

# 2. AUTOMOTIVE SUPPLIERS' DAY

ARBEITSPLATZ  
DER ZUKUNFT



SUPPLIER  
CLOUD



BUSINESS  
ENABLEMENT



SECURITY





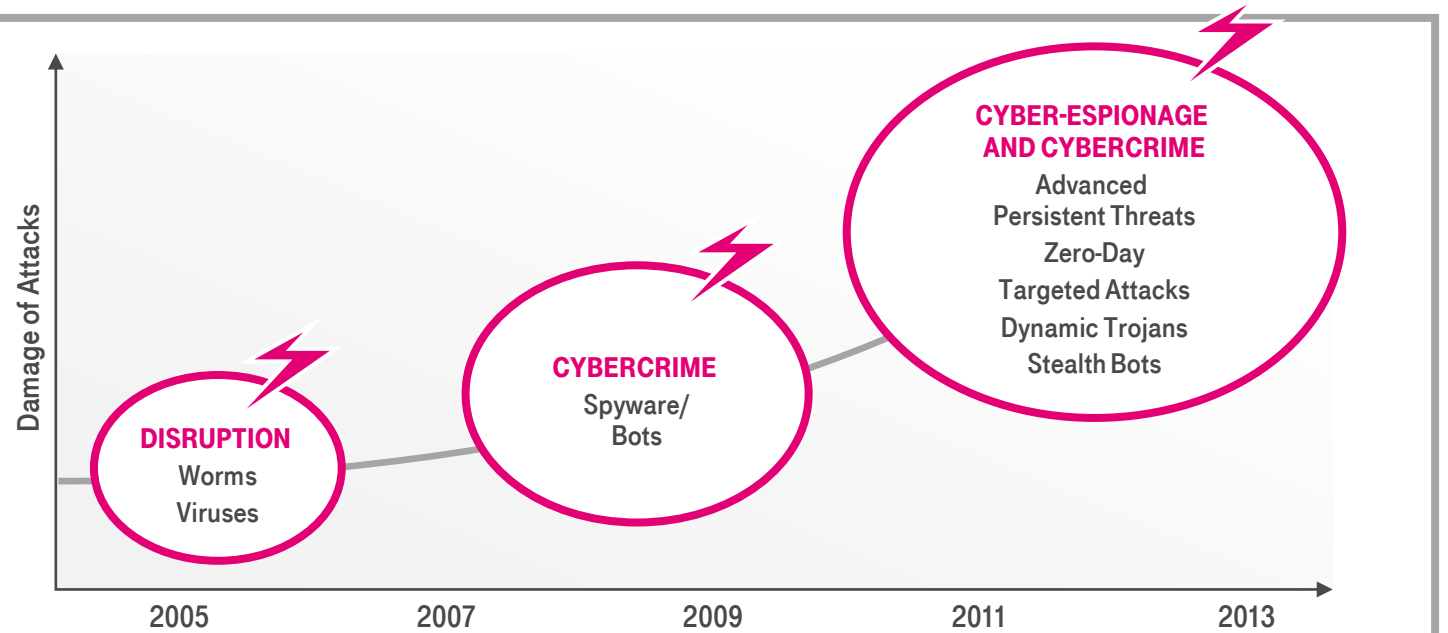
# **CYBER SECURITY: ADVANCED MALWARE DETECTION**

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

**ZDNet / News / Security**  
**Hacker nutzen Zero-Day-Lücke in IE für Angriffe auf Google-Mail-Konten**  
 von Stefan Beiersmann, 14. Juni 2012, 10:34 Uhr

**Spionageprogramm**  
**Flame-Virus erhält Selbstmordbefehl**

**Volkswagen und Allianz im Visier von Hackern**  
 25. May 2012 - Auto-Reporter.NET

**Zehntausende deutsche Zombie-Rechner**  
 Eine schädliche Software leitet den Datenverkehr zehntausender Computer um. Die Netzfahndung ermittelt innerhalb von 24 Stunden 38.000 befallene Rechner. Von Ulrich Clauß

**Angriffe auf fremde Netzwerke**  
**Bundeswehr greift mit Hackern in Cyberkrieg ein**  
 Dienstag, 05.06.2012, 04:06

**Deutsche Behörden warnen vor akuter Hacker-Gefahr**

**ZUM THEMA**  
 Cyberattacke mit Computervirus Stuxnet  
 Obama soll Viren-Angriff gegen Iran befähigen haben

**Lösche all deine Dateien, hinterlasse keine Spuren**  
 letzte Befehl, den der Flame-Spionageprogramm empfangen hat  
 Entwicklern empfing. Antivirus-Programme erkennen den Selbstmordbefehl ab - und stießen ihn ab

**Flame-Programmcode: Selbstmord-Instanz**

**Deutsche Behörden warnen vor akuter Hacker-Gefahr**

**Hacker der Gruppe 'The Shadow Brokers' greifen auf die Daten von NSA zu**

**12.01.12 | Hacker-Angriffe**

**Bild medium (103 KB)**  
**Bild large (2.678 KB)**  
**Artikel als PDF**  
**Artikel Versenden**

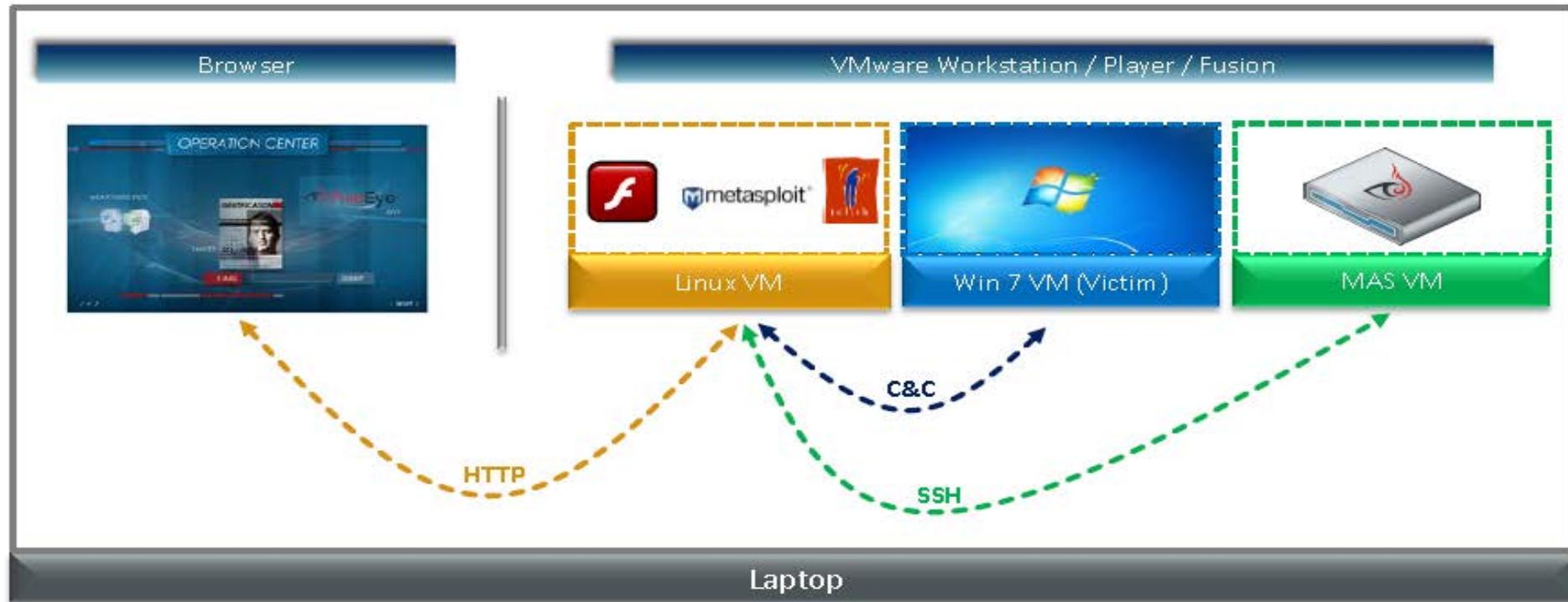


# CXO Level Demo



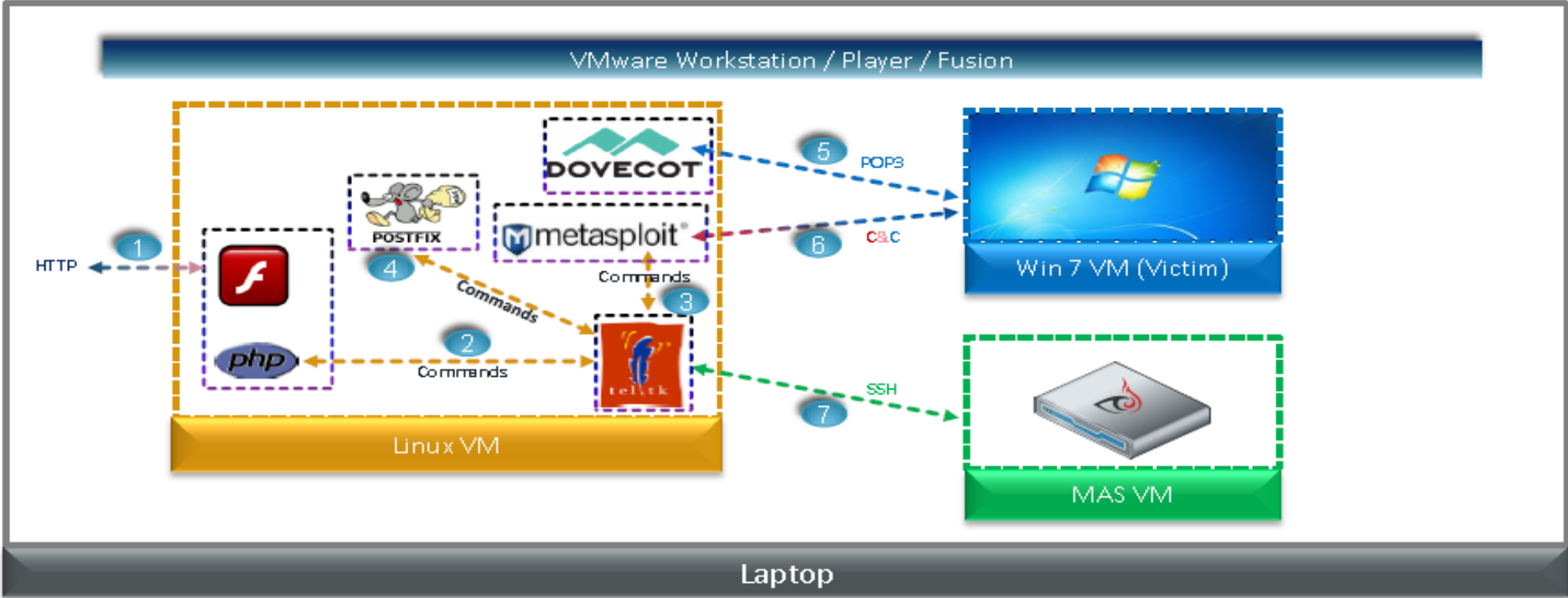
# DEMO AUFBAU

## HIGH LEVEL



# DEMO AUFBAU

## LOW LEVEL



# VIELEN DANK

**IHR ANSPRECHPARTNER:**

Thomas Schmitt

Telefon: 0151-52845407

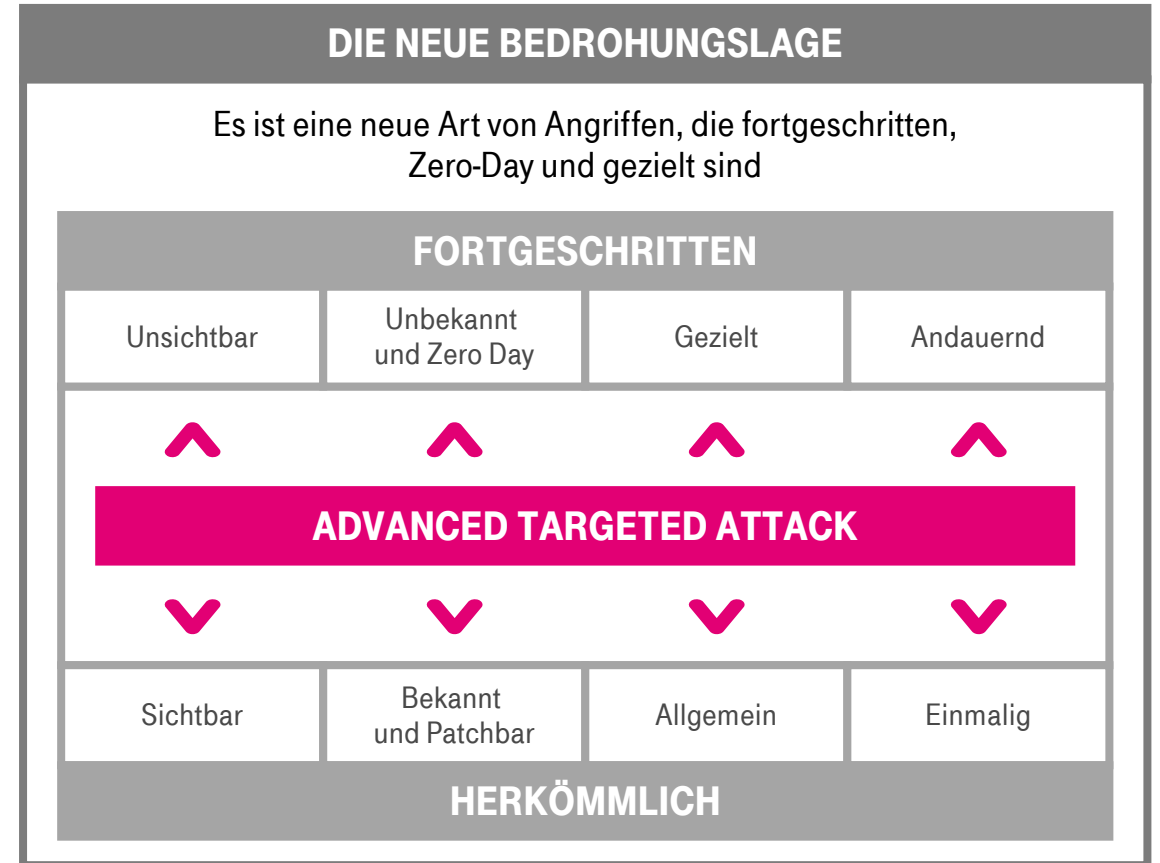
E-Mail: [T-Schmitt@t-systems.com](mailto:T-Schmitt@t-systems.com)



**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?

KOORDINIERT PERSISTENT THREAT AKTEURE



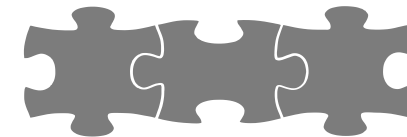
DYNAMISCHE, POLYMORPHIC MALWARE



NEUE BEDROHUNGSLAGE

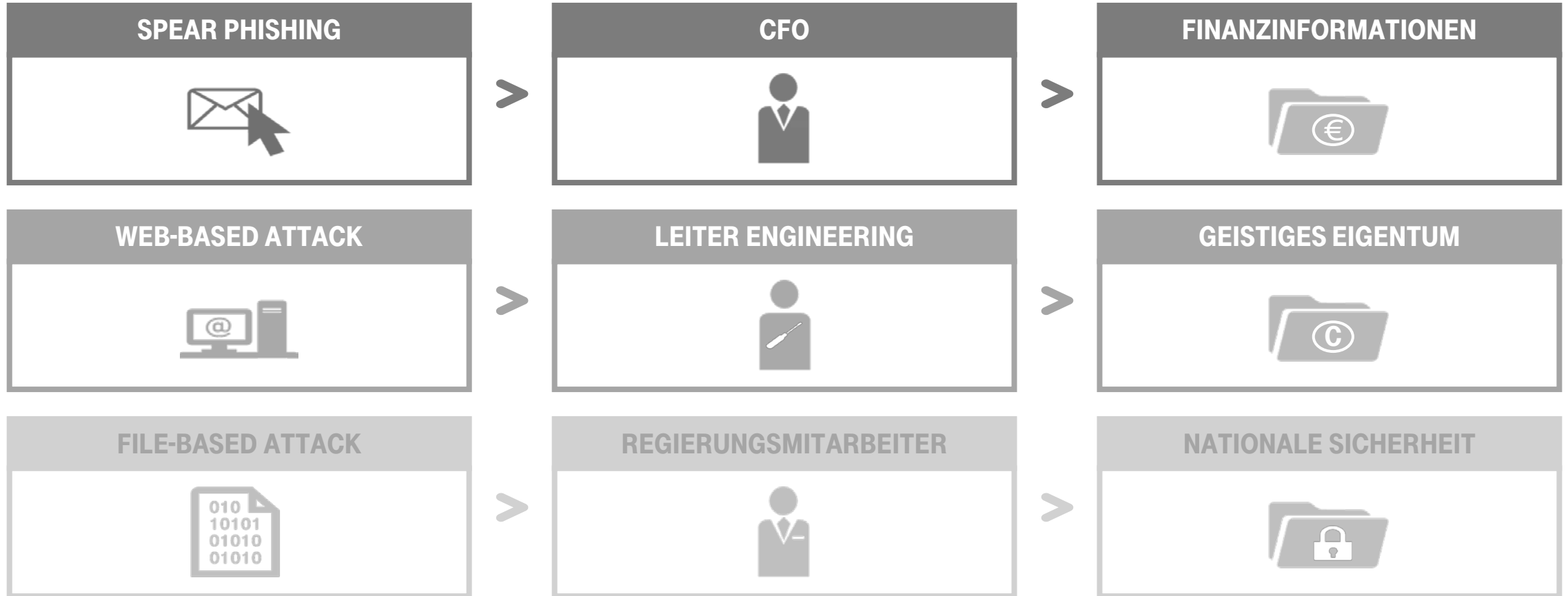


MULTI-VECTOR ATTACKS

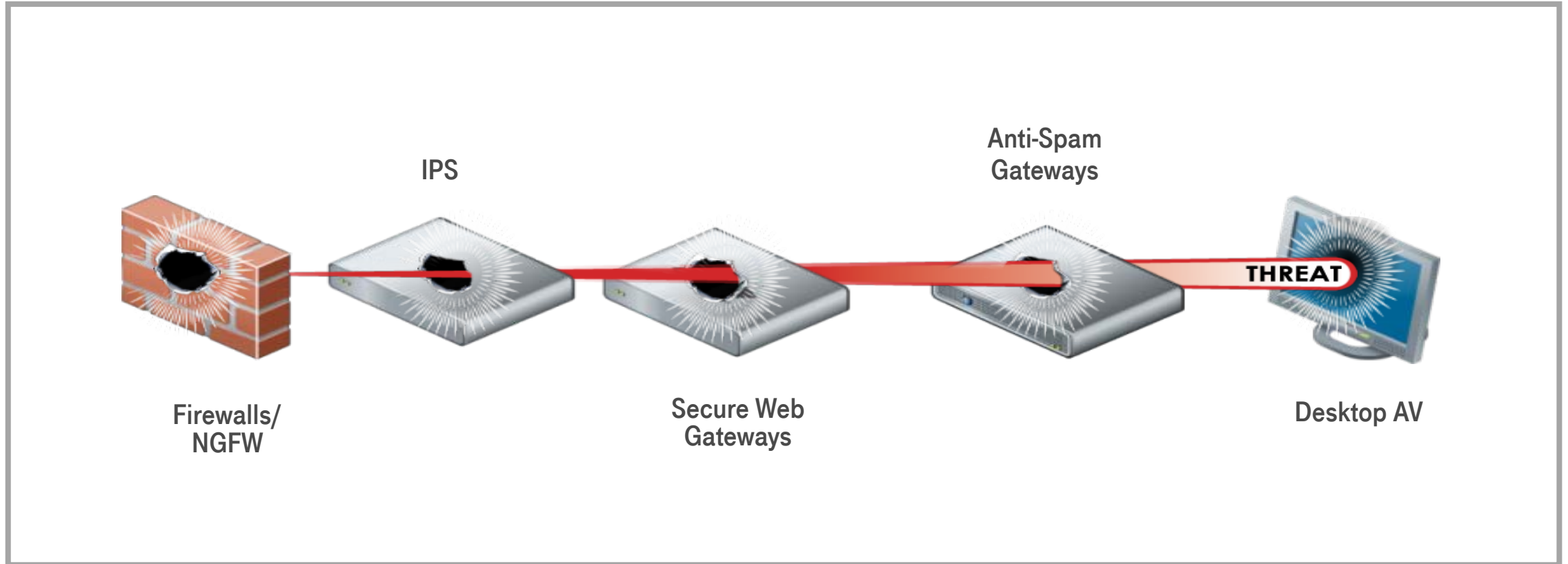


MULTI-STAGED ATTACKS

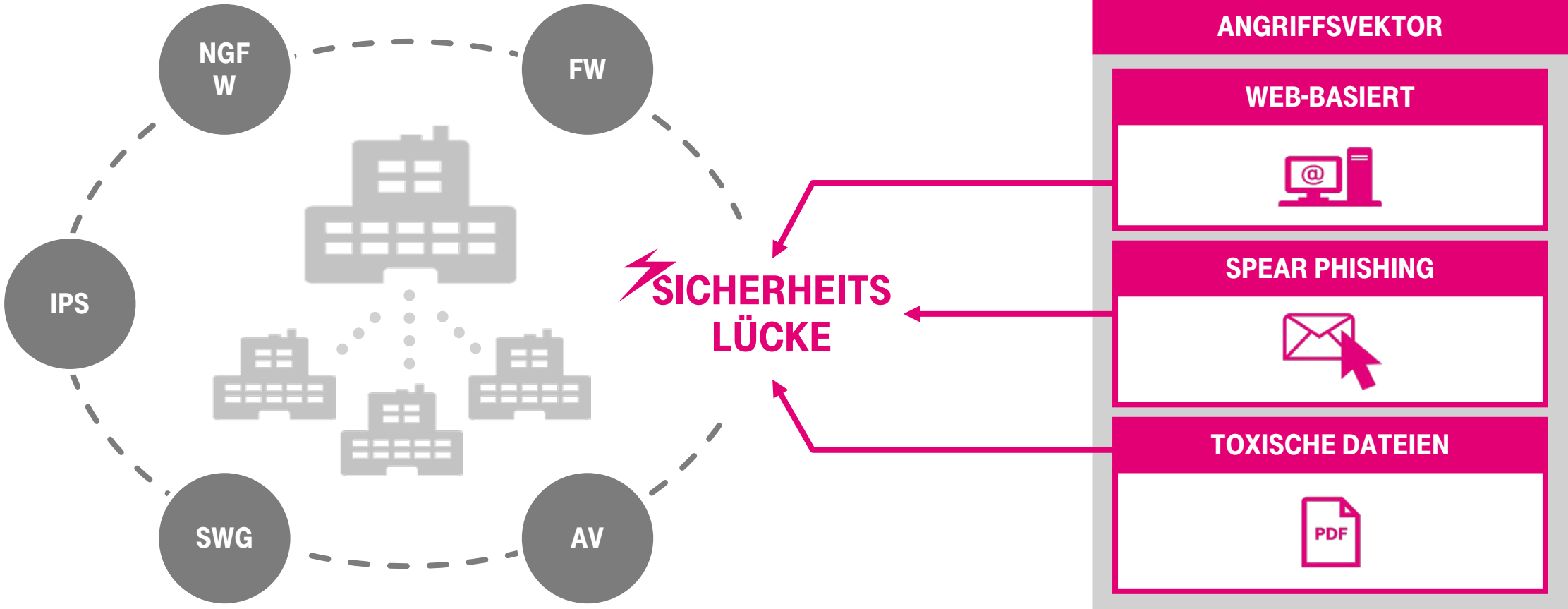
# ZIEL DER ANGRIFFE SIND DIE WERTVOLLSTEN GÜTER EINES UNTERNEHMEN



# TRADITIONELLE VERTEIDIGUNG FUNKTIONIERT NICHT MEHR ...



# DIE ENTERPRISE-SICHERHEITSLÜCKE





# EIN NEUES MODEL IST NOTWENDIG

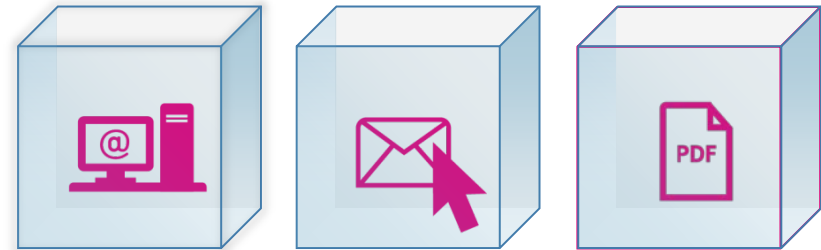
## DERZEITIGE METHODEN

### MATCH

```
10101101010111010001011110001101
01010101110011011111100101011001
001001001000101010001010100010
1001001110010101010101110101000
10101101010111010001011110001101
01010101110011011111001010100101
```

- 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

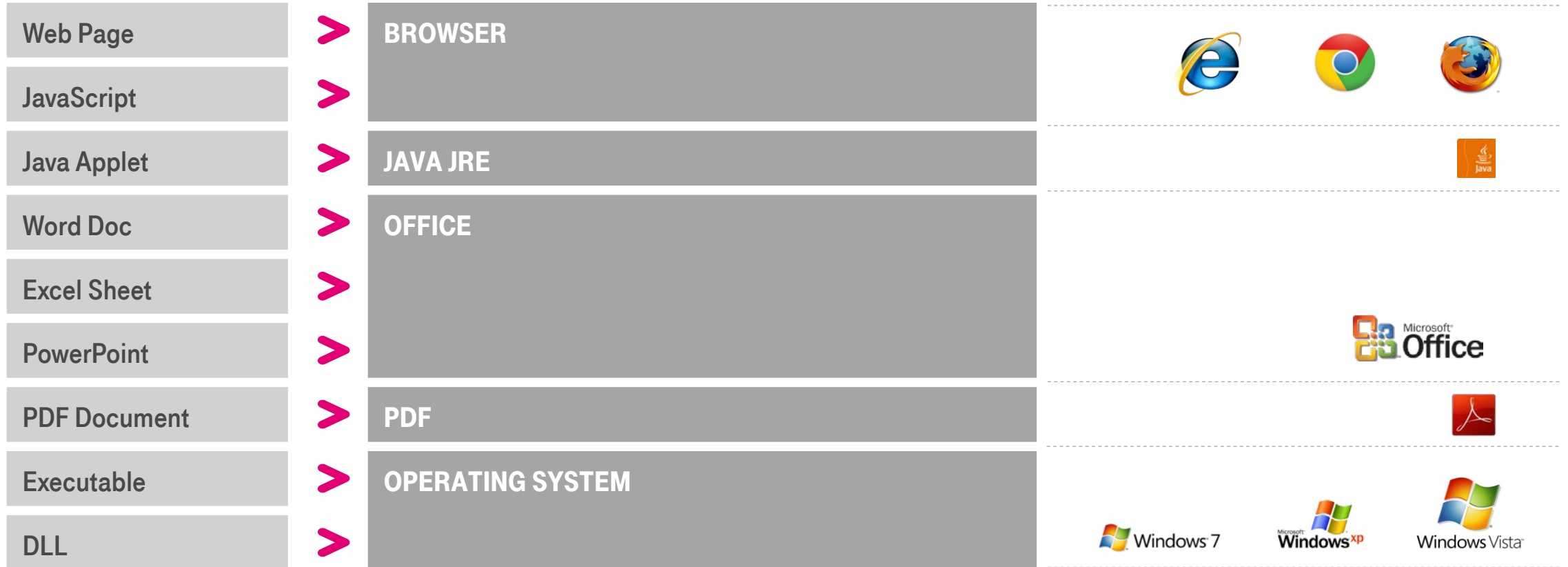


**MAP TO TARGET  
OS AND  
APPLICATIONS**

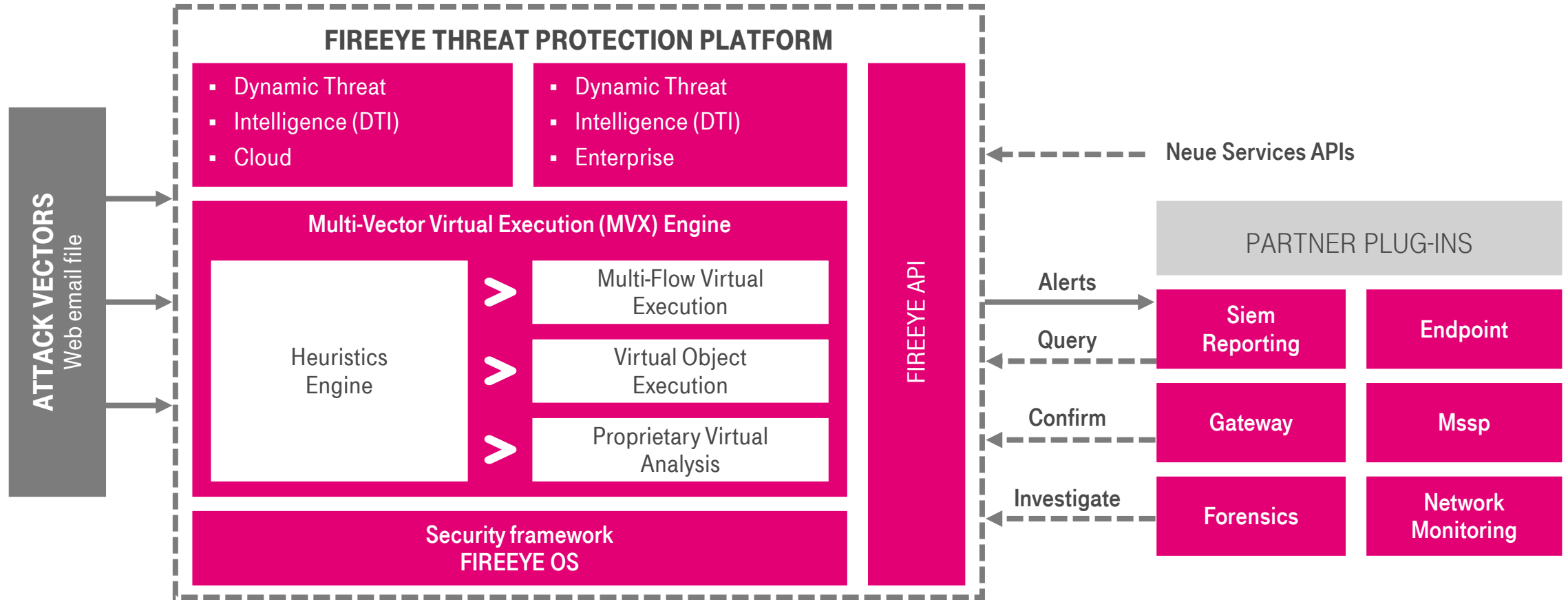
### DYNAMIC, REAL-TIME ANALYSIS

- 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

