Hire **Deep Security**
to automatically protect your servers

Taking care of the right level of protection against cyber threats should be given priority nowadays.
Perhaps ensuring security means that you have to deal with many problems, including:

- No time to take appropriate precautionary measures
- Limited human resources that could effectively ensure cybersecurity
- Use of old operating systems not supported by the manufacturer
- Loss of business continuity in connection with work carried out in the server environment
- Development of a comprehensive action strategy to protect against all types of threats.

If so, then our solution for you is **Deep Security of the Japanese company Trend Micro**. This name covers a set of several tools designed to protect servers: physical (bare metal), virtual, cloud and container. Deep Security means:

- **Flexible solution** that allows you to adjust the level of protection to the current needs, the ability to choose the relevant configuration of three modules
- **Automatic server protection** in real time, without loading the machine
- **Managing security policies** using an intuitive console.

Benefits of the implementation:

- **Minimization of the human factor** − the possibility of avoiding negligence, e.g. failure to update the system/application on time, accidental malware launch.

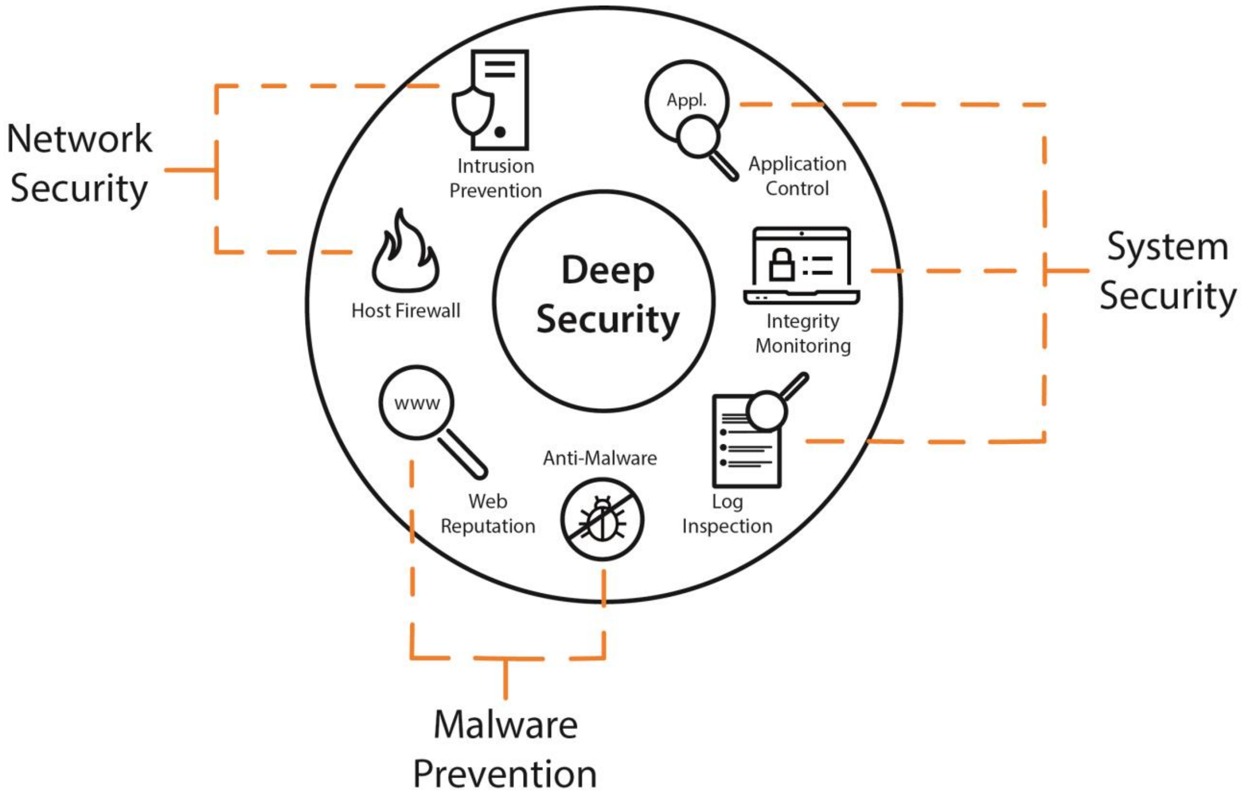
- **Ongoing control of security measures** − the possibility of generating security measures activity reports at any time. The ability to change security policies to more restrictive or mild ones.

- **Automation of processes ensuring cybersecurity** − relieving IT departments that can focus on other activities. Helpful both in companies with smaller, often one-person IT departments, as well as in those that have extensive server environments that require protection.

- **Easy management** − a convenient management console located in the professional Atman Data Center WAW-1. Management of all Deep Security tools from one place. In addition, provided onboarding material and knowledge of specialists.

- **Business continuity** − no need to shut down/restart servers to patch security vulnerabilities in operating systems and applications.

- **Comprehensive solution** − Deep Security protects against security vulnerabilities, malware and suspicious activity in a server environment.



Deep Security architecture

Network Security Module − consists of two tools: Firewall and Intrusion Prevention, provides protection against network attacks and system and application security vulnerabilities.

Firewall

- A flexible and configurable firewall that protects network endpoints
- At the moment of module installation it is inactive

Intrusion Prevention (Virtual Patching)

Virtual patching automatically protects the server against threats related to outdated software by “applying” patches until the update is performed:

- Protects servers that do not have uploaded manufacturer-released updates (Windows, Linux)
- It is applicable to web servers, database engines, frameworks
- Protects servers running on old operating systems that no longer have manufacturer’s support and official updates (Windows 2003, Windows 2008 Server, Debian 6, etc.)
- Thanks to the recommendation scanner launched once a day, it continuously provides the latest database of new vulnerabilities
- Eliminates the problem of server downtime and not performing updates on time

Did you know...

61 days − on average, that is how much faster Deep Security customers receive a “security patch” compared to people using updates from the manufacturer. Often, it only takes a few hours or days from the time the vulnerability is detected to launch the attack. In such case, response time is of the utmost importance!

Deep Security

Malware Prevention Module **– consists of two tools: Web Reputation and Antimalware, provides protection against malware and infected sites.**

Web Reputation
Scans sites for malicious code and categorizes content on the site. Through this analysis, the tool allows or blocks access to the site.

Antimalware
Protects against all types of malware, including:

- **Spyware** – malicious spyware that secretly observes the computer user's activity without their consent and reports it to the author of the software. It is usually unknowingly downloaded when installing legitimate applications or opening infected attachments in emails.
- **Keylogger –** software that records user's keystrokes on the keyboard and sends them to the hacker who thus receives confidential information, logins, and passwords.
- **Ransomware** – software that blocks/encrypts the device and data and demands a ransom. One of the most frequently used tools by cyber criminals.

Did you know...
It is recognized that the average antivirus software is able to detect only 45% of all attacks. Antimalware is definitely a more effective solution.

System Security Module **– consists of three tools: Application Control, Integrity Monitoring, Log Inspection, detects suspicious activity on the server.**

Application Control
Prevents the launch of malware by constantly monitoring changes on the protected servers.
Blocks files and scripts identified as unknown.

Integrity Monitoring
Scans the server for unexpected changes in the value of registry keys, installed software, files. The tool detects changes and informs the user about them.

Log inspection
The tool allows capturing security incidents, e.g. application errors, system shutdowns, excessive logins, policy changes.

See how little your server security costs:

Module	Cost
Network Security (Intrusion Prevention, Firewall)	**PLN 75 /month/server**
Malware Prevention (Antimalware, Web Reputation)	**PLN 40 /month/server**
System Security (Application Control, Integrity Monitoring, Log Inspection)	**PLN 75 /month/server**
All modules	**PLN 160 /month/server**