

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

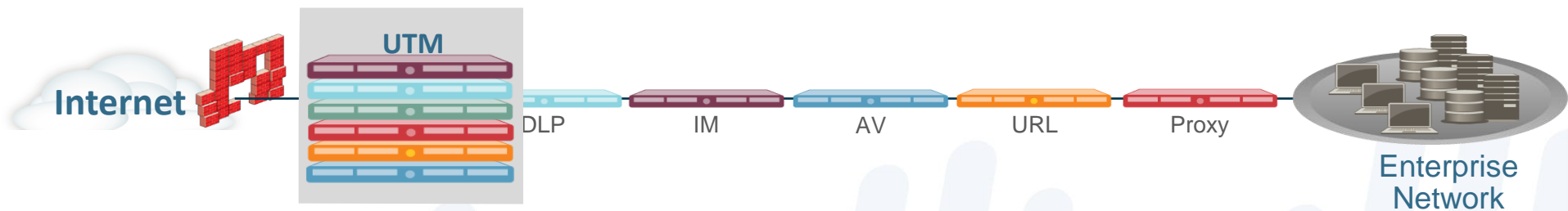
Gøran Tømte

March 2013

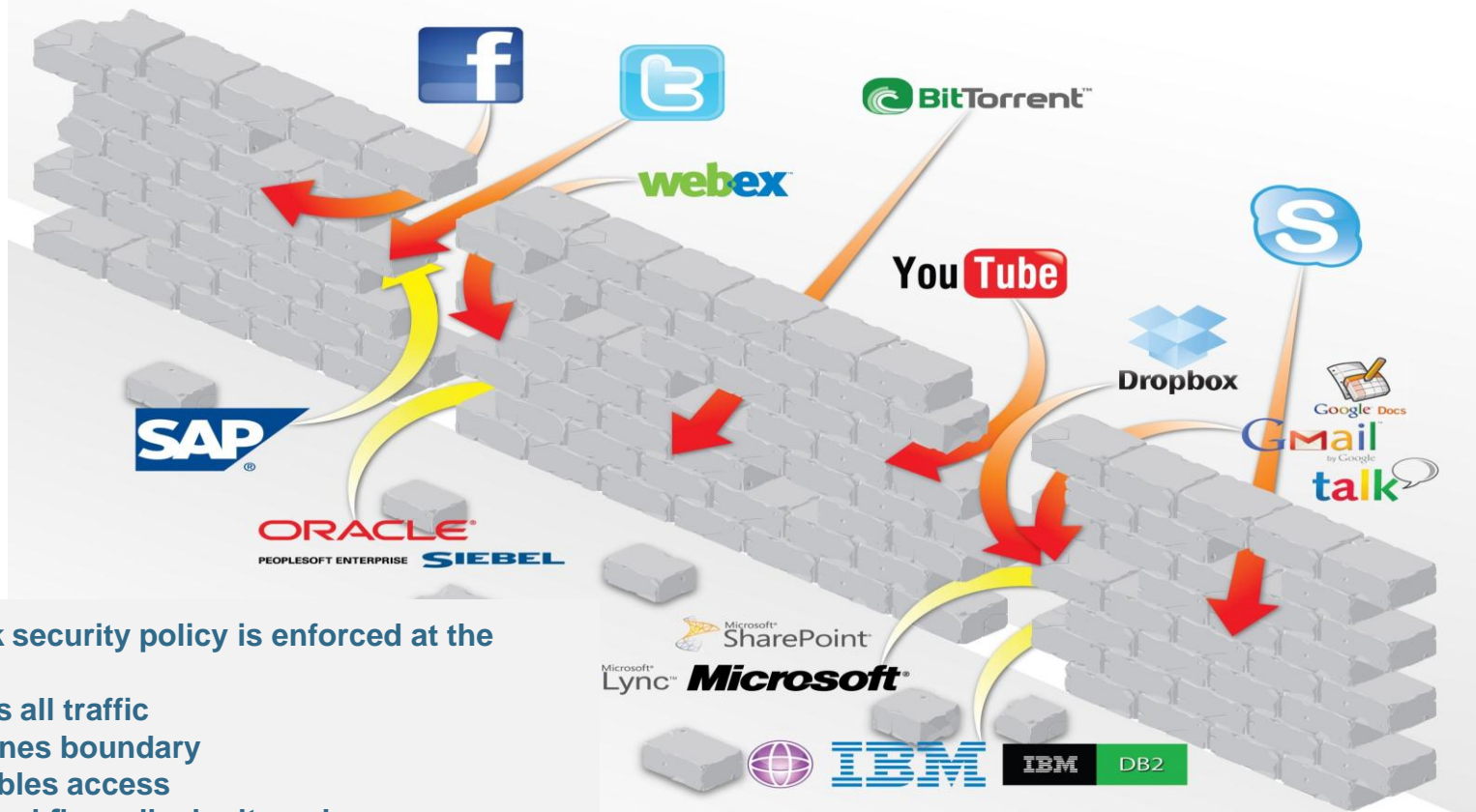


Technology Sprawl and Creep Aren't the Answer

- “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

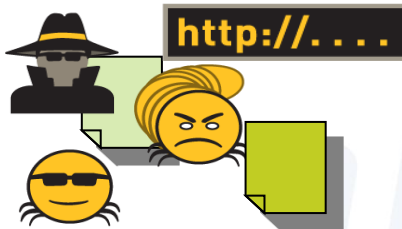
- Sees all traffic
- Defines boundary
- Enables access

Traditional firewalls don't work any more

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

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**.

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

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



The unknown! Scary hah?

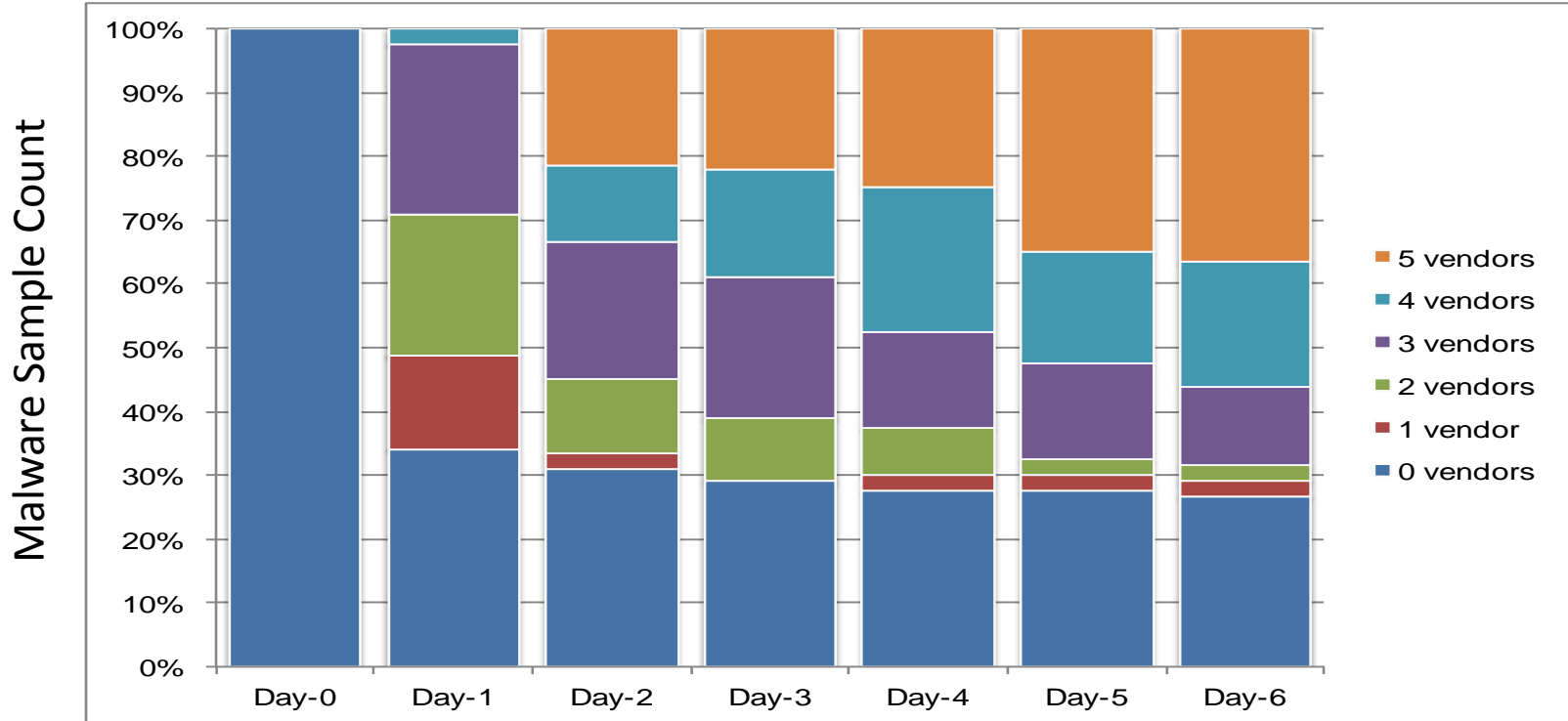
- Unknown applications
 - Control them
- Unknown users
 - Control them
- Unknown threats
 - Control them



Addressing Modern Malware

Daily Coverage of Top AV Vendors

Daily AV Coverage Rates for Newly Released Malware (50 Samples)



New Malware Coverage Rate by Top 5 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

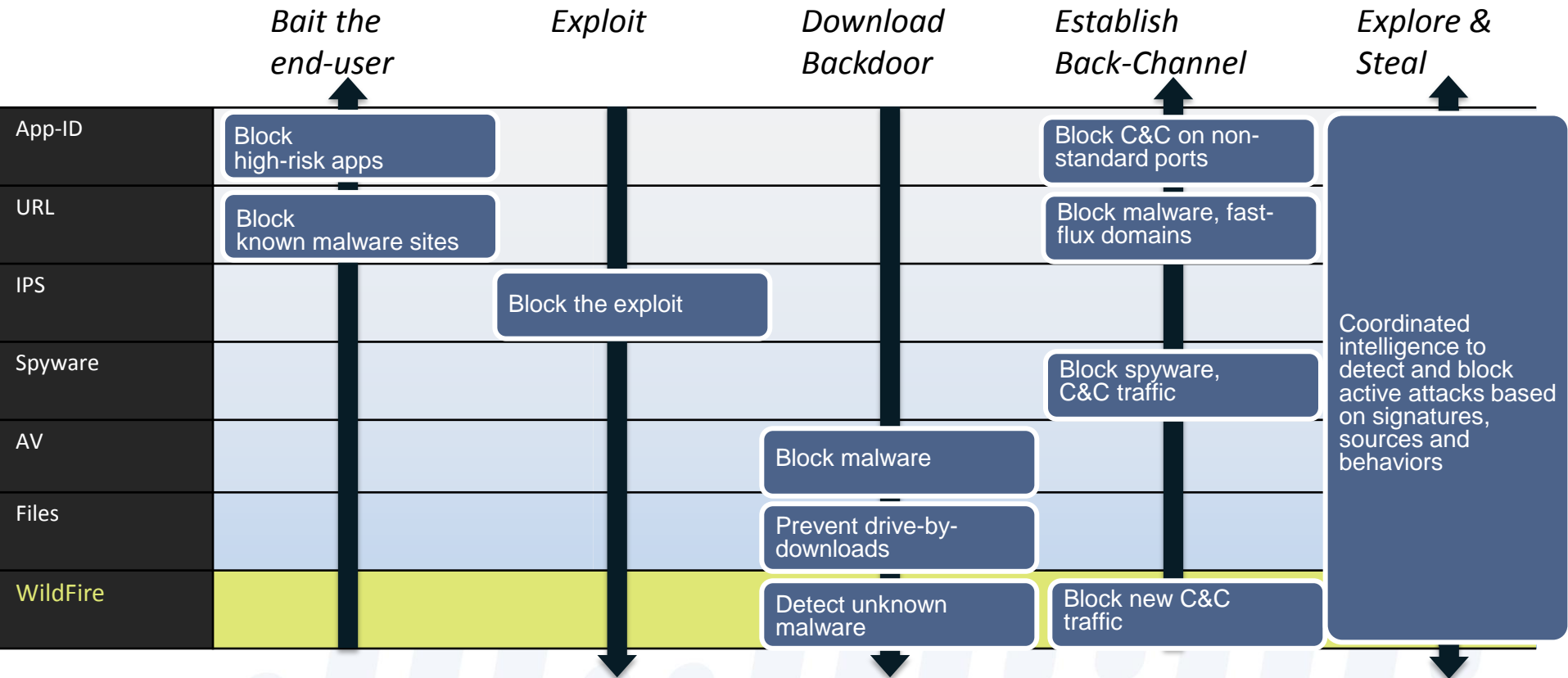
5

Explore & Steal

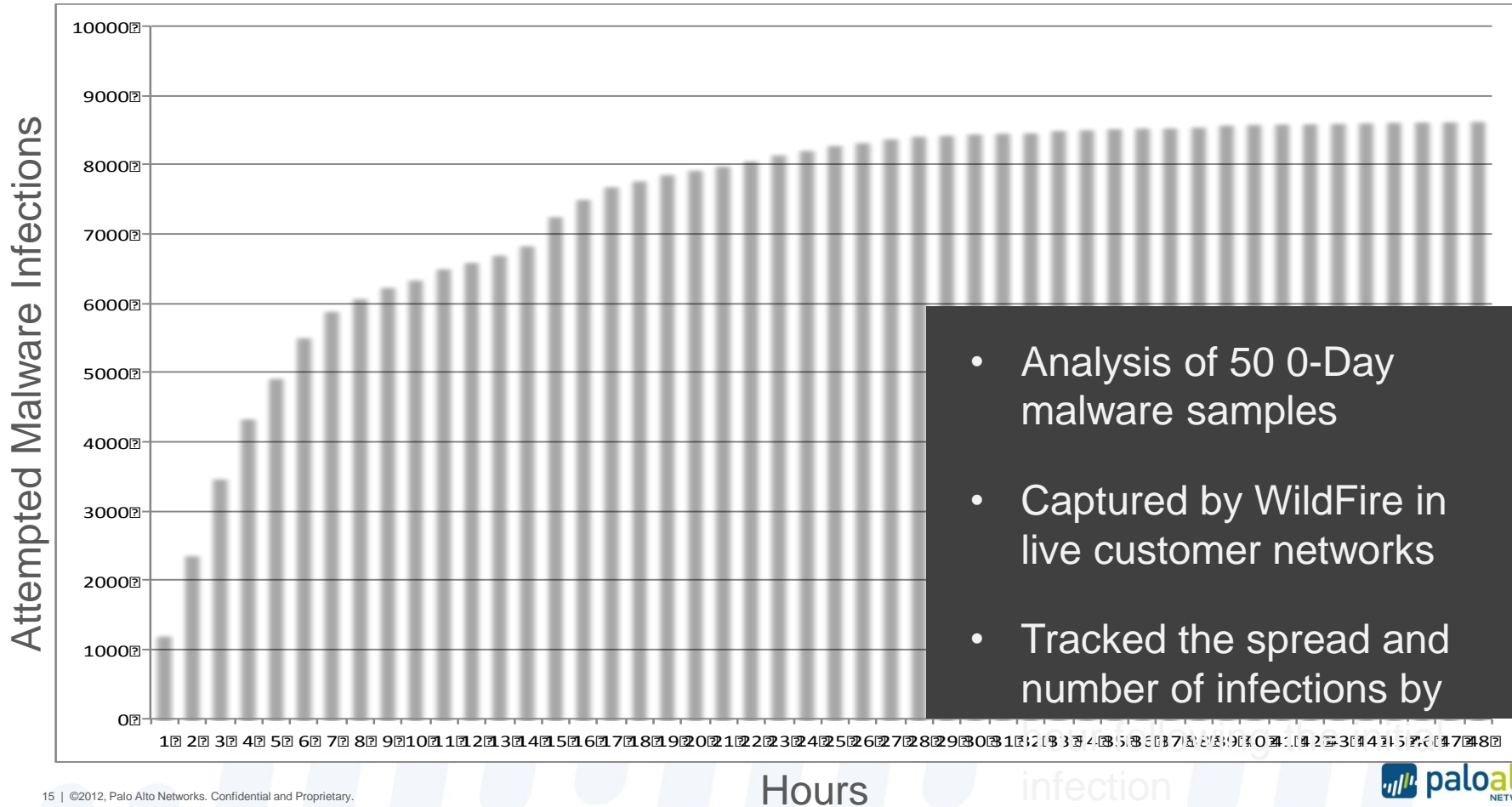
Remote attacker has control inside the network and escalates the attack



An integrated approach to threat prevention

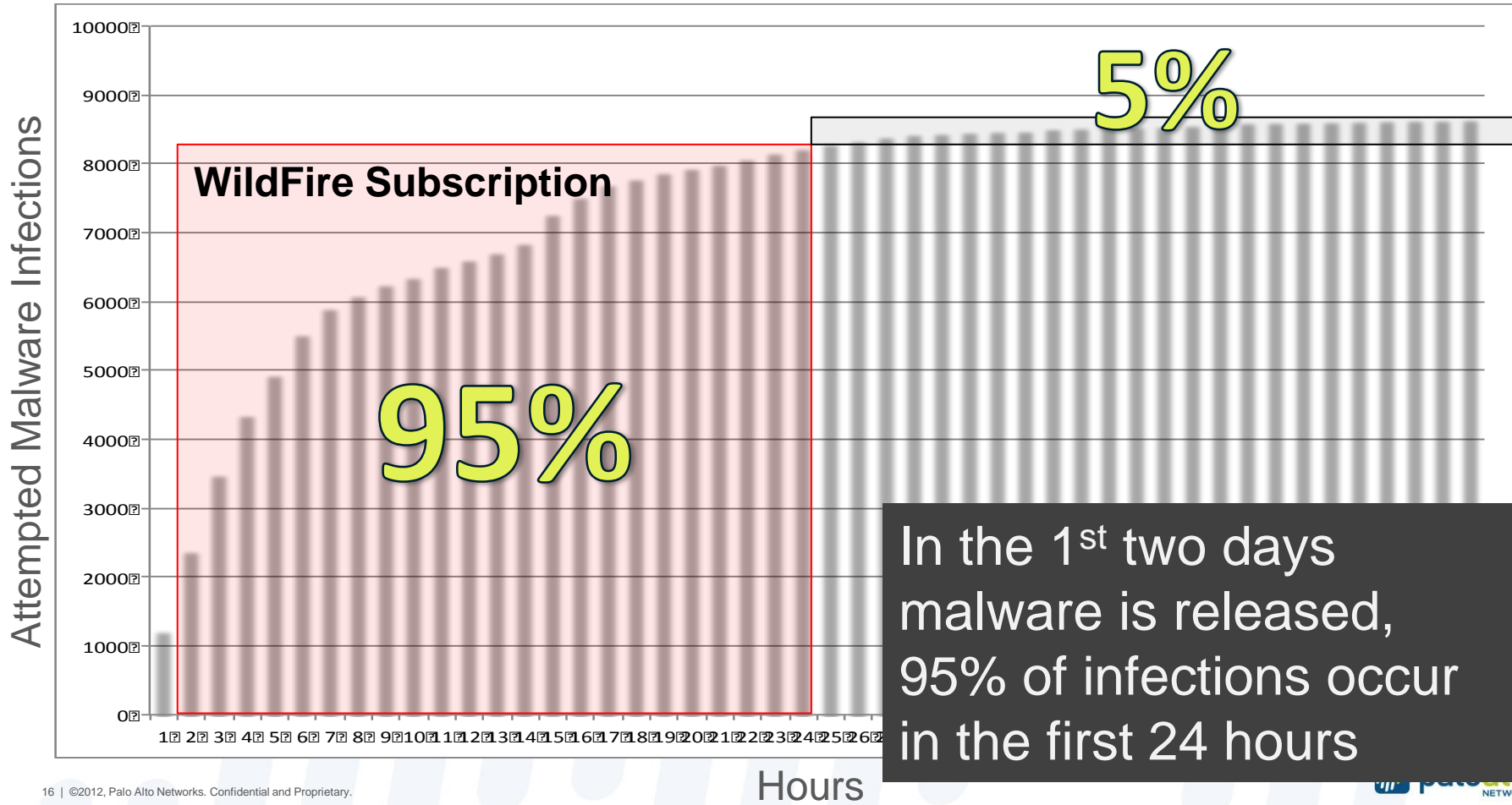


Real-World Spread of 0-Day Malware



- Analysis of 50 0-Day malware samples
- Captured by WildFire in live customer networks
- Tracked the spread and number of infections by

Real-World Spread of 0-Day Malware



WildFire Architecture

WildFire

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

Exfiltration
of sensitive data

WildFire Cloud
Observes and detects 100+
malicious behaviors to identify malware

FILE TRANSFER DECODERS

PATTERN DB

SINGLE PASS PATTERN MATCH

REPORT & ENFORCE POLICY

- Malware signatures developed and tested based on malware payload.

- Stream-based malware

Malware Visibility and Logging

Detailed Report

Overview

Filename:	fuOKJ.exe		
Serial Number:	0001A100211		
SHA256:	872534ca7c35b5b75691eb9166fe0860781dedee901f79f249f8a85cda2384b7		
User:	unknown	Received:	10/24/2012 11:00:06 PM
Attacker:	66.1.1.4 :24792		
Hostname/Mgmt. IP:	ca1demo		
Verdict:	Malware		

Analysis Summary

Behavior

- Spawned new processes
- Contained unknown TCP/UDP traffic
- Injected code into another process
- Modified Windows registries
- Changed security settings of Internet Explorer
- Used a known bad mutex name

Traffic

Domains

hgulh.no-ip.com

Protocol	IP Address
----------	------------

Log Details

General

Session ID	745	ID	12409442
Threat/Content Type	wildfire	Severity	medium
Action	alert	IP Protocol	tcp
Application	smtp	Log Action	
Rule	allow all	Repeat Count	1
Category	malicious	Filename	nrDyPLWSAkknH.EXE
Virtual System	vsys1		
Device	0001A100211		

Source

Source User		Destination User	pancademo\frances.chute
Source address	66.1.1.8	Destination address	10.154.10.157
Source Port	45332	Destination Port	25
Source Zone	Trust	Destination Zone	Trust
Inbound Interface	ethernet1/1	Outbound Interface	ethernet1/1

Destination

Destination User	pancademo\frances.chute
Destination address	10.154.10.157
Destination Port	25
Destination Zone	Trust
Outbound Interface	ethernet1/1

Time

Generate Time	2012/10/24 16:00:06
Receive Time	2012/10/24 16:00:06

Misc

Captive Portal	<input type="checkbox"/>
Proxy Transaction	<input type="checkbox"/>
Decrypted	<input type="checkbox"/>
Packet Capture	<input type="checkbox"/>
Direction	client-to-server

Related Logs (+/- 24 Hours)

Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL / Filename
10/24 16:00:06	threat	wildfire	smtp	alert	allow all			medium	malicious	nrDyPLWSAkknH.EXE
10/24 16:00:07	threat	file	smtp	wildfire-upload-skip	allow all			informational	any	nrDyPLWSAkknH.EXE
10/24 16:00:12	threat	file	smtp	forward	allow all			low	any	
10/24 16:00:38	traffic	end	smtp	allow	allow all	36,034	52			

[View WildFire Report](#) [Close](#)

1,300+

COMPANIES USING WILDFIRE

417,448

UNIQUE FILES SCANNED IN JANUARY

WILDFIRE

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

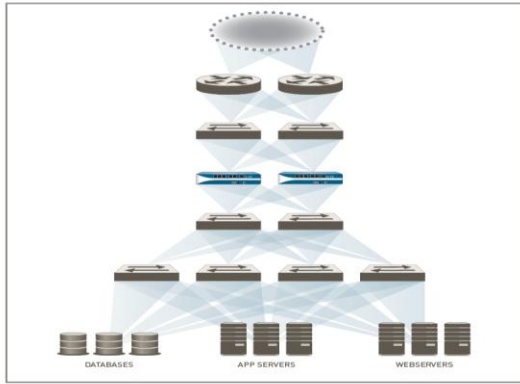


Enabling Applications, Users and Content



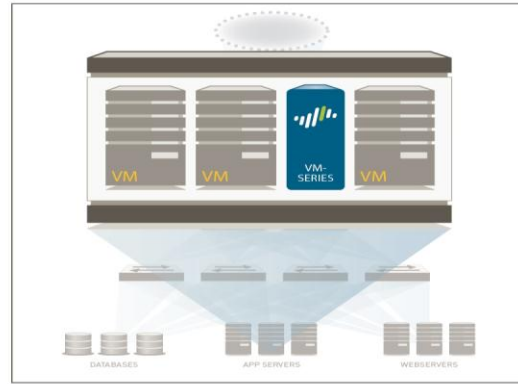
- **Applications:** Safe enablement begins with application classification by **App-ID**.
- **Users:** Tying users and devices, regardless of location, to applications with **User-ID** and **GlobalProtect**.
- **Content:** Scanning content and protecting against all threats – both known and unknown:

Data Center Evolution



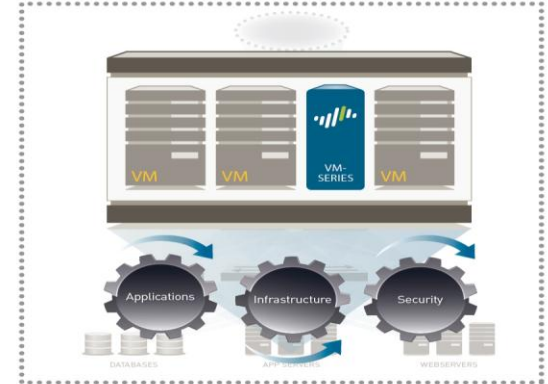
Traditional Data Center

- Dedicated application servers
- Server utilization=15%
- North-South traffic



Virtualized Data Center

- Multiple apps per server
- Higher operational efficiencies
- Improved server utilization



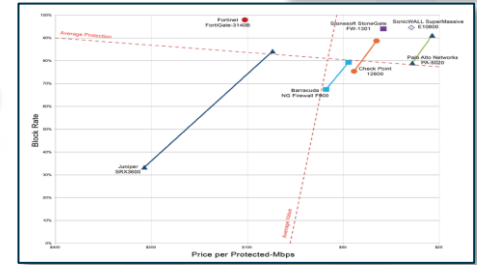
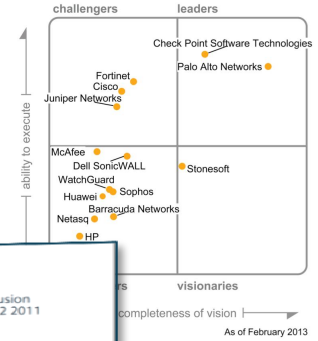
Cloud (Private/Public)

- IT as a "service"
- On-demand services
- Automation and orchestration

Dynamic, automated, "services-oriented"

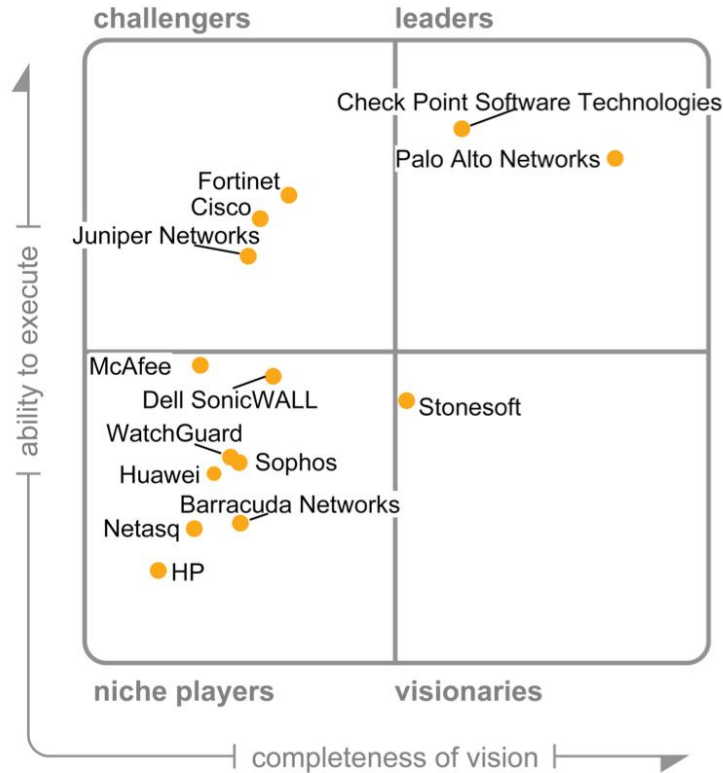
Many Third Parties Reach Same Conclusion

- 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.

As of February 2013

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



the network **security** company™