NetCaptain

NetCaptain
A brand of CyberAnt

WHAT IS NETCAPTAIN

Every day, new security vulnerabilities in software are discovered. Keeping up with this continuous stream of new vulnerabilities requires a lot of time and expertise.

NetCaptain has automated this process and is now one of the best vulnerability management tools in all of Europe. NetCaptain provides clear and understandable advice on how vulnerabilities can be resolved.

Compared to other vulnerability tools, NetCaptain scans many more times and is also very affordable.

NetCaptain features a Get Help function, which means that our cybersecurity experts are ready to answer all unanswered questions. NetCaptain can be installed by deploying either a physical or virtual appliance.

NETCAPTAIN KEEPS HACKERS OUT

Many cyberattacks are relatively easy to prevent. This is because hackers often exploit weaknesses in systems that are known and for which there is already a solution. However, it can be challenging to be sure that all systems are secure. How can you be certain that a security update has indeed fixed the problem? And are there no servers left out of the process?

WHAT SECURITY VULNERABILITIES EXIST?

Security scans are used to examine systems, network components, and web applications for security vulnerabilities. By addressing these vulnerabilities, the resilience against cyberattacks is increased, reducing the likelihood of a successful attack to a minimum.

UNDERSTANDABLE AND AFFORDABLE

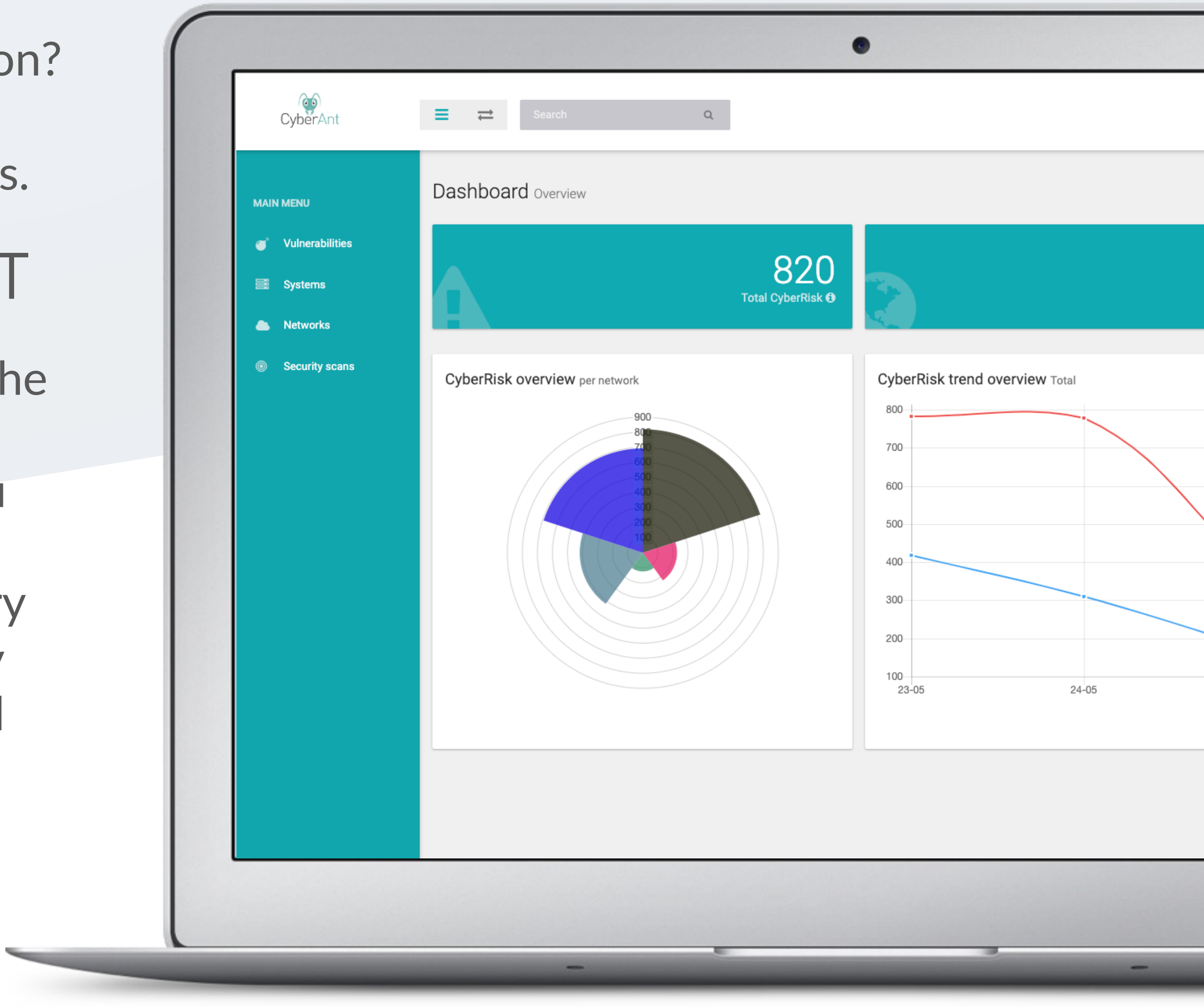
New vulnerabilities in software are discovered daily. Managing this continuous flow of new vulnerabilities requires a smart approach. This is known as Vulnerability Management. NetCaptain automates this process and provides clear and understandable advice.

CLEAR DASHBOARD

At a glance, you can see how you're doing: are we becoming more secure? Where are the biggest risks in my company? Which vulnerabilities need my immediate attention? The NetCaptain dashboard is designed to provide instant answers to these questions.

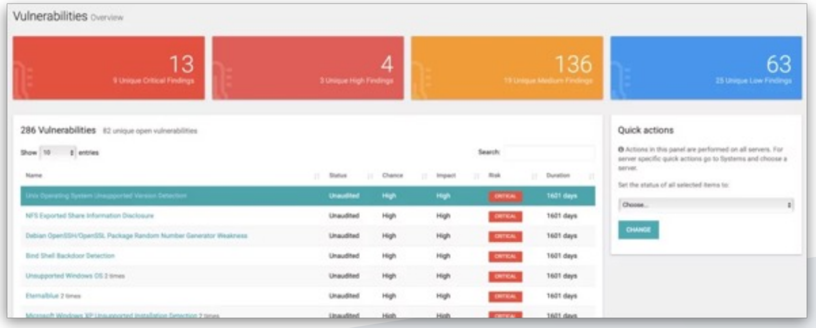
VULNERABILITY MANAGEMENT

All vulnerabilities are clearly displayed in the vulnerabilities tab. Vulnerabilities that are similar are automatically grouped, and you can see how long a vulnerability has been open. NetCaptain keeps a complete history of each vulnerability. When a vulnerability suddenly reappears on a machine, you will receive a warning for it.



AUTOMATE THE PROCESS

With NetCaptain, you can schedule when you want to perform scans. Workstations can be scanned during working hours, network equipment at night, and Windows servers after Patch Tuesday.



Vulnerabilities Overview

13	4	136	63
9 Unique Critical Findings	3 Unique High Findings	19 Unique Medium Findings	25 Unique Low Findings

286 Vulnerabilities 82 unique open vulnerabilities

Show 10 entries

Search:

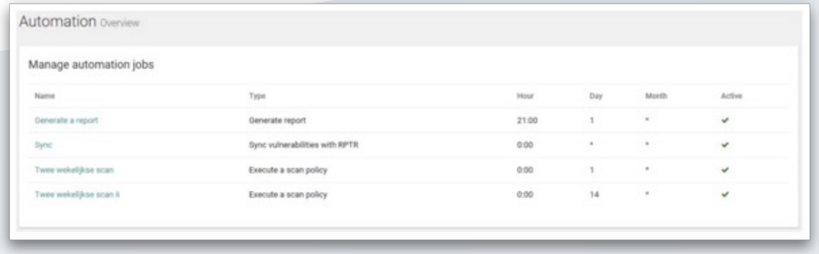
Name	Status	Chance	Impact	Risk	Duration
Unix Operating System Unsupported Version Detection	Unaudited	High	High	CRITICAL	1601 days
NFS Exported Share Information Disclosure	Unaudited	High	High	CRITICAL	1601 days
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Unaudited	High	High	CRITICAL	1601 days
Bind Shell Backdoor Detection	Unaudited	High	High	CRITICAL	1601 days
Unsupported Windows OS 2 times	Unaudited	High	High	CRITICAL	1601 days
Eternalblue 2 times	Unaudited	High	High	CRITICAL	1601 days
Microsoft Windows XP Unsupported Installation Detection 2 times	Unaudited	High	High	CRITICAL	1601 days

Quick actions

Actions in this panel are performed on all servers. For server specific quick actions go to Systems and choose a server.

Set the status of all selected items to:

Choose...



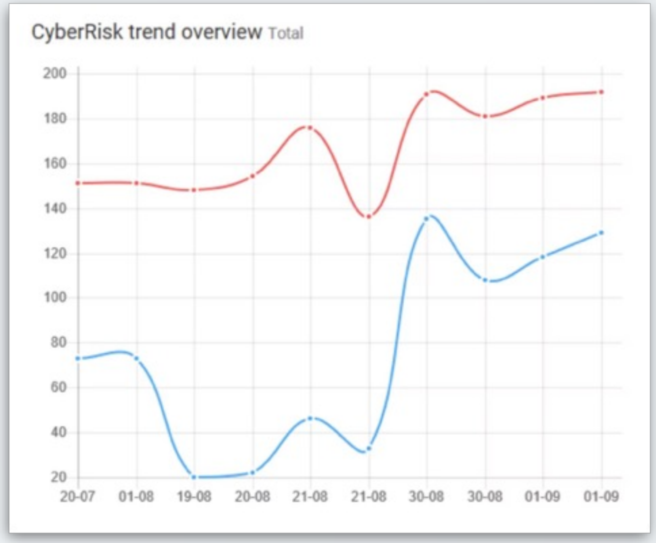
Automation Overview

Manage automation jobs

Name	Type	Hour	Day	Month	Active
Generate a report	Generate report	21:00	1	*	✓
Sync	Sync vulnerabilities with RPTR	0:00	*	*	✓
Twee wekelijkse scan	Execute a scan policy	0:00	1	*	✓
Twee wekelijkse scan II	Execute a scan policy	0:00	14	*	✓

TREND OVERVIEW

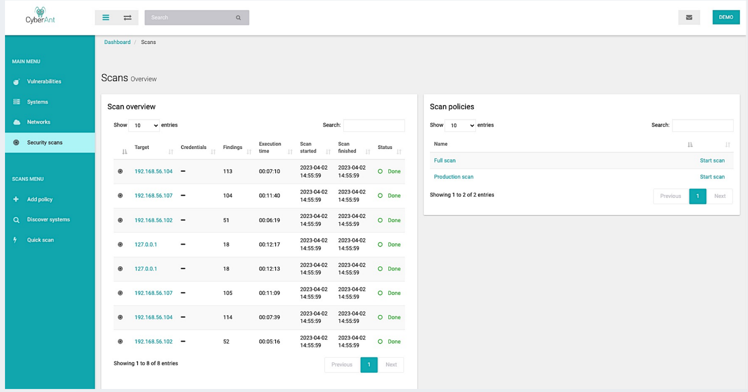
In the trend overview, you can track how secure your network is over time. It displays the number of vulnerabilities and the CyberRisk score. This allows you to closely monitor the progress of your vulnerability management process. The CyberRisk score is a value that NetCaptain automatically calculates based on the discovered vulnerabilities. Severe vulnerabilities carry more weight, and it takes into account the importance of a system and whether it is accessible from the internet.



CyberRisk trend overview Total

SCAN MANAGEMENT

From the scan overview, you can keep track of what you have scanned. Here, you can see which vulnerabilities have been detected, when a scan took place, whether credentials were used, and if any errors occurred. You can also manage discovery scans from this section. A discovery scan allows you to identify new systems in your network, preventing you from overlooking forgotten systems.



Dashboard / Scans

Scans Overview

Scan overview

Show 10 entries Search:

Target	Credentials	Findings	Execution time	Scan started	Scan finished	Status
192.168.56.104	–	113	00:07:10	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
192.168.56.107	–	104	00:11:40	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
192.168.56.102	–	51	00:06:19	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
127.0.0.1	–	18	00:12:17	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
127.0.0.1	–	18	00:12:13	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
192.168.56.107	–	105	00:11:09	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
192.168.56.104	–	114	00:07:39	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
192.168.56.102	–	52	00:05:16	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done

Showing 1 to 8 of 8 entries

Previous 1 Next

Scan policies

Show 10 entries Search:

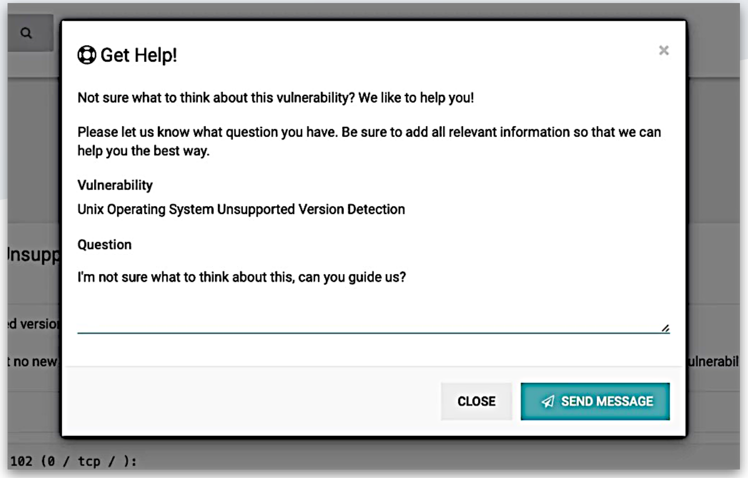
Name	
Full scan	Start scan
Production scan	Start scan

Showing 1 to 2 of 2 entries

Previous 1 Next

HELP IS ALWAYS CLOSE BY

With the Get Help functionality, you can ask questions directly from your dashboard to our ethical hackers about a vulnerability. This means you not only have access to the right tools but also to expertise. With NetCaptain, you are never alone. The Get Help functionality is available for Professional and Enterprise customers.



Get Help!

Not sure what to think about this vulnerability? We like to help you!

Please let us know what question you have. Be sure to add all relevant information so that we can help you the best way.

Vulnerability

Unix Operating System Unsupported Version Detection

Question

I'm not sure what to think about this, can you guide us?

WHAT DOES NETCAPTAIN CHECK

NetCaptain is capable of detecting vulnerabilities within servers, databases, IoT devices (such as cameras and printers), web applications, and workstations. It is also possible to use NetCaptain within cloud environments.

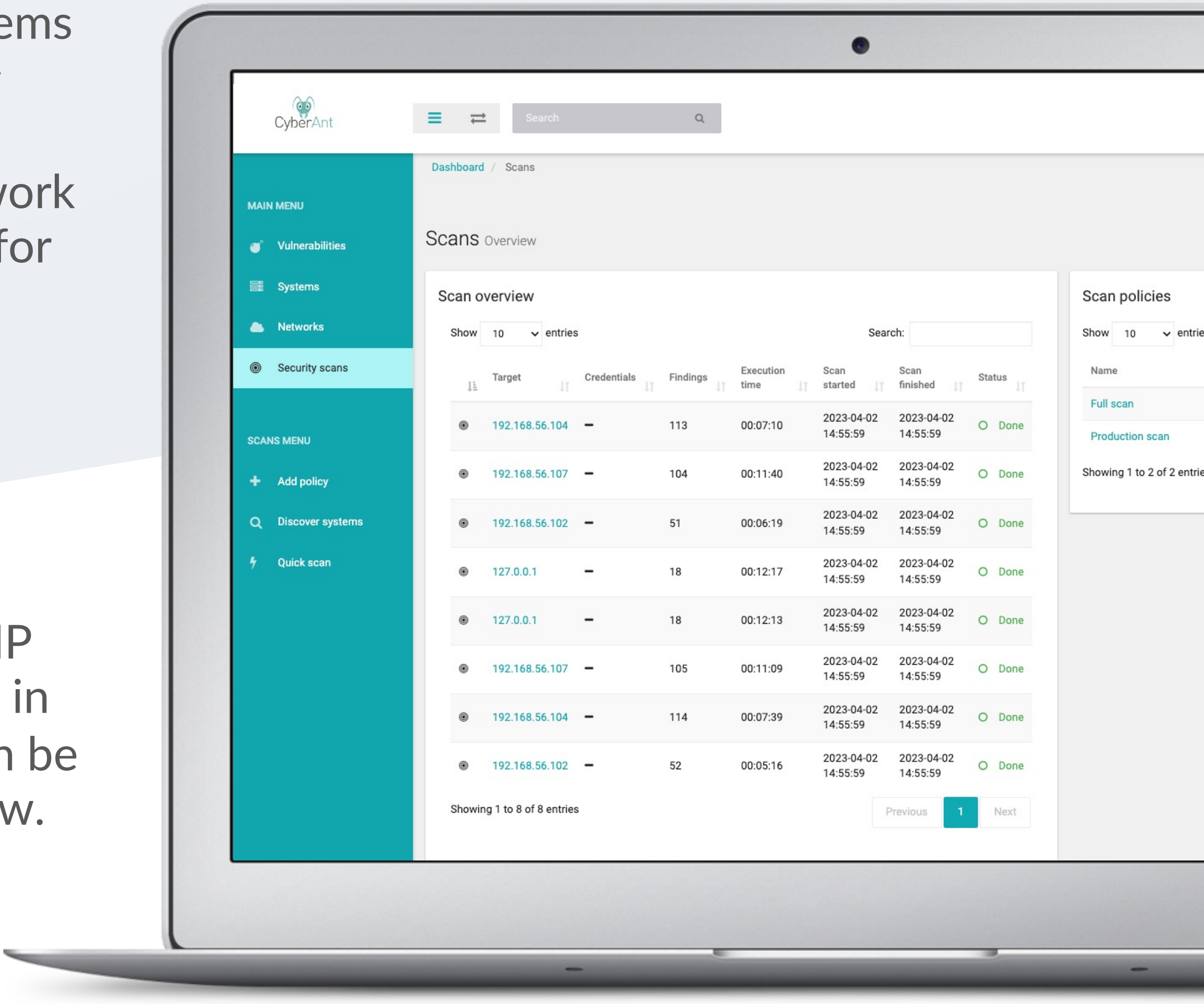
In essence, NetCaptain scans everything present in the network, including systems that one may not be aware of in the network. This includes both known and unknown systems, and it enables the software to identify hidden or forgotten devices and detect their vulnerabilities. This is a valuable feature to ensure the entire network's security, even if some systems are not on the radar.

HOW MANY SYSTEMS CAN NETCAPTAIN SCAN

Whether you are a large or small organization, NetCaptain can scan all systems within a network. In the case of extremely large numbers of systems, multiple scan engines will be deployed. To prevent network overload, scanning can also be scheduled for nighttime or limited to specific network segments, for example.

NetCaptain comes with a base number of systems that you can scan in the license.

A system is also referred to as a target or IP address. With the included discovery scan in NetCaptain, all systems in the network can be found. This way, all systems come into view.



Scans Overview

Scan overview

Show 10 entries Search:

	Target	Credentials	Findings	Execution time	Scan started	Scan finished	Status
◉	192.168.56.104	–	113	00:07:10	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	192.168.56.107	–	104	00:11:40	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	192.168.56.102	–	51	00:06:19	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	127.0.0.1	–	18	00:12:17	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	127.0.0.1	–	18	00:12:13	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	192.168.56.107	–	105	00:11:09	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	192.168.56.104	–	114	00:07:39	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done
◉	192.168.56.102	–	52	00:05:16	2023-04-02 14:55:59	2023-04-02 14:55:59	○ Done

Showing 1 to 8 of 8 entries

Previous 1 Next

Scan policies

Show 10 entrie

Name
Full scan
Production scan

Showing 1 to 2 of 2 entrie

HOW TO IMPLEMENT NETCAPTAIN

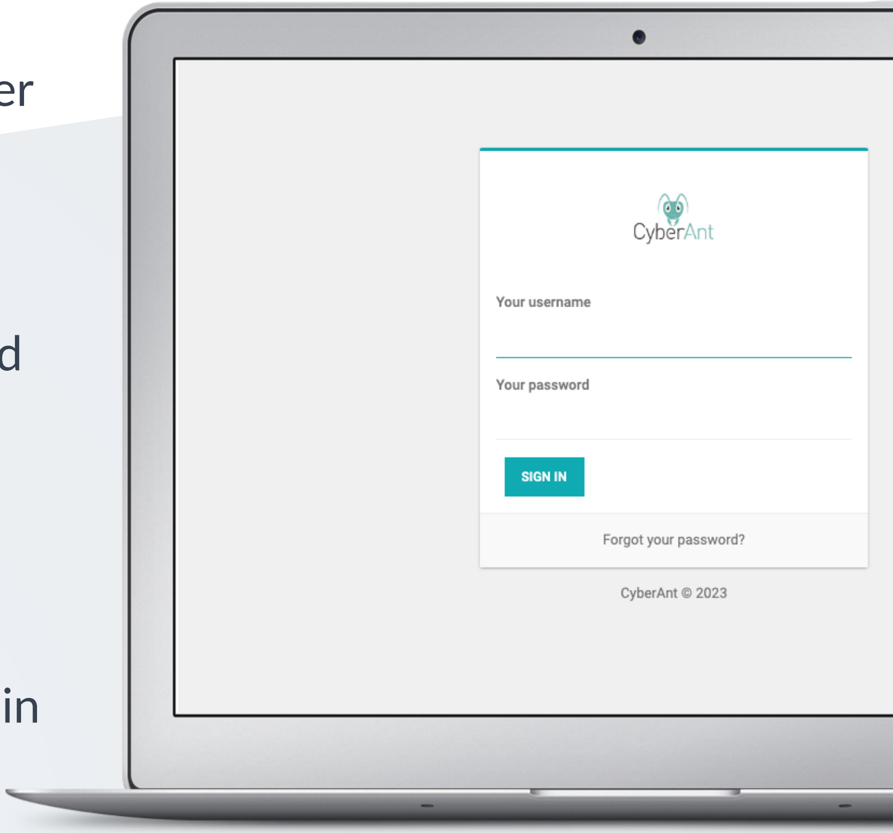
The process typically starts with an intake involving our technical specialists to assess the situation of the specific network.

Once it's clear how many systems are involved and whether multiple scan engines are required, an ISO file will be provided to install NetCaptain. The license code is used to activate NetCaptain.

Our technical specialists ensure that NetCaptain is installed correctly and offer support for the initial scans and setting up scan policies.

The strength of NetCaptain is its ease of use, so no special training is required to start using it.

The average installation duration is about 3 hours, though in exceptional cases, it may take a bit more time.



PRICING NETCAPTAIN

The cost of NetCaptain depends on the number of systems in the network (also referred to as targets or IP addresses). There are three different options, each with their own extensions.

ESSENTIAL

The essential foundation to prevent hack attacks. NetCaptain Essential is recommended for smaller IT environments. Essential Starts at € 295 pm.

PROFESSIONAL

No compromises, NetCaptain Professional includes the best tools for medium-sized IT environments. Professional Starts at € 495 pm.

ENTERPRISE

Advanced security for large companies, and organizations that run a custom software. Enterprise Starts at € 995 pm.

Along with our technical specialists, we can tailor the right package. We understand that every company has its unique needs, so we are flexible in this regard.

PRODUCT COMPARISON MATRIX

Essential

The essential foundation to prevent hack attacks. NetCaptain Essential is recommended for smaller IT environments.

Professional

No compromises, NetCaptain Professional includes the best tools for medium-sized IT environments.

Enterprise

Advanced security for large companies, and organizations that run a custom software.

	Essential	Professional	Enterprise
Number of systems included	50*	50*	100*
On-premise IT solution	✓	✓	✓
Automated scanning	✓	✓	✓
Management report	✓	✓	✓
Network vulnerabilities	✓	✓	✓
Encryption audits	✓	✓	✓
Configuration audits	✓	✓	✓
Web application vulnerabilities	✓	✓	✓
Open-source scanners	✓	✓	✓
Industrial standard scanners	✓	✓	✓
False positive reduction	✓	✓	✓
Additional information and consult	✓	✓	✓
Local scan (credential scan)	-	✓	✓
Get Help service	-	✓	✓
Malware detection	-	✓	✓
Advanced Web Vulnerabilities	-	-	✓
Multiple *scanning engines*	-	-	✓
Customization options	-	-	✓
Monthly costs	€ 295,-	€ 495,-	€ 995,-
Installation fee (one-off)	€ 495,-	€ 995,-	€ 1990,-

All prices are in euros and exclude VAT.
•Licenses can be expanded. For large numbers of servers, additional scan engines may be required.
** The Get Help service is subject to a Fair Use Policy (FUP). Exceeding the FUP may result in additional charges.

CONTACT

CyberAnt B.V.
Marconiweg 1
3899 BR Zeewolde
The Netherlands
Email: info@cyberant.com
Phone: +31 85 047 1590

NetCaptain
A brand of CyberAnt