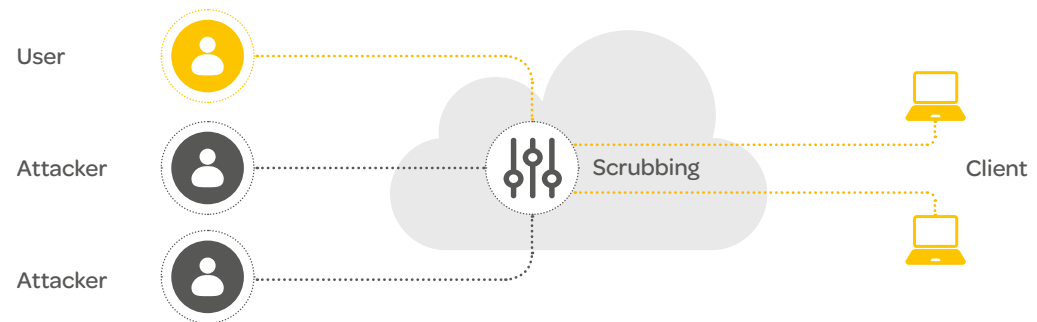
The anti-DDoS solution is available on Corporate Fibernet and iFiber internet products, and shields you against the following attacks:

- 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

Off-the-shelf security

Secured Internet Gateway is a ready-to-use next generation firewall that gives your network and data maximum protection. Telenet's security consultants and engineers implement the firewall completely, you manage the settings via a simple dashboard. No hardware or knowledge is required.

- Identifies, blocks or authorises applications
- Protection in real time: every threat is immediately addressed
- Security according to the highest and most recent standards
- Fully redundant for maximum peace of mind

Training courses and events

IT security evolves very quickly. In order to brush up your knowledge, we can give you training courses on security technologies. In addition, we keep you informed of interesting events relating to IT security. Choose a general training, ask for personal training or attend one of the security events.

- Training on a specific security problematic
- Workshop for your personnel
- Trade fairs, conferences, information days

Why choose Telenet Business

> **Proactive advice** from your Trusted Security Advisor

> **Lifecycle approach:** assessment, implementation and management

> A limited number of vendors for the **best security architecture**

> **Anti-DDoS technologies** on site, in the cloud and our own connectivity

> Keep your knowledge up to date with **training en events**

More information? Call us on 0800 66 066