Grant Thornton

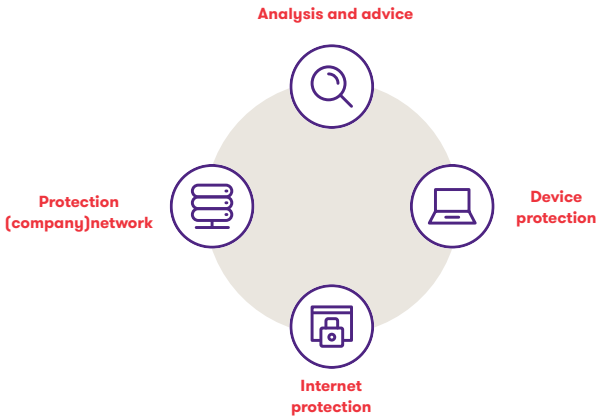
An instinct for growth™

Grant Thornton CyberHunter

Am I using outdated software somewhere in my company? How do I quickly know whether my employees are clicking on phishing messages? Where do I start with defending against cybercrime? What is the best approach? These are relevant questions. Information security and cyber resilience are essential today. We can help you. Grant Thornton CyberHunter (hereinafter referred to as CyberHunter) is an important part of our approach. Therefore we would like to explain our service to you here.

CyberHunter provides insight into possible vulnerabilities.

Our CyberHunter service gives you insight into unsafe behaviour by your employees and vulnerabilities in your internet traffic, network and information systems. To do this, we place our CyberHunter sensor in your organisation. With CyberHunter, we can detect automated attacks, configuration errors, missing patches, cyberattacks, unwanted behaviour or outbreaks of malware (such as ransomware).



Areas of focus

A good interaction between technology, processes, and people; that's what your resilience to cyber risks is all about. With CyberHunter, we search for vulnerabilities in your environment. We also advise which basic security measures can be improved within your organisation to increase your cyber resilience. We do this within three areas, for which we provide you with different modules: internet, network and device protection. Each module gives you access to the cybersecurity expertise of Grant Thornton. Here they come.

Internet protection

- CyberHunter's internet protection module simulates an attack on your infrastructure that is accessible through the internet. CyberHunter will look for possible entrances into your internal network – for example, through configuration errors or outdated software.
- The CyberHunter sensor analyses all incoming and outgoing traffic between the internal network and the Internet. This provides you insight into malicious traffic and potential attacks.
- If the CyberHunter sensor signals malicious traffic, this will be reported to us.
- We investigate the potential vulnerabilities and determine their severity. We also look at possible connections between these vulnerabilities.

Network protection

- CyberHunter's network protection module searches the network for vulnerabilities in system configurations and outdated software on systems such as computers, servers, printers and phones. Those vulnerabilities allow an attacker to access these systems or applications of access sensitive data.
- We investigate the potential vulnerabilities and determine their severity. We also look at possible connections between these vulnerabilities.

Device protection

- CyberHunter's device protection module can verify whether detected attacks have had an impact on your systems. In addition, device protection helps to protect against ransomware and other forms of malware.
- This module can detect and block attacks before an attack even reaches a system or user.
- Device protection also continues to protect devices when they are used outside the office. For example, on a business trip or when using public Wi-Fi networks.

Analysis and advice

Each module gives you access to our expertise.

- Technology cannot identify and solve all cyber risks, which is why we analyse the data and technical vulnerabilities and translate these into threats to your organisation. We also make recommendations to mitigate cyber security risks. We discuss the identified vulnerabilities and recommendations with you at recurring contact moments.
- All identified vulnerabilities will be shown on an online dashboard. Via this dashboard you always have insight into the vulnerabilities per system and ongoing investigations.
- The online dashboard can also be used to export data. For example, when using a 'Vulnerability Management Tracking' or ticket system within your organisation.

What do you get out of it?

- Through current insight and consultation, CyberHunter provides continuous improvement of the cyber resilience level of your organisation.
- Current insight into the systems connected to your network: asset management.
- You receive current insight into vulnerabilities and attacks on your networks, systems and applications.
- We can block malicious attacks automatically.
- You receive current insight into vulnerabilities and risks through a safe online dashboard.
- You have periodic contact moments to discuss cyber-related topics with our cyber security experts.
- The implementation of the CyberHunter sensor is easy and has no impact on your network or the speed of your network.
- Your organisation can meet the GDPR requirements with the help of CyberHunter.

Contact

Do you want to know how to reduce the cyber resilience of your organisation? Migiel de Wit-Beets is happy to tell you more about it. You just need to call him.

Migiel de Wit-Beets
Partner
T 088 676 91 86
E migiel.de.wit@nl.gt.com

Grant Thornton
An instinct for growth™