



MILANO 2015



# PALO ALTO NETWORKS

## what's next ...

to Next Generation FW

# WHAT'S CHANGED?

## THE EVOLUTION OF THE ATTACKER

### CYBERCRIME NOW

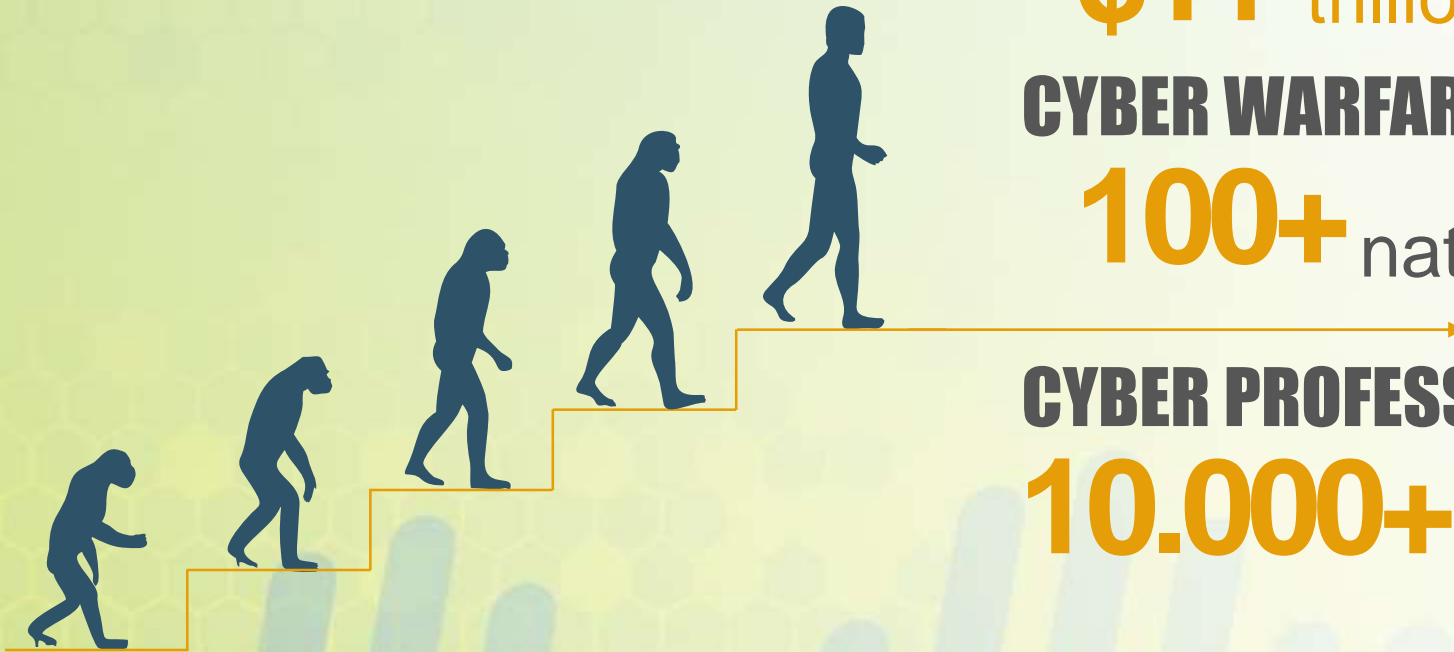
**\$1+** trillion industry

### CYBER WARFARE

**100+** nations

### CYBER PROFESSIONALISM

**10.000+** hours



# THIS IS WHAT CHANGED!

BAD vs GOOD



**\$1.2B SALES in 18 MONTHS**



**MALWARE UPDATES 24/7 SUPPORT**



**LIMITED VISIBILITY & CORRELATION ATTACKS ACCROSS PERIMETER, MOBILE AND CLOUD**

**CIO CONCERNS**



**CYBERCRIME COST: \$445B P/Y**

**\$60B IN GERMANY ALONE  
~1.6% ECONOMY LOSS**

# WHAT'S CHANGED?

## THE EVOLUTION OF BUSINESS

SaaS



SOCIAL +  
CONSUMERIZATION



Massive opportunity  
for cyber criminals



MOBILITY + BYOD



CLOUD +  
VIRTUALIZATION



# President Obama Speaks at the White House Summit on Cybersecurity and Consumer Protection

*"Our connectivity brings extraordinary benefits to our daily lives, but it also brings risks."*

## Four principles for combating cybersecurity

Shortly after taking office, President Obama said that threats to our cybersecurity were a major economic and national security challenge to our nation, and committed to confront these threats. In today's remarks, he laid out four basic principles for doing so:

1. **This has to be a shared mission.** Much of our country's computer networks and infrastructure are in the private sector, but government often has the most up-to-date information on new cyber threats. The only way to fully defend our country from these threats is by government and industry working together.
2. **We have to focus on our unique strengths.** As capable as our government is, it's not always appropriate or even possible for the government to secure private businesses' computer networks. At the same time, in the instance of a cyber attack, private businesses don't always have the necessary capabilities, situational awareness, ability to warn other companies in real time, or capacity to coordinate a response across different companies and sectors.
3. **We have to constantly evolve.** Cyber attacks are growing more sophisticated each and every day, and we have to be just as fast and flexible in improving our defenses.
4. **We must protect the privacy and civil liberty of the American people.** The President noted that we've pursued important reforms to ensure that, while keeping our nation secure, we're also respecting the privacy of Americans. "When government and industry share information about cyber threats, we've got to do so in a way that safeguards your personal information," he said. "When people go online, we shouldn't have to forfeit the basic privacy we're entitled to as Americans."

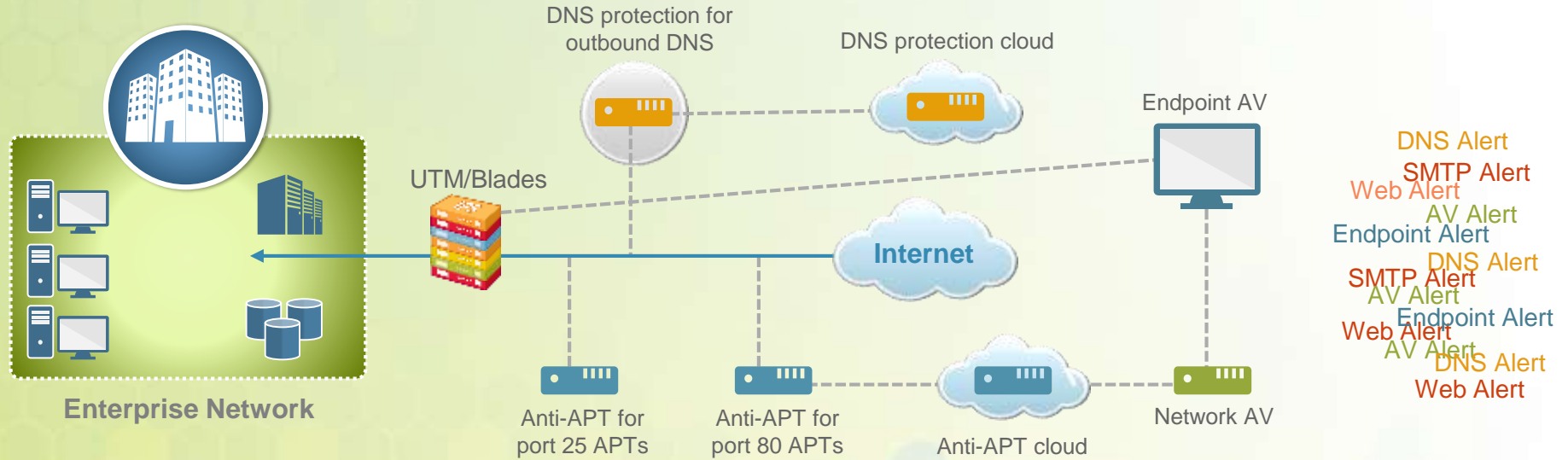








# FAILURE OF LEGACY SECURITY ARCHITECTURES

Limited visibility

Lacks correlation

Manual response



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

# WHY BREACHES STILL HAPPEN

## COMMON TRAITS



Port based  
Firewall



ID credentials  
hijacked

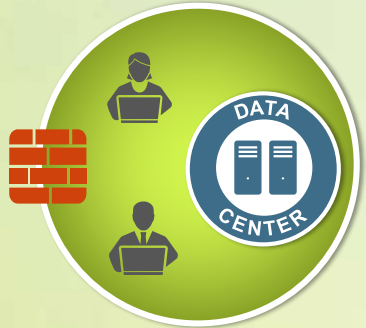
# WHY ONLY TRY TO DETECT MALWARE ONCE?

DETECT AND PREVENT THREATS AT EVERY POINT ACROSS THE ORGANIZATION

– ITS NOT JUST ABOUT THE INTERNET EDGE



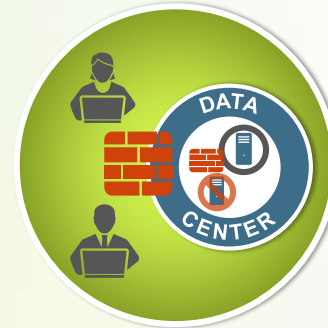
At the mobile device



At the internet edge



Between employees and devices within the LAN



At the data center edge, and between VM's



Within private, public and hybrid clouds

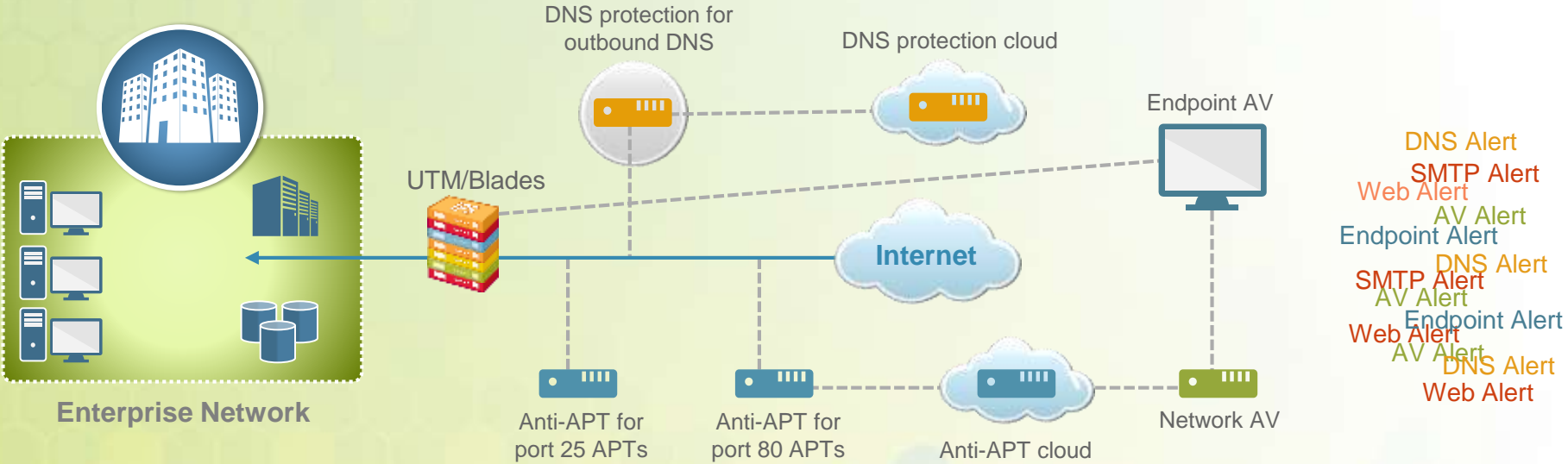


# AND MORE IMPORTANTLY, SIMPLIFY THIS...

Limited visibility

Lacks correlation

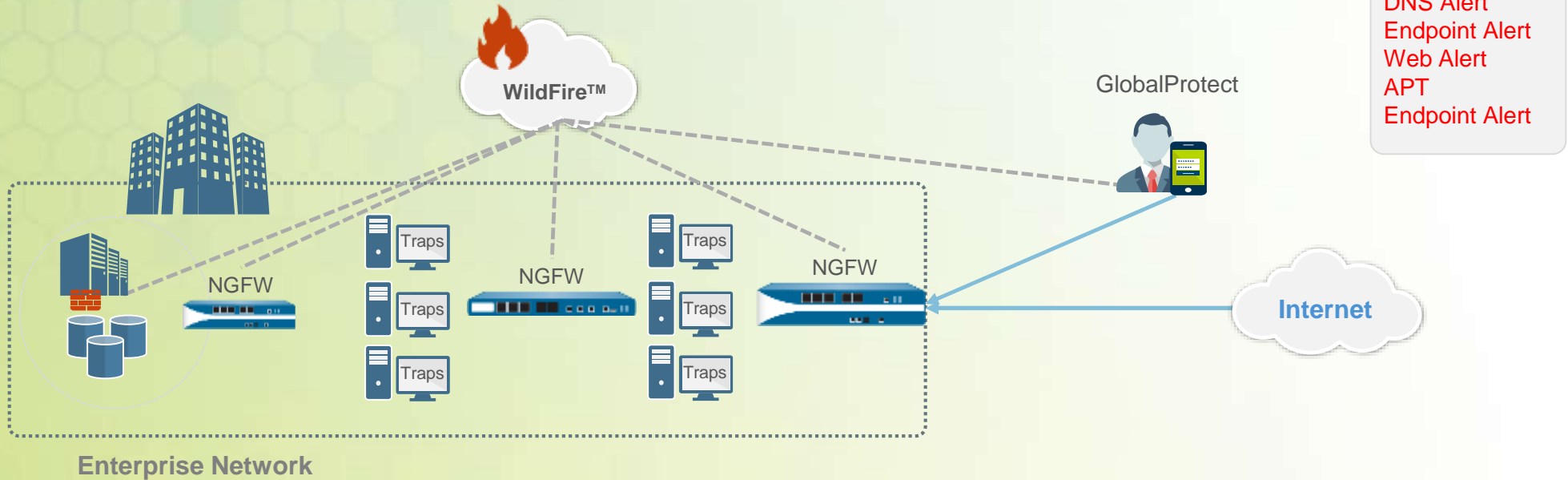
Manual response



- 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

# TO THIS...



- DNS Alert
- Endpoint Alert
- Web Alert
- APT
- Endpoint Alert

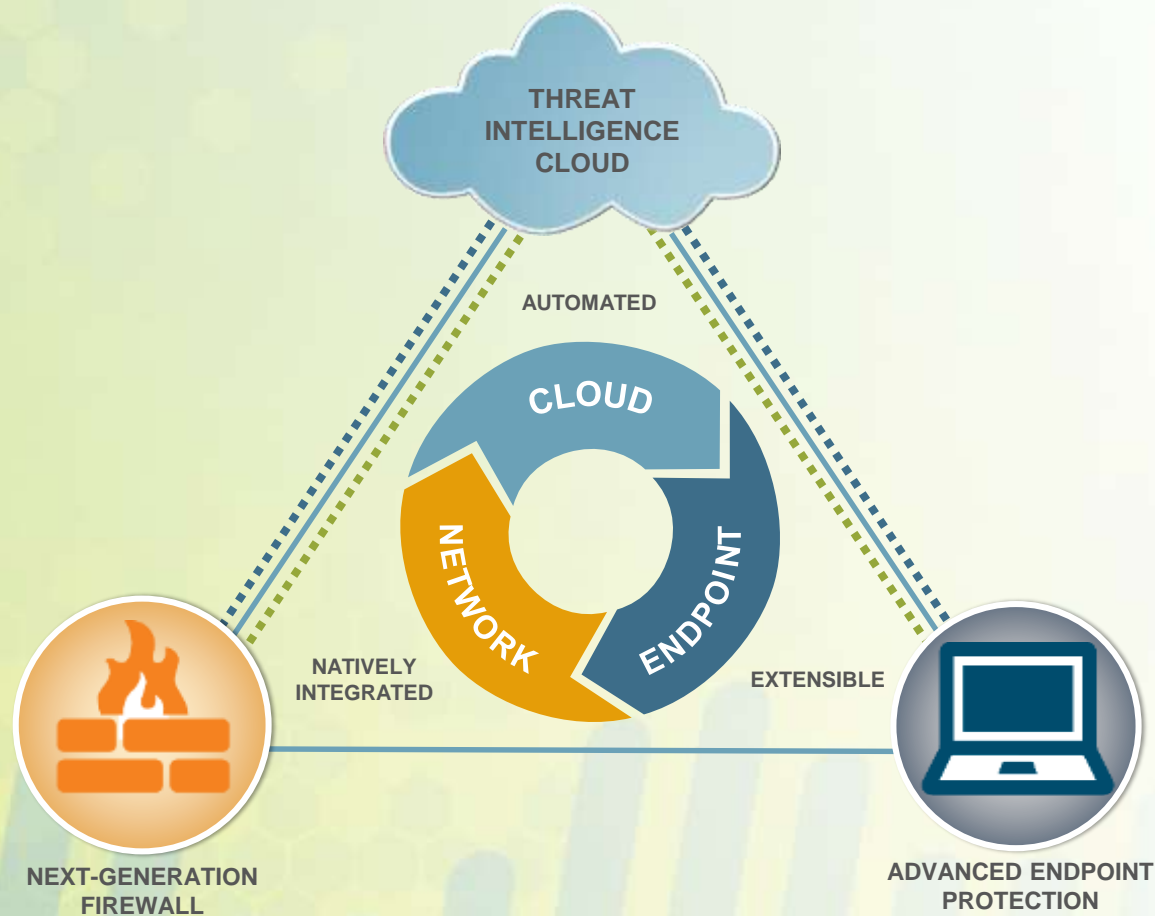
- ① Significantly reduced their risk
- ② Dropped their TCO
- ③ Increased their business agility

Palo Alto Networks  
Malware Prevention

# Requirements for Security in today's Threat Landscape

1. **Application** based security rules
  - Including the ability to **decrypt** flows
2. Rules based on **User Identity**/User Groups
3. **Wildfire** subscription to detect unknown malware
4. **Threat** Prevention subscription to enable dynamic prevention signatures for malware
5. **URL (PAN-DB)** subscription to enable dynamic prevention of malware Command & Control
6. **GlobalProtect** to secure against the threat of time and to help assert Identity

# DELIVERING THE NEXT-GENERATION SECURITY PLATFORM



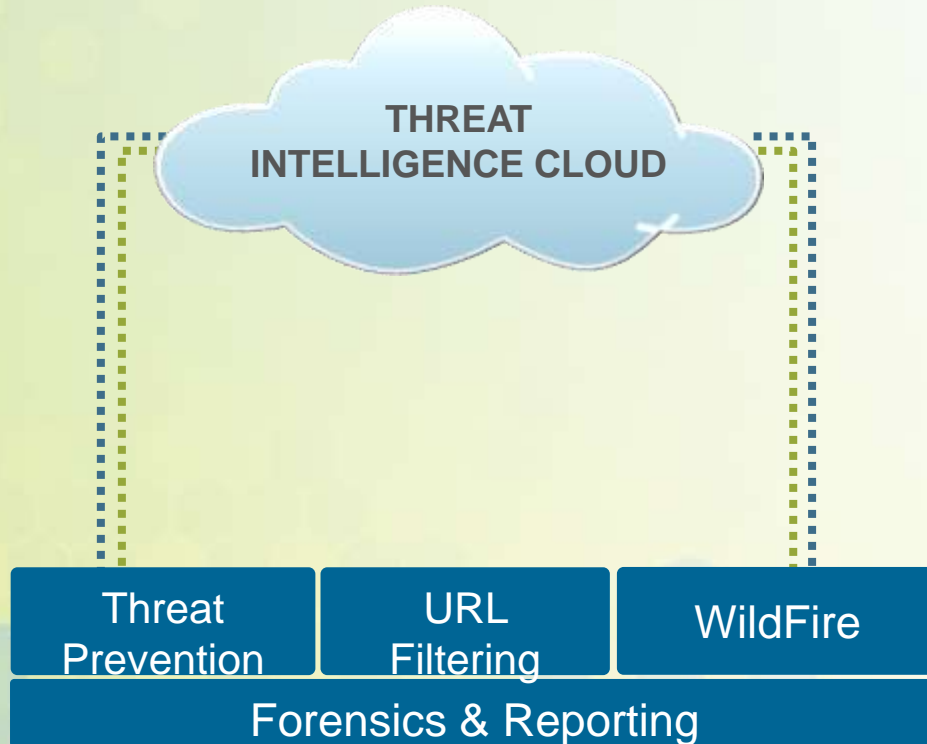


# TRAPS : benefits



# Threat Intelligence Cloud

Automated Prevention & Reporting



**192,000**  
Anti-malware

**24,000**  
URL

**13,500**  
DNS

New protections  
per day

Delivered in **15**  
minutes

# WildFire: Protecting Against The Unknown

## Sandboxing The Unknown

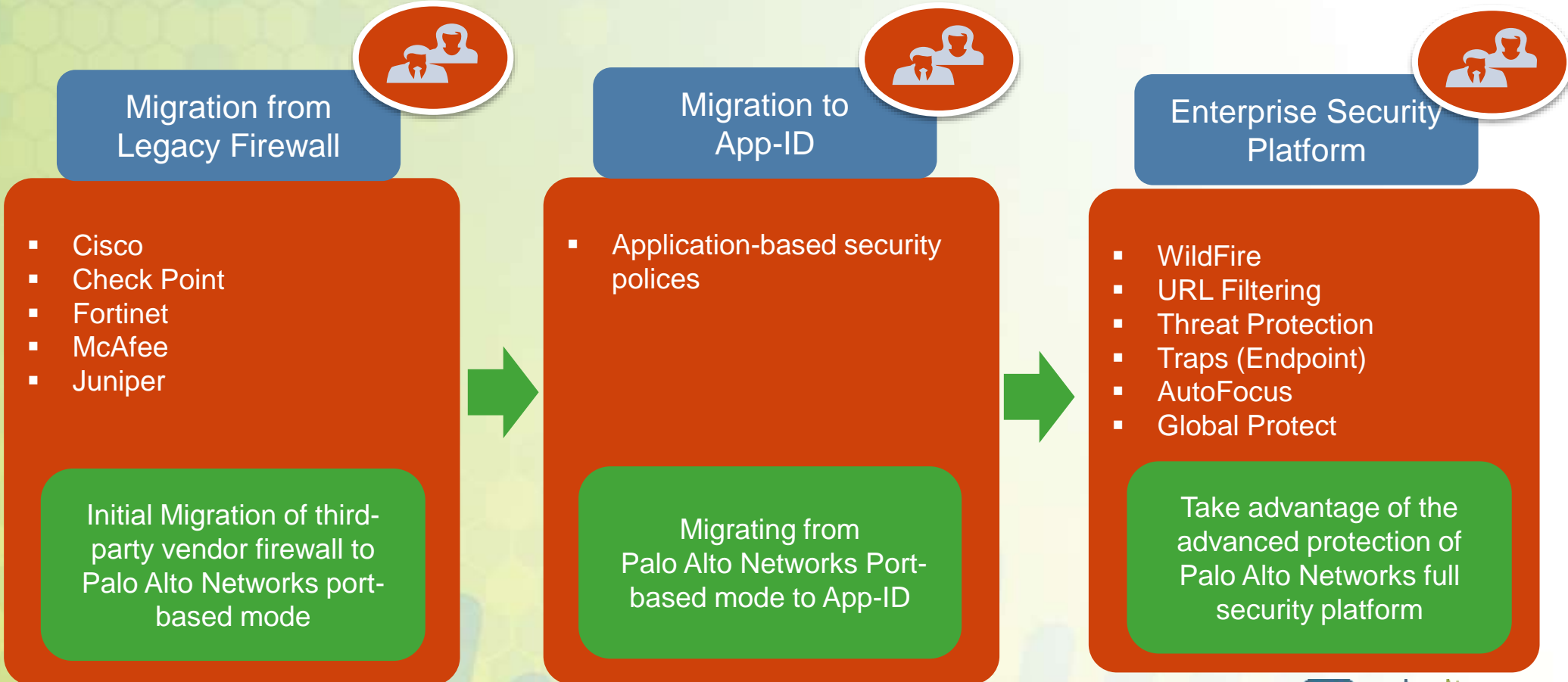


### Detect unknown

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

# There's Never Been A Better Time to Migrate to Palo Alto Networks

## Minimize Risk by Migrating in Phases





# WHY PALO ALTO NETWORKS

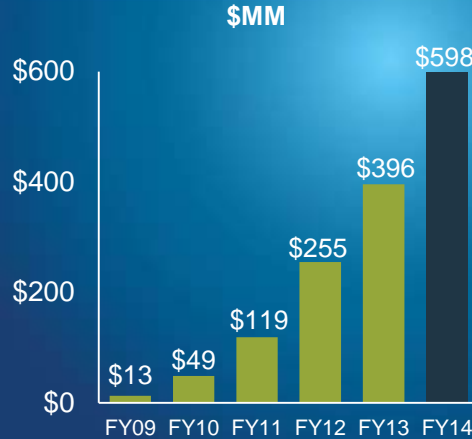


# PALO ALTO NETWORKS AT-A-GLANCE

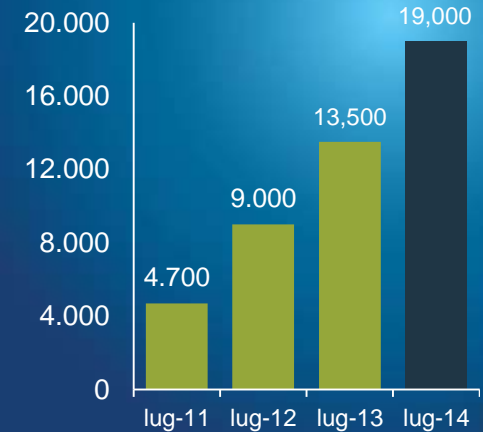
## CORPORATE HIGHLIGHTS

- Founded in 2005; first customer shipment in 2007
- Safely enabling applications and preventing cyber threats
- Able to address all enterprise cybersecurity needs
- Exceptional ability to support global customers
- Experienced team of 2,000+ employees
- Q3FY15 : \$234M (55% YoY)

## REVENUES

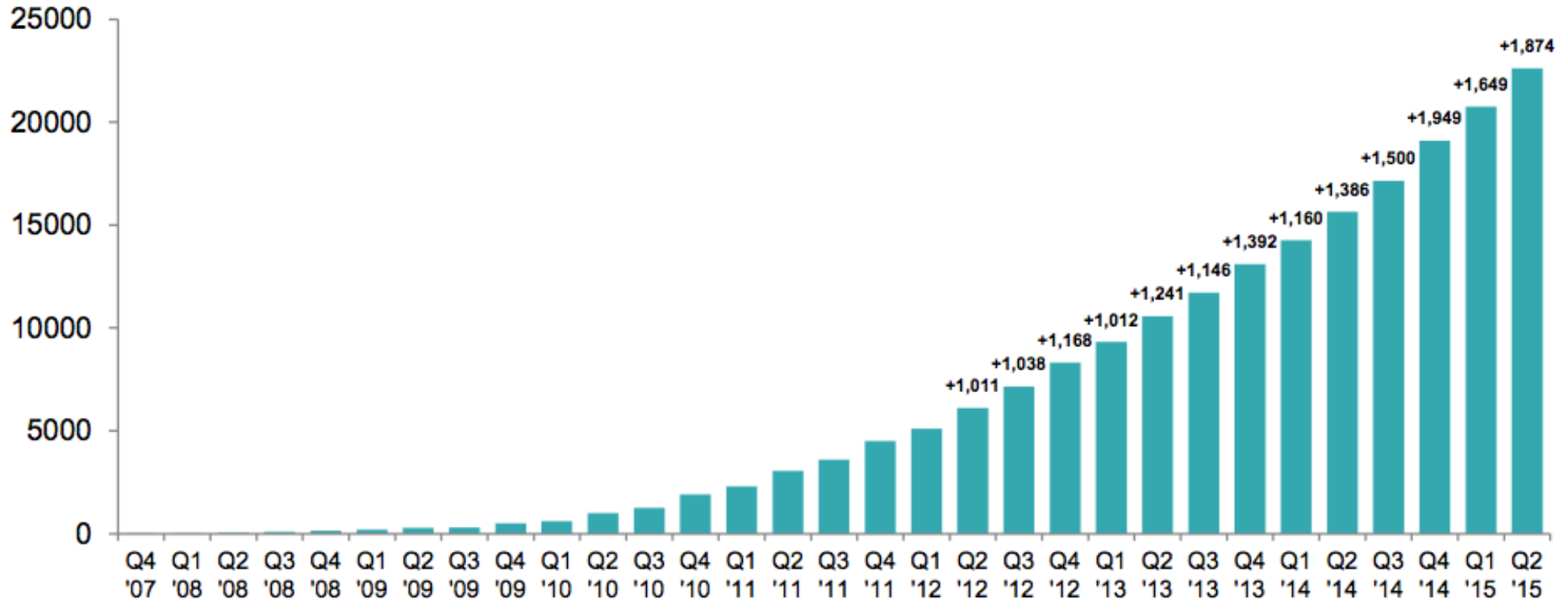


## ENTERPRISE CUSTOMERS



# Customer growth

## Customer Growth by Quarter



Source: Palo Alto Networks.

# Recent Highlights

- **Acquired CirroSecure** - This acquisition expands the functionality of our enterprise security platform by providing additional security for SaaS applications and is expected to be available as a new subscription-based service in the second half of 2015.
- **Introduced new AutoFocus threat intelligence offering** - At Ignite, our annual user conference, we introduced our newest subscription service AutoFocus, which provides prioritized, actionable intelligence to help customers take quick, preventive action against targeted cyber threats. More than 750 customers have already submitted requests to enroll in the AutoFocus community access program.
- **Positioned in the "Leaders" quadrant of Gartner, Inc.'s April 2015 Magic Quadrant for Enterprise Network Firewalls** - This is the fourth consecutive year in which Palo Alto Networks has been recognized as a leader in the Magic Quadrant for Enterprise Network Firewalls report.<sup>[1]</sup>
- **Received Superior Security Score in head-to-head product test** - In the NSS Labs 2015 Next-Generation Intrusion Prevention System (NGIPS) test, our platform achieved the highest security efficacy ratings of any other offering tested when exposed to live (real-time) drive-by exploits.

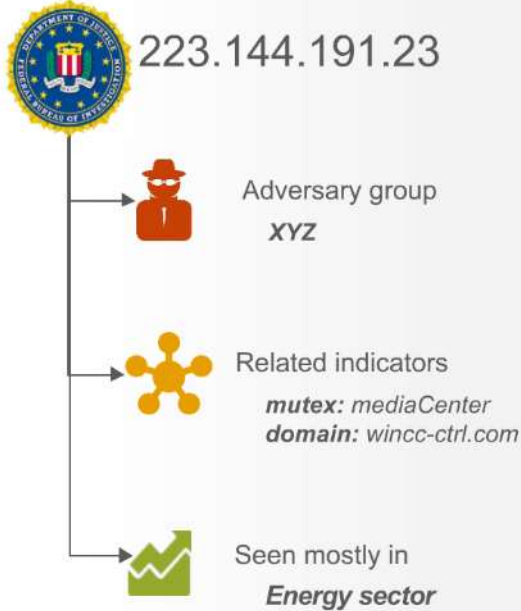


# Autofocus : cyber threat intelligence

Prioritize important events



Provide context around indicators and incidents



Enable quick and proactive response



Policy action on security devices:

- Infected users
- Malicious IP/URLs
- Malicious DNS queries
- Known-bad process activity

# 2015 Magic Quadrant for Network Enterprise Firewalls

*“Palo Alto Networks is assessed as a Leader, mostly because of its NGFW focus, and because of its consistent visibility in Gartner shortlists for advanced firewalls use cases, frequently beating competition on feature quality.”*

**—Gartner, Magic Quadrant for Enterprise Network Firewalls**





paloalto  
networks®

the enterprise **security** company™