CyberAnt

NetCaptain product sheet

Product sheet version 1.6.0
CyberAnt © 2022
Randstad 22 147, 1316 BM, Almere

Managed vulnerability scanning

Even with decent vulnerability scanners it could be a tough and time consuming job to gain real-time insight in the security level of an organisation. Orchestrating vulnerability scanners can save time and helps to speed up the mitigation time.

All Tools in One Box
CyberAnt combines the industry leading tools and orchestrate them, combining them to the best solution currently on the market. We carefully selected the scanners and made clear agreements with the suppliers. Because of that we can deliver one contract at a very competitive price.

Physical or Virtual Appliance
Depending on your architecture, we can deliver a physical appliance, or a virtual image, in the most common formats to ensure a seamless integration. Either way, your sensitive data will not leave your site.

A Clear Story
Even though we only use the best tools available, we improve the scanners by completing the results and the risk assessments. Based on the output of multiple scanners, we calculate a *CyberRisk* to indicate whether your environment is safe or not.

Fully Automated
We believe vulnerability management is a task that should be done by computers, so we made it possible to schedule tasks, such as the scanning of a network.
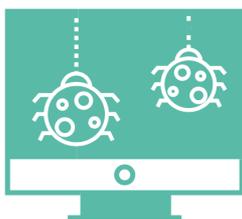
Dashboard
The CyberAnt dashboard gives insight in the CyberRisk ordered by network.

Relevant metrics
CyberAnt collects relevant metrics regarding to Cyber Security. With CyberAnt Insights you can create directly reports in HTML and PDF format.

Boost your process
We discover the security risks in your network, so you can spend your time with fixing them.

Network Scanning

Computer criminals are using security weaknesses in systems and networks to steal sensitive data and disrupt your business. By eliminating vulnerabilities as much as possible it will become increasingly difficult for hackers to infiltrate your organisation.

Asset Management
To protect your network, you must know what assets you have. CyberAnt helps to keep track of the CyberRisk of your systems, and even to discover those servers everybody forgot about.

Scan Every Device
Our solution can discover security holes in operating systems like Windows, Linux / Unix, FreeBSD and others, but also databases like Oracle, SQL server and MySQL, and network devices such as routers, switches and firewalls.

Know What's Installed on Your Assets
It's possible to scan assets without credentials, but to know exactly what software is on an asset CyberAnt can login to discover more vulnerabilities and reduce false positives.

Team-up With Your Anti-Virus
CyberAnt can detect backdoors, viruses, malware URL's and malicious content. It's the perfect companion of your anti-virus software.

Patch Management
Never miss a patch again! CyberAnt detects missing and incorrect deployed patches that leave your system vulnerable to the bad guys.

Scan Them All
CyberAnt can scan and discover a wide range of devices, from workstations to network devices.

Cloud Ready
CyberAnt is also able to perform audits on Cloud based solutions.

Configuration checks
CyberAnt checks for weak configuration to ensure that your systems are not only up-to-date, but also safely configured.

Web Applications

According to studies, more than 70% of all websites contain vulnerabilities that can lead to data breaches. Nowadays we see an increase of the ability of attackers to scan the whole internet in a short amount of time. Often organisations are not aware of the holes in their websites, or fully rely on inadequate solutions such as Web Application Firewalls.

Testing of Common Technology
CyberAnt can audit common technology such as frameworks and open source Content Management Systems (CMS), along with their plugins.

Authenticated Web Applications
Most web applications are using authentication to identify their users. CyberAnt can automatically perform a login action with a username and password.

Advanced Vulnerability Detection
Our web application scanner can find complex and hard-to-find vulnerabilities such as DOM-based XSS and blind SQL injections.

Discover sensitive content
Sometimes websites contain test data or files that weren't supposed to be on the production server. CyberAnt can detect this and warn you before others find them.

Audit your HTTPS websites
Often users are instructed to look for the little green lock in the address bar. While users assume they are safe, misconfiguration of an SSL / TLS connection can still result in the decryption of sensitive data such as passwords.

Most complete Solution
CyberAnt contains all the relevant tools to identify security weaknesses, from simple CMS websites to complex web applications

OWASP top 10
The OWASP top 10 is a list of the most common internet vulnerabilities. CyberAnt can detect all of them.

Optimal support
CyberAnt helps with a clear advice on how to fix vulnerabilities in your environment, right when we find it.

Need more assistance? Our consultants are there to help you.

Technology support

CyberAnt supports a wide range of technologies. Although it would be impossible to list all the technologies that could be scanned, the following page sums a list with software that is supported:

Operating systems

Windows 2003	Windows 7	Red Hat
Windows 2008	Windows 8	Solaris
Windows 2008 R2	Windows 10	AIX
Windows Server 2012	Windows 11	FreeBSD
Windows Server 2016	Mac OS X	HPUX
Windows Server 2019	Ubuntu / Debian	Solaris
Windows Vista	SUSE	Cisco IOS

Databases

MSSQL	MongoDB	IBM DB2
MySQL	Oracle 10	PostgreSQL
MariaDB	Oracle 11g	Informix

Applications and technologies

IIS	Spring framework	HTML5
Apache	Struts	Ruby on Rails
Nginx	Sharepoint	AngularJS
PHP	Internet Explorer	Joomla
ASPX / .NET	Firefox	Drupal
Java	Safari	Wordpress
Tomcat	Microsoft Office	jQuery
JBoss	Adobe Reader	Mootools
	Adobe Flash	…and many others

Network devices

Cisco	Palo Alto	F5 Networks
Juniper	Dell SonicWall	SCADA
Checkpoint	FireEye	Asterisk
		…and many others