Threats have Changed, Security Has Not

Alfred Lee

VP, Product Management, Palo Alto Networks

paloalto networks.

Today’s threat landscape

Organized attackers

Increasing volume

Sophisticated

Remediation is broken

Must prevent attacks across perimeter, cloud and endpoint

Limited correlation across disjointed security technologies

Limited security expertise

Security challenges

paloalto networks.

Detection-focused technology investments

Network Security

- IPS deployed as IDS
- App blades that only detect and report
- SSL traffic allowed without decryption
- When decrypted, SSL just port-mirrored
- Sandboxes deployed to detect malware
- Snort engines to detect traffic to high risk IPs

Endpoint Protection

- Forensics agents to capture what happened
- IOC scanners
- Massive PCAP storage
- Remediation tools to try and fix what was detected
- $1,000/hour incident response consultants to tell you who stole your data

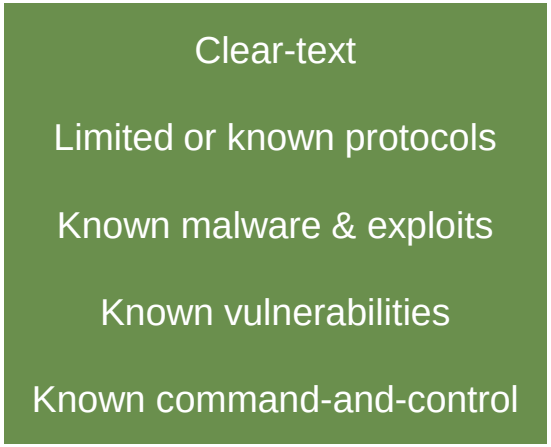
DETECTION FOCUSED

Answer: Detection and Prevention of Advanced Threats

paloalto networks

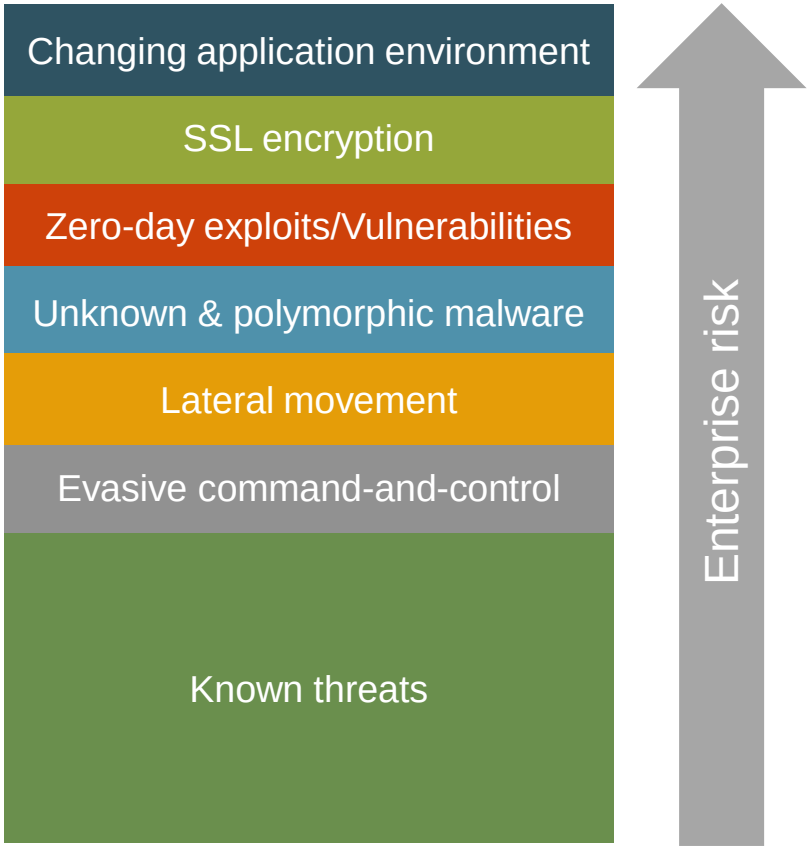
Commoditization of threats

Advanced tools available to all



BEFORE

Sophisticated & multi-threaded

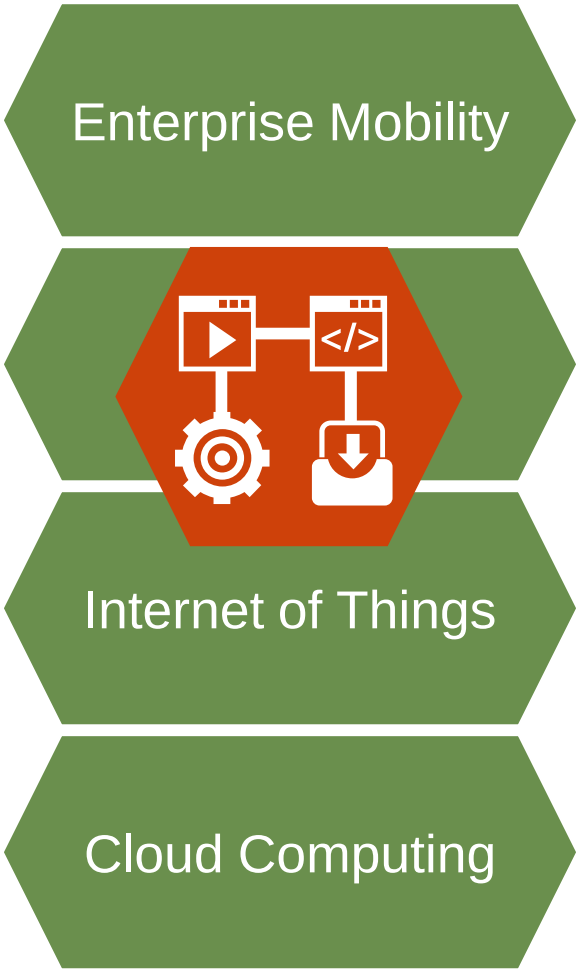


TODAY

paloalto networks

Tectonic shifts in business

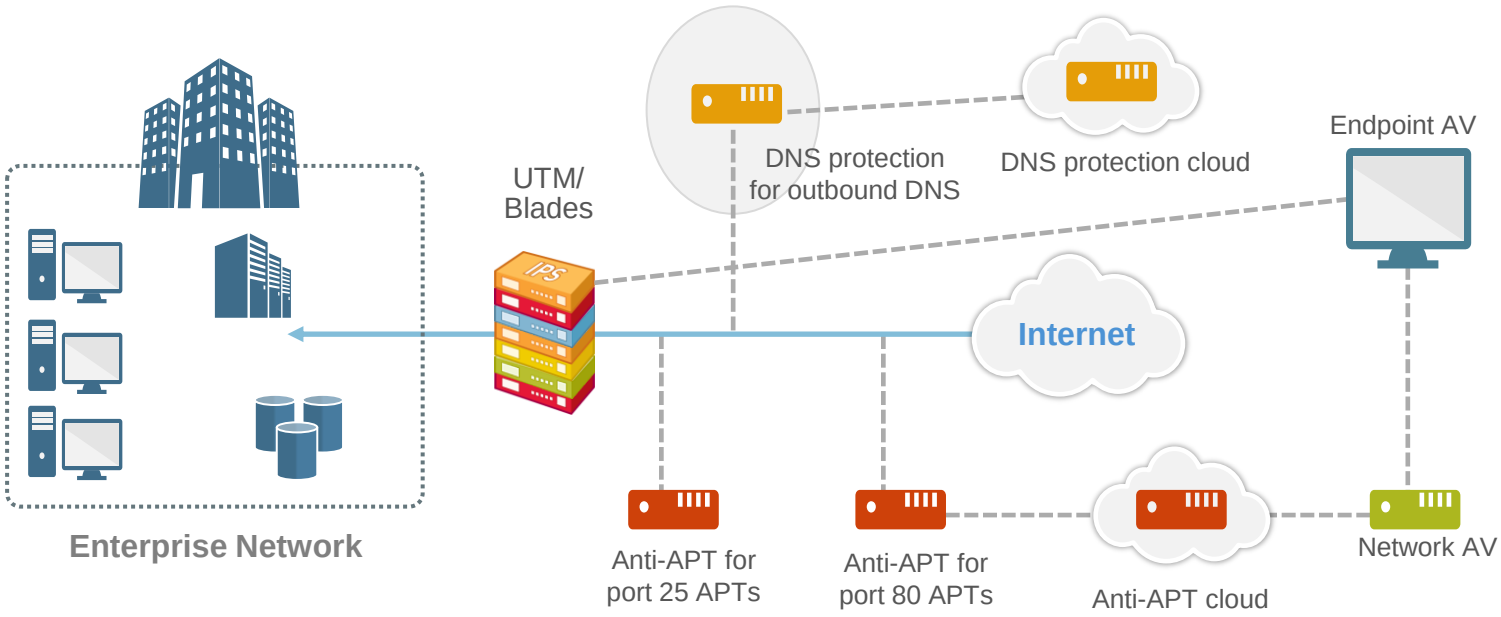
Give rise to a new era of advanced cyber threats



paloalto networks

Current approaches are failing

Detection-focused **Alert Overload** **Manual Response Required**



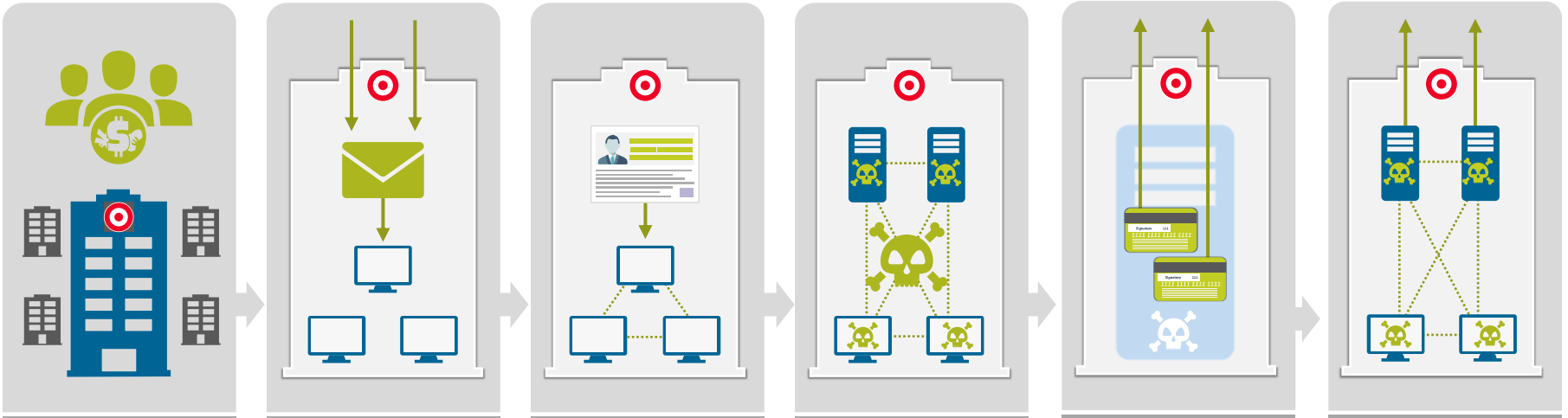
DNS Alert
Endpoint Alert
Web Alert
SMTP Alert
SMTP Alert
SMTP Alert
SMTP Alert
Web Alert
DNS Alert
DNS Alert
SMTP Alert
APT
Web Alert
Web Alert
AV Alert
AV Alert
Web Alert
DNS Alert
SMTP Alert
Endpoint Alert

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

paloalto networks

Target data breach – APTs in action

TARGET



Recon on companies Target works with	Spearphishing third-party HVAC contractor	Breached Target network with stolen payment system credentials	Moved laterally within Target network and installed POS Malware	Compromised internal server to collect customer data	Exfiltrated data command-and-control servers over FTP

Maintain access

paloalto networks.

Changing face of security

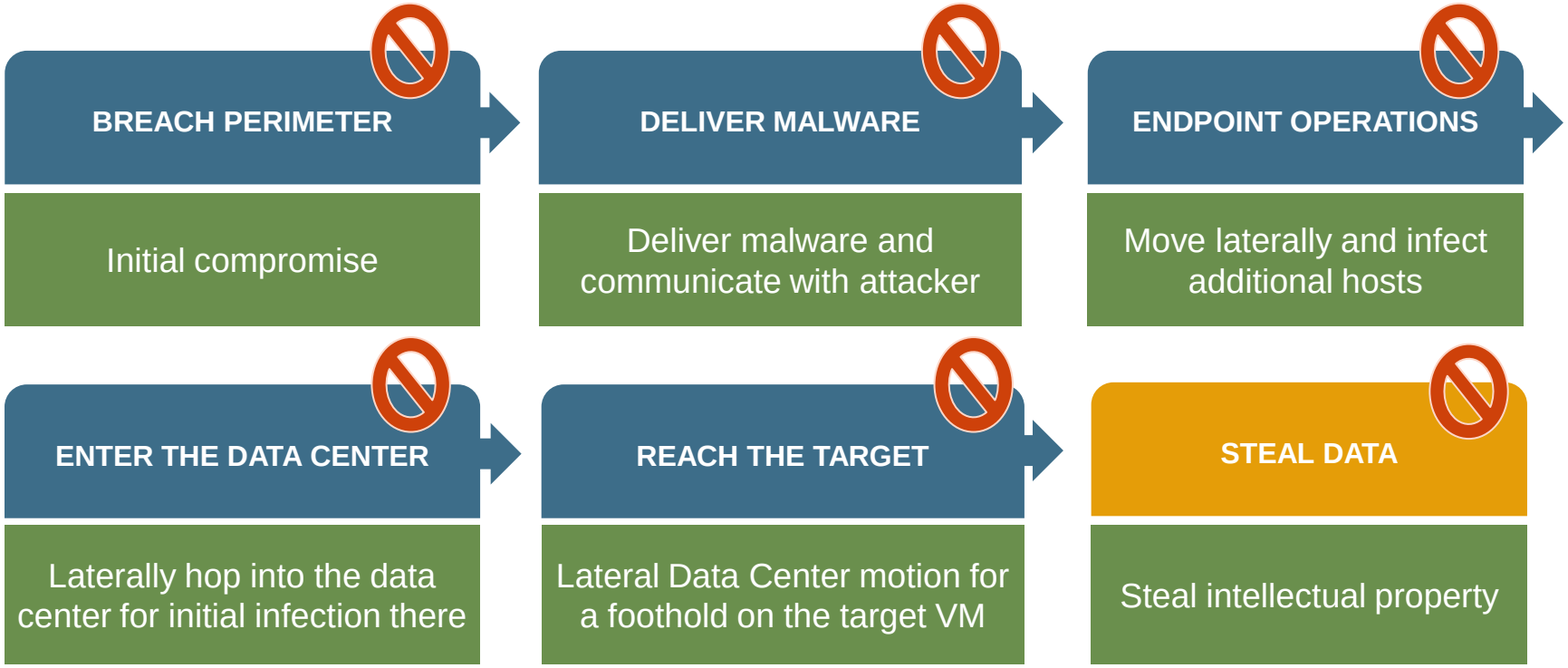
- Has Been
  - Block known bad traffic
  - Pass rest of traffic as good
- New Challenge
  - The Unknown
- Need to investigate unknown traffic and define it as either known good or known bad
  - Then block the newly defined bad
- New World – Top Down Security Architecture
  - Known good
  - Known bad
  - Unknown

Continuous Loop

paloalto networks

Understanding the attack kill-chain

Attack kill-chain



Prevent attacks by stopping one step in the kill-chain

paloalto networks

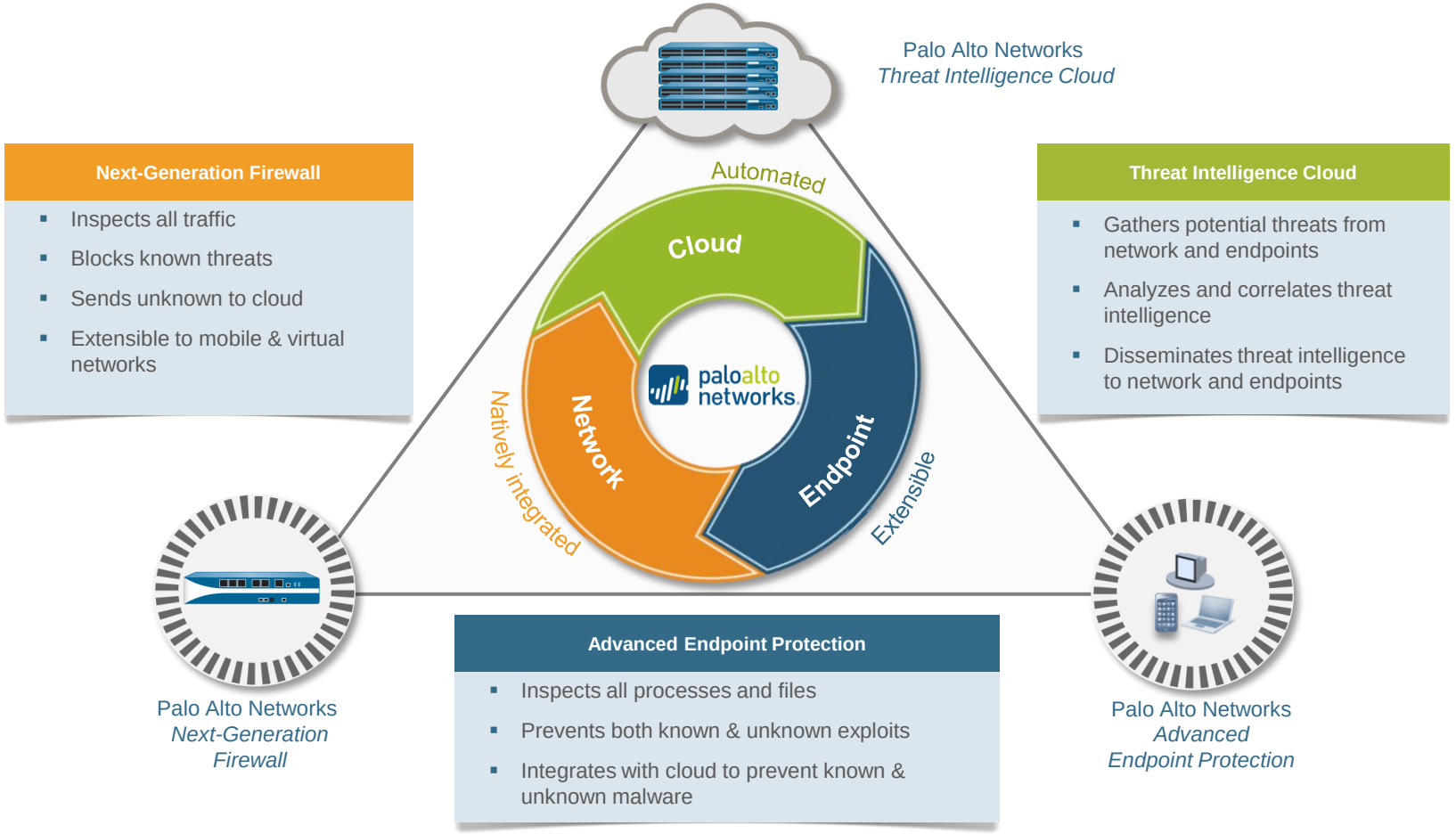
Requirements for a new approach

1. Prevent attacks - even attacks seen for the first time
2. Protect all users and applications - including mobile and virtualized
3. Seamlessly combine network and endpoint security, as each has unique strengths
4. Provide rapid analysis of new threats

Requires next-generation **network**, **endpoint**, and **threat intelligence cloud** capabilities

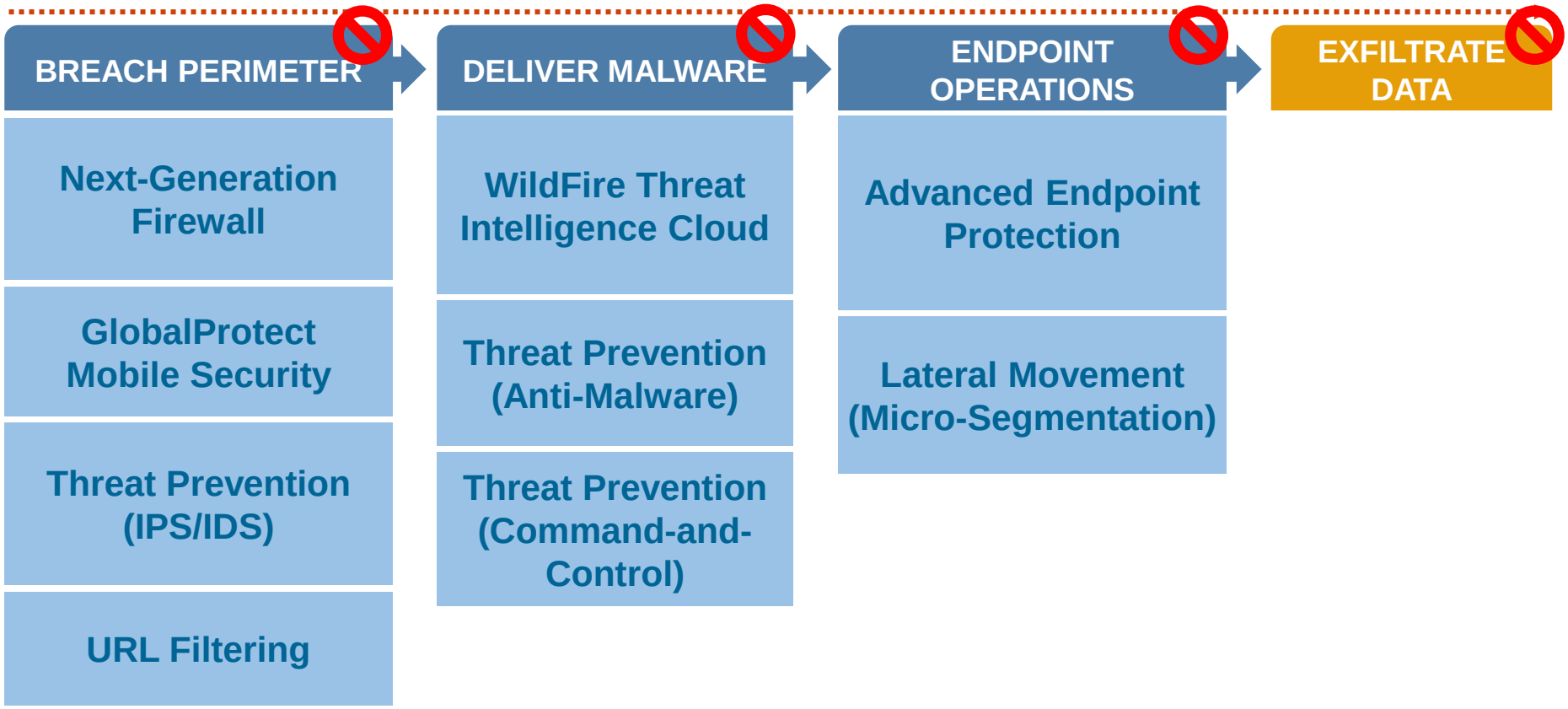
paloalto networks

Next-generation enterprise security platform



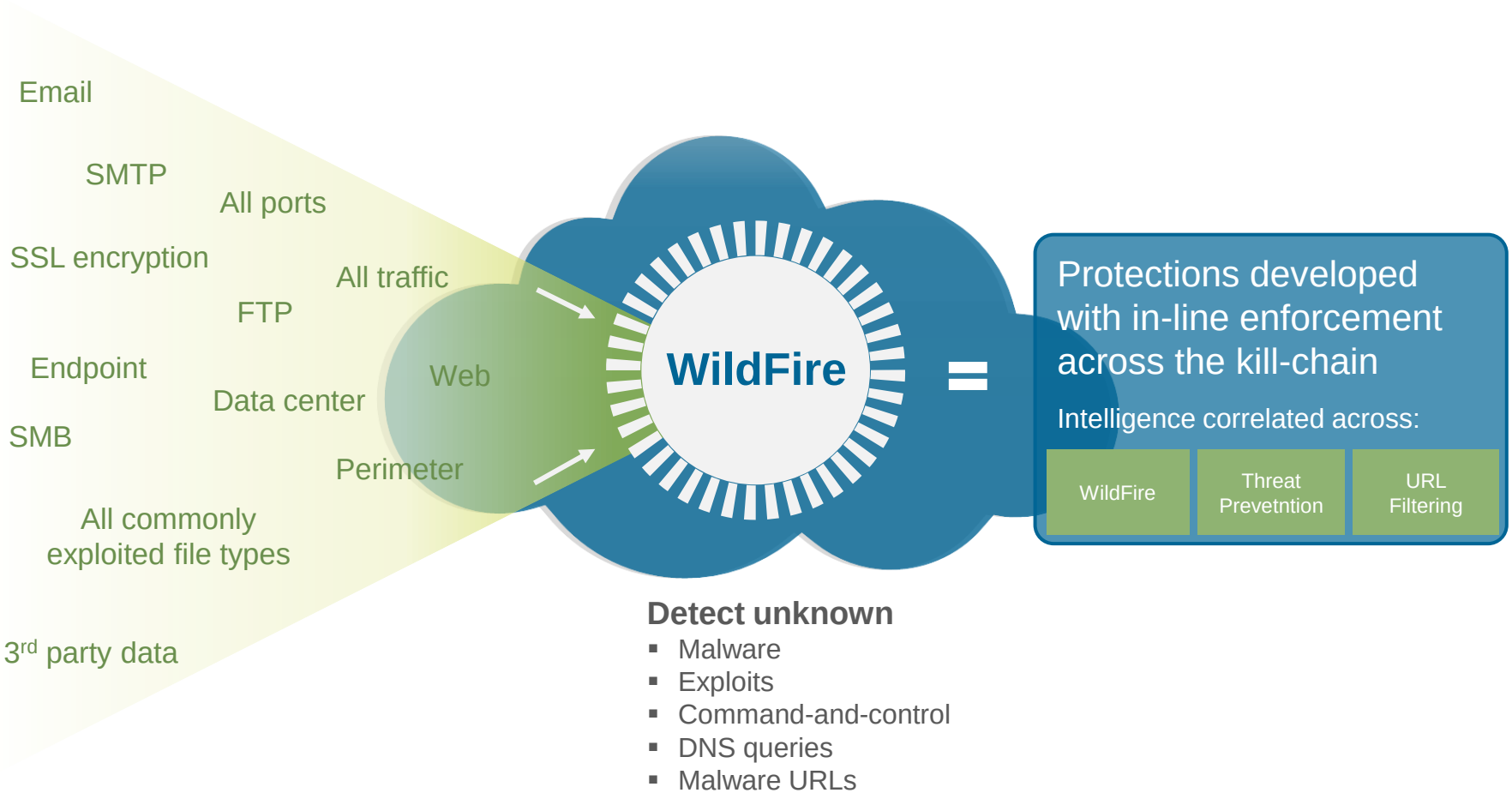
paloalto networks.

Palo Alto Networks and the kill-chain



paloalto networks.

WildFire



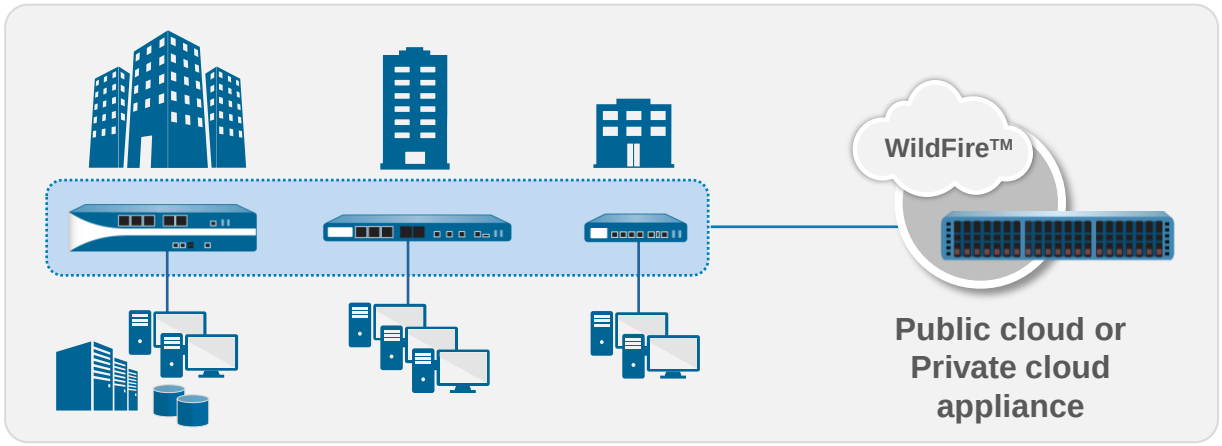
Detect unknown

- Malware
- Exploits
- Command-and-control
- DNS queries
- Malware URLs

paloalto networks.

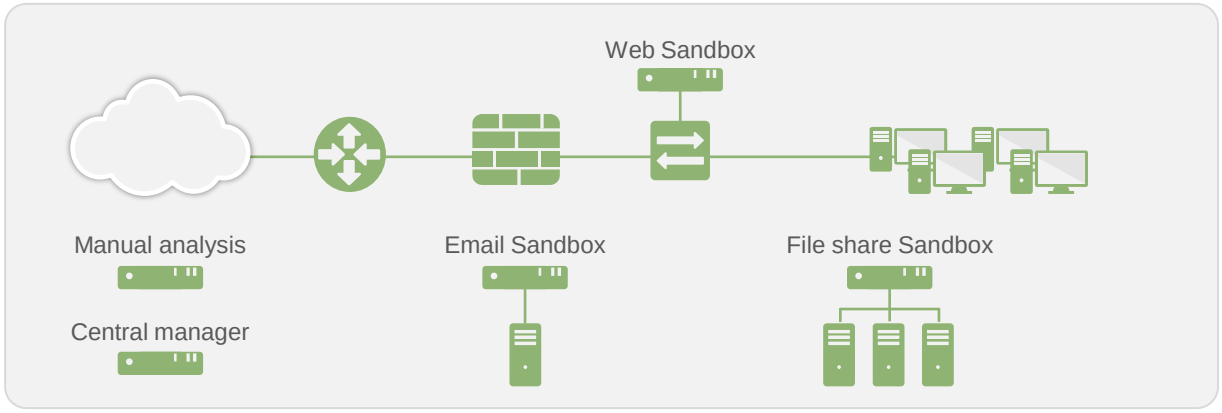
WildFire cloud-based architecture scales

WildFire Approach



- Easy to manage and operationalize
- Scalable
- Cost effective

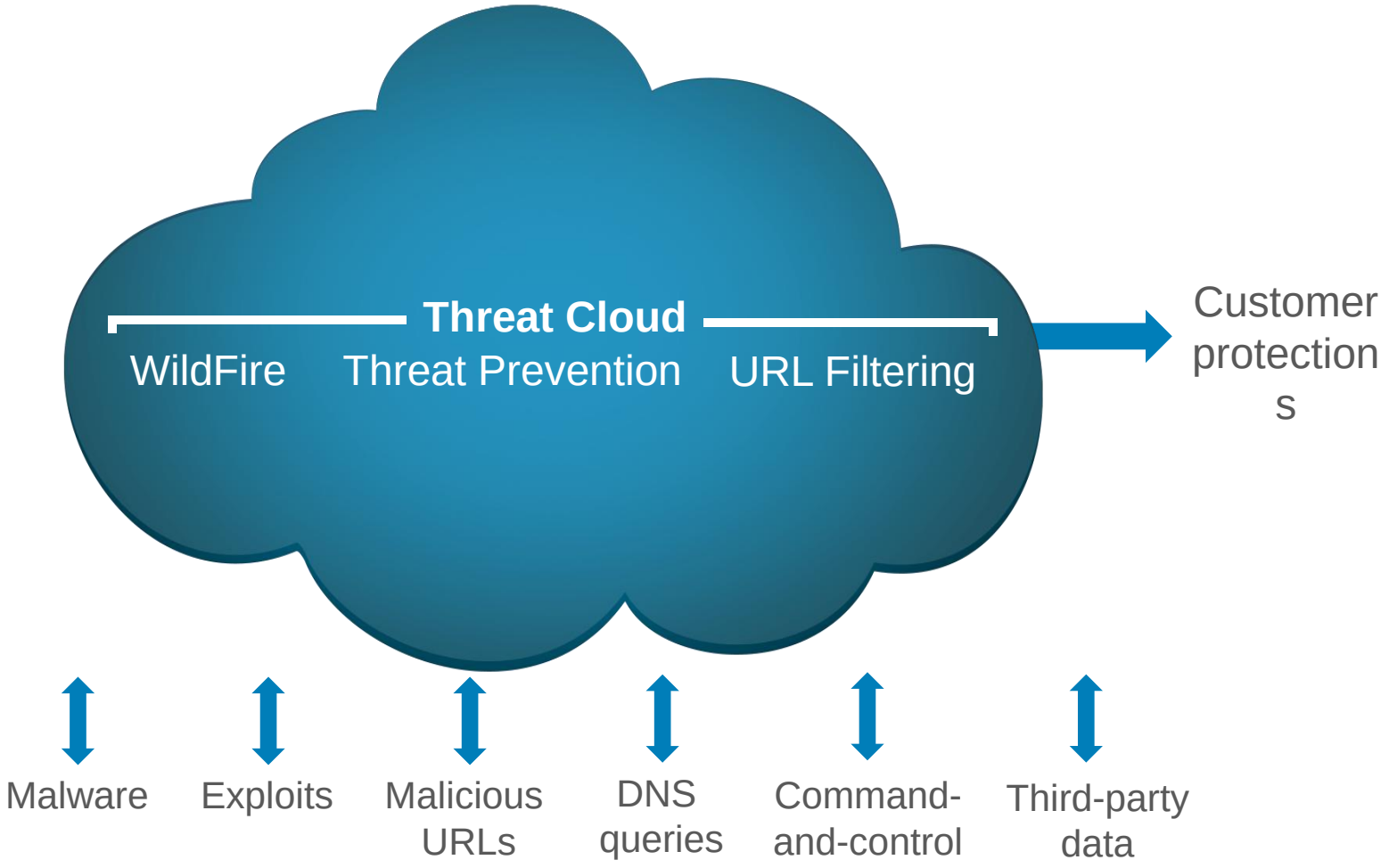
APT Add-on Approach



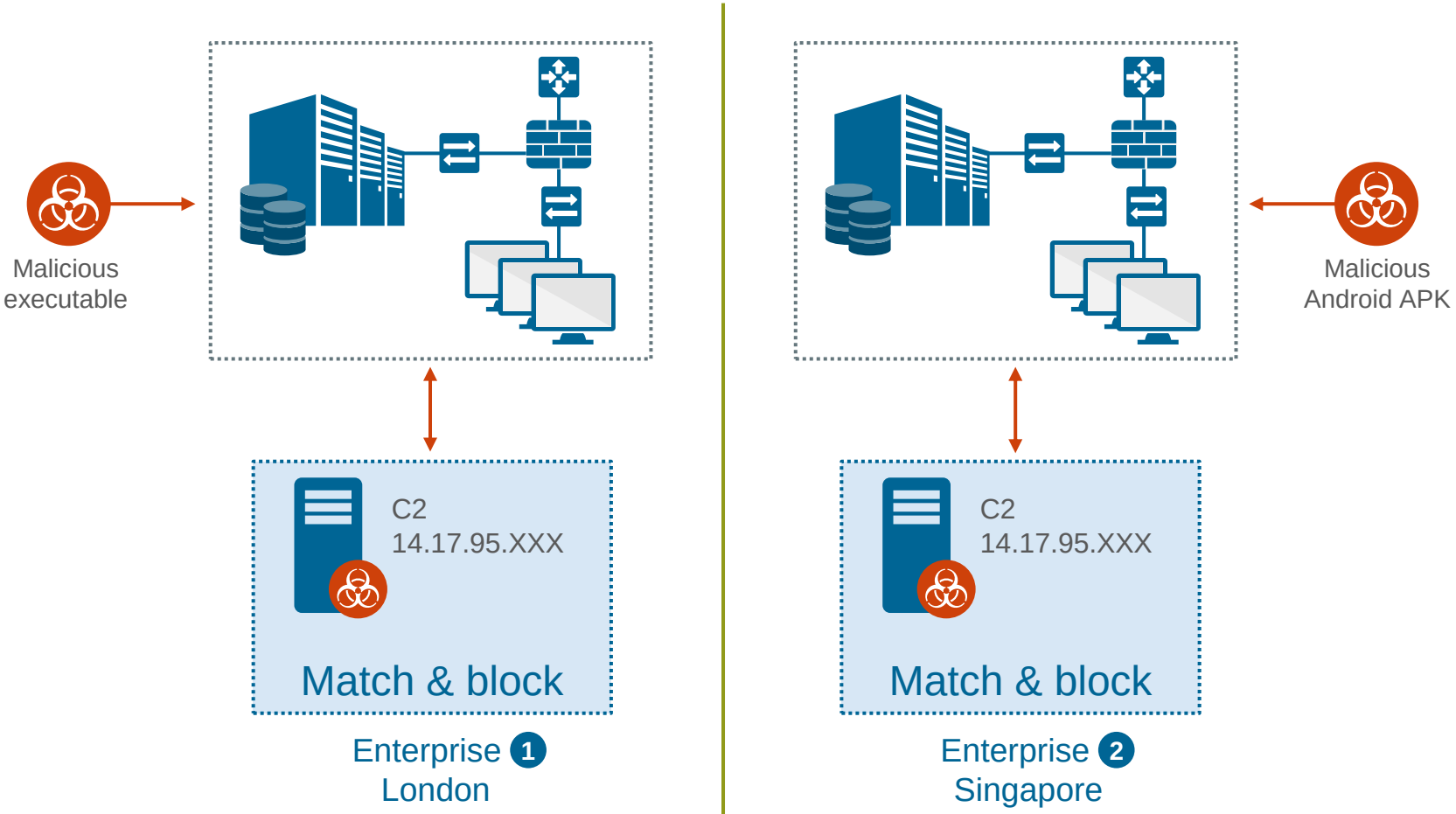
- Hard to manage
- Doesn't scale
- Expensive
- Requires multiple devices at each ingress, egress, and point of segmentation

paloalto networks.

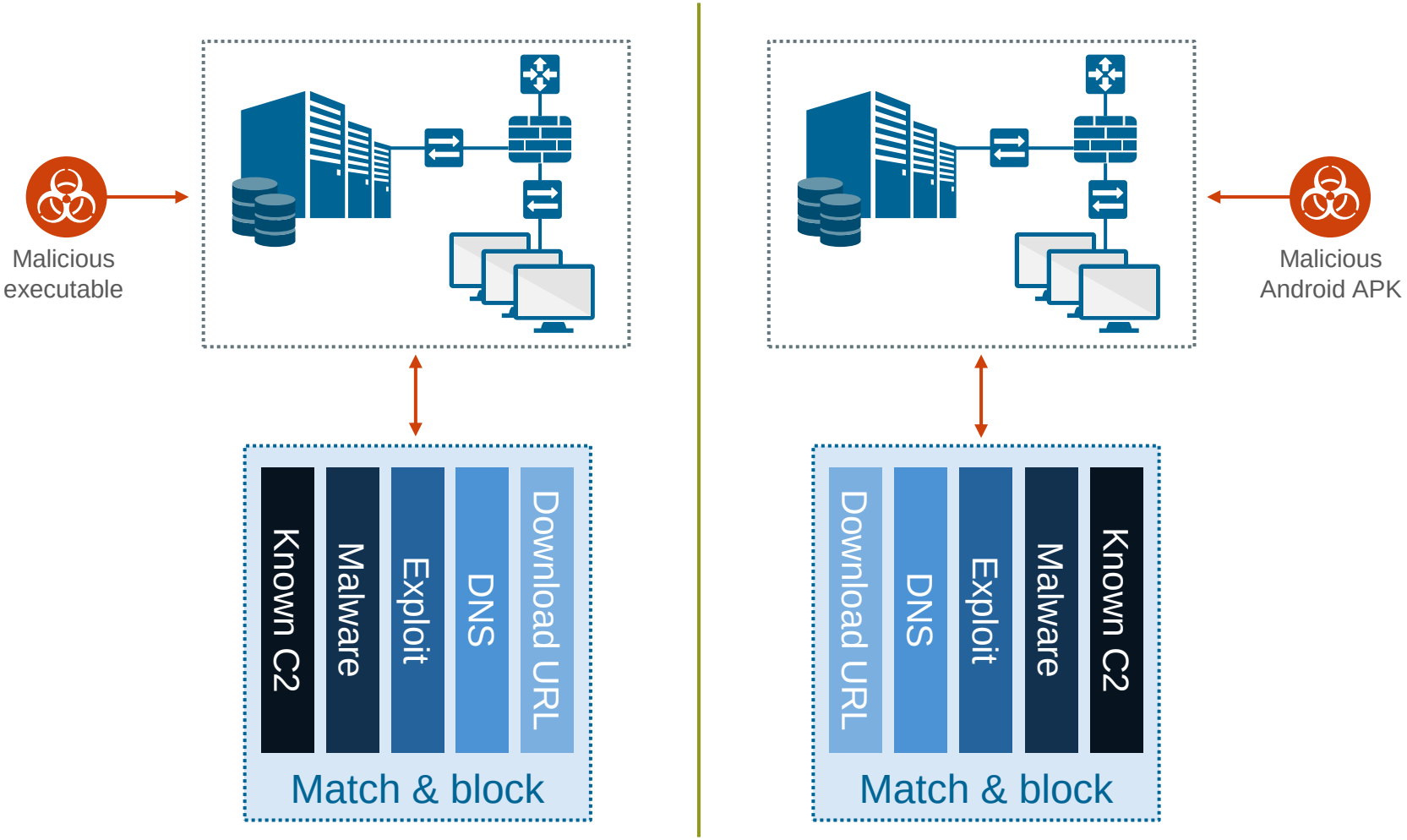
Threat Intelligence Cloud



Threat intelligence cloud correlation

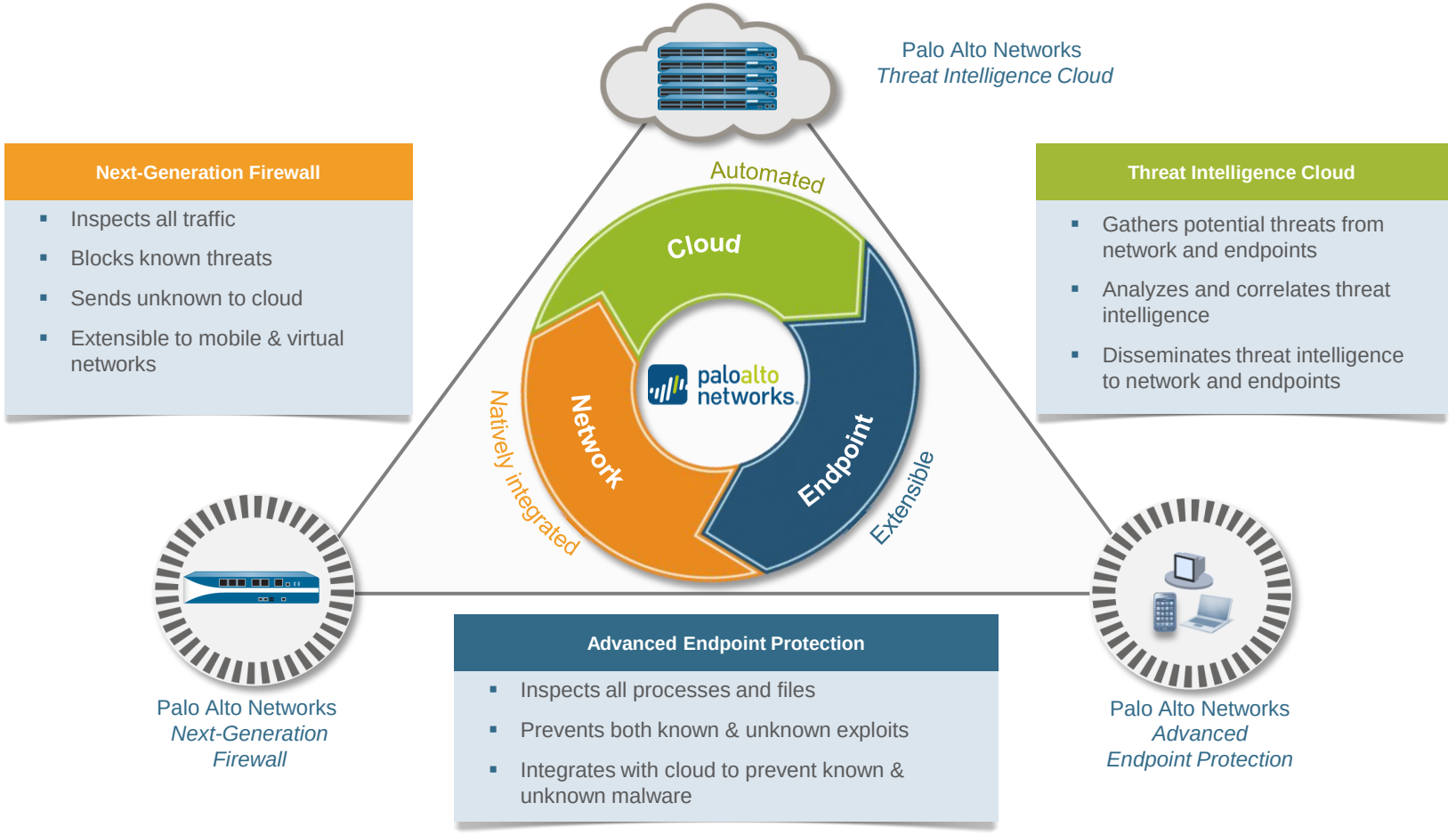


Threat intelligence cloud correlation



paloalto networks.

Next-generation platform



paloalto networks.

paloalto networks®

the enterprise security company™