APT Defense Service – Protection against targeted attacks.

Managed security service to defend against hacker offence

More than 60 percent of small and medium-sized companies were among the hardest hit by acts of IT espionage or sabotage. Most of the organizations have already been compromised without having even the slightest idea. Companies often cannot handle the recognition and targeted treatment of security incidents, technologically as well as with respect to the required special know-how.

Our solution – the APT Defense Service:
The principle is as practically oriented as effective: comprehensive know-how combined with top technology. Easy on the budget as „Security as a Service".

Customized protection against cyber attacks

For conventional security systems, they are often no longer detectable: Targeted attacks with which cyber criminals attempt to gain access to company data. Recognizing and successfully blocking Advanced Persistent Threats (APT) requires innovative security technology and experts who have mastered these technologies.

Both are no longer reserved just for large corporations: The new APT Defense Service now also offers small and medium-sized companies targeted protection against cyber attacks.

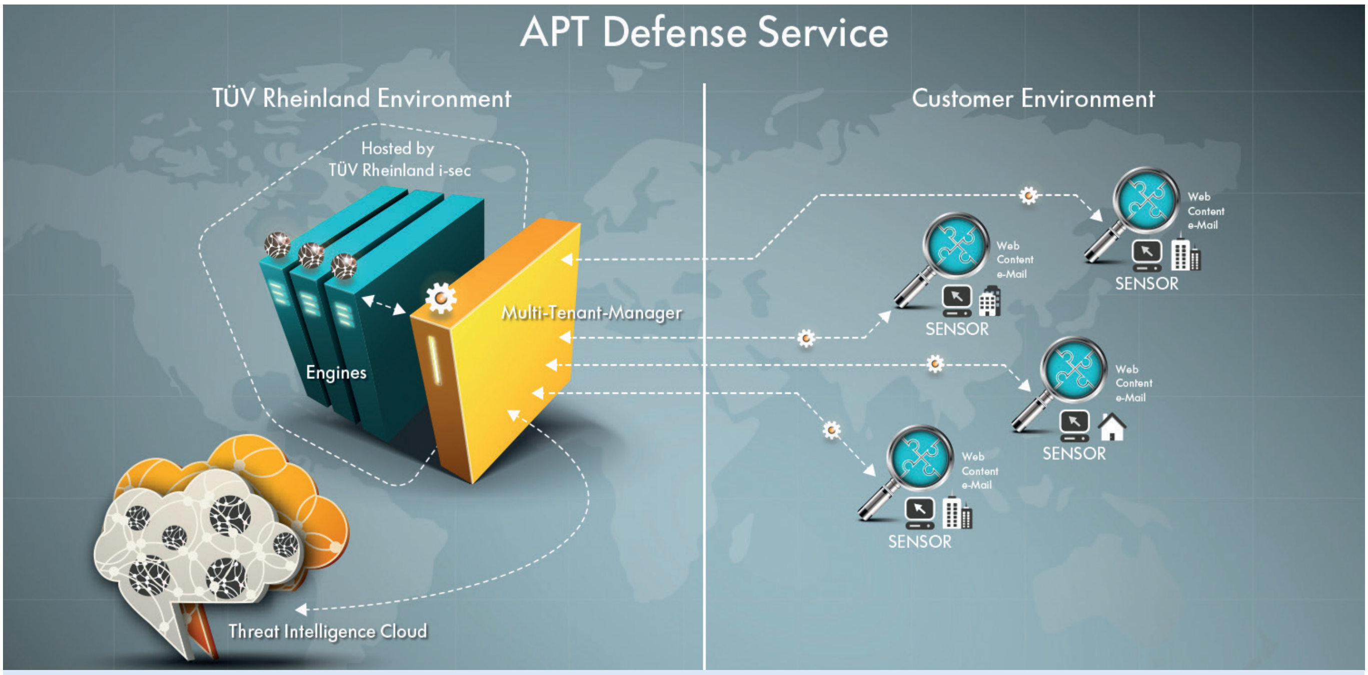
Provide your intellectual property with long-term protection against data theft, espionage and sabotage – with the APT Defense Service from TÜV Rheinland.

Your benefits

- **Best practice – at an attractive price:** Your company utilizes highly innovative behavior-based sensor technology that is currently available on the market for the protection against cyber attacks.
- **Permanent security monitoring:** The detection of security incidents is done completely automatically. The information is provided in real time to the TÜV Rheinland CSIRT for analysis, assessment as well as recommendations for mitigation actions.
- **Take the strain from your IT staff and train them:** Working together with experts from TÜV Rheinland helps not only to relieve pressure on your IT employees but provides them with training at the same time.
- **Customized solutions:** You determine the service level yourself. The APT Defense Service can be booked with modular Service Level Agreements: from operation up to forensics.
- **Planning reliability through Security as a Service:** Once the sensors are installed, the company does not encounter any operational tasks until the time at which a security incident has been identified.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.



1. **Technical requirements:**
   Purchasing extensive hardware is not required. TÜV Rheinland merely places small, cost-effective sensors in monitoring mode (TAP) in the customer network infrastructure. These sensors subject the network traffic generated in the company (web, mail, etc.) to a preanalysis.
2. **Detection of anomalies:**
   If the sensors detect indicators that point to an attack or an infection, the suspicious network traffic is diverted completely encrypted to a TÜV Rheinland data center.
3. **Qualification of the security incident:**
   In the analysis environments of TÜV Rheinland, the possible damage potential of the traffic is being checked, i.e. tests are run how these data behave when they are viewed or executed.
4. **Limiting the attack:**
   In the form of a managed security service, the experts of TÜV Rheinland test and qualify the results. In case of an infection or an attack, they define targeted defensive measures and support the internal IT of the customer for specific defensive measures.

In the last two years, half of all the companies in Germany were the victim of digital industrial espionage, sabotage or data theft*.

*Survey by the digital association Bitkom in 2015, www.bitkom.org; the survey questioned managers and authorized security personnel of 1,074 companies as a representative sample.

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.