Secutec
Secure DNS

DETECT AND BLOCK NEW THREATS FASTER
THAN YOUR CURRENT SECURITY SOLUTION.

Secure DNS

POWERED BY SECUTEC

Internet traffic and DNS queries are the main gateway for malware, phishing, ransomware and other cyberattacks. Failing to secure your DNS connections could lead to any cybercrime, such as expensive company downtime and catastrophic data theft.

Secutec Secure DNS helps you to monitor and protect your company network, by detecting and blocking malicious DNS queries that your current anti-spam, firewall and proxies are not yet aware of. It is the most effective security solution to outsmart malware, phishing attacks or any other cyberattack.

Secutec Secure DNS is a solution from Secutec, a leading expert in cybersecurity in the Benelux.

What is a DNS?

When a user in your network types a **URL**, the name of a website, into your web browser, a **Domain Name Server** (DNS) matches this URL to an IP address. The IP address belongs to the server that hosts the requested website. Every URL on the internet has a unique IP address linked to it. You can consider a DNS as **the internet phone book,** listing URLs and their corresponding IP addresses. Once the browser receives the correct IP address, it will build a connection with the server that matches the IP address to transfer information.

91% of all malware comes from unsafe DNS connections

Internet Service providers mostly use DNS connections without securing them. That means that your company is using the same unsecured connections every day. No wonder more than 91% of all malware uses DNS to communicate with your server, to steal data or to redirect traffic to malicious sites. Today, the dangers are very often hidden in innocent applications, documents and websites, invisible to firewalls and other security solutions. The amount of cybercrime worldwide keeps increasing. An average malware attack costs organizations around $ 2750*, this is a year-on-year increase of 11%. Phishing- and ransomware attacks are rising.

> *Without secure DNS monitoring, your company network is exposed to a wide range of cyberthreats.*
>
> Geert Baudewijns - CEO Secutec
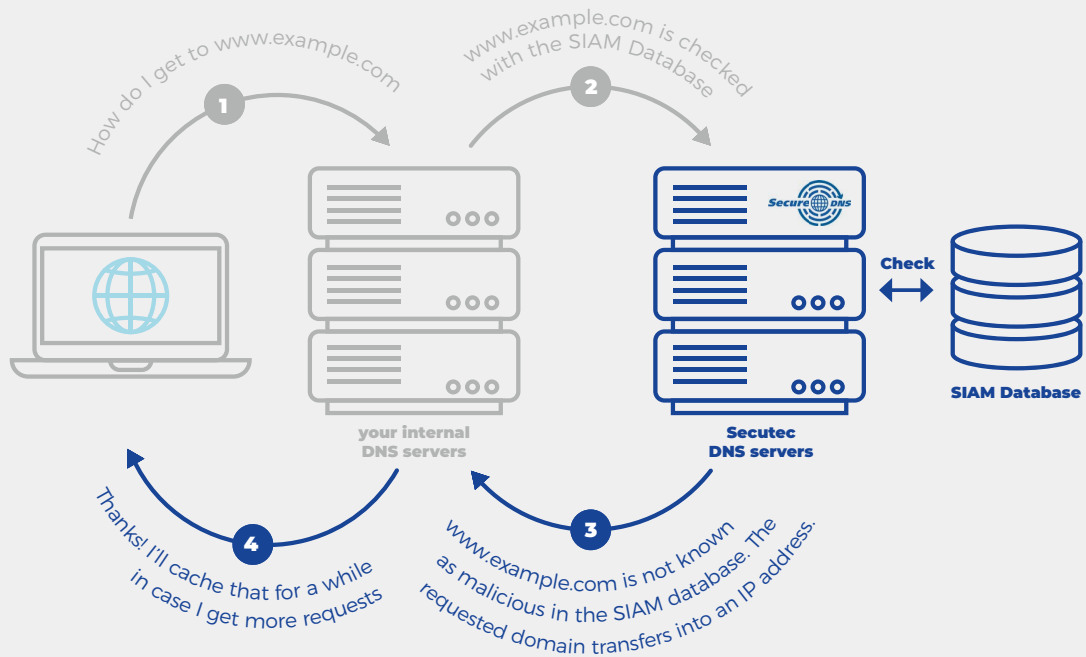
* Accenture Security Report 2019

How Secutec Secure DNS outperforms all Cyber Security vendors

Secutec Secure DNS is an add-on solution for your current security solution. We are vendor independent and we use local and international cybersecurity knowledge.

BLOCK FASTER

DETECT MORE

PREVENT PROACTIVELY

How do I get to www.example.com

1

www.example.com is checked with the SIAM Database

2

Check

your internal DNS servers

Secutec DNS servers

SIAM Database

Thanks! I'll cache that for a while in case I get more requests

4

www.example.com is not known as malicious in the SIAM database. The requested domain transfers into an IP address.

3

What is the SIAM Database?

The SIAM database, or Secutec Integrated Advanced Malware Database.

The SIAM database is an intelligent database which gathers information from different sources at a very early stage. Secutec Secure DNS receives feeds from this SIAM database to get intelligence if a domain is malicious or not.

How can Secure DNS help you to be one step ahead of cyberthreats?

Secutec Secure DNS is a fast protocol that protects your company against malicious host names. It serves as an extra security software that protects your network against malware, phishing attacks or any other cyberattack.

Secutec Secure DNS will forward all DNS queries from your network to our Secutec Secure DNS Server. This server will check the domain reputation of the requested URL. If a user browses to a domain that has been blocked, they will not be able to access that webpage, as the connection will not be initiated. If the domain is whitelisted or if it is not known as "bad", the connection will be initiated, allowing the user to access the requested domain.

By blocking malicious connections on DNS level, we are not only blocking the web traffic that should go through your web proxies, but also the traffic that is bypassing the proxy.

We can also reroute the internet traffic of remote workers through the Secutec Secure DNS to make sure everyone in your company can establish safe DNS connections, regardless of their location.

"Secure DNS works nice and simple; I can see that our antivirus is working but Secure DNS offers an extra protection layer".

Pieter Verheyden – VAB

A more detailed look into Secutec Secure DNS
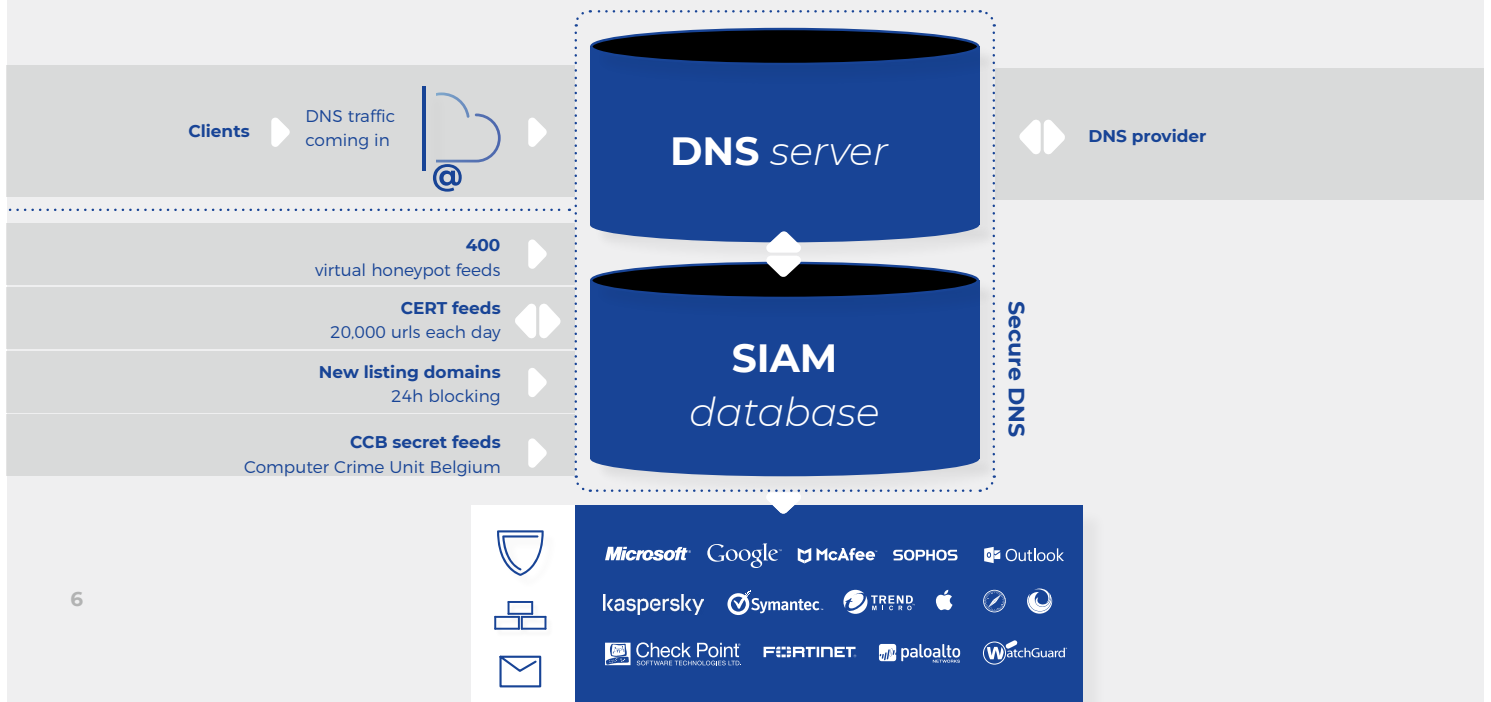
- **Honeypot service:** A honeypot simulates an operating system and allows an attacker to log in and execute commands or download malware. Our honeypot network consists of 12 data centres and 400 machines.

- **CERT feeds:** Thanks to our exclusive collaboration with the Belgian Federal Cyber Emergency Response Team (CERT), we have access to information about 20,000 suspicious local URLs per day.

- **New listing domains:** More than 22% of all newly registered domains are used for cybercrime. That's why we block new domains for 24 hours, giving us the time to analyze them properly and recategorize when needed.

- **CCB secret feeds:** We exchange information about local cyberattacks with the Centre for Cybersecurity Belgium (CCB).

- **Web browsers:** Data (URLS that we identify as bad) will be provided to Microsoft, Google and Apple from actions on Internet Explorer, Chrome, Firefox, Safari …

- **Multiple vendor information:** We use a combined database of more than 20 antivirus, firmware and anti-spam vendors.

Benefits of
Secutec Secure DNS

Block faster – detect more – prevent proactively

- **Reporting dashboard:** In order to keep track of your performance, we provide a detailed dashboard of all DNS queries and blocked threats. The reporting and alerting dashboard can be fully customized with personalized reports and alerts.

- **High-performant security service:** More malicious domains are blocked at an earlier stage. We also detect local Belgian threats which are unknown to other safety solution vendors.

- **Complete network security:** Secure DNS protects every element in your network, including PCs, laptops, servers, printers, scanners, IOT, Blackbox, cryptocurrency mining, etc.

Peace of mind

- **Support within 24 hours:** Need our help? Our solution specialists are here for you.

- **Implementation in less than 60 minutes:** Our solution specialist will configure your DNS setting during a remote call. So easy, yet so efficient!

Easy to implement

- **System independent:** It works with any IT, network or security setup in your corporation.

- **Seamless infrastructure integration:** Secure DNS can be integrated easily with your IT infrastructure, be it DXL, PXGRID, SIEM, or any other.

- **No additional hardware or software required:** No downtime, service interruption, or server reboots are needed. All it takes is a change in the configuration of your DNS settings, without additional load on your system.

A safe team, wherever they work

- **Safe web browsing guaranteed:** leading to increased IT security.

- **Fast connections assured:** No latency or extra processing time.

- **Remote and mobile cybersafety:** Working from home or active on another network? We can reroute the internet traffic of remote workers through the Secutec Secure DNS.

- **We keep all your devices safe** including those over which you have no control, f.e. schools with a guest network for students.

Block not yet categorized domains

Minimizing the time between the registration of a new malicious domain and its blacklisting is crucial to minimize the risks and the potential damage to companies and organizations. Especially the local information from sources like CCB and CERT, allows us to block malicious domains 12 to 24 hours before the regular anti-spam vendors do. By proactively blocking newly seen domains for 24 hours, we avoid attacks from new domains that are often used for malware, phishing, ransomware, etc. And that is exactly how we outperform your current antimalware vendor.
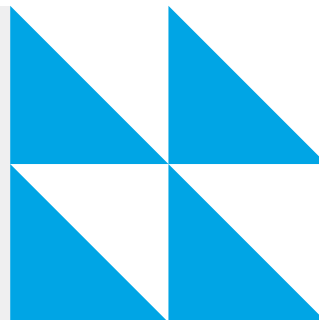
Be safe, even if you are outside your network or traveling

With the Secure DNS Agent, all DNS connections of non-VPN users outside your company network will be monitored, giving you more peace of mind. All DNS queries will be automatically forwarded to the Secutec Secure DNS server, which will check the domain reputation of the requested URL. If the domain is safe, the connection will be built. The Secure DNS Agent doesn't require any hardware installation. The Secure DNS Agent is the latest addition to our Secure DNS solution. It fits our philosophy of continuous innovation.

Why you should try it yourself?

· **Affordable multi-vendor solution:** Secutec Secure DNS gathers information from more than 20 antivirus, firmware and anti-spam vendors, honeypot services and local cyber security agencies.

· **Automatic monitoring and detection alerts:** Secutec Secure DNS automatically monitors all your DNS connections, 24/7. When it spots a malicious detection, you will be alerted immediately.

· **Customization:** Every customer is different. That's why we offer a tailor-made approach. Do you need specific changes or want certain domains to be blocked? Let us know and we will make it happen.

Try Secutec Secure DNS for free

Do you want the most performant solution to protect your company network and valuable data?

Try Secutec Secure DNS during a free 4-week trial period.

Contact us on sales@secutec.be or +32 3 877 82 93

Secutec Secure DNS

Ready, set, go!

Implement Secure DNS in 4 easy steps!

1. Create account

To create your account, we need a list of public IP addresses used by your company.

2. Configuration

Configuring Secure DNS only takes 60 minutes. After that, you are all set!

3. Testing

We will contact you to perform a test query and configure your DNS forwarders. This will ensure that the DNS queries are being received and resolved by our service.

4. Ready to go

Secutec Secure DNS is now installed. Log in to the portal to check your traffic stats.