Palo Alto Networks

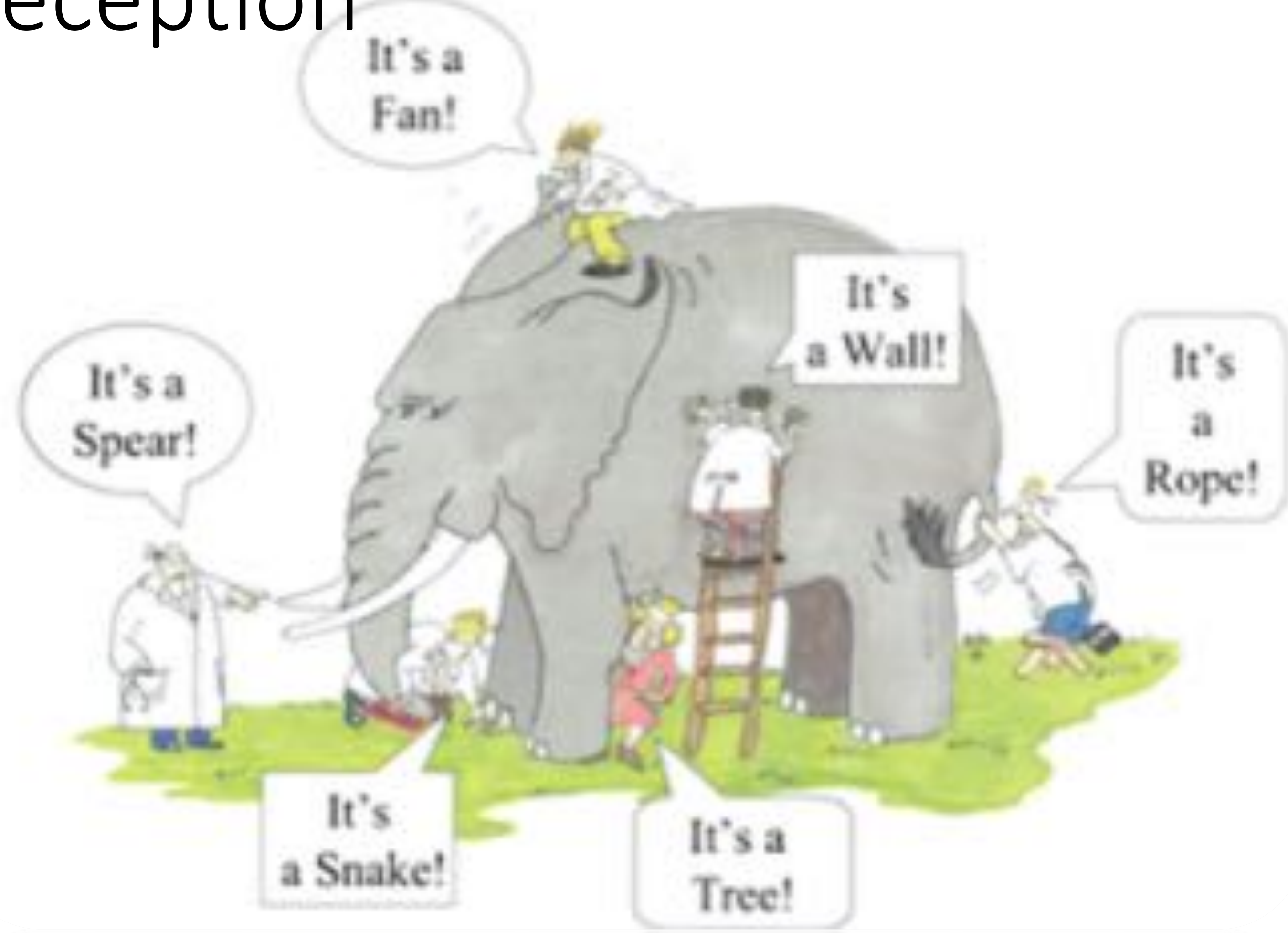
What's changed?
Volume

Attack vectors
Zero days
Sheer volume

Traditional security design fails to cope with the sheer attack volume and keep pace

What’s changed?
Multi-stage attacks and deception

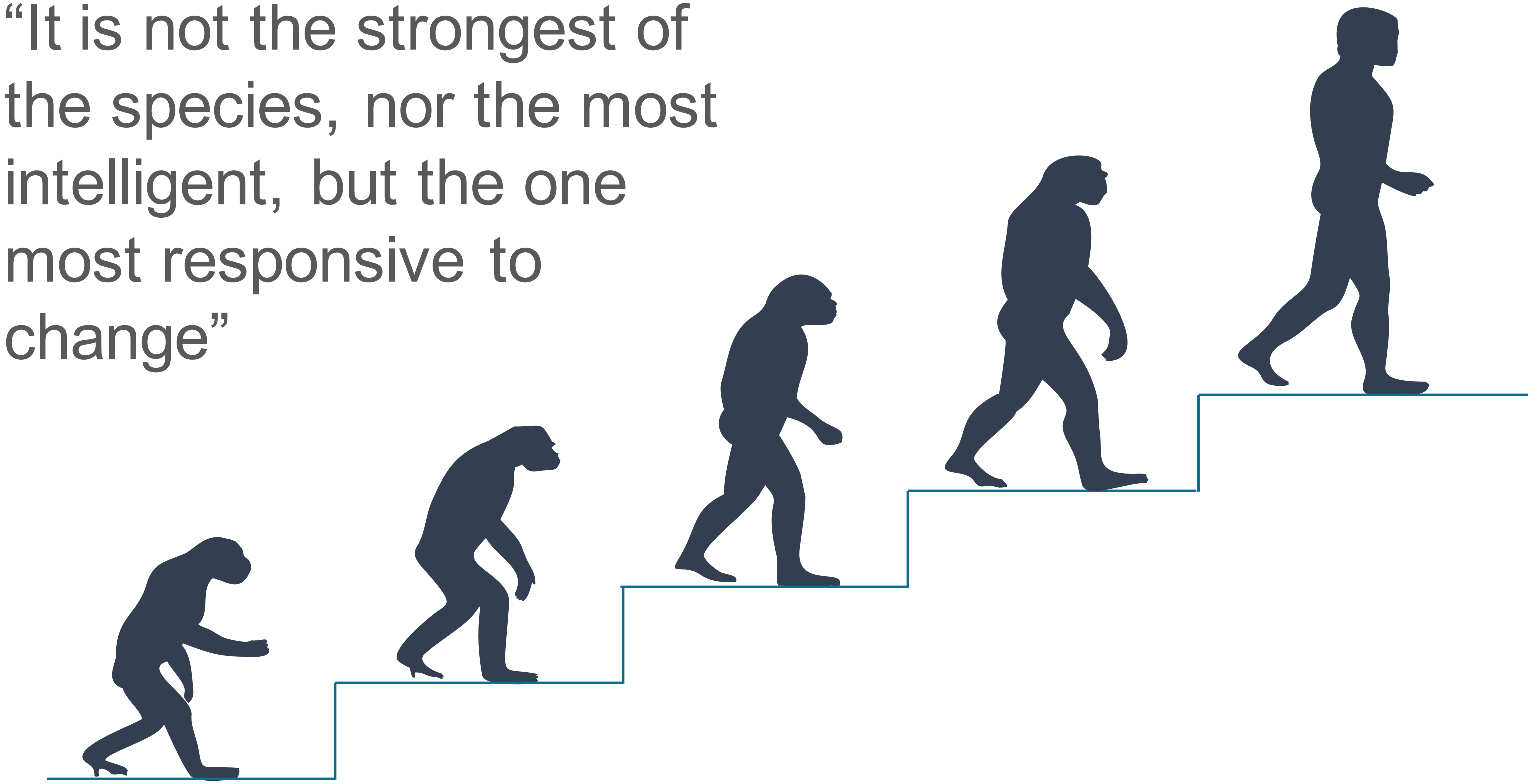
Each man is partly right, though all
are in the wrong.



Traditional security design fails to give full visibility and communicate context to other security technologies

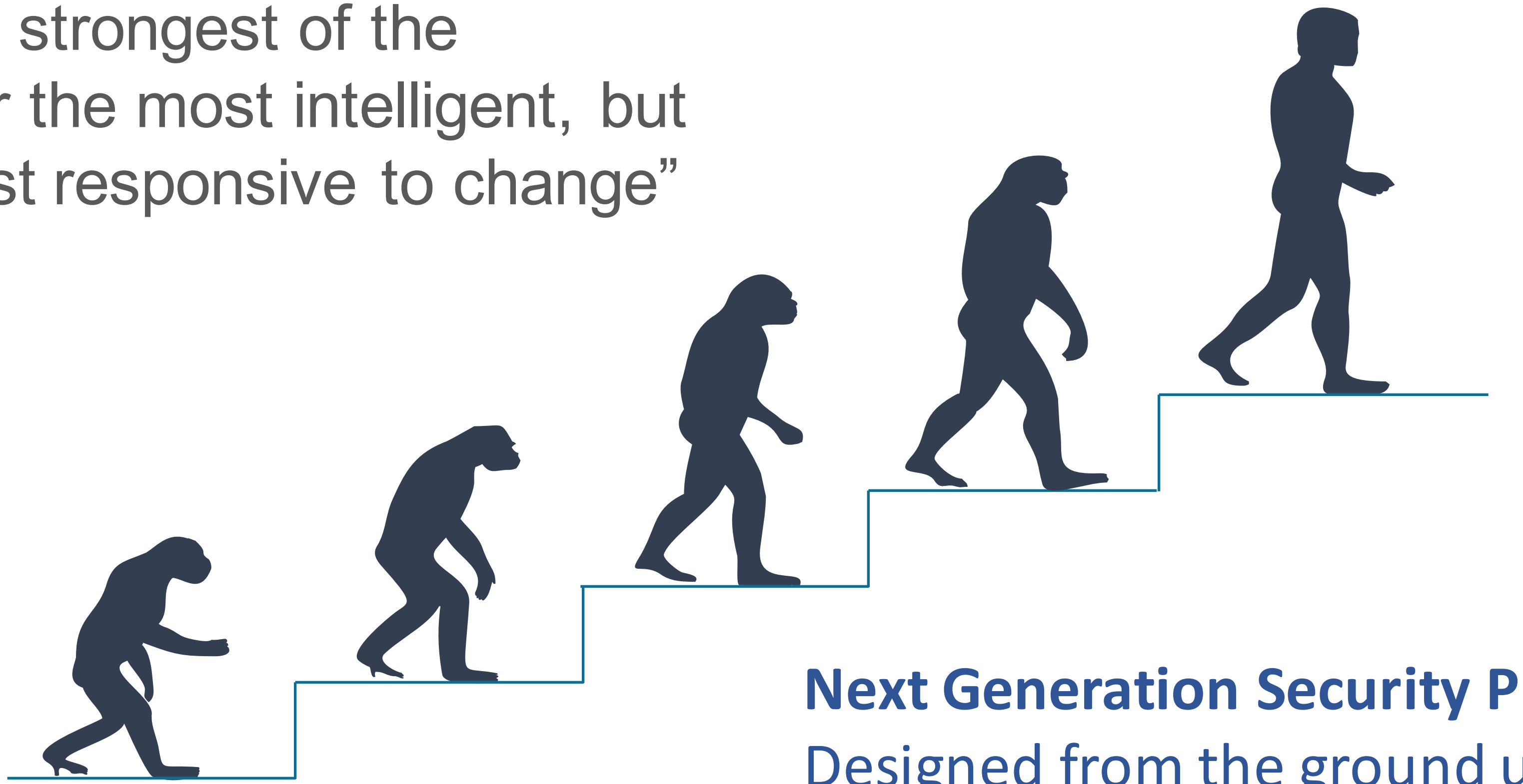
The quote that Darwin never said

“It is not the strongest of the species, nor the most intelligent, but the one most responsive to change”



The quote that Darwin never said

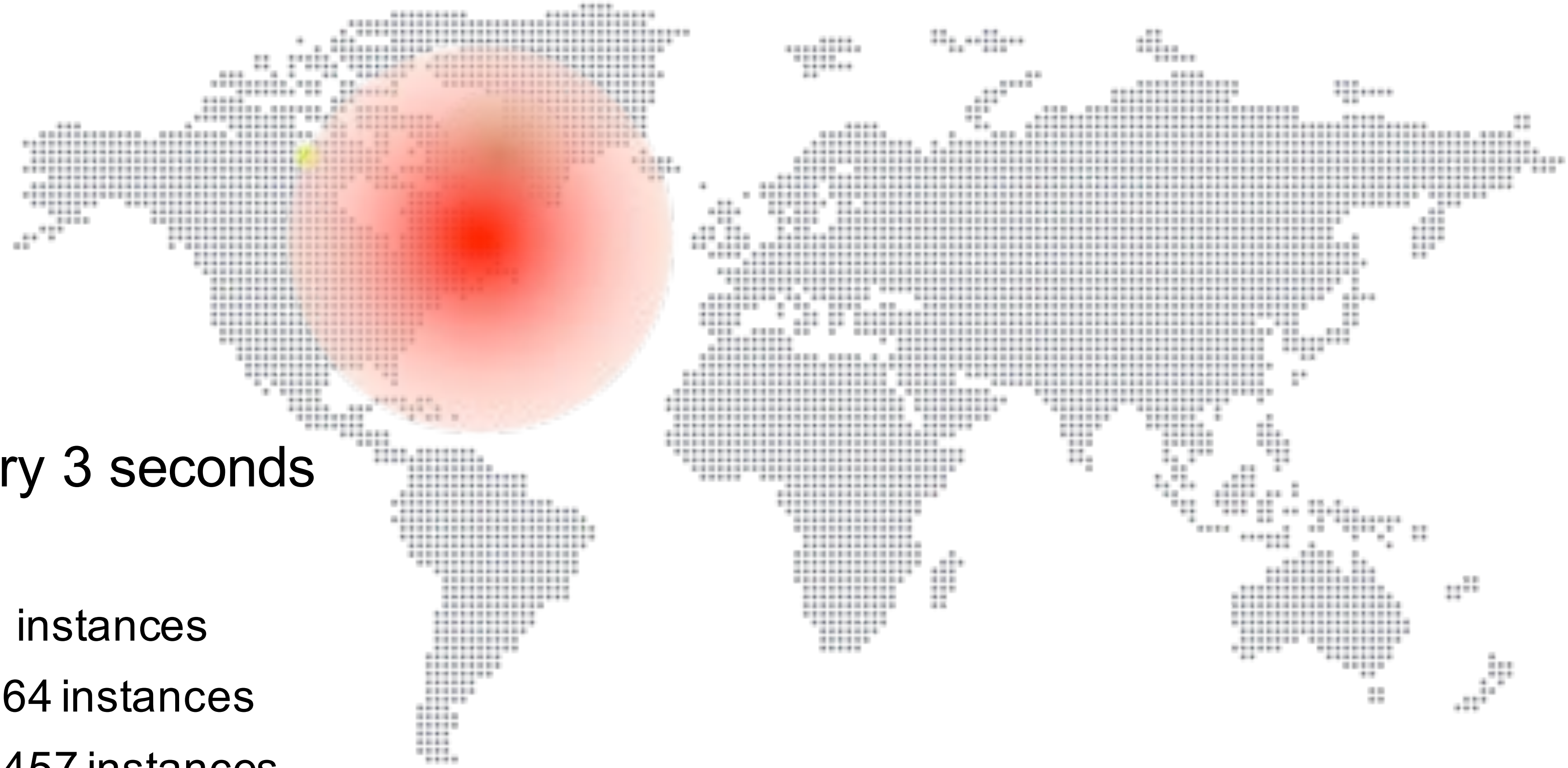
"It is not the strongest of the species, nor the most intelligent, but the one most responsive to change"



Next Generation Security Platform
Designed from the ground up to counter attacks as they manifest and morph across the endpoint, network and cloud

Stop the spread, prevent attacks

30 Minutes of malware



New infection every 3 seconds
After….

1 minute = 2,021 instances

15 minutes = 9,864 instances

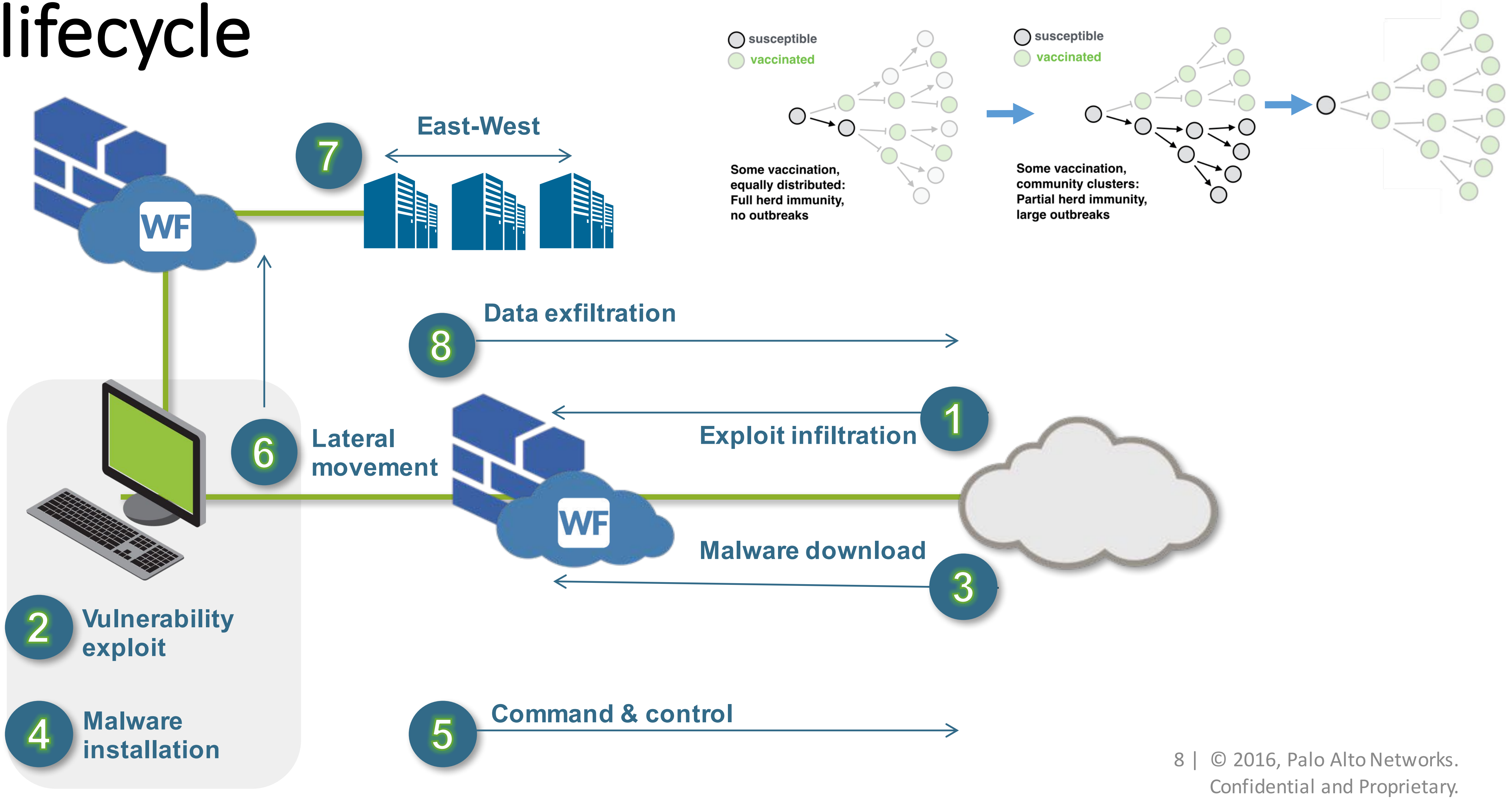
30 minutes = 45,457 instances

Prevention first

You think that you are overwhelmed now, can you imagine your incident response without prevention?

Reduce the attack surface across all locations, traffic, applications and users

Opportunities to prevent attacks – attack lifecycle



Some vaccination, equally distributed: Full herd immunity, no outbreaks

Some vaccination, community clusters: Partial herd immunity, large outbreaks

7 East-West

8 Data exfiltration

1 Exploit infiltration

6 Lateral movement

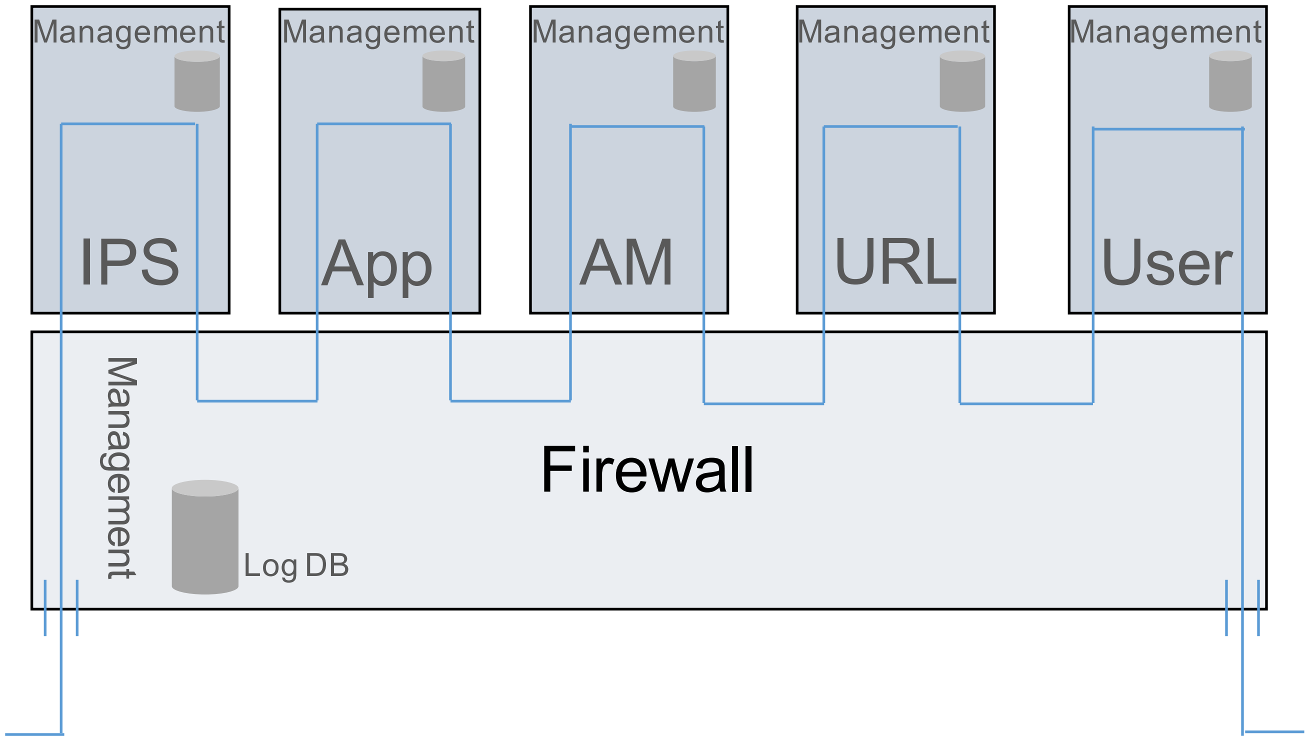
Malware download 3

2 Vulnerability exploit

4 Malware installation

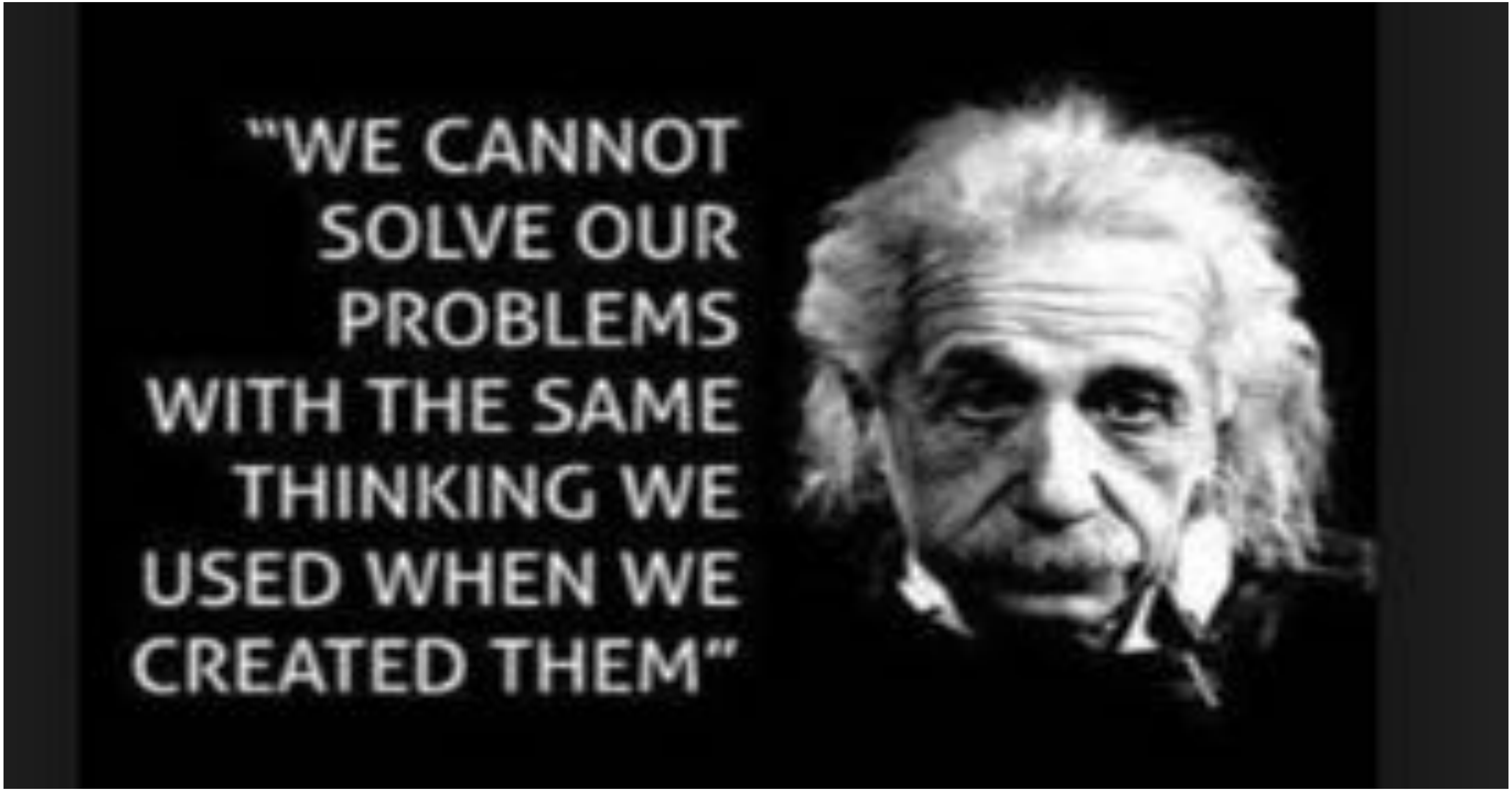
5 Command & control

UTM Architecture



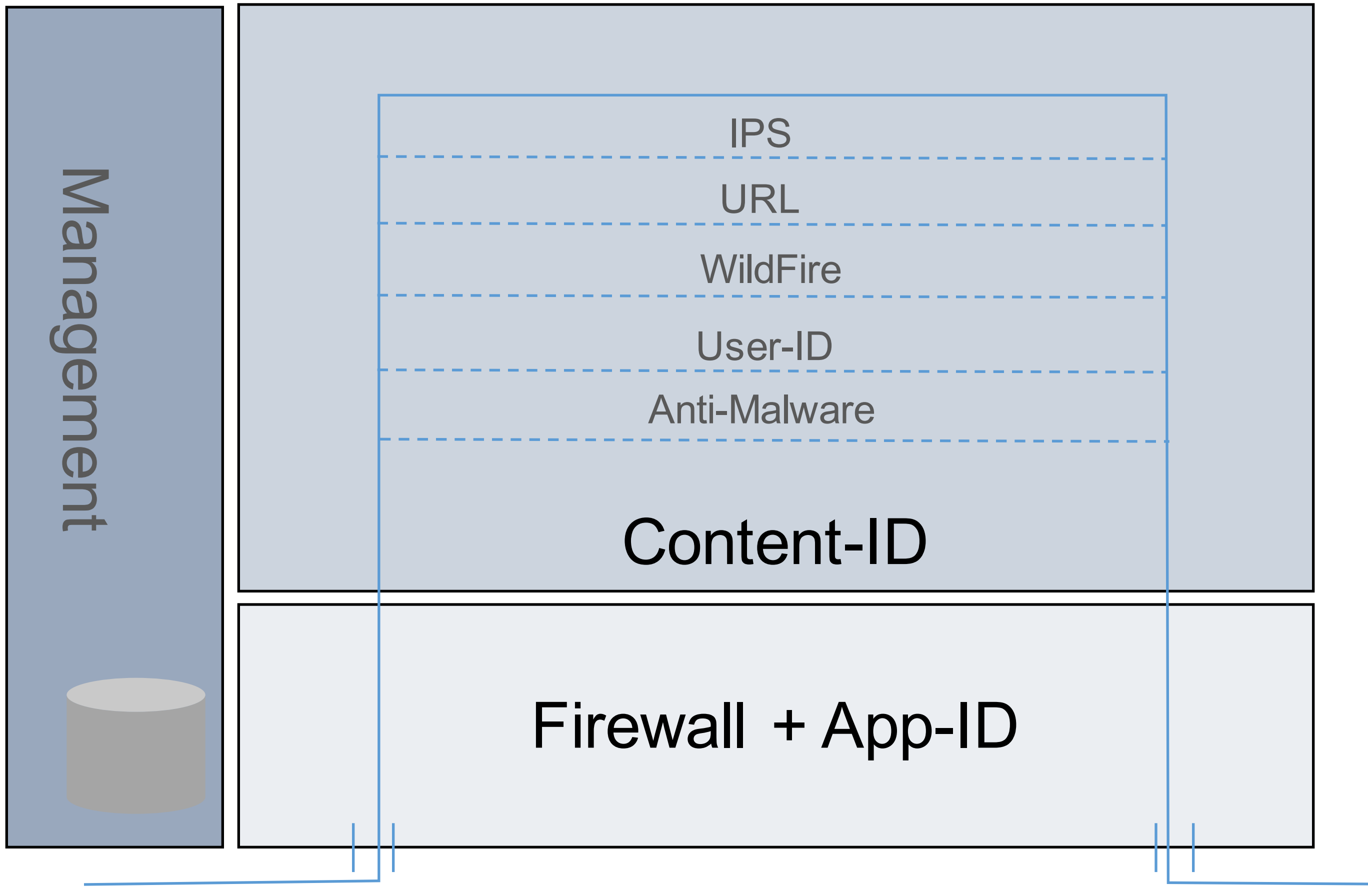
Serial Processing

NO Predictability



"WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM"

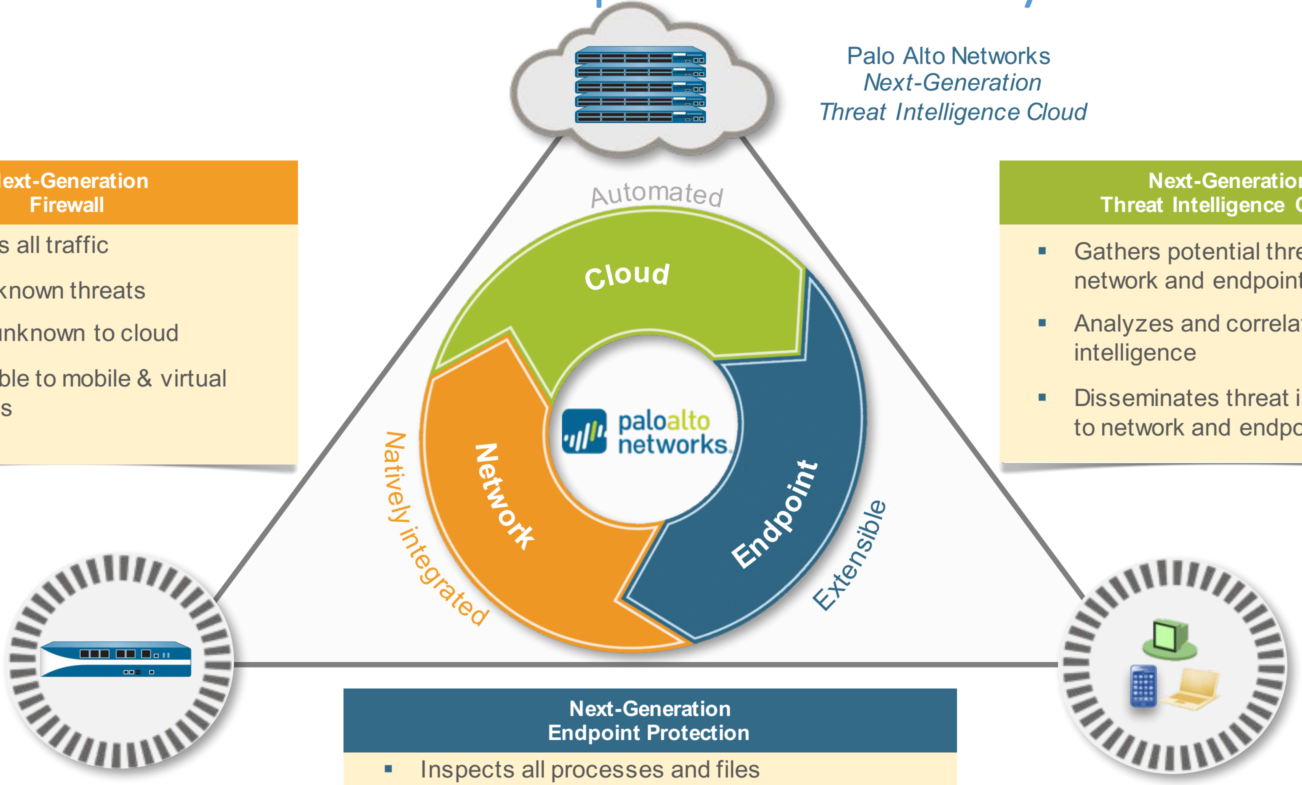
NGFW Architecture



Single Pass Parallel Processing

Predictability

Next-Generation Enterprise Security Platform



Next-Generation Firewall

- Inspects all traffic
- Blocks known threats
- Sends unknown to cloud
- Extensible to mobile & virtual networks

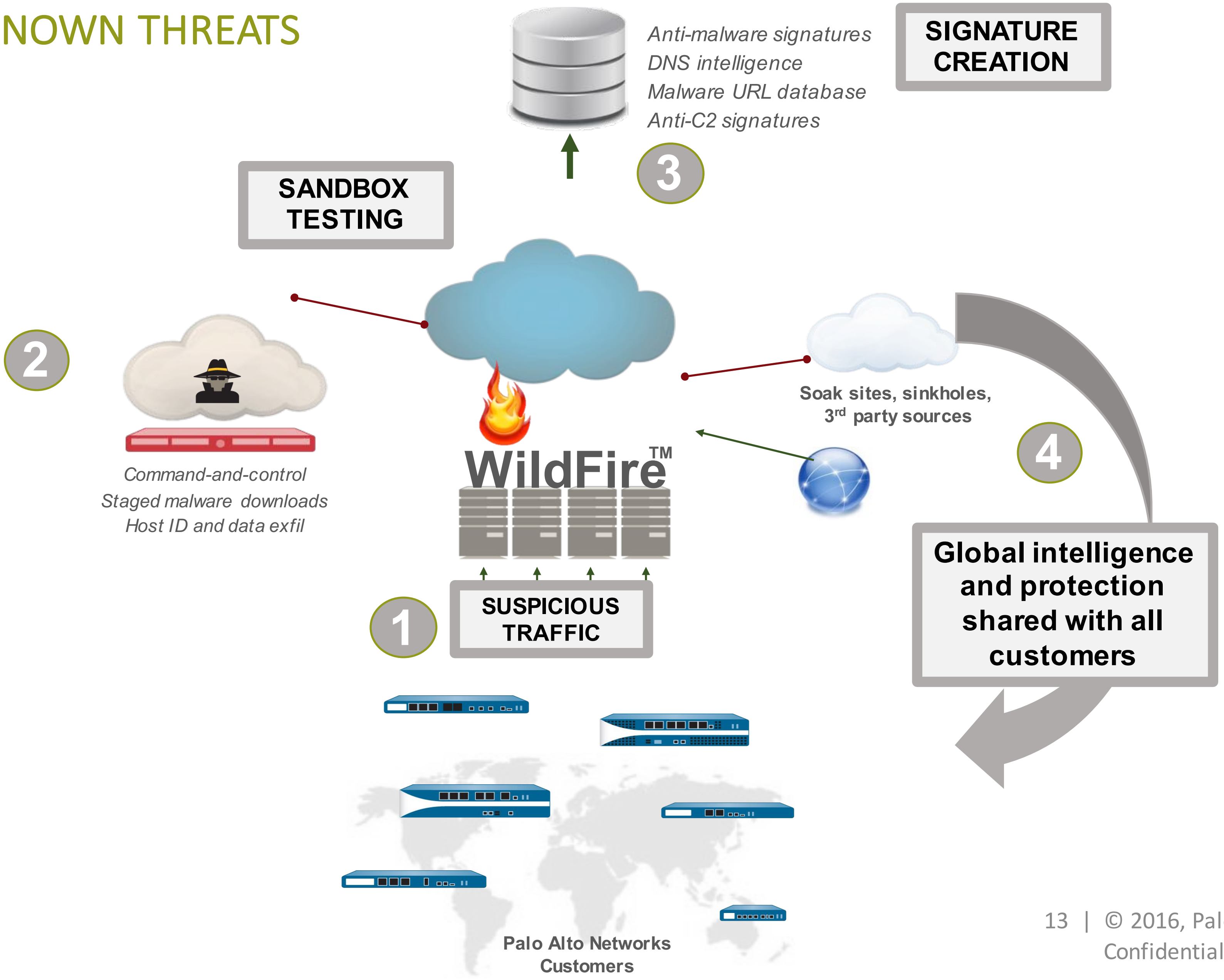
Next-Generation Threat Intelligence Cloud

- Gathers potential threats from network and endpoints
- Analyzes and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

Next-Generation Endpoint Protection

- Inspects all processes and files
- Prevents both known & unknown exploits
- Integrates with cloud to prevent known & unknown malware

PREVENTION AGAINST UNKNOWN THREATS



3

Anti-malware signatures
DNS intelligence
Malware URL database
Anti-C2 signatures

SIGNATURE CREATION

SANDBOX TESTING

2

Command-and-control
Staged malware downloads
Host ID and data exfil

WildFire™

Soak sites, sinkholes, 3rd party sources

4

Global intelligence and protection shared with all customers

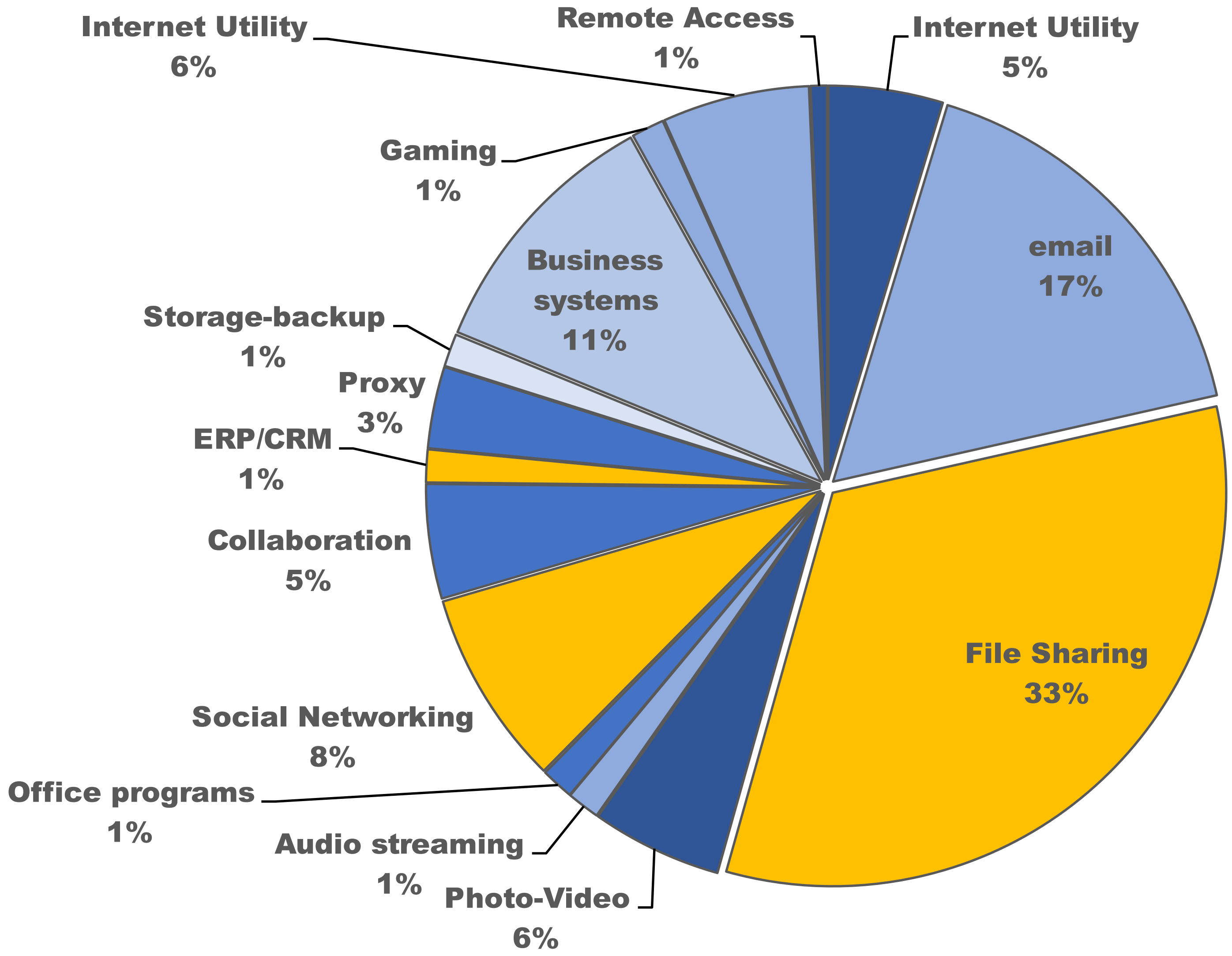
1

SUSPICIOUS TRAFFIC

Palo Alto Networks Customers

Detect new unknown attacks across all traffic

154 total different application types used in the past year



Detection to prevention

- **GENERATE SMART PROTECTIONS**
  - Content-Based vs. Hash-Based Signatures
  - Up to **331,000** malware variants have been prevented by **a single signature**.

- **ON AVERAGE PER WEEK:**
  - **20 million** samples analyzed
  - **200,000+** unique malware identified
  - WildFire threat intelligence is sourced from **9,000+ customers** worldwide.

Correlation Engine
Who is trying to steal your treasure?

Automated threat correlation engine for identifying malicious patterns of activity

- Looks for confirmed IOCs
- Reduces manual data mining
- Automatically highlights compromised hosts

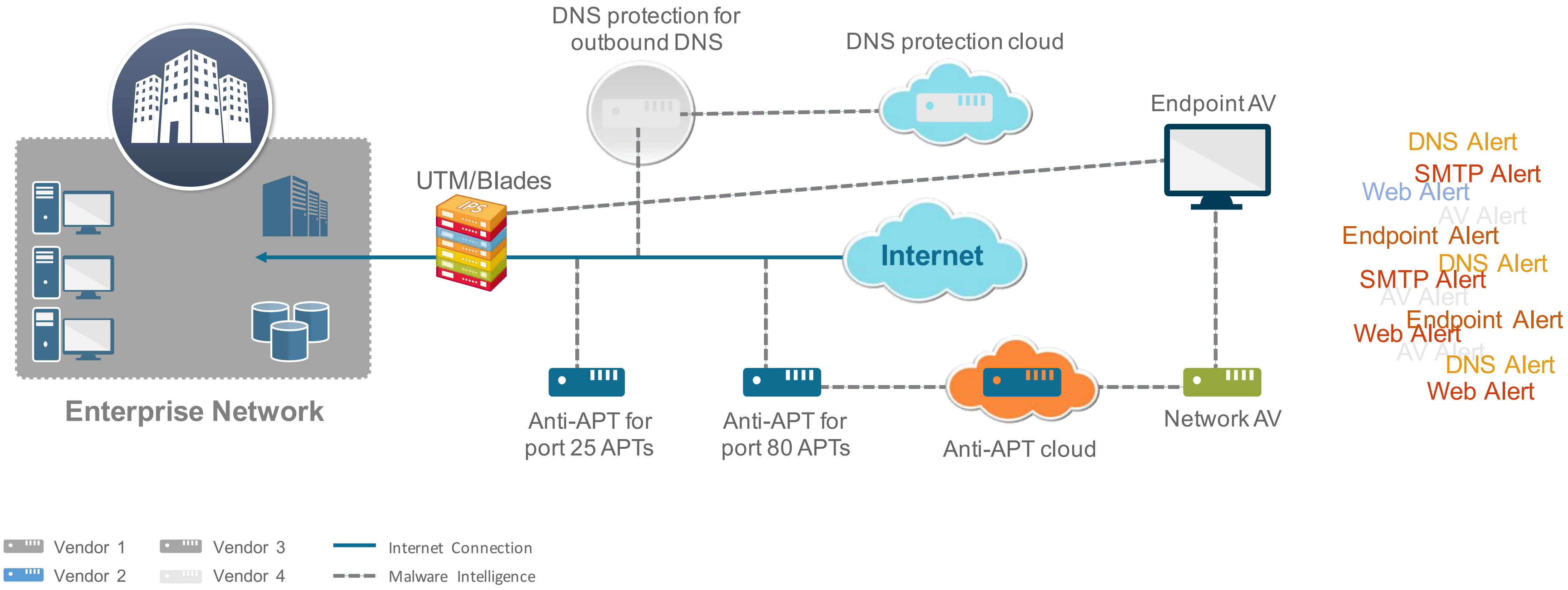
A Change is needed

Traditionally	The new world
• Limited visibility	• Full visibility, leveraging the Firewall + User ID, App ID, SSL Decryption
• Another box, built to maintain productivity	• Key threat prevention component • Cloud-based URL categorization database • Core technology present on the firewall (Built in-house)
• Solitary functionality, easily bypassed	• Coordinates protections with all other platform technologies • Prevents malicious web sites and phishing pages • Continually updated with current threat intelligence • Designed for performance and accuracy

paloalto NETWORKS®

Failure of legacy security architectures

Limited visibility | **Lacks correlation** | **Manual response**



DNS protection for outbound DNS

DNS protection cloud

Endpoint AV

UTM/Blades

Internet

Enterprise Network

Anti-APT for port 25 APTs

Anti-APT for port 80 APTs

Anti-APT cloud

Network AV

DNS Alert
SMTP Alert
Web Alert
AV Alert
Endpoint Alert
DNS Alert
SMTP Alert
AV Alert
Endpoint Alert
Web Alert
AV Alert
DNS Alert
Web Alert

Vendor 1
Vendor 2
Vendor 3
Vendor 4
Internet Connection
Malware Intelligence