2. AUTOMOTIVE SUPPLIERS' DAY

T · · Systems ·

CYBER SECURITY:
ADVANCED MALWARE DETECTION

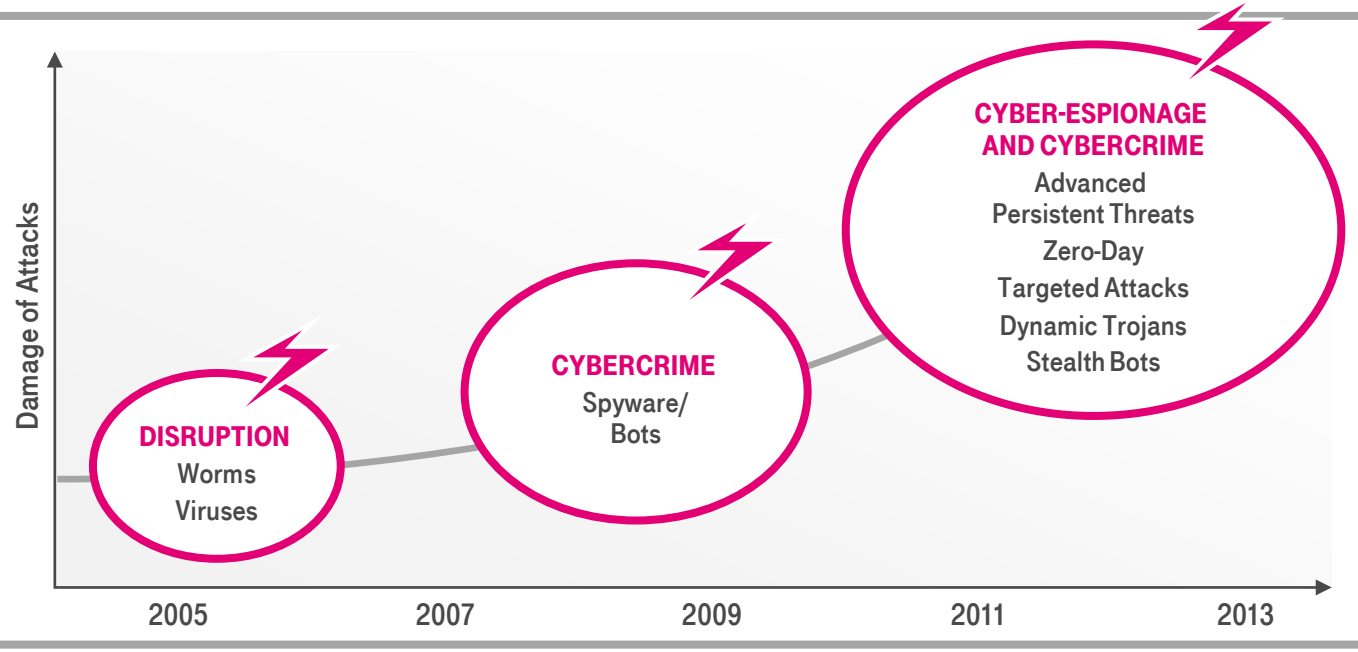
Demo

T · · Systems ·

CYBERANGRIFFE STEIGEN RASANT AN

BEDROHUNGEN VERÄNDERN SICH:

Heutige Angriffe **durchdacht** und **erfolgreich**



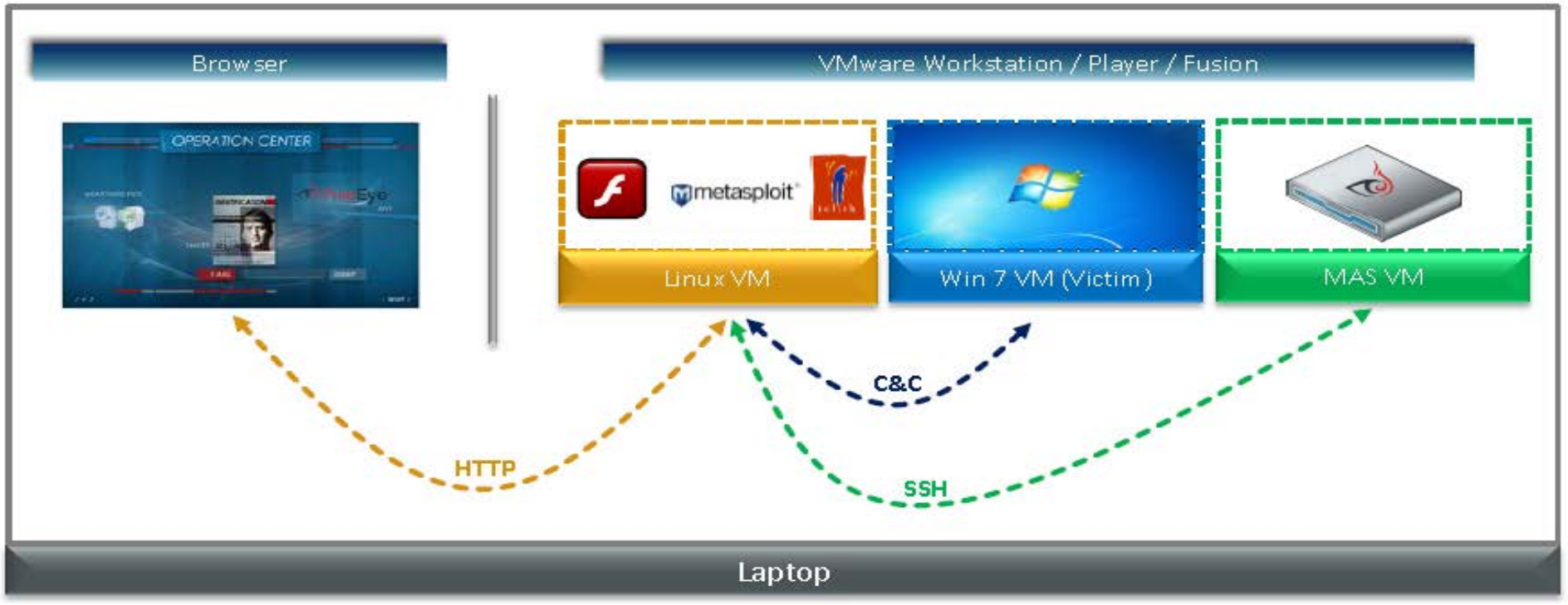
"Organizations face an evolving threat scenario that they are ill-prepared to deal with ...
threats that have bypassed their traditional security protection techniques and reside undetected on their systems."

Gartner, 2012

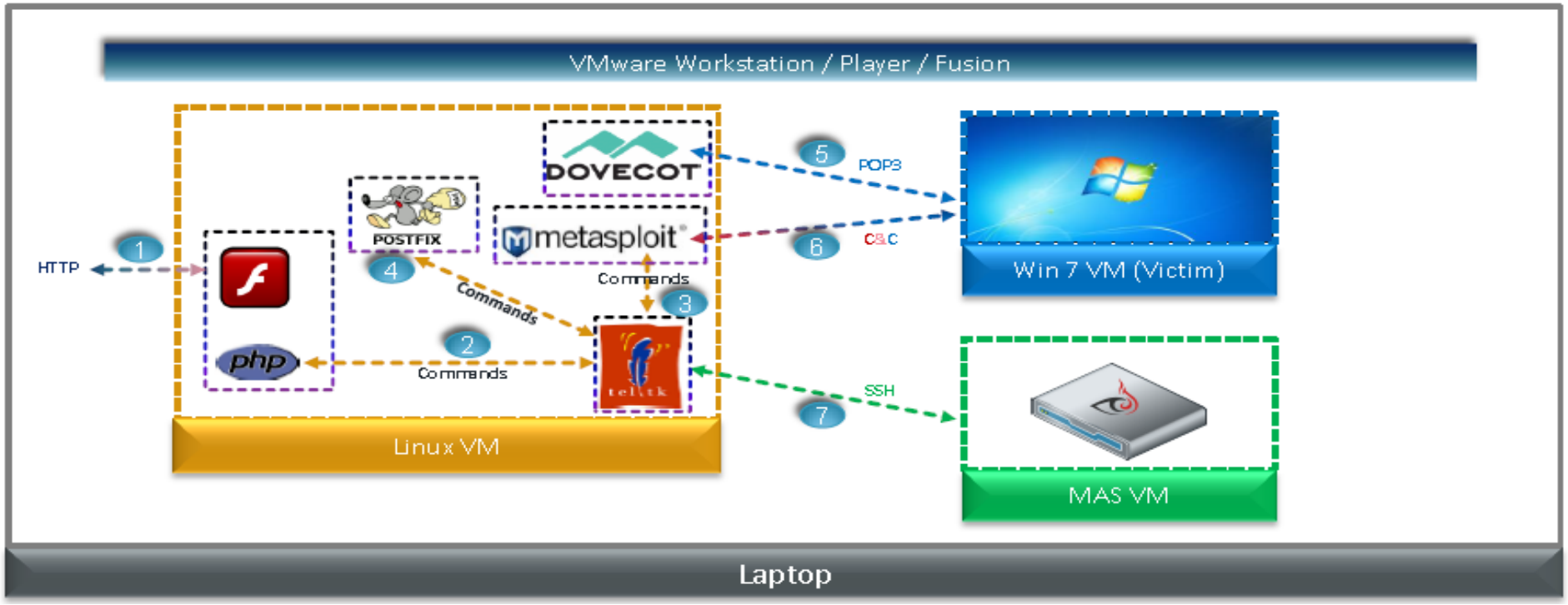
HOCHKARÄTIGE ANGRIFFE WERDEN IMMER HÄUFIGER

CXO Level Demo

DEMO AUFBAU
HIGH LEVEL



DEMO AUFBAU
LOW LEVEL



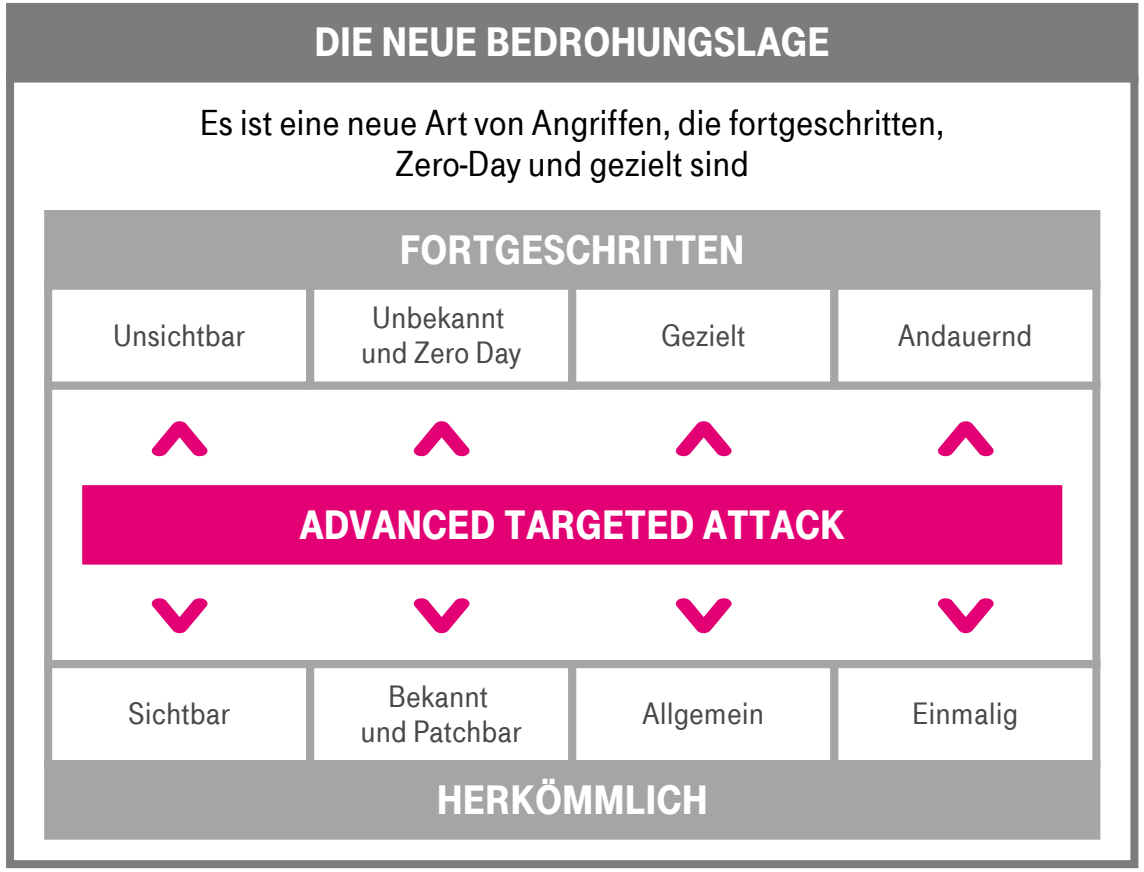
VIELEN DANK

IHR ANSPRECHPARTNER:
Thomas Schmitt
Telefon: 0151-52845407
E-Mail: T-Schmitt@t-systems.com

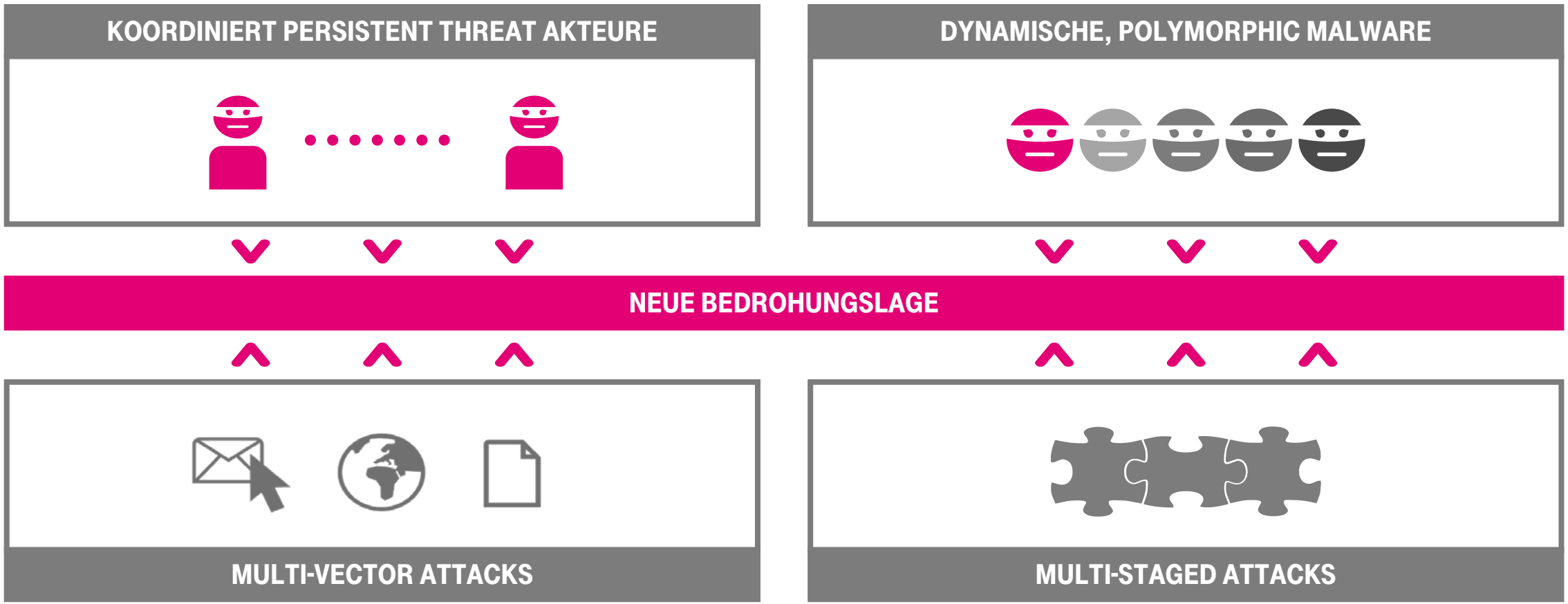
BACKUP

DEFINITION VON ADVANCED TARGETED ATTACKS

- Verwenden fortgeschrittene Techniken und/oder Malware
  - Unbekannt
  - Gezielt
  - Polymorph
  - Dynamisch
  - Personalisiert
- Verwenden Zero-Day Angriffe, handelsübliche Toolkits und Social Engineering
- Zielen oft auf geistiges Eigentum und Passwörter ab und breiten sich im gesamten Netzwerk aus
- Auch bekannt als Advanced Persistent Threat (APT)



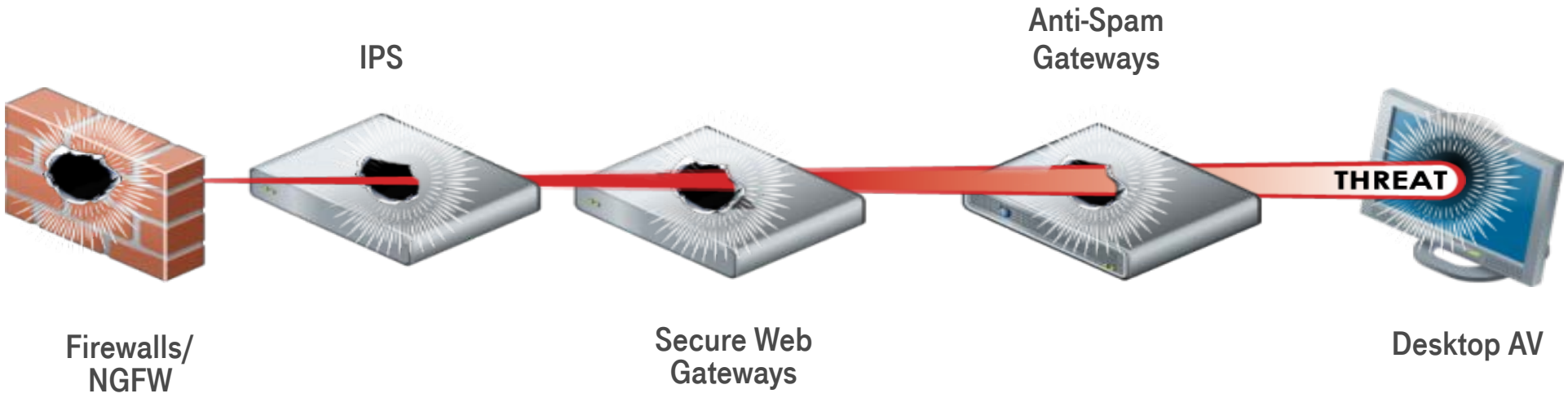
WAS HAT SICH VERÄNDERT?



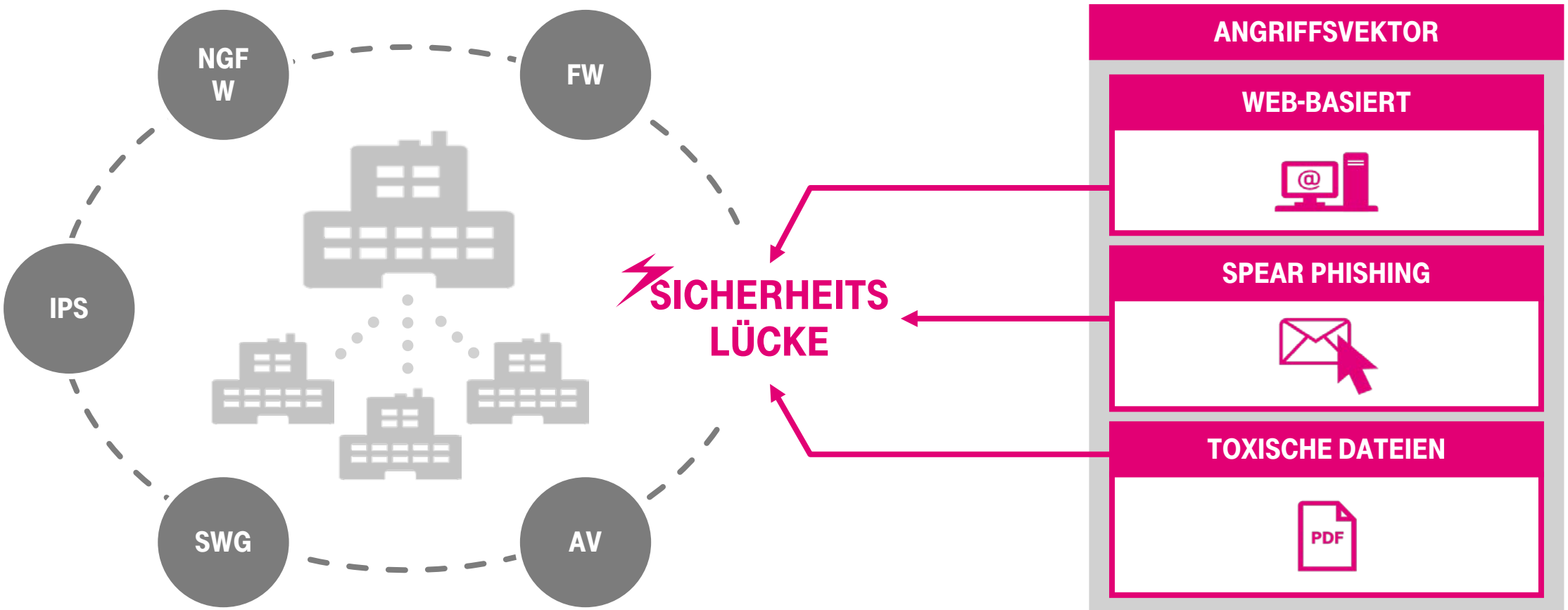
ZIEL DER ANGRIFFE SIND DIE WERTVOLLSTEN GÜTER EINES UNTERNEHMEN

SPEAR PHISHING	> CFO	> FINANZINFORMATIONEN
WEB-BASED ATTACK	> LEITER ENGINEERING	> GEISTIGES EIGENTUM
FILE-BASED ATTACK	> REGIERUNGSMITARBEITER	> NATIONALE SICHERHEIT

TRADITIONELLE VERTEIDIGUNG FUNKTIONIERT NICHT MEHR ...



DIE ENTERPRISE-SICHERHEITSLÜCKE



EIN NEUES MODEL IST NOTWENDIG

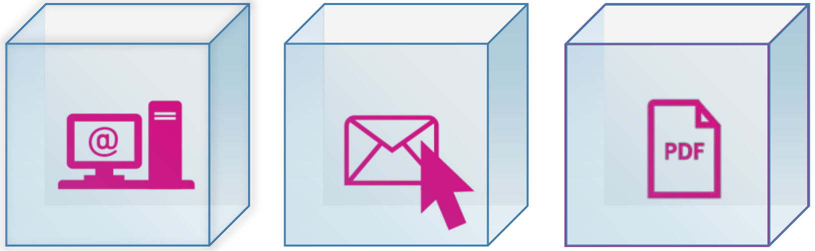
DERZEITIGE METHODEN

MATCH

101011010101101000101110001101
010101011001101111100101011001
001001001000101010001010100010
100100111001010101010110101000
101011010101101000101110001101
010101011001101111001010100101

- Signature-Based
- Reactive
- Nur bekannte Threats
- Viele false positives

NEUES VIRTUAL EXECUTION MODEL



- Weniger Signaturen
- Dynamisch, Real-Time
- Known/unknown threats
- Minimale false positives

MULTI-PROTOCOL, REAL-TIME MVX ENGINE

PHASE 1
Multi-Protocol
Object Capture

PHASE 1: WEB
- Aggressive Capture
- Web Object Filter

PHASE 1: EMAIL
- Email Attachments
- URL Analysis

PHASE 1: FILE
- Network File Shares

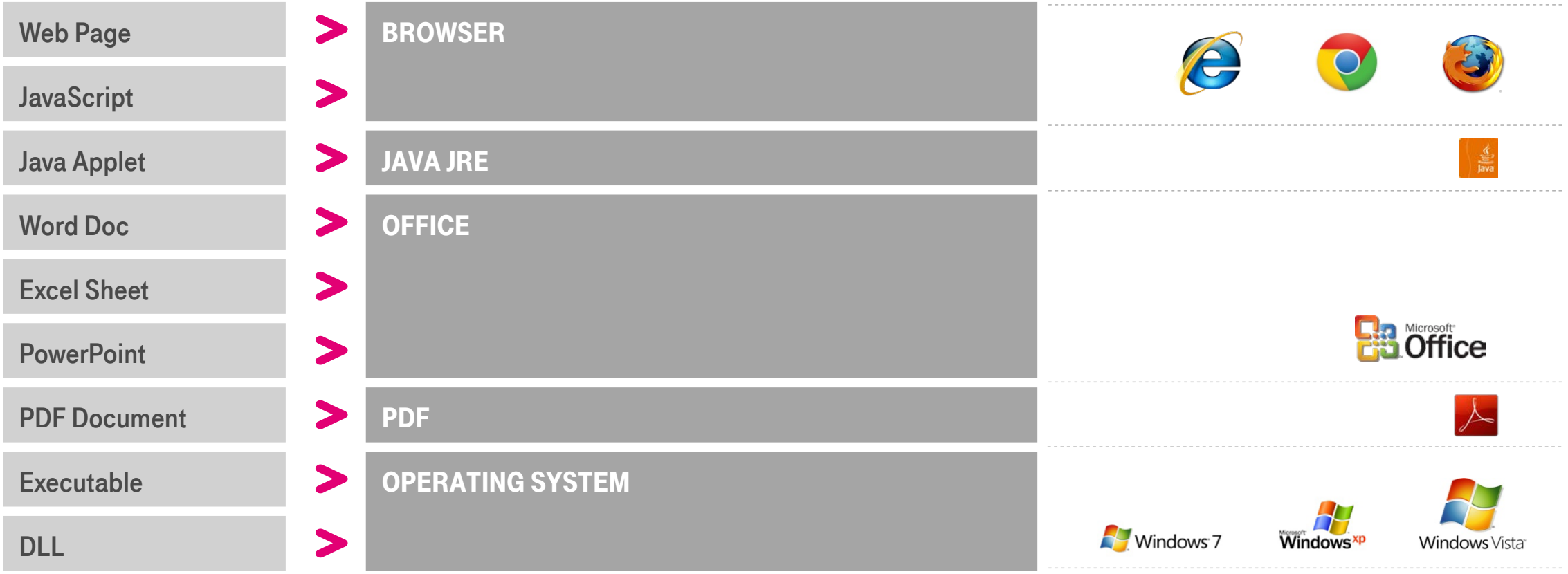
PHASE 2
Virtual Execution
Environments

MAP TO TARGET

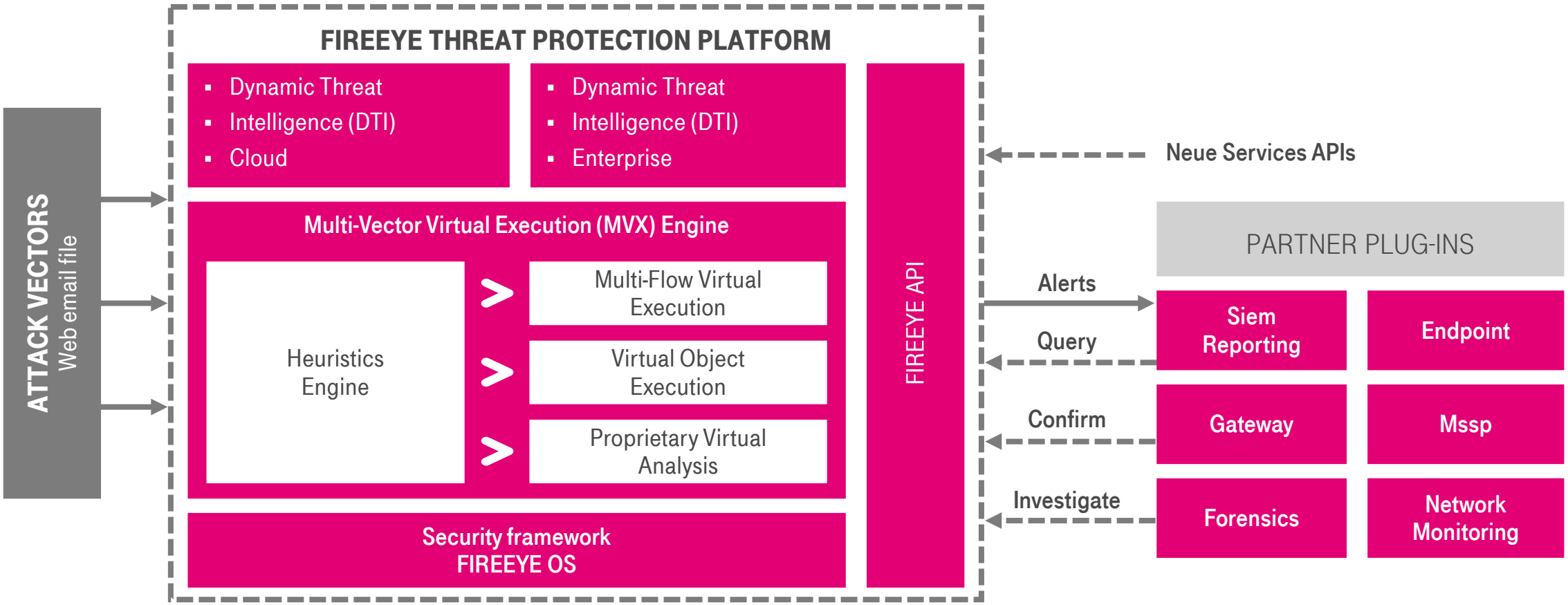
OS AND APPLICATIONS

DYNAMIC, REAL-TIME ANALYSIS
- Exploit detection
- Malware executable analysis
- Cross-matrix of OS/apps
- Originating URL
- Subsequent URLs
- OS modification report
- C&C protocol descriptors

INNERHALB DER MASCHINE



FIREEYE PLATTFORM:
ARCHITEKTUR UND APIS



FIREEYE ECOSYSTEM