What's Next for Network Security - Visibility is king!

Gøran Tømte

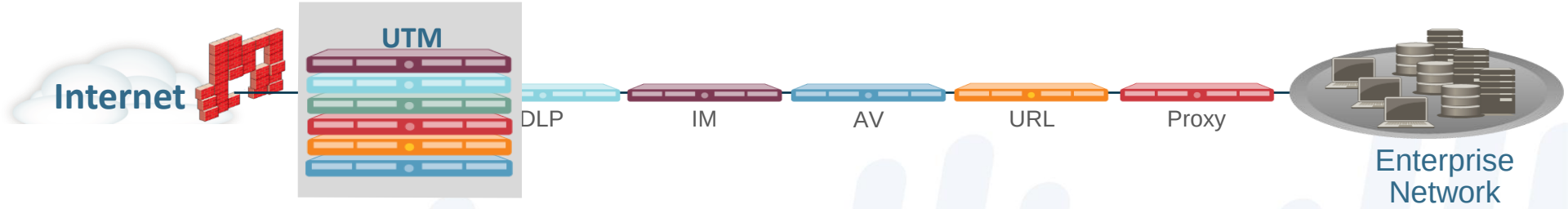
March 2013

paloalto NETWORKS

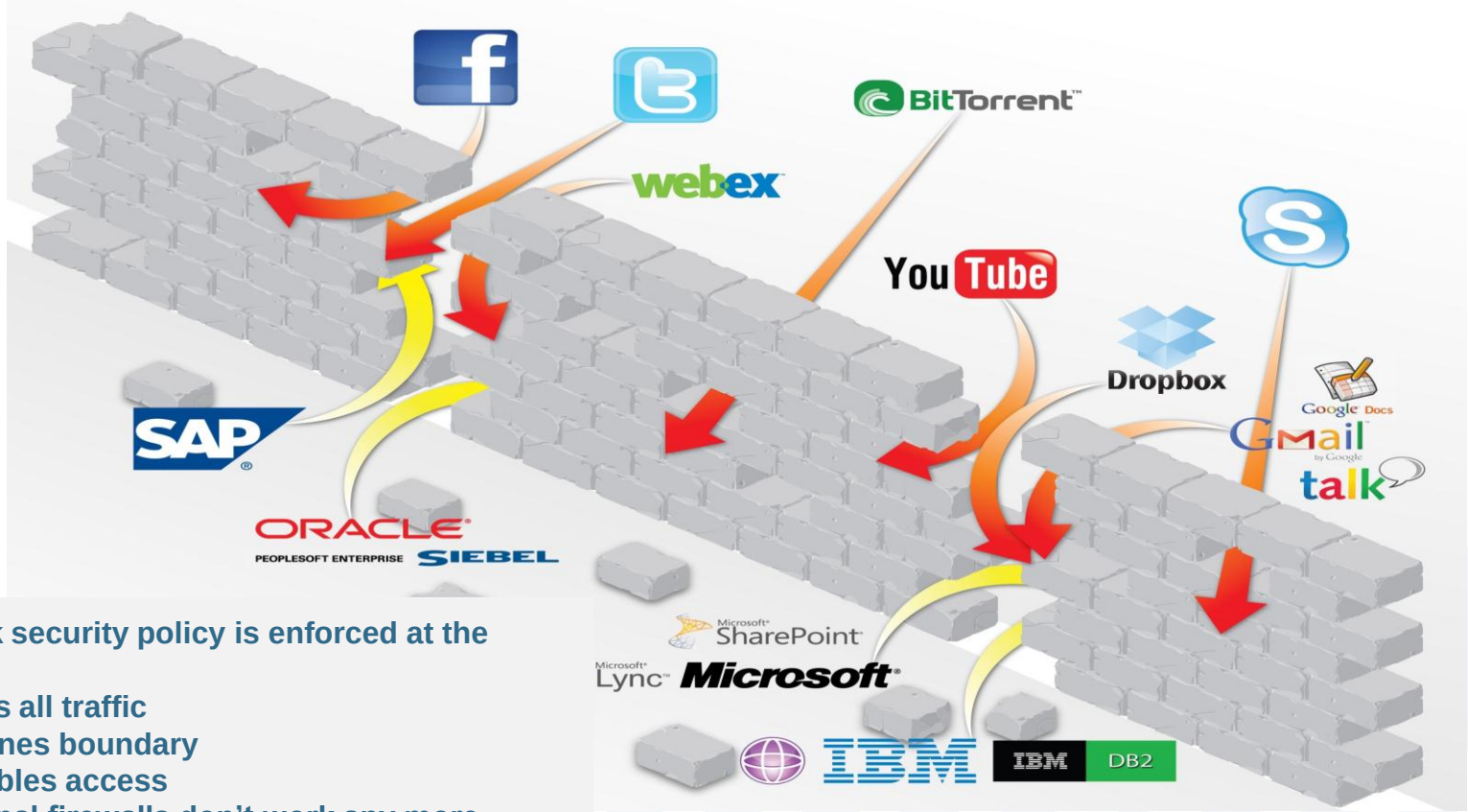
the network security company™

Technology Sprawl and Creep Aren't the Answer

- **"More stuff" doesn't solve the problem**
- **Firewall "helpers" have limited view of traffic**
- **Complex and costly to buy and maintain**
- **Doesn't address applications**



Applications Have Changed, Firewalls Haven't



Network security policy is enforced at the firewall

- **Sees all traffic**
- **Defines boundary**
- **Enables access**

Traditional firewalls don't work any more

paloalto NETWORKS

Core functions of a next-generation firewall

1. Identify applications regardless of port, protocol, evasive tactic or SSL
2. Identify and control users regardless of IP address, location, or device
3. Protect against known and unknown application-borne threats
4. Fine-grained visibility and policy control over application access / functionality
5. Multi-gigabit, low latency, in-line deployment

paloalto NETWORKS

Making the firewall a business enablement tool

- **Applications:** Enablement begins with application classification by App-ID.

- **Users:** Tying users and devices, regardless of location, to applications with User-ID and GlobalProtect.

- **Content:** Scanning content and protecting against all threats, both known and unknown, with Content-ID and WildFire.

paloalto NETWORKS

All Apps, All ports, All users, All the time

- Signature, protocol and evasive tactic based App-ID
  - Skype
  - Bittorrent, p2p
  - SSL
  - Etc

paloalto NETWORKS

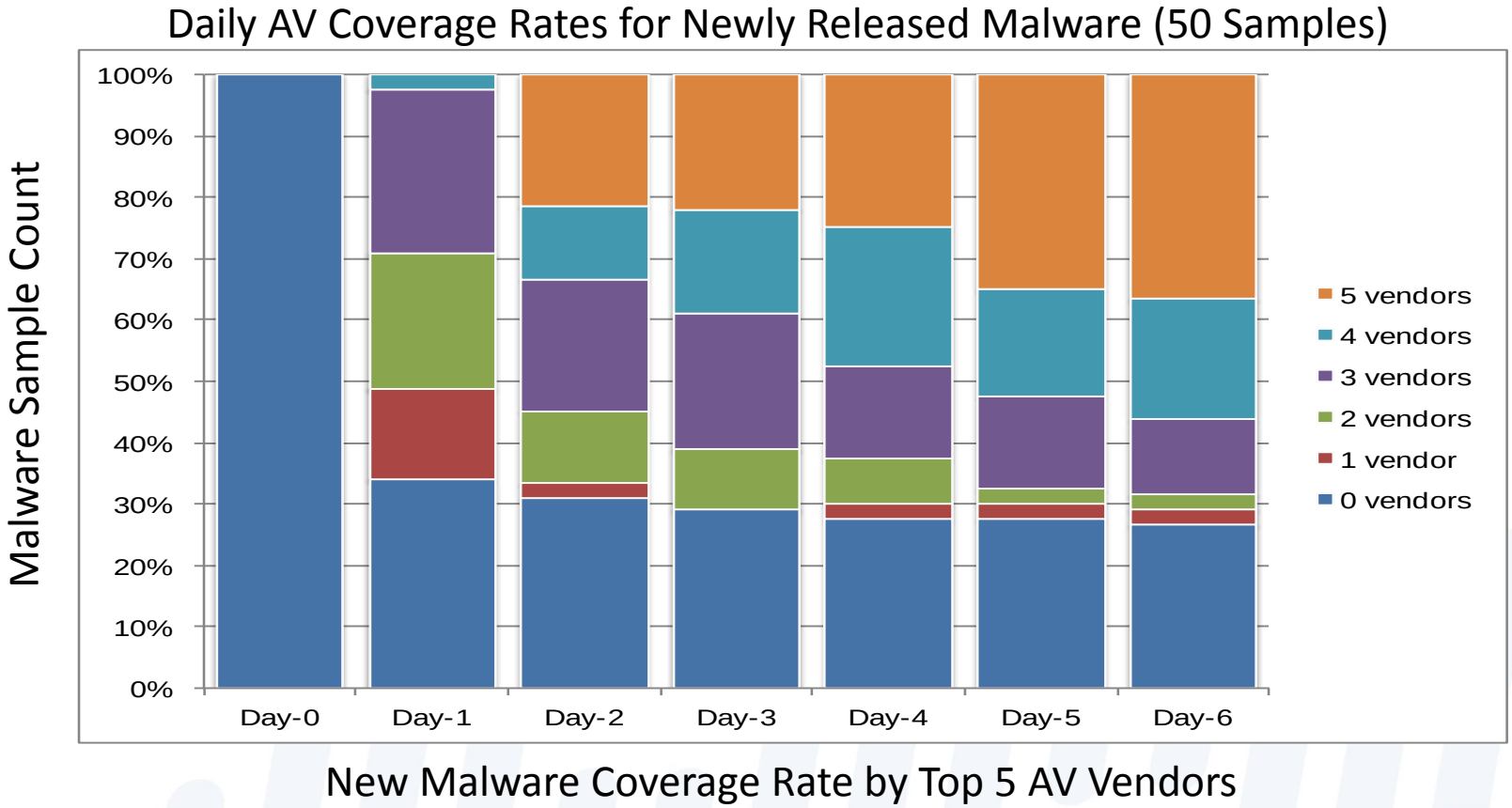
The unknown! Scary hah?

- Unknown applications
  - Control them
- Unknown users
  - Control them
- Unknown threats
  - Control them

paloalto NETWORKS

Addressing Modern Malware

Daily Coverage of Top AV Vendors



The lifecycle of network attacks

1

Bait the end-user

End-user lured to a dangerous application or website containing malicious content

2

Exploit

Infected content exploits the end-user, often without their knowledge

3

Download Backdoor

Secondary payload is downloaded in the background. Malware installed

4

Establish Back-Channel

Malware establishes an outbound connection to the attacker for ongoing control

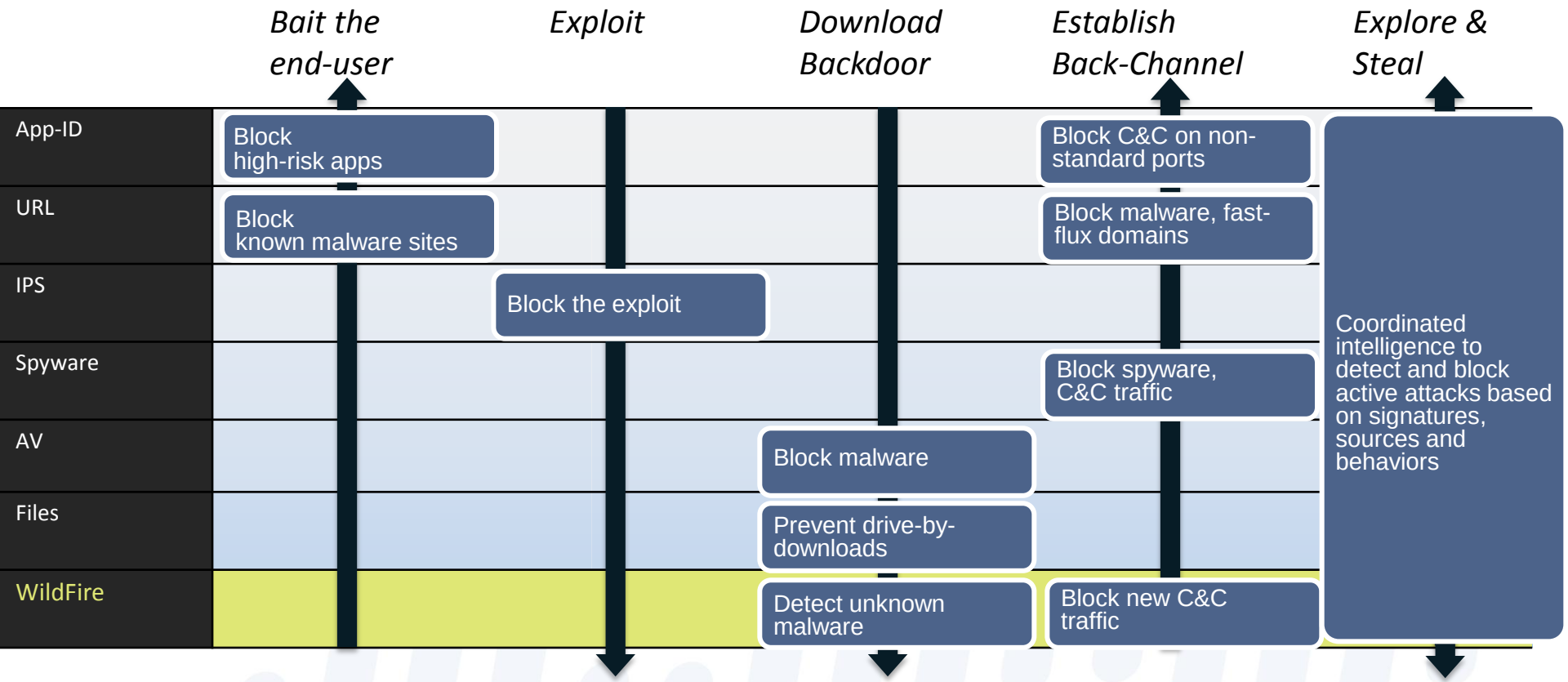
5

Explore & Steal

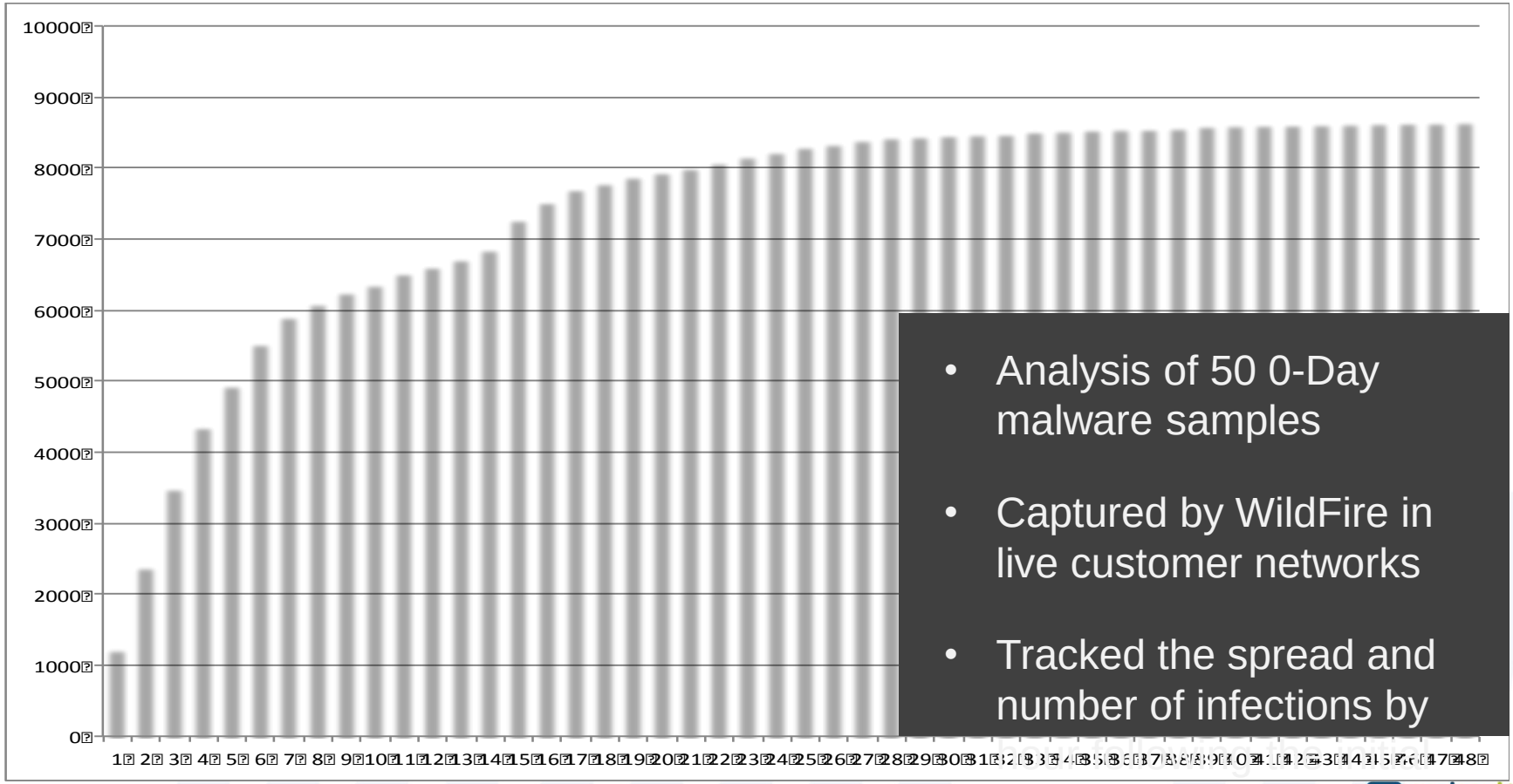
Remote attacker has control inside the network and escalates the attack

paloalto NETWORKS

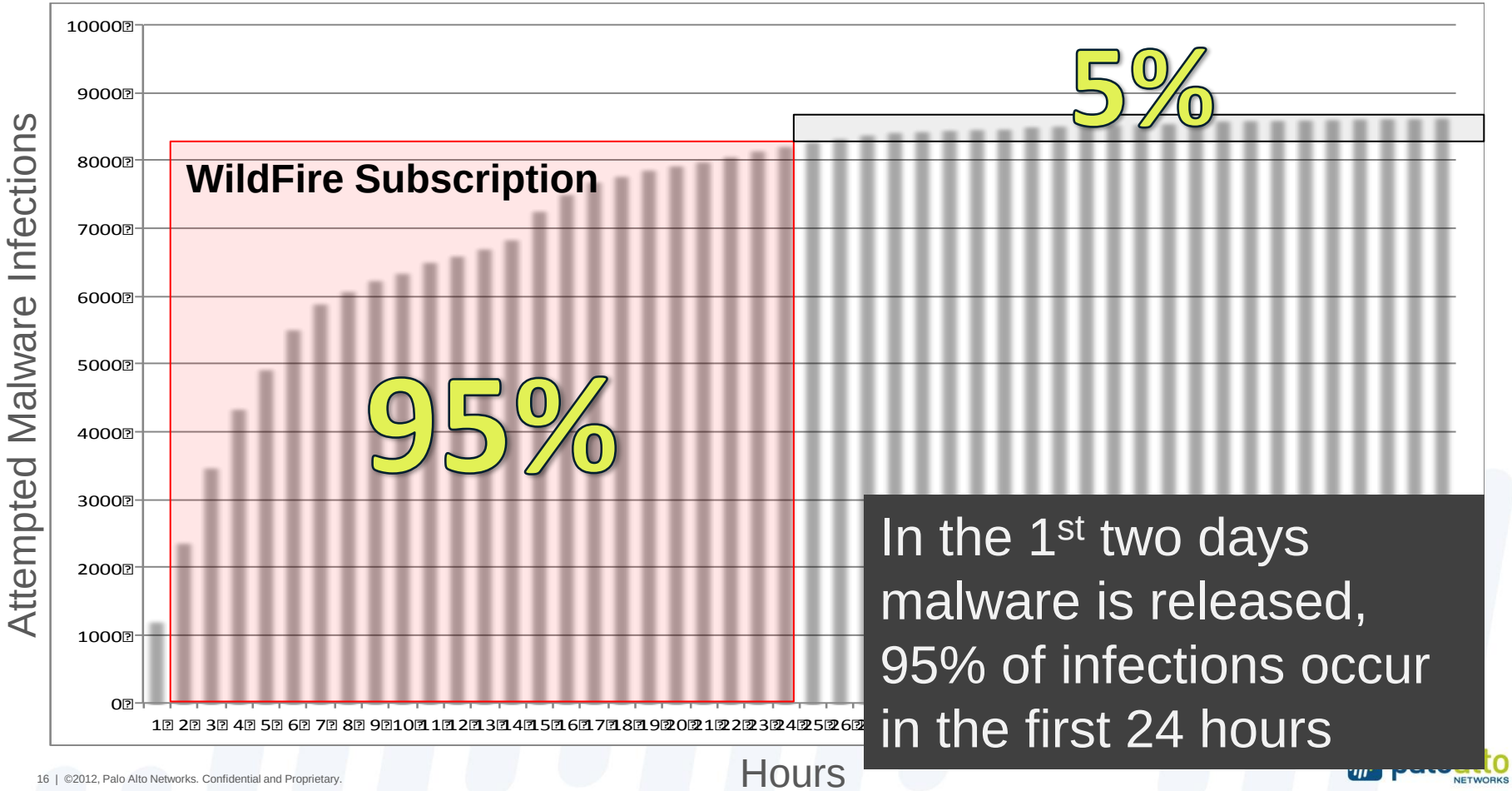
An integrated approach to threat prevention



Real-World Spread of 0-Day Malware

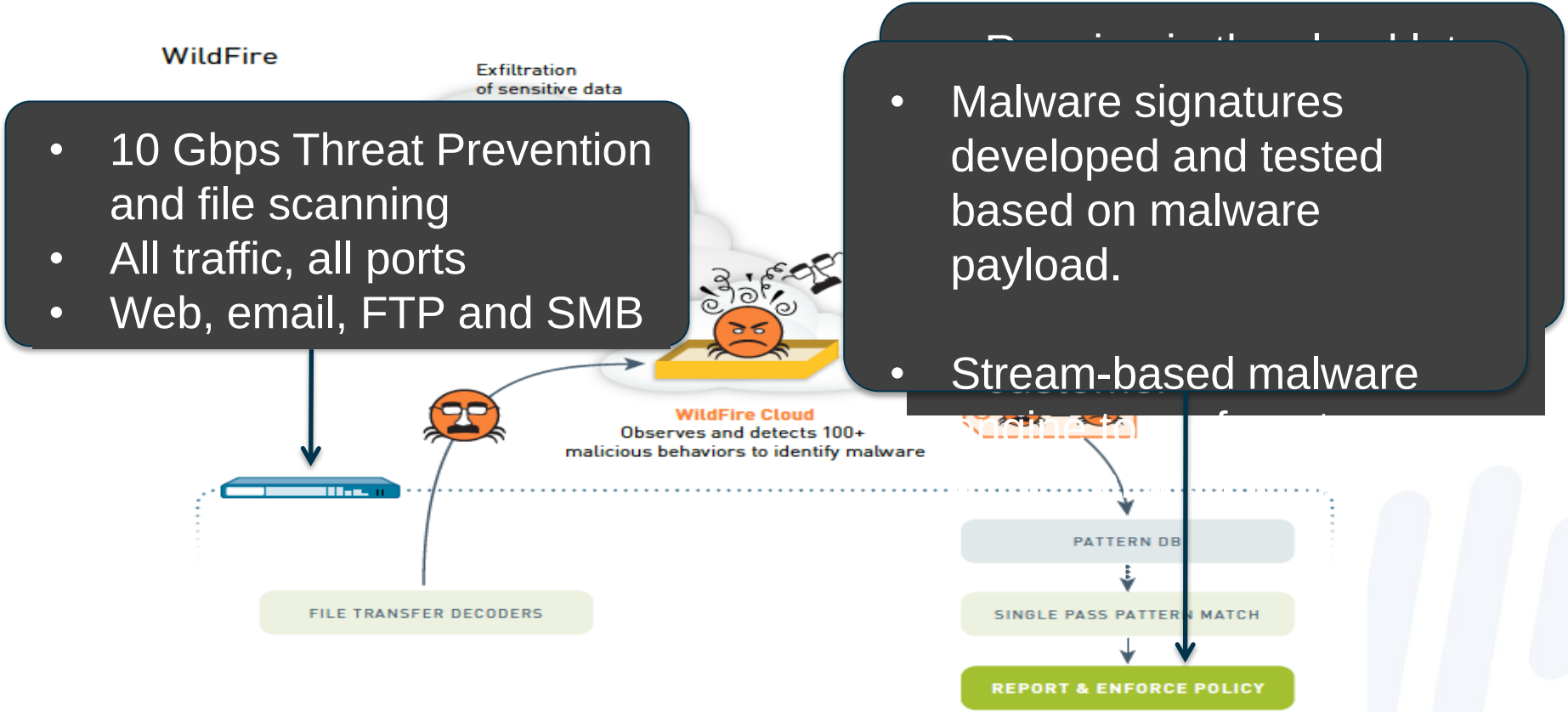


Real-World Spread of 0-Day Malware



In the 1st two days malware is released, 95% of infections occur in the first 24 hours

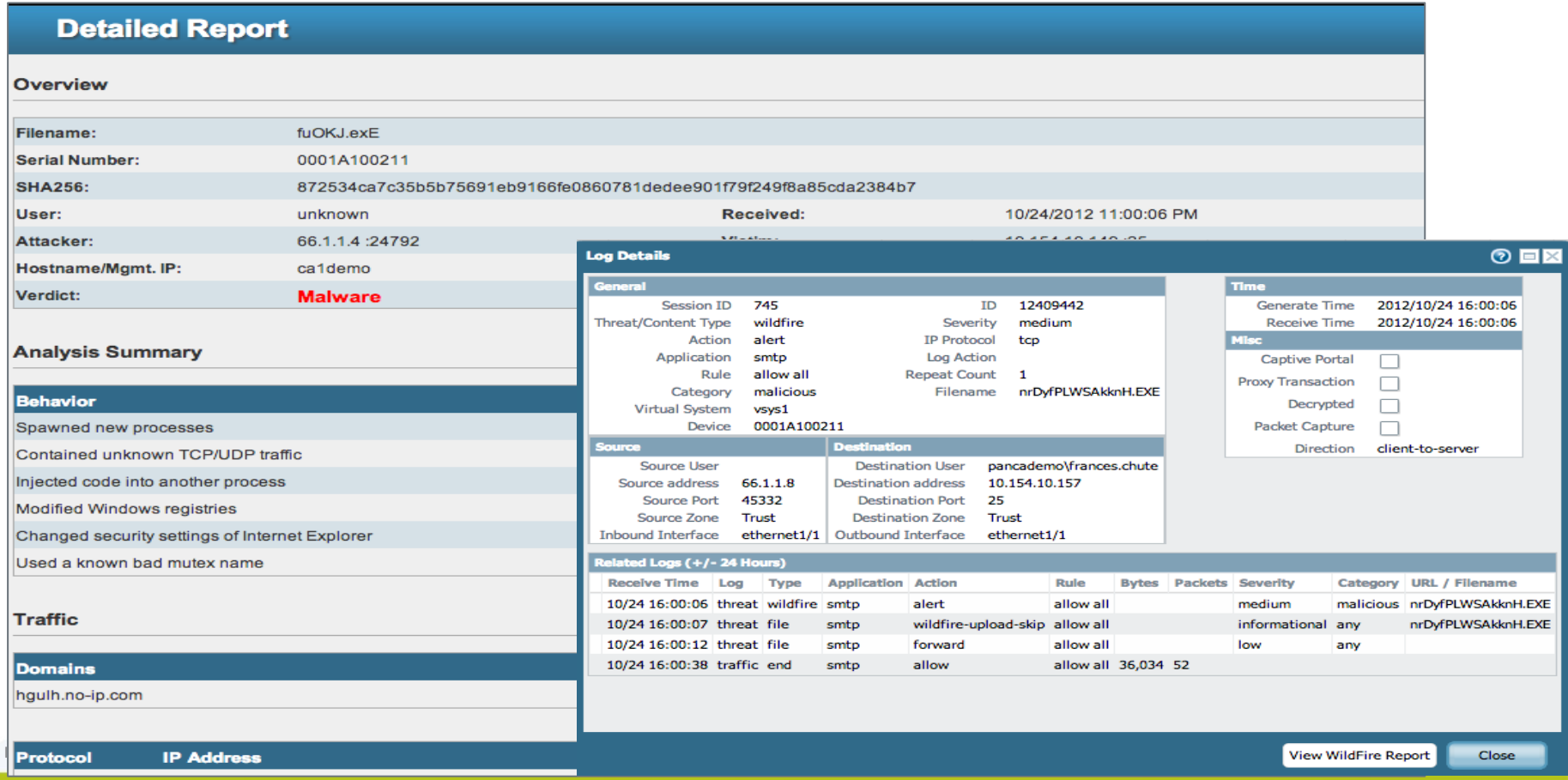
WildFire Architecture



- 10 Gbps Threat Prevention and file scanning
- All traffic, all ports
- Web, email, FTP and SMB

- Malware signatures developed and tested based on malware payload.
- Stream-based malware

Malware Visibility and Logging



WILDFIRE

1,300+

COMPANIES USING WILDFIRE

417,448

UNIQUE FILES SCANNED IN JA

28,612

NEW MALWARE FILES FOUND IN JANUARY USING WILDFIRE

13,233 (46%)

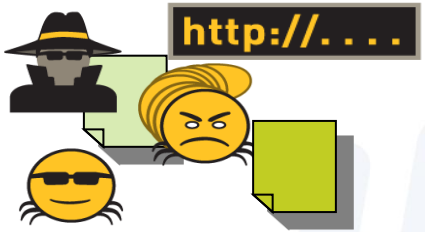
MALWARE NOT INITIALLY DETECTED BY TOP HOST AV PRODUCTS

Palo Alto Networks in the DataCenter

Enabling Applications, Users and Content

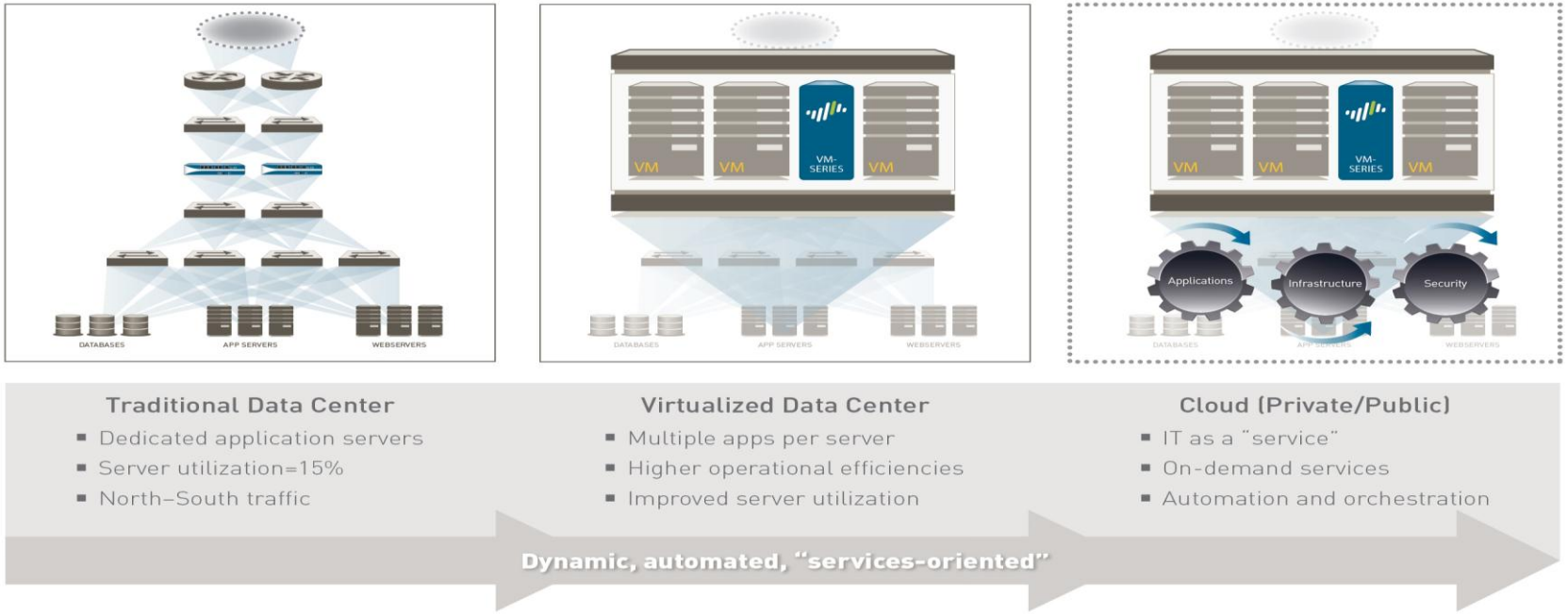
- **Applications:** Safe enablement begins with application classification by App-ID.

- **Users:** Tying users and devices, regardless of location, to applications with User-ID and GlobalProtect.



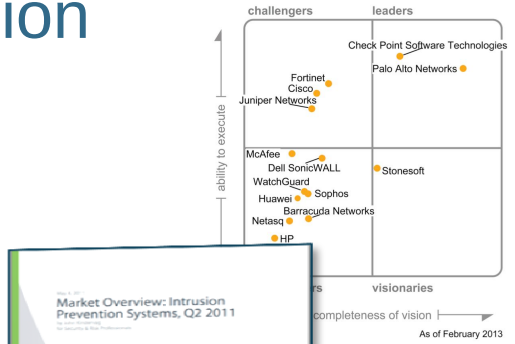
- **Content:** Scanning content and protecting against all threats – both known and unknown;

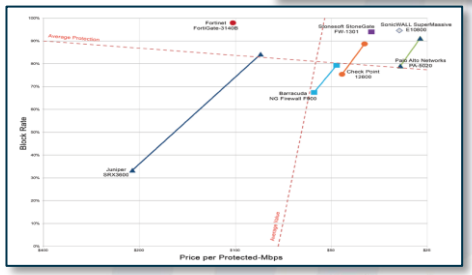
Data Center Evolution



Many Third Parties Reach Same Conclusion

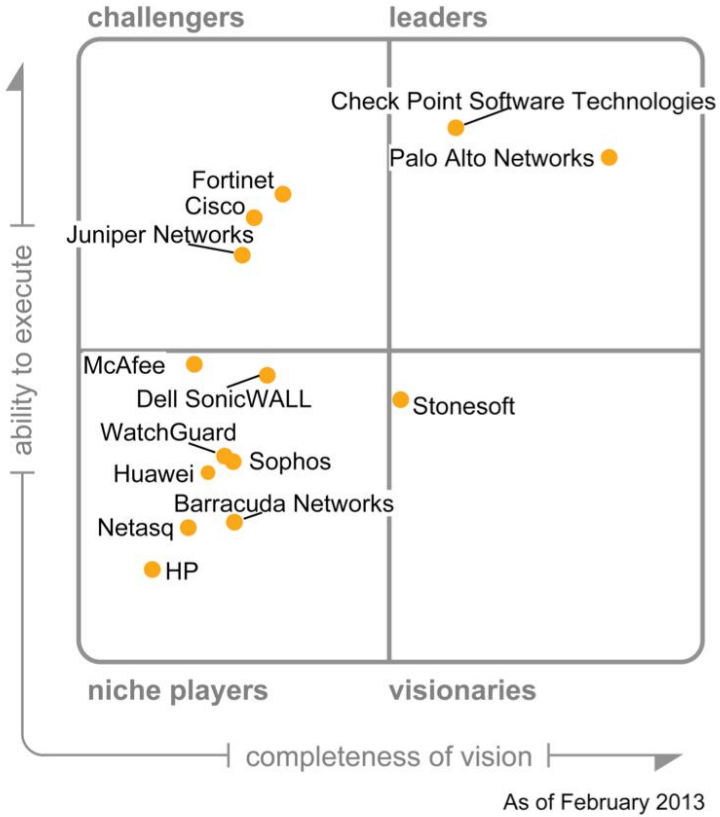
- Gartner Enterprise Network Firewall Magic Quadrant
  - Palo Alto Networks leading the market
- Forrester IPS Market Overview
  - Strong IPS solution; demonstrates effective consolidation
- NetworkWorld Test
  - Most stringent NGFW test to date; validated sustained performance
- NSS Tests
  - IPS: Palo Alto Networks NGFW tested against competitors' standalone IPS devices; NSS Recommended
  - Firewall: Traditional port-based firewall test; Palo Alto Networks most efficient by a wide margin; NSS Recommended
  - NGFW: Palo Alto Networks provides the best combination of protection, performance, and value; NSS Recommended (1 of only 3 NGFW recommended)





Say no more!!! Leaders quadrant in the leaders quadrant

A crisp focus on enterprise NGFW features and messaging is viewed positively by firewall operators in enterprises.



Most firewall vendor road maps are following the Palo Alto Networks NGFW road map, placing these vendors at a competitive disadvantage.

Next Generation Customer meeting, Ultimate Test Drive

- Ultimate Test Drive
  - En halv dags «hands-on»
  - En PA-200 trekkes blant deltagerne
  - Audi driving school trekkes en gang hvert kvartal

Thank You