Traps – Advanced Endpoint Protection

Jakub Jiricek, CNSE, CISSP

jjiricek@paloaltonetworks.com

paloalto networks®

the enterprise security company™

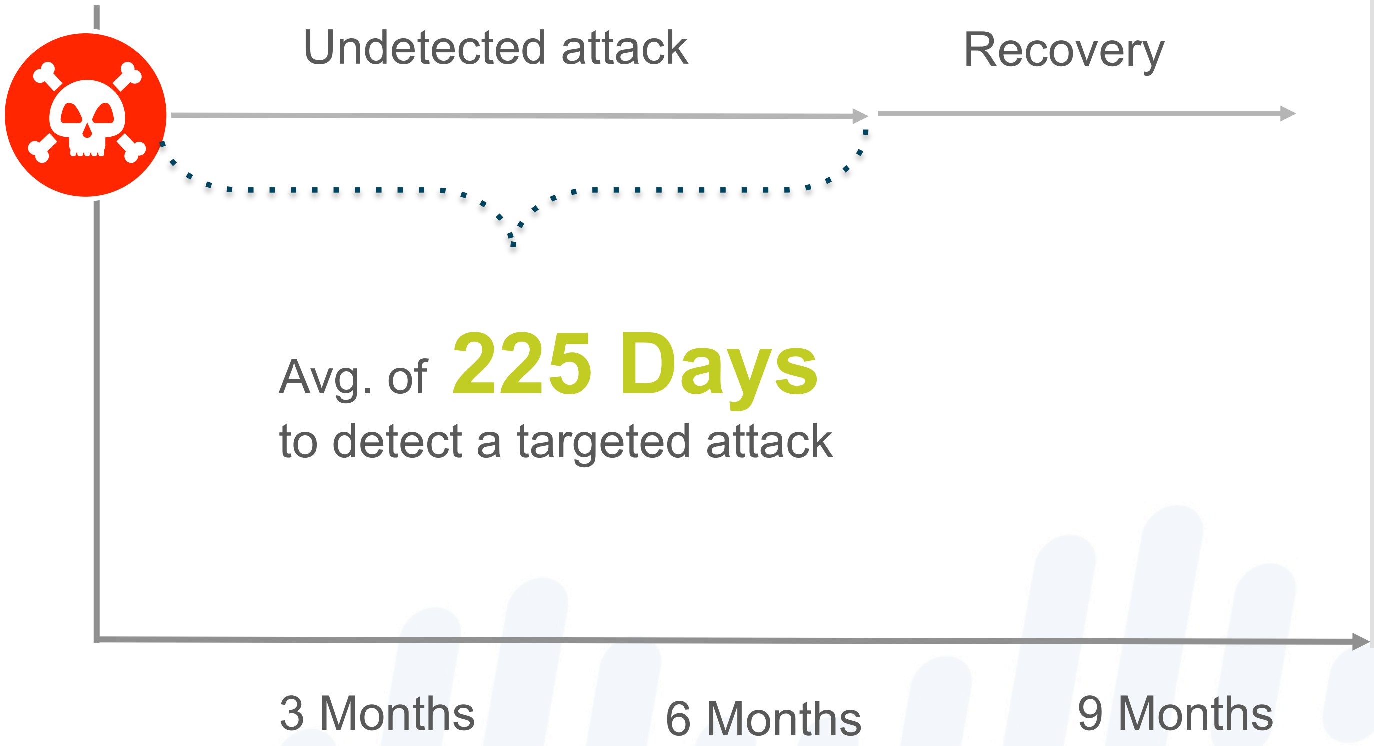
Harsh Reality

91% increase in targeted attacks in 2013

78% of exploit kits utilize vulnerabilities less than 2 years old

71% of breaches involve a targeted user device

The cost of a detection-only strategy



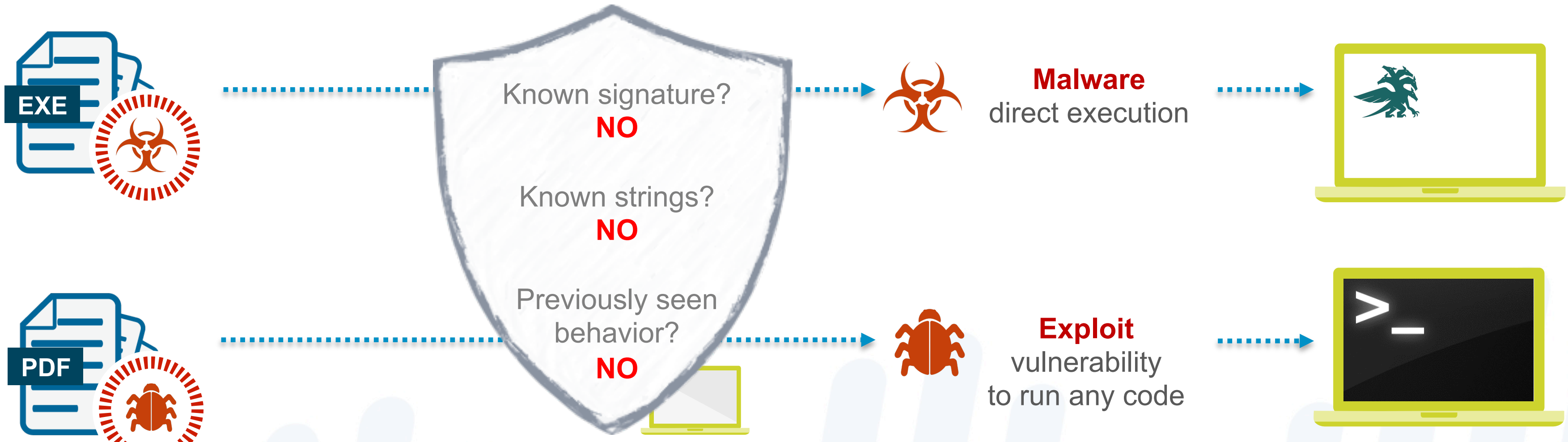
Avg. of **225 Days**
to detect a targeted attack

84%

Discovered the attack through a 3rd party

The failures of traditional approaches

Targeted | **Evasive** | **Advanced**



EXE

PDF

Known signature?
NO

Known strings?
NO

Previously seen behavior?
NO

Legacy
Endpoint Protection

Malware
direct execution

Exploit
vulnerability
to run any code

Introducing Traps

The right way to deal with advanced cyber threats

Prevent Exploits

Including zero-day exploits

Prevent Malware

Including advanced & unknown malware

Collect Attempted-Attack Forensics

For further analysis

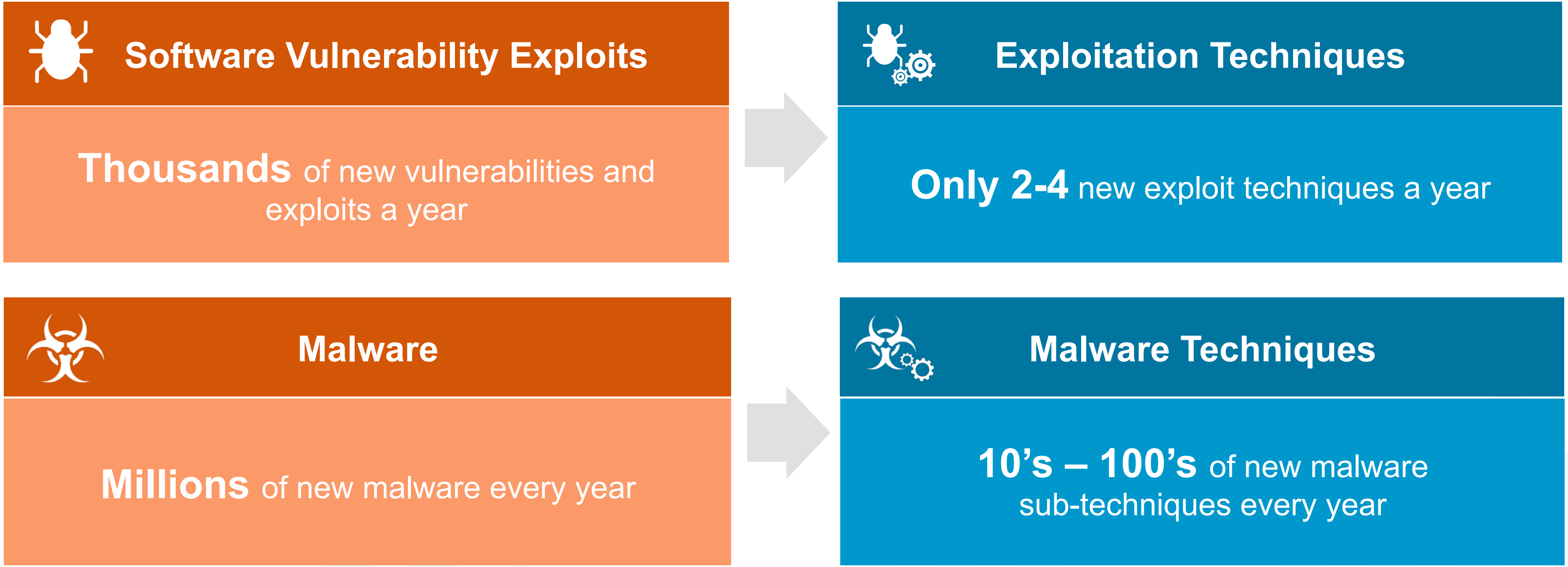
Scalable & Lightweight

Must be user-friendly and cover complete enterprise

Integrate with Network and Cloud Security

For data exchange and crossed-organization protection

Block the core techniques – not the individual attacks



Software Vulnerability Exploits

Thousands of new vulnerabilities and exploits a year

Exploitation Techniques

Only 2-4 new exploit techniques a year

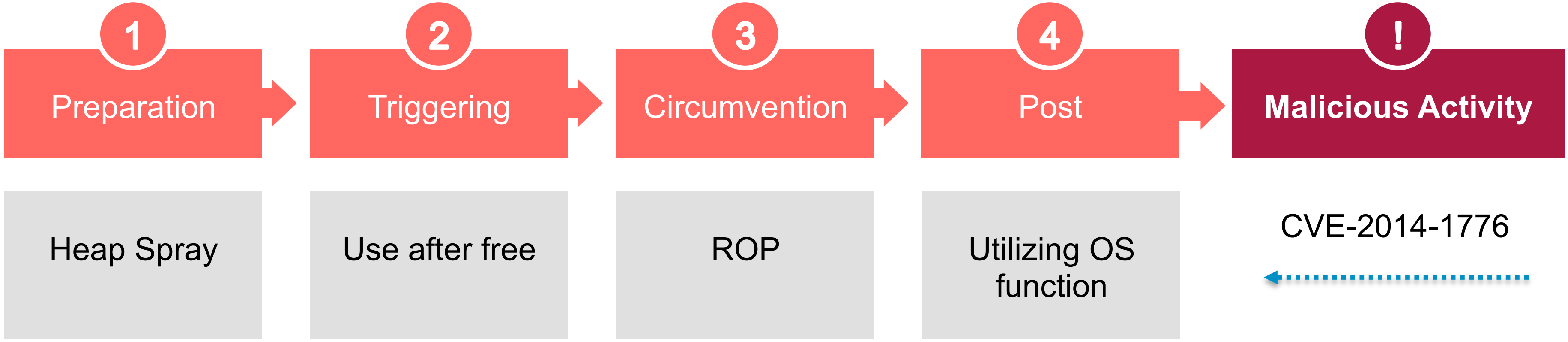
Malware

Millions of new malware every year

Malware Techniques

10's – 100's of new malware sub-techniques every year

Exploit prevention – Clandestine Fox



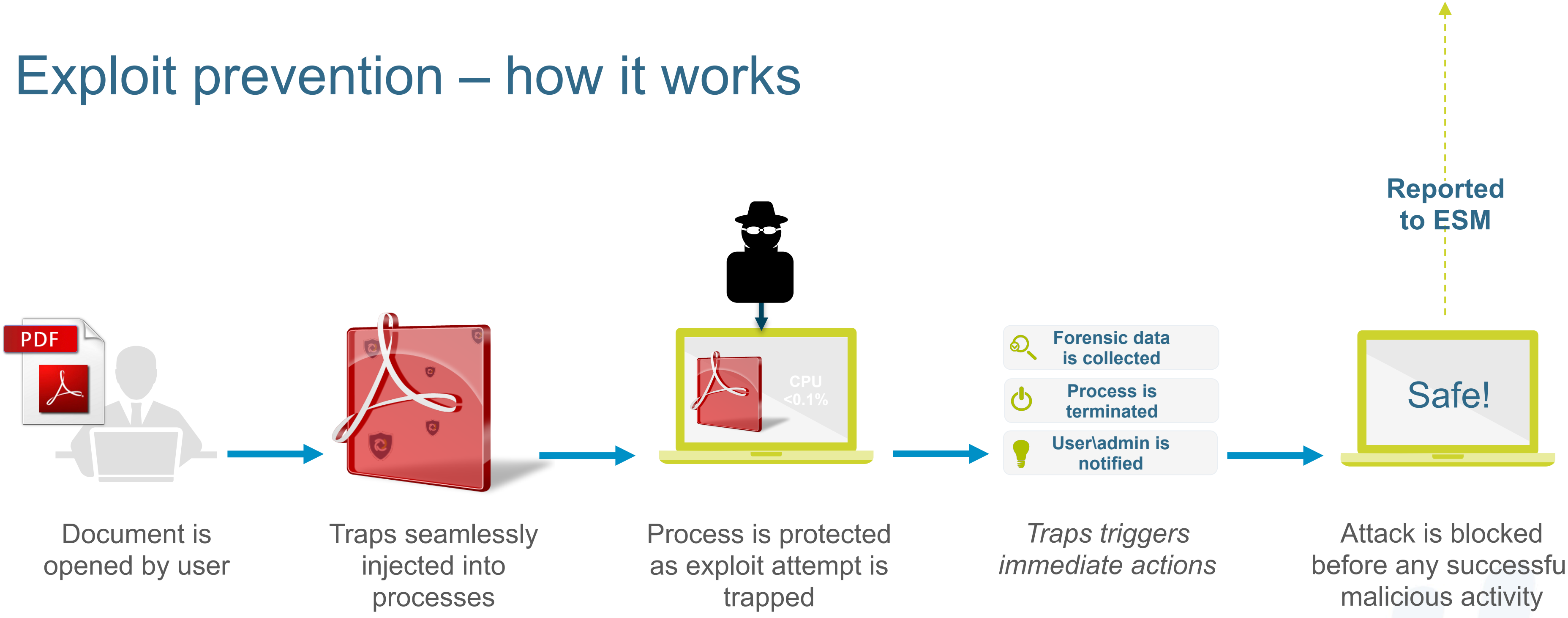
1 Preparation → 2 Triggering → 3 Circumvention → 4 Post → ! Malicious Activity

- Heap Spray
- Use after free
- ROP
- Utilizing OS function
- CVE-2014-1776

Prevention of one technique in the chain will block the entire attack

- Algorithmic Memory Traps Placement
- Logic-Flaws Real-Time Intervention
- Memory Corruption Mitigation
- OS Functions Shielding

Exploit prevention – how it works



Reported to ESM

Document is opened by user

Traps seamlessly injected into processes

Process is protected as exploit attempt is trapped

Forensic data is collected

Process is terminated

User\admin is notified

Traps triggers immediate actions

Attack is blocked before any successful malicious activity

When an exploitation attempt is made, the exploit hits a "trap" and fails before any malicious activity is initiated.

Malware prevention

Policy-Based Restrictions

Limit surface area of attack
control source of file installation

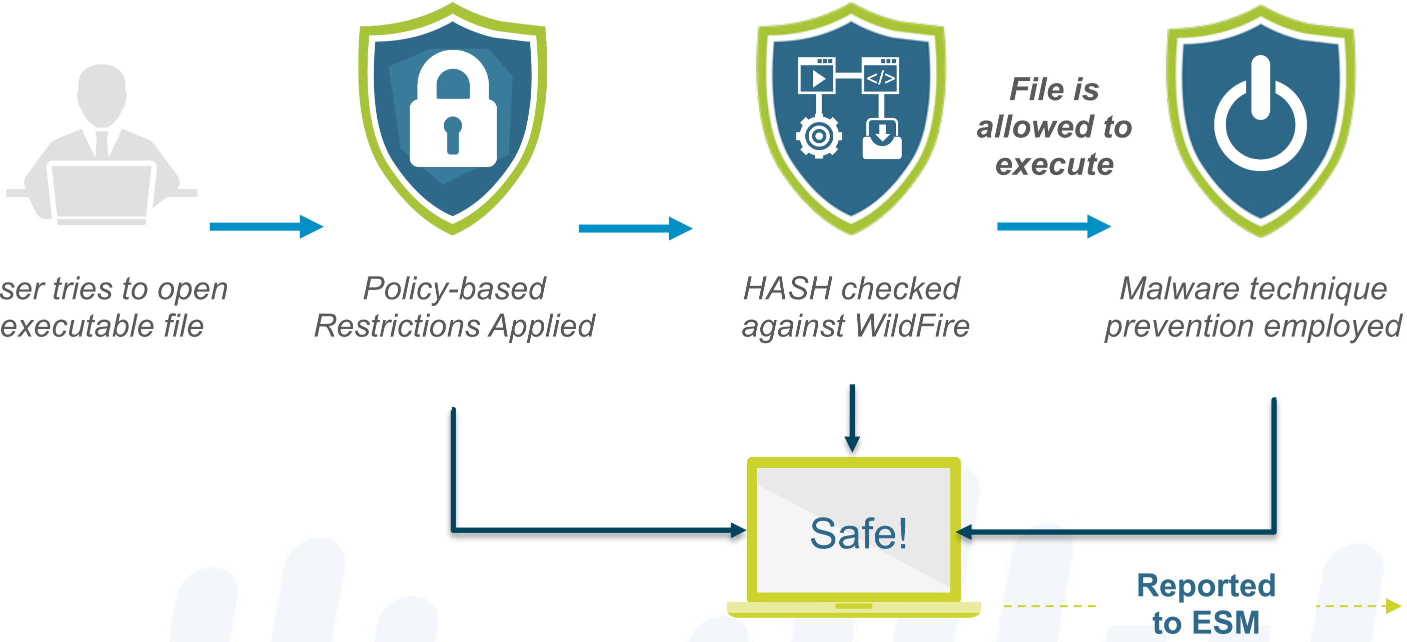
WildFire Inspection

Prevent known malware
with cloud-based integration

Malware Techniques Mitigation

Prevent unknown malware
with technique-based mitigation

Malware prevention – how it works



User tries to open executable file

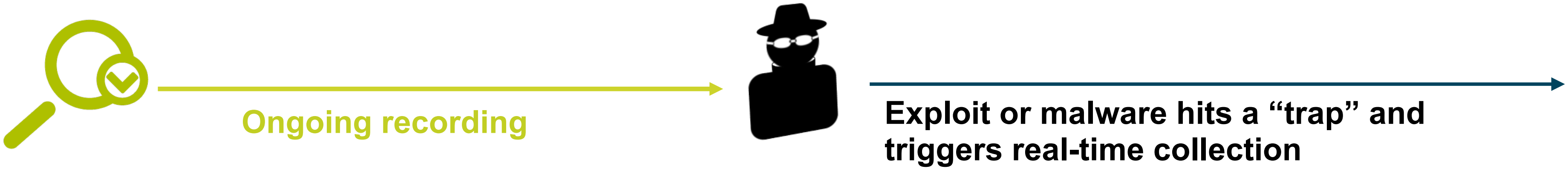
Policy-based Restrictions Applied

HASH checked against WildFire

Malware technique prevention employed

Reported to ESM

Ongoing attack-triggered forensics



Ongoing recording

Exploit or malware hits a “trap” and triggers real-time collection

- **Any files execution**
  - Time of execution
  - File name
  - File HASH
  - User name
  - Computer name
  - IP address
  - OS version
  - File’s malicious history

- **Any interference with Traps service**
  - Traps Process shutdown attempt
  - Traps Service shutdown attempt
  - Related system logs

- **Attack-related forensics**
  - Time stamp
  - Triggering File (non executable)
  - File source
  - Involved URLs\URI
  - Prevented exploitation technique
  - IP address
  - OS version
  - Version of attempted vulnerable software
  - All components loaded to memory under attacked process
  - Full memory dump
  - Indications of further memory corruption activity
  - User name and computer name

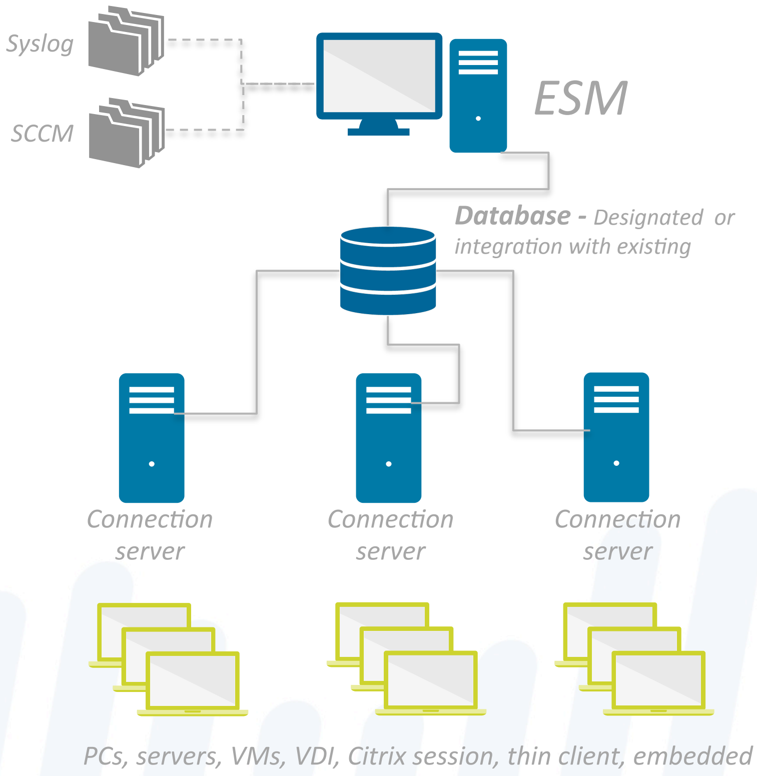
Endpoint Security Manager (ESM)

3-tier management structure

- ESM platform
- Database
- Connection server
  (each supports ~10,000 endpoints -scales horizontally)

All-in-one management center

- Configuration management
- Logging and DB query
- Admin dashboard and security overview
- Forensics captures
- Integration configuration


Syslog
SCCM
ESM
Database - Designated or integration with existing
Connection server
Connection server
Connection server
PCs, servers, VMs, VDI, Citrix session, thin client, embedded

Coverage and system requirements

Supported operating systems

Workstations

- Windows XP SP3
- Windows 7
- Windows 8.1

Servers

- Windows Server 2003
- Windows Server 2008 (+R2)
- Windows Server 2012 (+R2)

Footprint

- 25 MB
- 0.1% CPU
- Very Low I\O

paloalto
networks®

the enterprise security company™