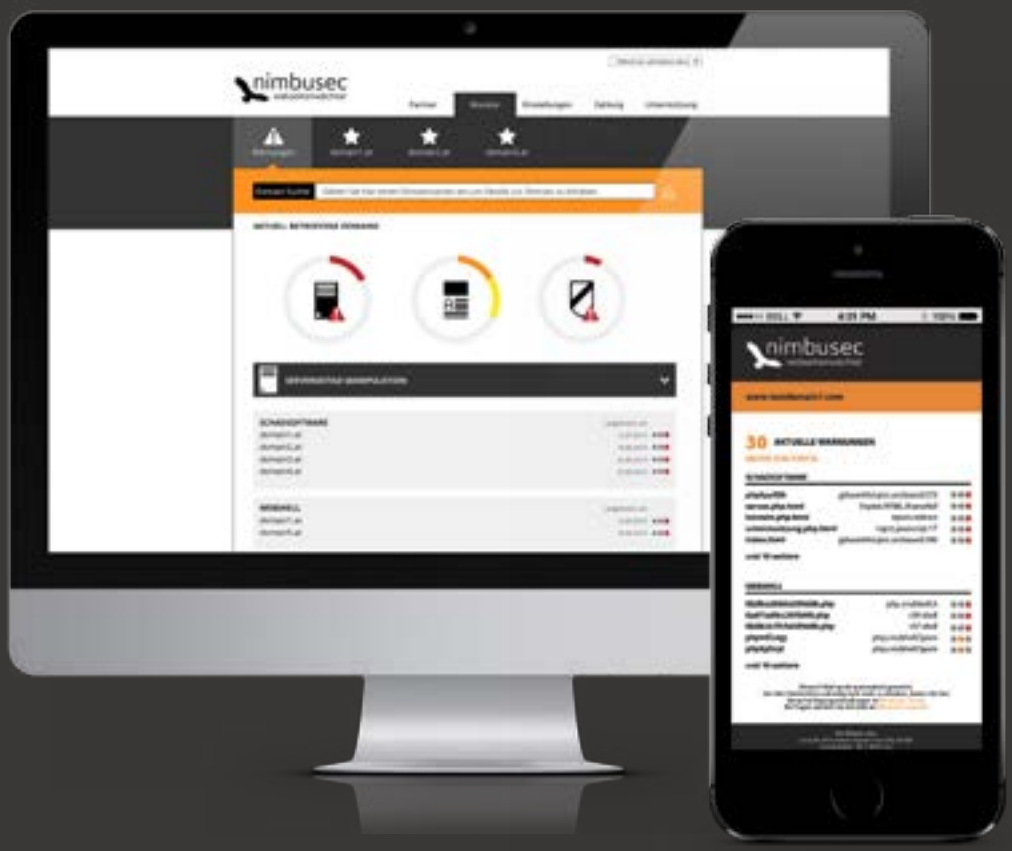
Security made in **Austria**

ENGLISH



nimbusec

website security monitor

Security made in **Austria**

IS MY WEBSITE A TARGET FOR HACKERS?

Today most hacking attacks are done by automated systems. These attackers do not care about what you do or who you are. They only aim at your websites' resources.

nimbusec monitors your websites and detects attacks when all other security measures have failed. It also informs once CMS updates are available or insecure configurations increase security risks.

Receive the right information at the right time to make sure that all your websites are secured and safe to use for your customers.

NIMBUSEC DETECTS:

- Distribution of malware
- Defacements
- Blacklisting
- Malicious webshells
- Suspicious links
- Outdated CMS
- Changed source code
- Insecure SSL certificates
- Downloadable source code
- Other security risks

DETECT ATTACKS ON YOUR WEBSITES FAST.

nimbusec monitors your websites. When it detects a security threat you will be alarmed. Fully automatic. Every day around the clock.
For thousands of websites at the same time.

- React faster
- Minimize damage
- Protect your customers
- Cost efficient

90 MILLION

different kinds of malware exist. Most are distributed through infected websites. When did you last check if your websites are safe to use?

89 PERCENT

of all Content Management Systems are not maintained with security updates. Are you sure your CMS is always up to date?

9.5 THOUSAND

websites are blacklisted by Google every day due to malware infections. They lose most of their visitors. What impact would this have on your business?

MALWARE INFECTIONS THREATEN YOUR BUSINESS

- Liability for delivering a computer virus through your website
- Breach of data security laws
- Loss of customer trust
- Breach of non-disclosure-agreements due to data loss
- Cost of lost brand value
- Lost investment in Search Engine Optimization/rank
- Risk of losing passwords through hacked web applications

ONLINE MALWARE STAYS UNDETECTED FOR 255 DAYS

Every day thousands of automated attacks aim at every public website. If a security vulnerability is successfully found the whole system will be infected within seconds. Two thirds of all affected website's administrators need weeks, months or even years to realize they have been hit.*

Today websites are the most exposed online target in corporate networks. They are a starting point for attacks aiming at data theft and digital abuse.

On average online malware stays undetected for 255 days. nimbusec monitors through regular scans and alarms within seconds. React before any damage can be done.

*Verizon Data Breach Report 2014

The nimbusec Cloud Service checks your websites from the outside in and sees it just like a human visitor would do. All analysis is done in the cloud so attackers cannot interfere.

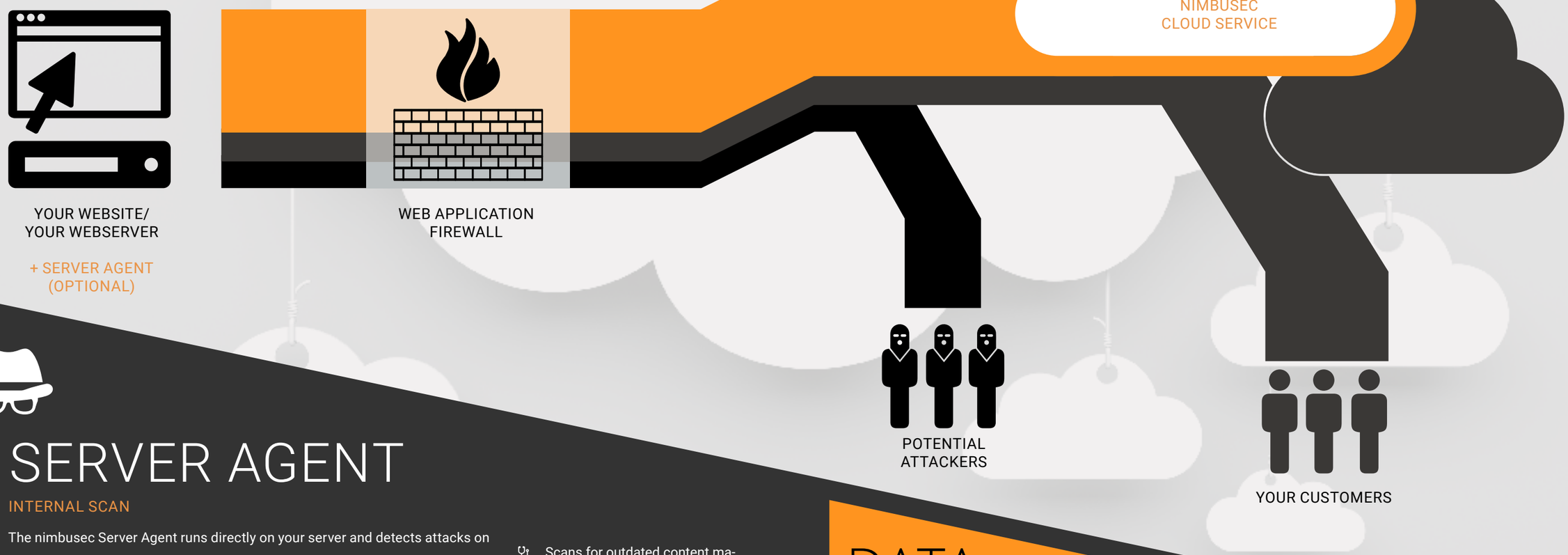
Combined with nimbusec's optional Server Agent you get a 360° view of your systems to protect your online reputation.

CLOUD SERVICE

EXTERNAL SCAN

Recognizes and alarms upon:

- Distribution of malware
- Malicious content changes
- Malicious design changes
- Blacklisting of your domains
- Suspicious external links
- SSL/TLS encryption problems



SERVER AGENT

INTERNAL SCAN

The nimbusec Server Agent runs directly on your server and detects attacks on your websites from the inside out. This gives you an edge over hidden malware in your source code. Its blazing fast algorithms are able to scan millions of files every day so you can be sure your backups are malware free.

- Detects malicious PHP code like spam shells, web shells and backdoors
- Detects server side configuration errors like forgotten installation files and unsafe file permissions
- Scans for outdated content management systems that cannot be seen from the outside
- Tracks file changes and file deletions directly on your server

DATA PROTECTION

REGULAR SCANS WITHOUT DIRECT ACCESS TO YOUR DATA

- Developed for strictest EU data protection laws - your data never leaves your server
- Code review of nimbusec Server Agent possible and encouraged

SERVER AGENT

KEY FEATURES

WEB SHELL AND BACKDOOR DETECTION

nimbusec uses proprietary heuristic analysis to detect malicious code that slips through signature based antivirus scanners. The nimbusec Server Agent extracts behavior patterns and understands what your code does. Cloud based pattern analysis recognizes never before seen malware. This unique approach leads to massively increased recognition rates compared to traditional server side security solutions.

CONFIGURATION CHECK & CMS RECOGNITION

Content management systems run more than 40% of all websites. 89% are not maintained in time. This is the single biggest reason for malware infections today. nimbusec recognizes leading CMS and alerts when new updates are available.

The Server Agent also scans for left over installation files and insecure file permissions that allow attackers to gain entry into your system.

CHANGE-TRACKING

Track all file changes in your web space and receive alerts when suspicious activities are recorded.

nimbusec's risk classification technology gets to know your standard file interactions over time. You are only informed when you really need to know what is going on.

Safe time and avoid analyzing endless log files

NIMBUSEC API FOR AUTOMATIC RESPONSE AND SCANNING MANAGEMENT

Hackers do not care about your office hours.

For immediate response nimbusec can trigger retaliation actions through its API-interface. Using universal machine to machine communication you can fully integrate nimbusec with your existing infrastructure.

Ready to use modules for automatic webshell removal, backup server activation or emergency shutdown are available.

The nimbusec API also supports automatic provisioning of new websites and remote roll-out across entire server farms.

HOSTING-ENVIRONMENTS

nimbusec offers plugins for Odin Service Automation and cPanel.

INTEGRATION IN YOUR SIEM

nimbusec integrates with SIEM solutions like HP ArcSight, AlienVault or IBM QRadar.

Security made in **Austria**

CLOUD-SERVICE

KEY FEATURES

DEFACEMENT MONITORING

Hackers change website content to embarrass the original owner or even replace it with illegal web shops. Nimbusec's statistical content analysis recognizes such attacks so you can react before your reputation takes damage.

MALWARE ALERTING

Nimbusec's Cloud Service behaves like a normal website visitor, but scans all data it receives in multiple ways. If malware is detected we alert immediately. These scans are performed from the outside cannot be manipulated.

BLACKLIST MONITORING

We track blacklists like Google Safe Browsing or Web of Trust. If your website is listed there it will not only lose its search engine ranking, but visitors even receive warnings. The faster you react the smaller the damage to your reputation.

SSL-ENCRYPTION CHECKS

SSL/TLS is the base technology for secured websites and online shops.

Nimbusec tests acceptance and correct configuration of your SSL certificates.

We also warn before your certificate expires.

Find even more information at:

www.nimbusec.com

www.nimbusec.com

Nimbusec GmbH
Fadingerstraße 15 | 4020 Linz | Austria
office@nimbusec.com | +43 699 11 093 985

FN 394170m | FBG Linz | VAT ID ATU67830957
Responsible authority:
Magistrate of the city of Linz/Danube

Member of the Upper Austrian
Chamber of Commerce
section UBIT