# BECAUSE NO TWO ATTACKS ARE THE SAME
## APT PROTECT PRO

### A GROWING THREAT

Businesses have never been more vulnerable to cybercrime. Increasingly, their core capabilities are the subject of coordinated attacks. Industrial spies are out to capture valuable knowledge. Black hats driven by politics or profits are setting their sights on business-critical processes. If these are manipulated or disrupted, the consequences are serious and damaging. Traditional defense strategies are no obstacle to these new and determined assaults. Often, as with zero-day exploits, vulnerabilities for which no patches are available are exploited to launch multi-stage attacks that evade typical commercial firewall and antivirus solutions. The objective is to spy on the target organization and explore its network unnoticed – allowing the perpetrator to steal intellectual property or other assets undetected.

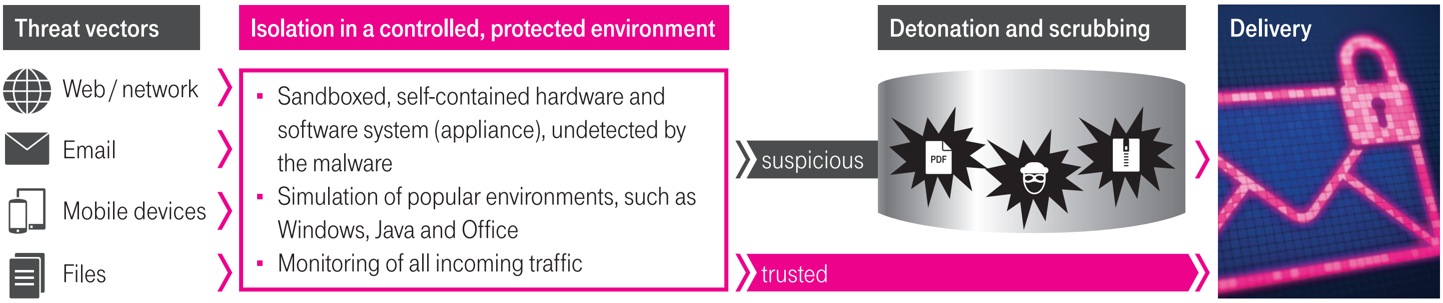
### EFFECTIVE PROTECTION

Today's cybercriminals employ diverse and dynamic malware. They attack via multiple vectors – for example, they can be Web-based and / or email-based, and employ spear phishing and malicious files. Conventional firewalls and antivirus solutions are insufficient, as they are signature-based, reactive, and only recognize known threats. False positives are common. In contrast, APT (Advanced Persistent Threat) Protect Pro offers effective defenses against Internet, email and network hazards – to stave off sophisticated cyberattacks with potentially severe outcomes. All files that enter the network via the Internet or email are checked for unknown attack patterns. APT Protect Pro is available as a cloud or an on-premises solution. The latter can be optionally hosted in a T-Systems data center. All versions are modular and vendor-agnostic, and can be integrated into an SOC / SIEM (security operations center / security information and event management) system.

APT Protect Pro features virtual machine-based execution and threat emulation, giving businesses effective defenses against attacks that conventional security solutions fail to identify in time, if at all.

T · · Systems ·

# THREATS COME IN A VARIETY OF GUISES
## THE VM-BASED EXECUTION ENGINE DETECTS THEM ALL



Threat vectors

Web / network

Email

Mobile devices

Files

Isolation in a controlled, protected environment

- Sandboxed, self-contained hardware and software system (appliance), undetected by the malware
- Simulation of popular environments, such as Windows, Java and Office
- Monitoring of all incoming traffic

suspicious

trusted

Detonation and scrubbing

Delivery

## AUTOMATED RECOGNITION

APT Protect Pro offers especially powerful defenses against targeted attacks, for example via bogus email attachments, or unintentional downloads of malware from websites. These dangers are identified immediately.

**How it works:** All incoming traffic is monitored. If suspicious files or code is discovered – for instance, in an email with an attachment – the file is isolated and opened automatically in a controlled environment to examine its behavior. In other words, it is executed and analyzed in a virtual "detonation chamber" – a self-contained, protected appliance that simulates common desktop environments such as Windows, Java and Microsoft Office, without this action being recognized by the malware. The solution determines within seconds whether the email, document or Internet traffic is infected. Safe content is delivered to the addressee. Dangerous files are "scrubbed", and then forwarded. Information on threats and non-threats is automatically added to blacklists or whitelists for use in future scanning routines. APT Protect Pro is also a source of intelligence for management reports on threats, infections and countermeasures.

## A UNIQUE SOLUTION ONLY AVAILABLE FROM T-SYSTEMS

T-Systems is Germany's leading provider of ICT security solutions, with operations in 25 countries and over 25 years' hands-on experience of combatting cyberthreats. More than 1,200 security experts ensure the success of large-scale, multinational projects, and provide cast-iron protection for complex infrastructures. Enterprises that opt for APT Protect Pro also benefit from T-Systems' one-stop, end-to-end solution – including consulting, integration and ongoing operations. Optional services, such as event monitoring and analysis, and security-incident response, are also available.

## APT PROTECT PRO CLOUD

This security-as-a-service solution for email traffic is an optional addition to E-Mail Protect Pro. It guards against zero-day exploits, APTs, and unknown malware. Files in diverse formats are checked at operating-system and CPU level to prevent malware from bypassing security mechanisms.

**Detect package:** files are delivered and threats emulated; reporting only.
**Prevent package:** files cached and delivered after threat emulation.
**Prevent Plus package:** elimination of threats; immediate delivery of scrubbed file as a PDF.

**Benefits:**

- Cost-effective and usage-based – OpEx not CapEx
- No need to install hardware or software
- Maximum security provided by a Deutsche Telekom data center
- Simple to integrate into existing IT architectures

## APT PROTECT PRO ON PREMISES

This solution runs on dedicated systems, either on the customer premises or hosted at a T-Systems data center. It adds protection against APTs to the perimeter defenses of a firewall. On one hand, it wards off conventional threats through URL filtering, antivirus and spam scanning, anti-bot and application control, plus regularly updated pattern and blocking lists. On the other hand, the virtual machine-based execution and threat emulation engine provides insulation from zero-day exploits and unknown threats.

**Predefined bundles:** based on data volume, number of users and features.
**Support:** central user helpdesk.
**24 / 7 operation:** Deutsche Telekom security experts; optional SOC service.

**Benefits:**

- Maximum protection, including IPS, Web activity, email and APT defenses
- Try-and-buy versions (for Cisco)
- End-to-end solution including management, licensing, liaison with vendor support
- No CapEx (rental solution)

**CONTACT**
T-Systems International GmbH
E-Mail: security-info@t-systems.com
Internet: www.t-systems.com/security

**PUBLISHED BY**
T-Systems International GmbH
Hahnstrasse 43d
60528 Frankfurt am Main, Germany

Published 07/2017 | subject to errors, omissions and change | typix