RADAR
SMART SOLUTION

Spare yourself such a morning!

PLUG & **DETECT**

Continuous IT security monitoring for companies with up to 500 employees

The success concept of RadarServices

Specially for companies with up to 500 employees.

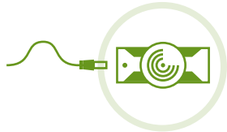
PLUG & DETECT

Continuous IT security monitoring made easy

RadarServices is Europe's leading provider of continuous IT security monitoring. The portfolio was developed for timely IT risk detection – originally for large companies and public authorities. It has been tested, improved and perfected over the years.

The experts at Europe's largest competence centre for IT security also have an eye on the security of small and medium-sized enterprises. Radar Smart Solution was developed for these organisations with up to 500 employees.

Plug & Detect comprises:



Plug

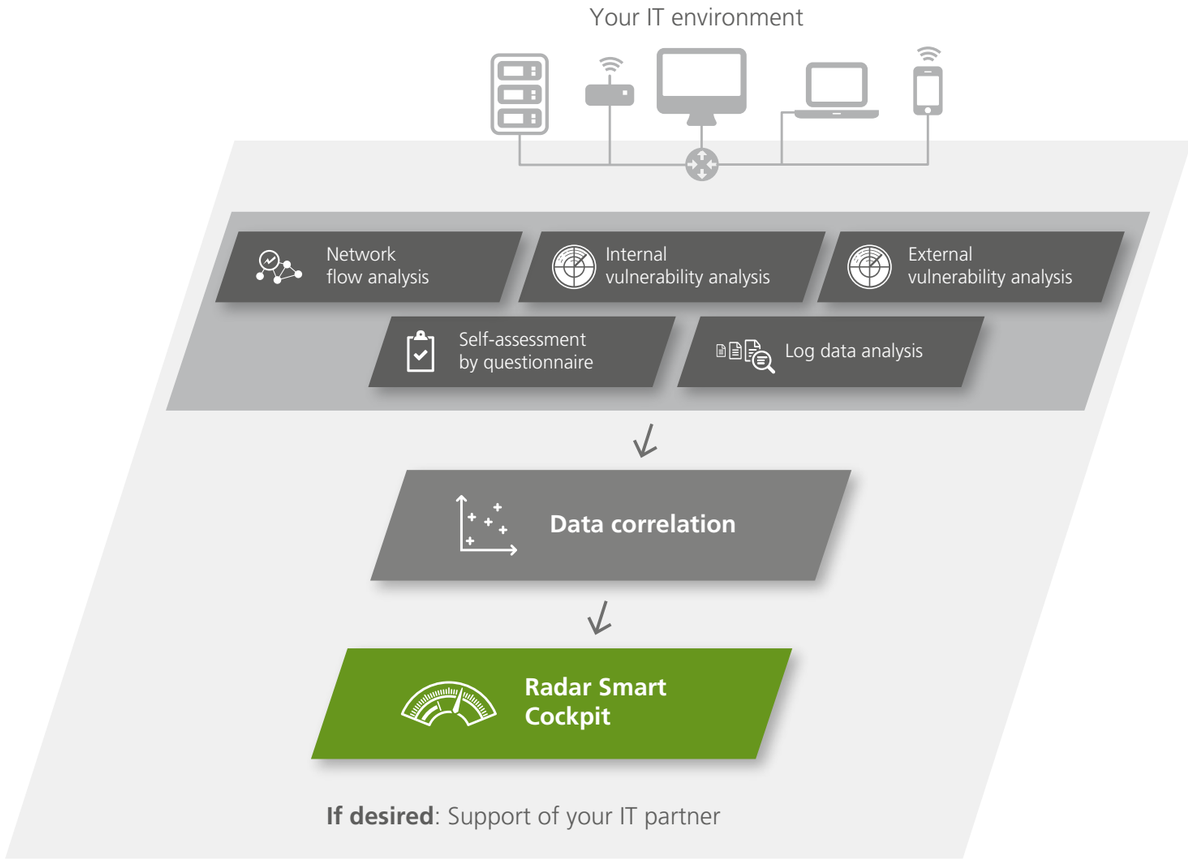
Radar Smart Solution consists of hardware, the "Radar Smart Box", which is used for data collection. Connecting the Radar Smart Box to your corporate network is easy.

Detect

After implementing the Radar Smart Box, data that may potentially indicate security risks are collected from multiple sources and analysed automatically within the network as well as externally. The Radar Smart Cockpit gives you an overview of the insights gained: where do security problems exist? Has any unauthorised access to your network been detected? And: what do you need to do specifically to counter identified problems and improve your overall level of IT security?

RADAR SMART SOLUTION

The system



Your benefits

Do you continuously monitor your network for security incidents?

WHICH IT SECURITY MEASURES ARE YOU CURRENTLY TAKING?

Firewalls and anti-virus software are standard today.

THE BAD NEWS:

Attackers focus specifically on what conventional security measures do not recognise as a threat. They recognise only what has been given to them in advance as a pattern and that is not enough today. This explains the global trend in the area of IT security: away from threat prevention and more towards identifying threats and mitigating actual rather than fictitious risks.

Radar Smart Solution detects the current threats – attacks or vulnerabilities in your IT – and reports them to you in a structured and prioritised order, providing assistance on how to remove them.

Protecting data, patching, identifying, assessing and managing risks – how do you prioritise the numerous tasks of IT security?
Time resources are a very scarce commodity. This often applies especially to the IT security department in companies. The tasks are numerous and varied. The level of complexity is high and requires profound expert knowledge from various disciplines. **How can you manage the many tasks in such a way that your overall IT security level is as high as possible?**

Radar Smart Solution arranges the tasks of IT security for you. The decisive factor is prioritisation according to the estimated level of risk. This means you know exactly which priorities to set and where you should use your time resources most effectively to increase your IT security to the highest degree possible.

Unique

State-of-the-art security
in a lean form.

Radar Smart Solution has been specially developed for small and medium-sized businesses.

Continuous IT security monitoring comprises the most important sources of security-relevant information.

The cloud base and the standardised, fully automated service components enable the lean form of IT security monitoring that was previously only affordable for large organisations.

The Radar Smart Cockpit, including safety troubleshooting guides, is written in an easy-to-understand form.

The selection of different service packages allows the maximum possible coverage of IT security monitoring in line with your budget.

The selective or permanent involvement of an IT partner, depending on your needs, gives you flexibility for the expert support you actually need and the possibility of working with a partner you prefer.

Network flow analysis

Dangerous malware and other network traffic risks are analysed based on signature and behaviour.

Data are constantly being received from the internet and sent to the internet. This does not only apply to the data that you have intentionally sent and received. Attackers also use this exchange. The Radar Smart Solution detects suspicious patterns and anomalies such as malware, command and control servers, bots, spyware, drive-by sources, DDoS targets and sources.

Signature-based recognition is based on given patterns. However, attackers are increasingly using routes into your network that were not previously known. Behaviour-based detection is focused specifically in this area.

Depending on the package you have selected, a maximum amount of data to be analysed is included.

External and internal vulnerability analysis

Continuous external and internal vulnerability scans detect existing vulnerabilities in your IT system and report them so you can resolve them in a structured way.

External and internal vulnerability scans (known as vulnerability management and assessment) give you an overview of currently existing vulnerabilities in your network. You can see the result in your Radar Smart Cockpit: a clear list of priorities to be dealt with.

In addition to fast and efficient authenticated or unauthenticated vulnerability scans, compliance and password checks detect configuration issues related to applications as well as password and user policies. Standard or missing passwords are identified. Outdated patch versions of installed software and services are exposed in Windows systems with registry and dll checks.

Vulnerabilities are categorised into high, medium and low risk and the possibility of their exploitation. The result is an easy-to-understand overview of the current vulnerabilities and ready-made information to meet compliance requirements. Employee training is not necessary.

The number of devices that matter for the scans varies depending on the package you choose. Depending on the package you choose, either one or both types of scans will be performed.

Log data analysis

Logs are an important source for tracking down security-relevant events. As such, they are collected, analysed, correlated and possibly result in alerts.

Logs from various sources in a network (servers, clients, network devices, firewalls, applications, etc.) provide crucial information on security-relevant events. The goal is to filter out the really relevant information from millions of events. In technical terms, this IT risk detection module is called Security Information and Event Management (SIEM).

Numerous common log formats are supported. Define from a list of standardised log sources the ones that are relevant to your company. Depending on the package you have chosen, a maximum number of log sources is included.
Information and events from these log files are aggregated. A state-of-the-art correlation engine with continuously enhanced and tailor-made rules and policies identifies potential risks.

Self-assessment by questionnaire

In addition to findings from the automated risk analysis, additional factors of your IT security are included.

What is the current risk that your company might incur damage as a result of a cyberattack? The Radar Smart Solution gives you an overview of the facts that underlie your current IT risk. This includes not only the findings that are drawn from the automated risk analysis with the help of our tools. Frame factors that determine your IT security are also crucial. Organisational details inside and outside your company are regularly queried and included in the risk analysis as part of a simple and understandable self-assessment.

Data correlation

Security-relevant data are derived from the large mass of data with the help of a comprehensive correlation. Data are correlated both within a risk detection module and across several modules.

A single piece of information within a mass of data often does not immediately indicate its security relevance. Only by combining information do the valuable pieces of the puzzle necessary to track down an attacker come together. Correlating logs with vulnerabilities, IDS data, or SIEM findings provides an overall view of security-related data.

Correlation and cross-correlation are based on rules, policies, and self-learning algorithms: Rules are predefined to recognise patterns. They are expanded on an ongoing basis. Policies are used to determine if specific actions take place at the right time and in the right place. Self-learning algorithms include the correlation engine's ability to distinguish between normal and abnormal occurrences, and to recognise behavioural changes in applications, servers, and other network areas. Off-hours use, overuse of applications or other IT services, and patterns of network traffic over time and compared to past periods (taking into account daily, weekly, monthly, and seasonal variations) are examples of anomaly detection.

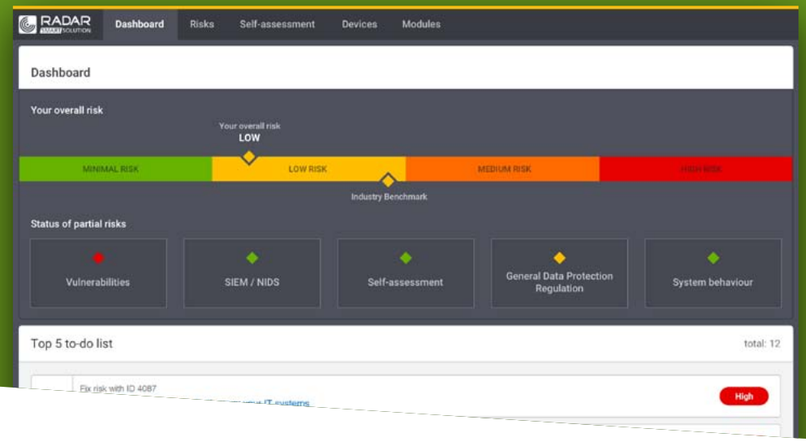
Threat intelligence

Brings together the latest security-relevant information.

Threat intelligence information is gathered from numerous internal and external globally leading sources, both commercial and open source. Thanks to this information, harmful behaviour can be detected faster – for example, connections to or from suspicious IPs of the internal IT infrastructure.

Apart from the IP addresses with bad reputation, this information includes URLs with the same characteristics, e-mail addresses used for phishing, and file names, file paths and user agents used for malware.

The security-relevant data extensively collected and processed by RadarServices in combination with the comprehensive threat intelligence information from various sources allow RadarServices to be exceptionally fast when it comes to detection & response.



Radar Smart Cockpit

All insights gained are presented centrally, understandably and clearly in the Radar Smart Cockpit. They are prioritised and come with information on how to remove them. So you know what to do when.

The cockpit contains your individual overview of the security-relevant information that the automated detection has delivered. The results are presented with identified, classified and prioritised security issues.

The overview of the existing devices offers the possibility of selecting which devices should be included in the check.

You know what should be done in what order and hold the information you need for the next steps to be taken to correct or minimise the risk. Save yourself hours of searching the websites of individual manufacturers. Radar Smart Solution provides the most important information in your cockpit.

Expert support on request

How an IT partner can subsequently assist you.

Depending on how much capacity you have in your company for IT security, it may make sense to include an IT partner in the tasks surrounding continuous IT security monitoring.

He can assist you in the following areas, for example:

- Deeper expert analysis of automatically obtained results
- Support in removing risks and/or vulnerabilities
- Help in case of emergencies/acute attacks
- Contact person for further questions or handling the risk detection tools
- Advice with questions relating to your ongoing IT security
- Carrying out IT security and employee training

Overview of the editions

Your company size*	**1–50** employees	**50–100** employees	**100–250** employees	**250–500** employees
RADAR SMART SOLUTION **Starter**	NIDS (50 MBit) VAS external (2 IPs)	NIDS (100 MBit) VAS external (5 IPs)	NIDS (200 MBit) VAS external (10 IPs)	NIDS (300 MBit) VAS external (25 IPs)
RADAR SMART SOLUTION **Basic**	NIDS (100 MBit) VAS external (2 IPs) VAS internal (50 IPs) Risk questionnaire	NIDS (200 MBit) VAS external (5 IPs) VAS internal (100 IPs) Risk questionnaire	NIDS (500 MBit) VAS external (10 IPs) VAS internal (250 IPs) Risk questionnaire	NIDS (1 GBit) VAS external (25 IPs) VAS internal (500 IPs) Risk questionnaire
RADAR SMART SOLUTION **Plus**	NIDS (100 MBit) VAS external (2 IPs) VAS internal (50 IPs) SIEM (5 log sources) Risk questionnaire	NIDS (200 MBit) VAS external (5 IPs) VAS internal (100 IPs) SIEM (10 log sources) Risk questionnaire	NIDS (500 MBit) VAS external (10 IPs) VAS internal (250 IPs) SIEM (25 log sources) Risk questionnaire	NIDS (1 GBit) VAS external (25 IPs) VAS internal (500 IPs) SIEM (50 log sources) Risk questionnaire

* Your company size is a rough indicator for the number of IT devices in use/to cover for risk detection.
The number of IT devices is the basis for the pricing.

RADAR SERVICES

The European Experts
in IT Security Monitoring
and IT Risk Detection

RadarServices is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client's Security Operations Centre (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT security monitoring and an overview of security-related information throughout the entire IT landscape of an organization.

Radar Smart Solution is the Plug & Detect Solution for IT Security Monitoring in companies with up to 500 employees.

RadarServices
Zieglergasse 6
1070 Vienna
Austria

Phone: +43 (1) 929 12 71-0
Fax: +43 (1) 929 12 71-710
Email: sales@radarservices.com
Web: www.radarservices.com

RadarServices Germany
Taunustor 1
60310 Frankfurt a. M.

Phone: +49 (69) 2443424 655
Email: sales_germany@radarservices.com