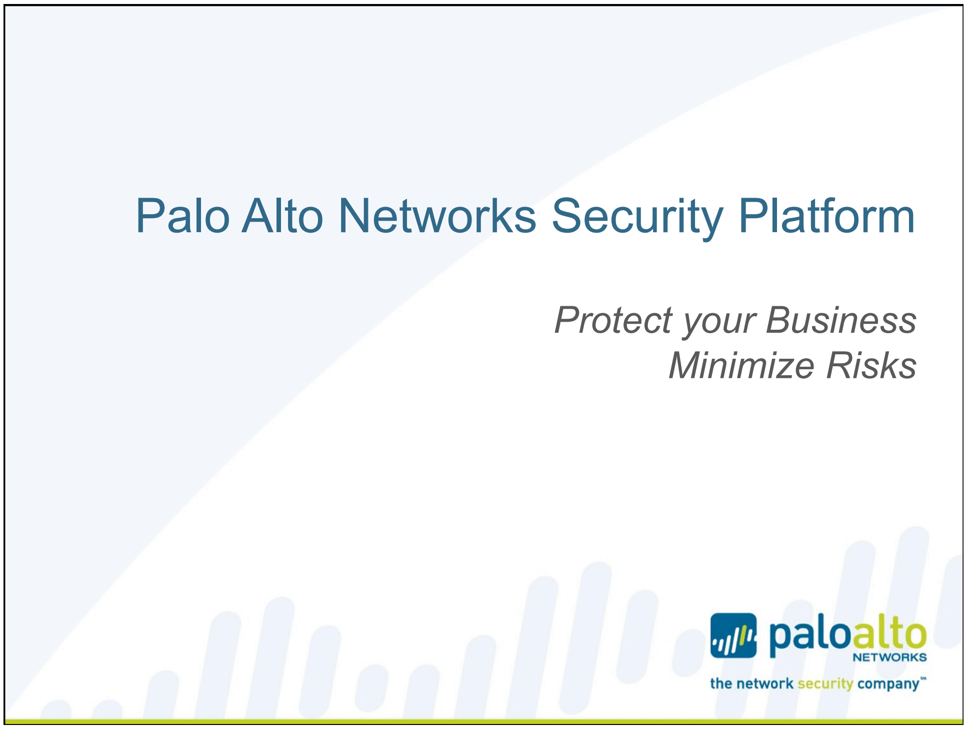
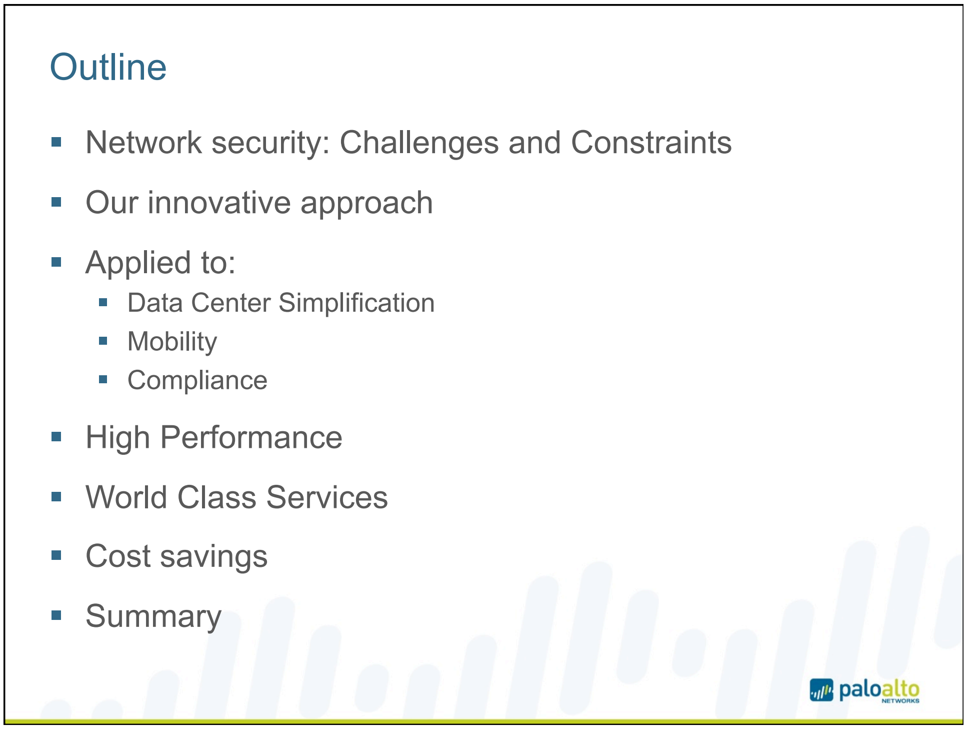


Palo Alto Networks Security Platform

Protect your Business
Minimize Risks

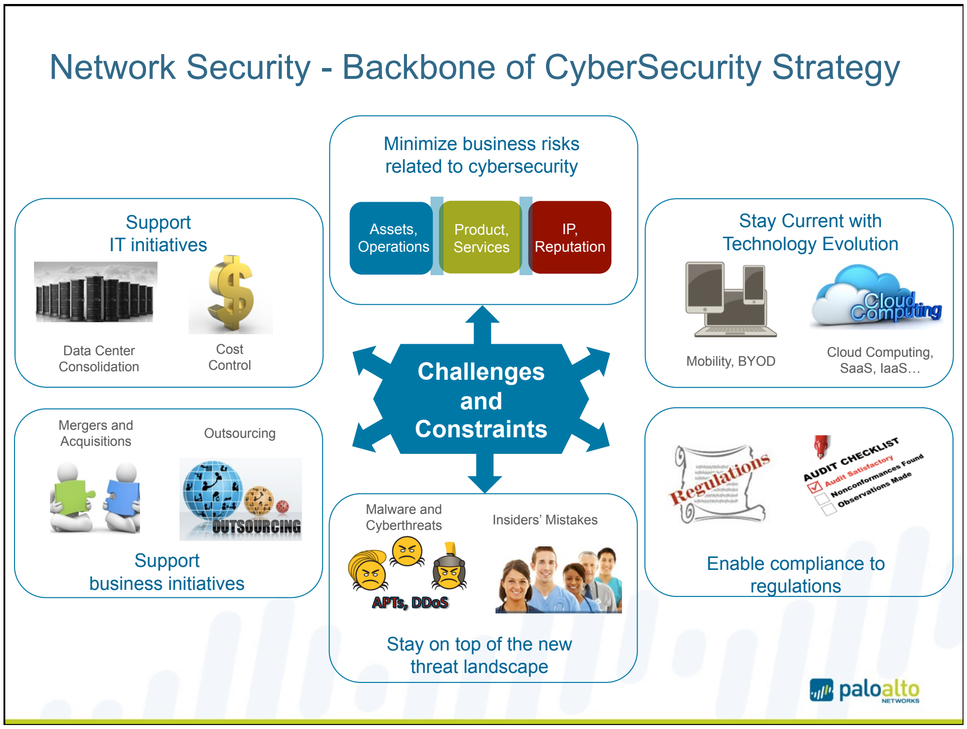
paloalto NETWORKS
the network security company™



Outline

- Network security: Challenges and Constraints
- Our innovative approach
- Applied to:
  - Data Center Simplification
  - Mobility
  - Compliance
- High Performance
- World Class Services
- Cost savings
- Summary

paloalto NETWORKS



Network Security - Backbone of CyberSecurity Strategy

Challenges and Constraints

Minimize business risks related to cybersecurity

Assets, Operations

Product, Services

IP, Reputation

Support IT initiatives

Data Center Consolidation

Cost Control

Stay Current with Technology Evolution

Mobility, BYOD

Cloud Computing, SaaS, IaaS…

Mergers and Acquisitions

Outsourcing

Support business initiatives

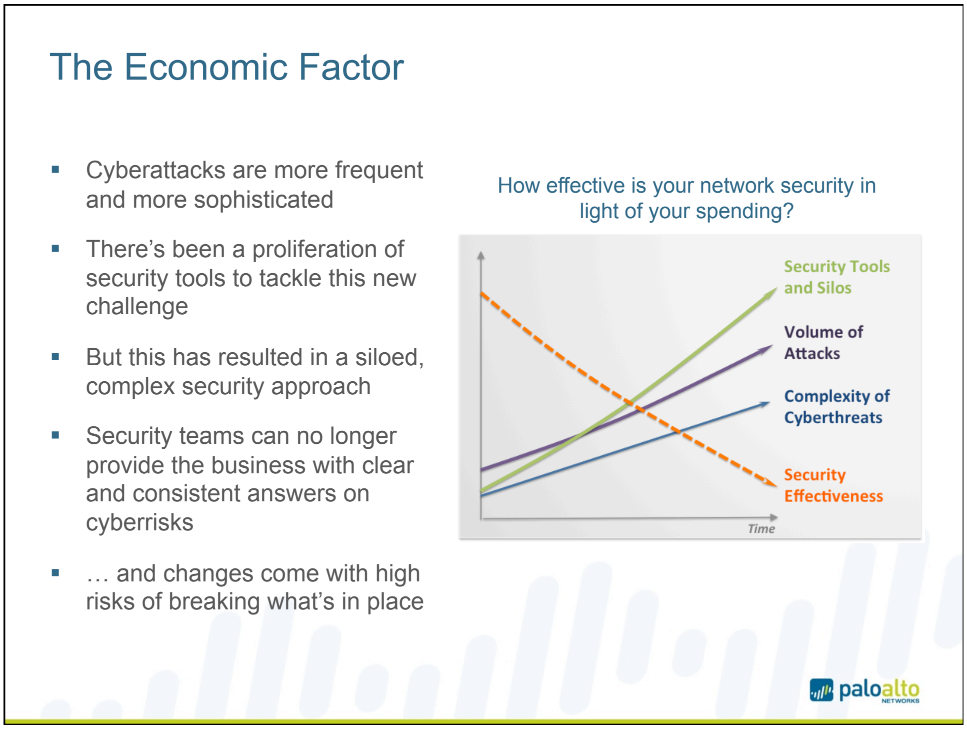
Malware and Cyberthreats

APTs, DDoS

Insiders' Mistakes

Stay on top of the new threat landscape

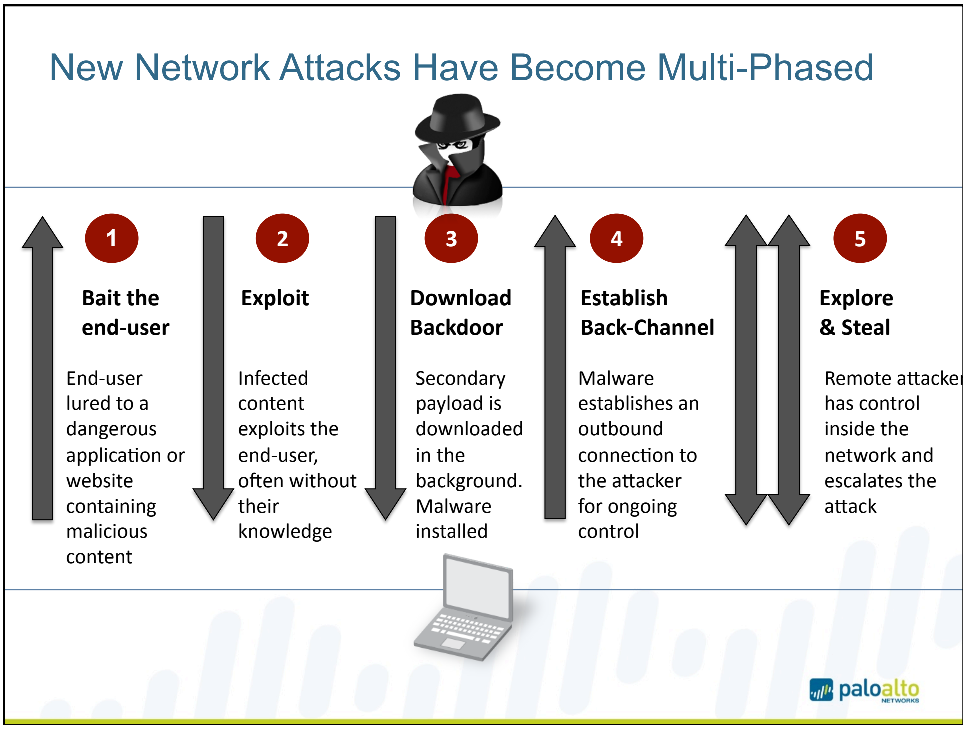
Enable compliance to regulations



The Economic Factor

- Cyberattacks are more frequent and more sophisticated
- There's been a proliferation of security tools to tackle this new challenge
- But this has resulted in a siloed, complex security approach
- Security teams can no longer provide the business with clear and consistent answers on cyberrisks
- … and changes come with high risks of breaking what's in place

How effective is your network security in light of your spending?



New Network Attacks Have Become Multi-Phased

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

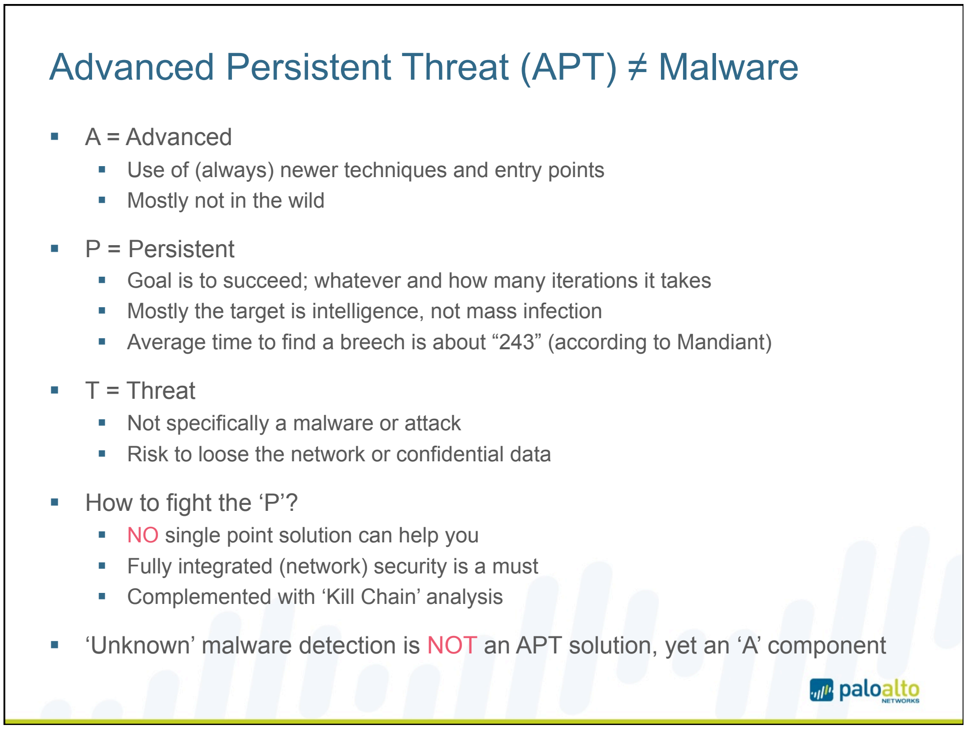
4 **Establish Back-Channel**

Malware establishes an outbound connection to the attacker for ongoing control

5 **Explore & Steal**

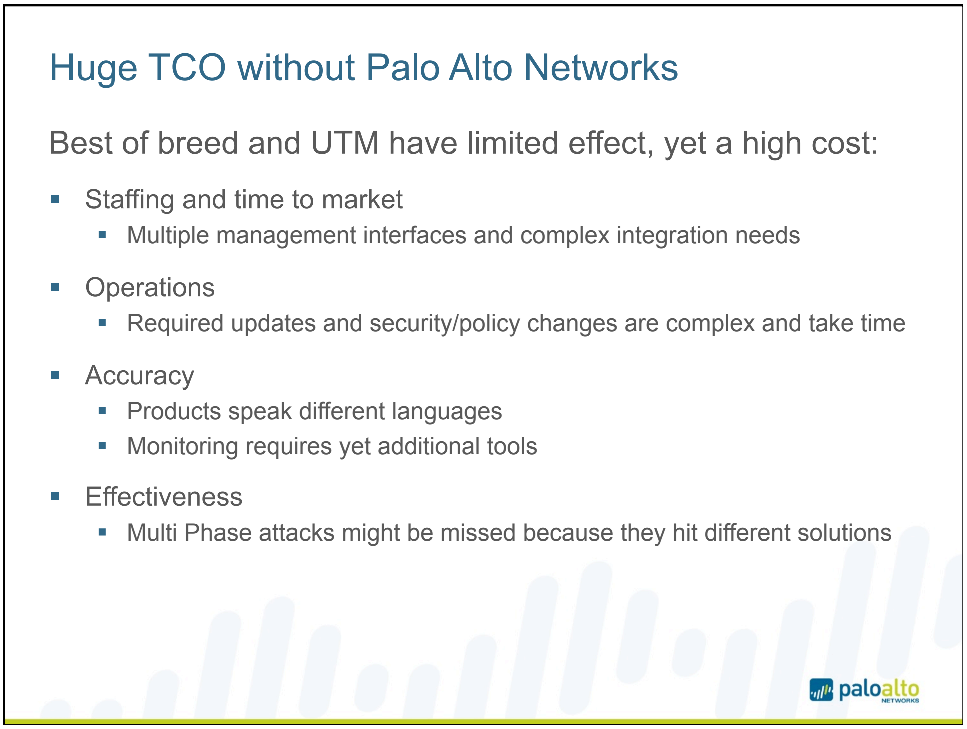
Remote attacker has control inside the network and escalates the attack

paloalto NETWORKS



Advanced Persistent Threat (APT) ≠ Malware

- A = Advanced
  - Use of (always) newer techniques and entry points
  - Mostly not in the wild
- P = Persistent
  - Goal is to succeed; whatever and how many iterations it takes
  - Mostly the target is intelligence, not mass infection
  - Average time to find a breech is about “243” (according to Mandiant)
- T = Threat
  - Not specifically a malware or attack
  - Risk to loose the network or confidential data
- How to fight the ‘P’?
  - NO single point solution can help you
  - Fully integrated (network) security is a must
  - Complemented with ‘Kill Chain’ analysis
- ‘Unknown’ malware detection is NOT an APT solution, yet an ‘A’ component



Huge TCO without Palo Alto Networks

Best of breed and UTM have limited effect, yet a high cost:

- Staffing and time to market
  - Multiple management interfaces and complex integration needs
- Operations
  - Required updates and security/policy changes are complex and take time
- Accuracy
  - Products speak different languages
  - Monitoring requires yet additional tools
- Effectiveness
  - Multi Phase attacks might be missed because they hit different solutions

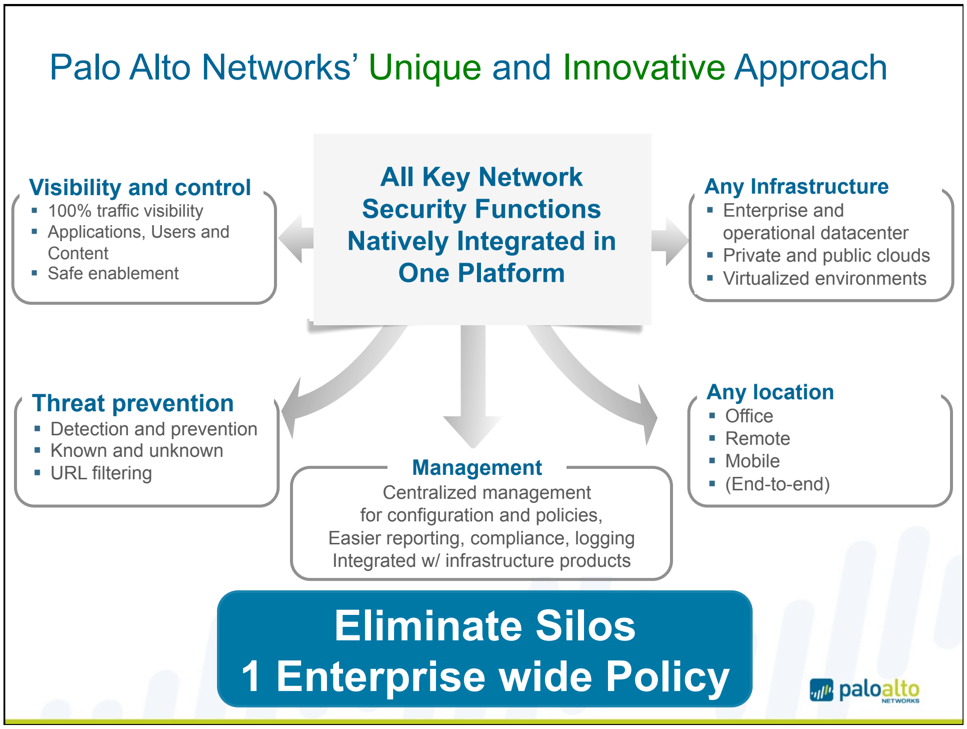
paloalto NETWORKS

Palo Alto Networks Innovative Approach

paloalto NETWORKS

the network security company™

8 | ©2013, Palo Alto Networks. Confidential and Proprietary.



Palo Alto Networks' Unique and Innovative Approach

All Key Network Security Functions Natively Integrated in One Platform

Visibility and control
- 100% traffic visibility
- Applications, Users and Content
- Safe enablement

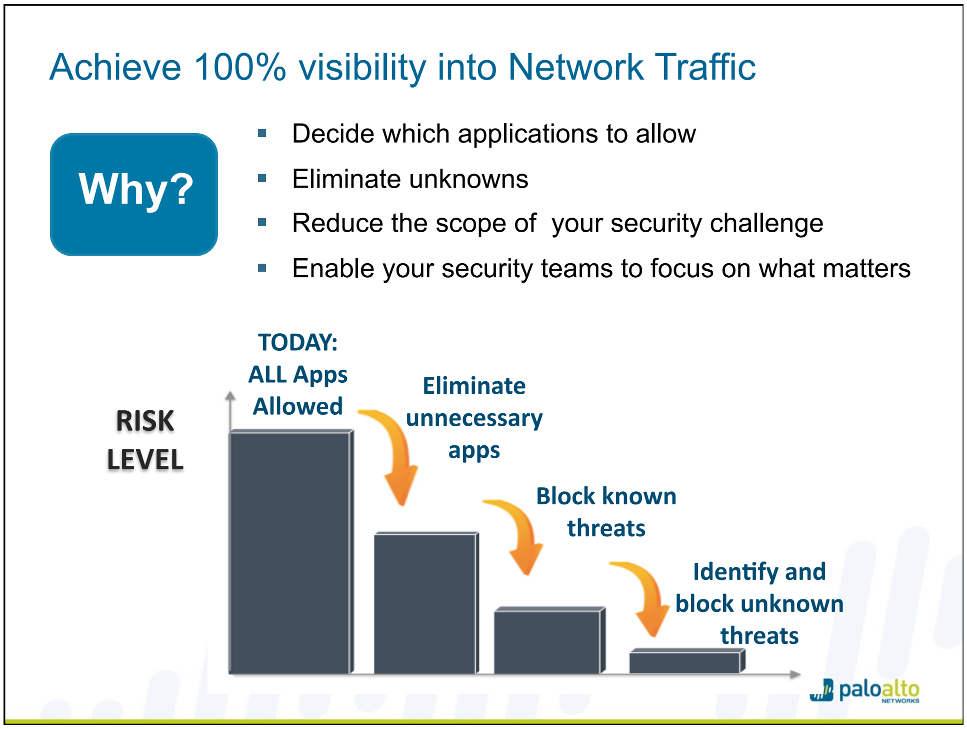
Any Infrastructure
- Enterprise and operational datacenter
- Private and public clouds
- Virtualized environments

Threat prevention
- Detection and prevention
- Known and unknown
- URL filtering

Any location
- Office
- Remote
- Mobile
- (End-to-end)

Management
Centralized management
for configuration and policies,
Easier reporting, compliance, logging
Integrated w/ infrastructure products

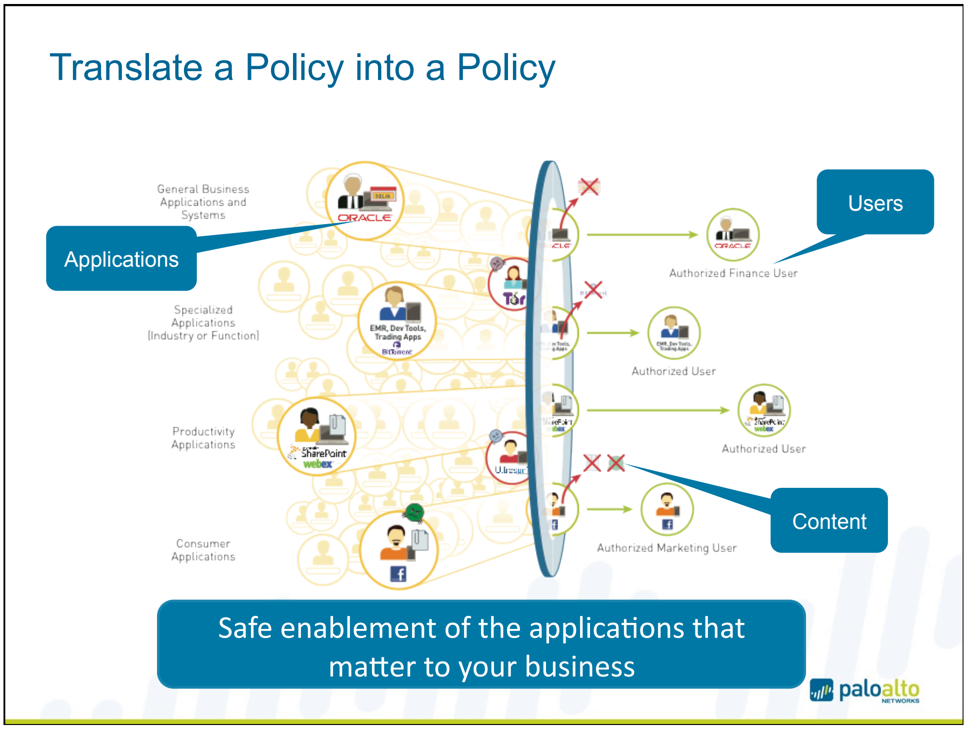
Eliminate Silos
1 Enterprise wide Policy



Achieve 100% visibility into Network Traffic

Why?

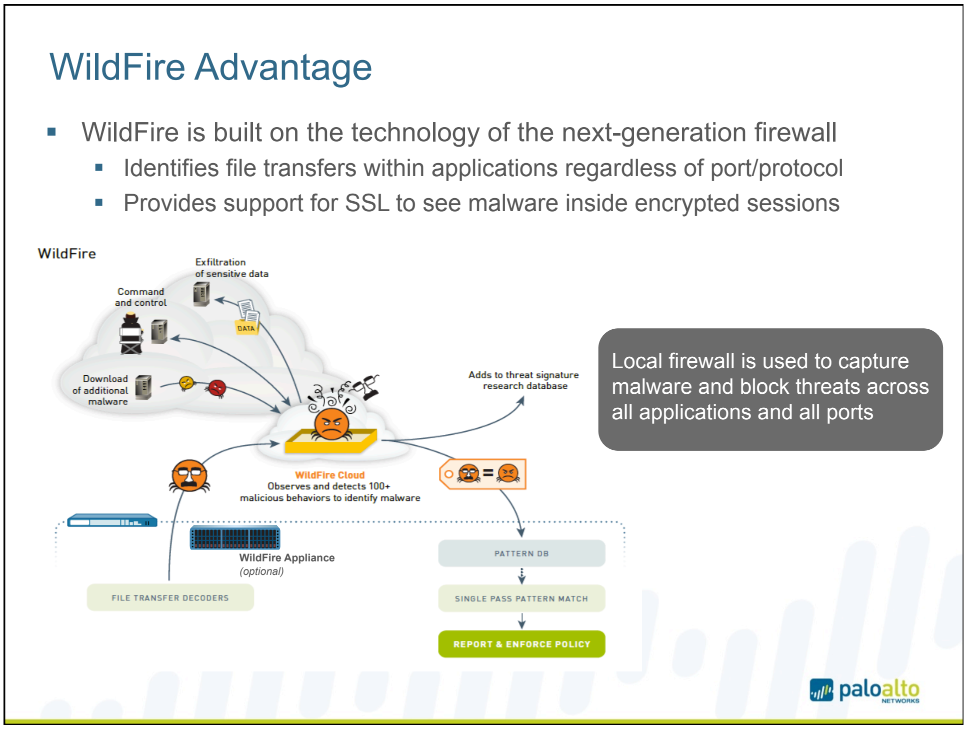
- Decide which applications to allow
- Eliminate unknowns
- Reduce the scope of your security challenge
- Enable your security teams to focus on what matters



Translate a Policy into a Policy

General Business Applications and Systems
Applications
ORACLE
Specialized Applications (Industry or Function)
EMR, Dev Tools, Trading Apps
BitTorrent
Tor
Productivity Applications
SharePoint
webex
Ultrasurf
Consumer Applications
Users
Authorized Finance User
Authorized User
Authorized User
Content
Authorized Marketing User

Safe enablement of the applications that matter to your business

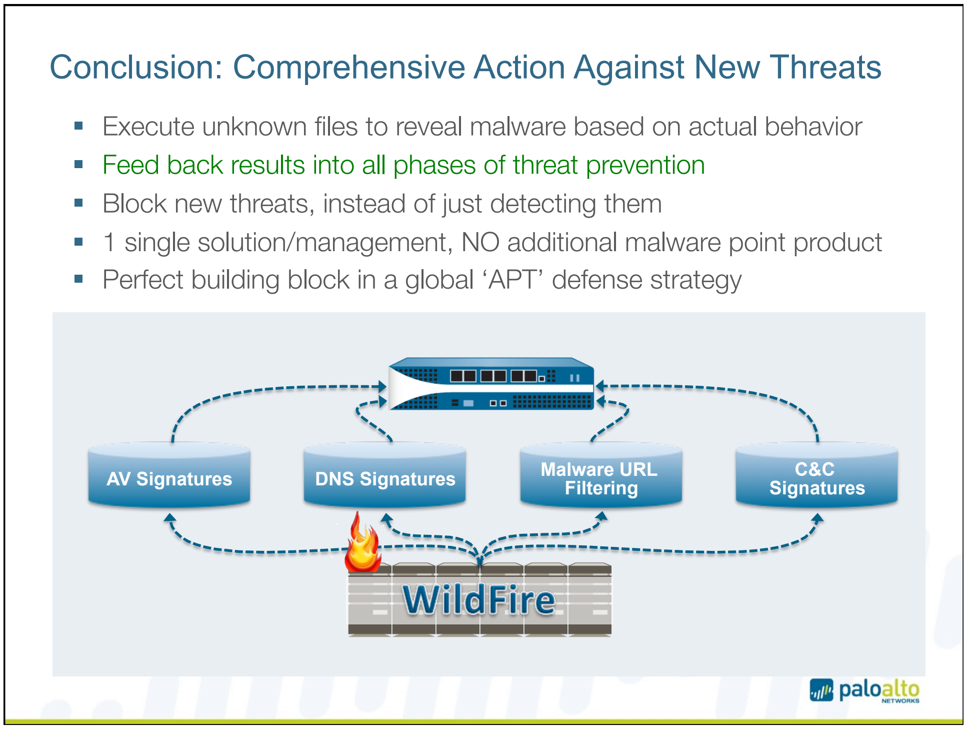


WildFire Advantage

- WildFire is built on the technology of the next-generation firewall
  - Identifies file transfers within applications regardless of port/protocol
  - Provides support for SSL to see malware inside encrypted sessions

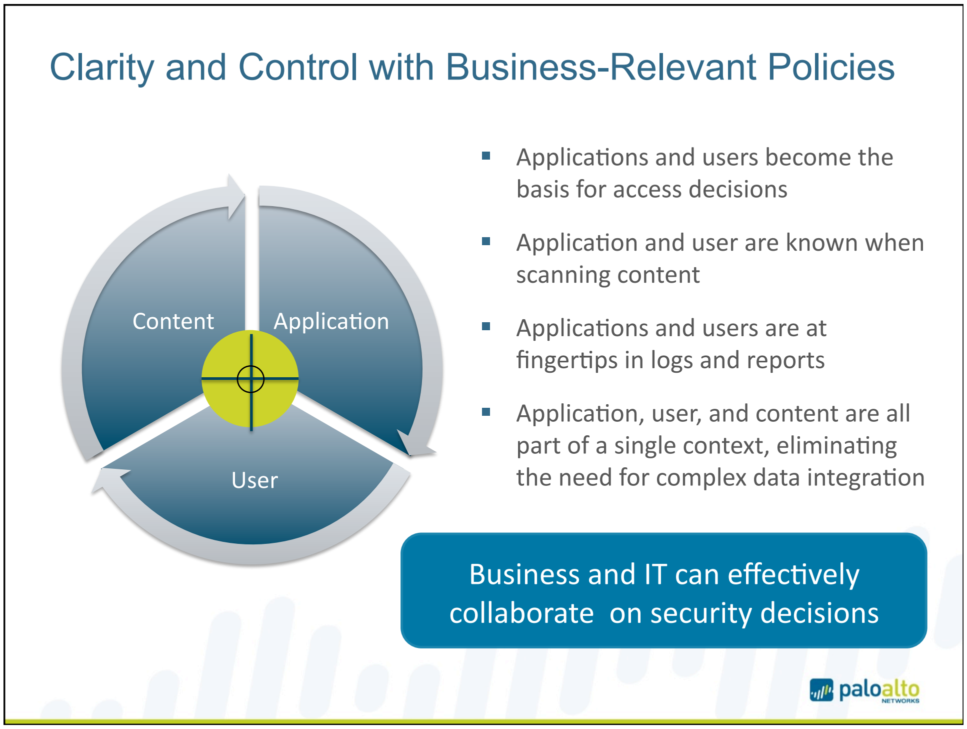
WildFire
Exfiltration of sensitive data
Command and control
DATA
Download of additional malware
Adds to threat signature research database
WildFire Cloud
Observes and detects 100+ malicious behaviors to identify malware
WildFire Appliance
(optional)
FILE TRANSFER DECODERS
PATTERN DB
SINGLE PASS PATTERN MATCH
REPORT & ENFORCE POLICY

Local firewall is used to capture malware and block threats across all applications and all ports



Conclusion: Comprehensive Action Against New Threats

- Execute unknown files to reveal malware based on actual behavior
- Feed back results into all phases of threat prevention
- Block new threats, instead of just detecting them
- 1 single solution/management, NO additional malware point product
- Perfect building block in a global 'APT' defense strategy



Clarity and Control with Business-Relevant Policies

- Applications and users become the basis for access decisions
- Application and user are known when scanning content
- Applications and users are at fingertips in logs and reports
- Application, user, and content are all part of a single context, eliminating the need for complex data integration

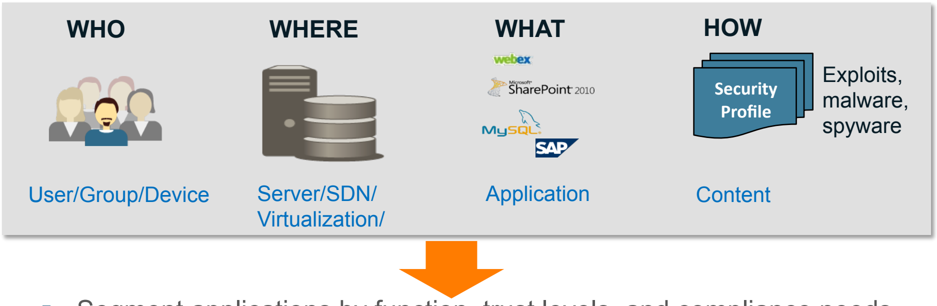
Business and IT can effectively collaborate on security decisions

Datacenter, Cloud Computing, Virtualization

paloalto NETWORKS

the network security company™

Our Safe Enablement Approach Applied to the Datacenter



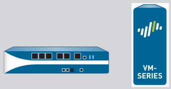
WHO	WHERE	WHAT	HOW
			Exploits, malware, spyware
User/Group/Device	Server/SDN/ Virtualization/	Application	Content

- Segment applications by function, trust levels, and compliance needs
- Inspect all traffic between security zones by default
- Systematically manage unknown traffic

Reduce the scope of your security challenge

paloalto NETWORKS

Unique Technologies to Secure Your Datacenter

Physical and Virtual Solutions	• Physical form factor (PA5000 series) • Virtual form factor (VM-Series) • Native VMWare NSX integration • 1 feature set, independent of the form factor 
Full support for Virtualization	• Policies that are natively integrated with VMWare objects • Firewalls automatically deployed in Virtual Infrastructure • Finally a fully integrated and cost efficient SDN design
Flexible integration	• Plugged directly into the hypervisor • NO (virtual) network change requirements • Traffic insertion via VMWare NSX hypervisor rules • Rock solid User Identity
Centralized management	• Centralized provisioning, logging and reporting • 1 integrated policy for the phyiscal and virtual devices

paloalto NETWORKS

Extended Mobile Enterprise

CyberSecurity does NOT stop at the Campus Perimeter

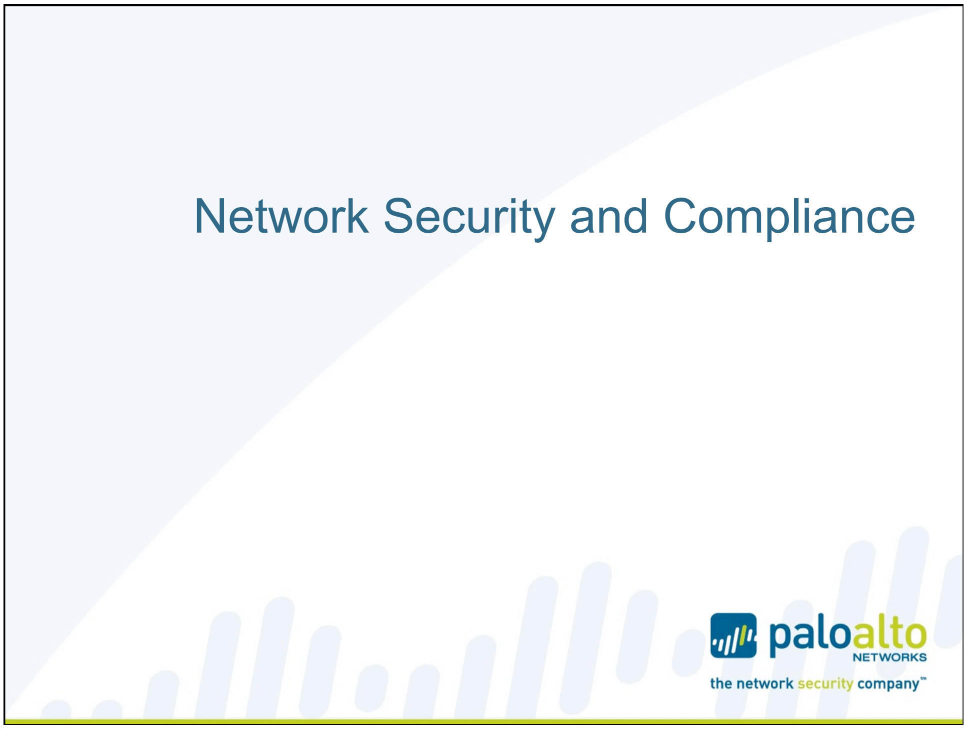
paloalto NETWORKS
the network security company™

Mobile security – not just about Connectivity

- Many App-IDs cover for the mobile app versions as well
- Over 130,000 Android APK malware signatures added and growing
- Partnerships with key MDM and Intelligence vendors

Globally Protect Users and Content

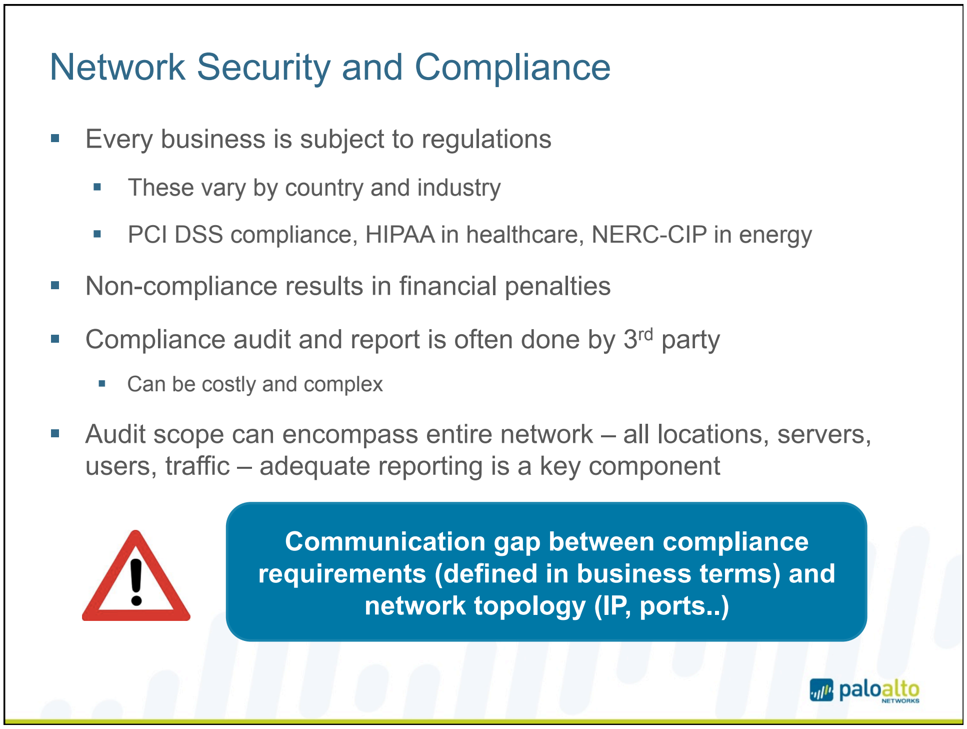
- Needs
  - Consistent user experience
  - Unified policy
  - Transparent security enforcement
  - Best performance possible
  - Supporting traditional and mobile devices
  - No complex endpoint components/enforcement
- Building Blocks
  - Re-use existing infrastructure and User aware policies
  - Lightweight agent connects devices automatically to the enterprise network
- ‘Integrated Secure Mobility’ means
  - Less (complex) policies = Lower management cost
  - Less devices = Lower TCO = Less administration, support contracts, …
  - ROI: 1 single solution of proven enterprise wide ‘Enforcement’ points



Network Security and Compliance

paloalto NETWORKS

the network security company™



Network Security and Compliance

- Every business is subject to regulations
  - These vary by country and industry
  - PCI DSS compliance, HIPAA in healthcare, NERC-CIP in energy
- Non-compliance results in financial penalties
- Compliance audit and report is often done by 3rd party
  - Can be costly and complex
- Audit scope can encompass entire network – all locations, servers, users, traffic – adequate reporting is a key component

⚠ **Communication gap between compliance requirements (defined in business terms) and network topology (IP, ports..)**

paloalto NETWORKS

Palo Alto Networks Facilitates Compliance and Audits

1. **Network Segmentation**
   - Limit the scope of compliance audits: only relevant servers are subject to the audit
2. **Applications, Users, Content based Traffic Control**
   - Audit report created automatically at the right level of information
   - No need to collect and integrate data from multiple sources
3. **Integration with 3rd parties supports more stringent requirements**
   - Example: Tufin for deeper audit of configuration and change management activities
4. **Centralized management streamlines the audit process**
   - Consistent policies, reporting, and logging across locations with one view of all appliances

100% visibility and control
WHO uses WHICH
Application for WHAT

+

=

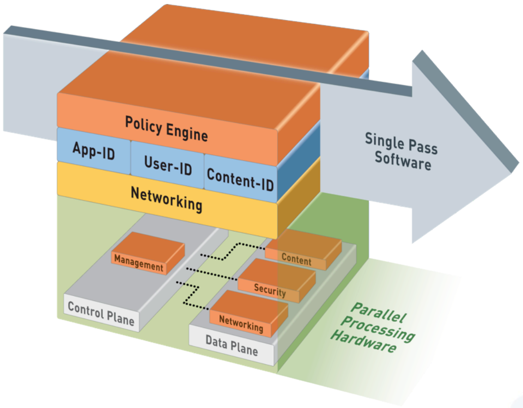
Streamlined Compliance and Audits

High performance platform

the network security company™

High Performance Architecture

Single-pass, Parallel Processing

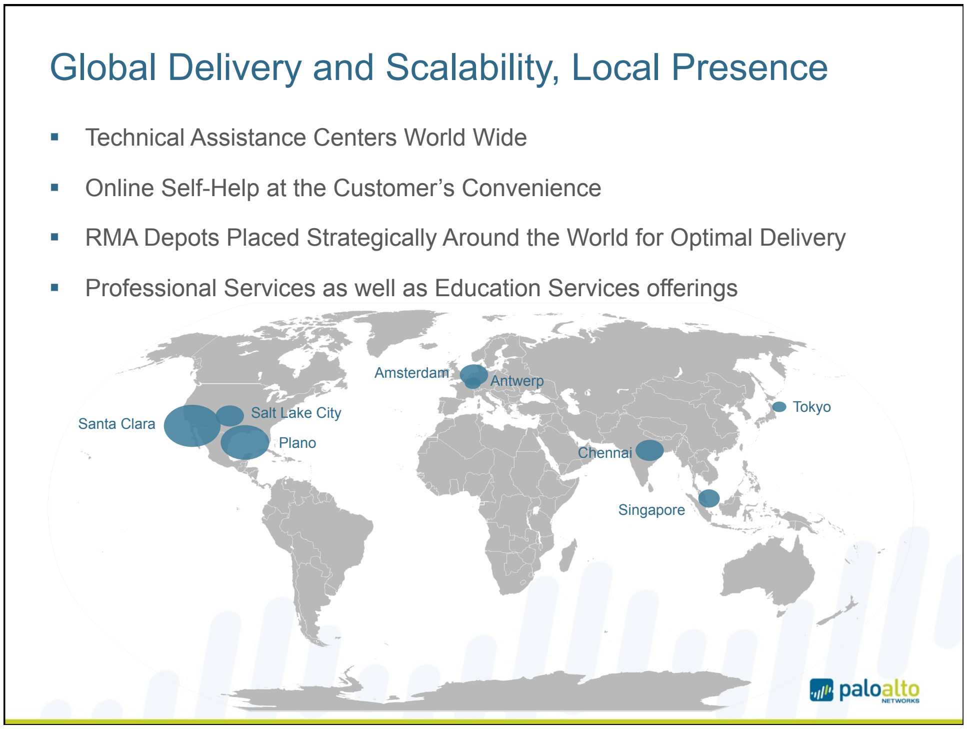


- Redesigned from the ground up with next-generation and **future** security requirements in mind
- Single-pass processing
  - Performs app, user, content scanning **once** per packet
  - **One** policy that integrates apps, user and content
- Parallel processing hardware
  - **Function-specific** parallel processing HW engines
  - Separate data plane and control plane

World Class Services

Customer Satisfaction Is Our Goal

paloalto NETWORKS
the network security company™



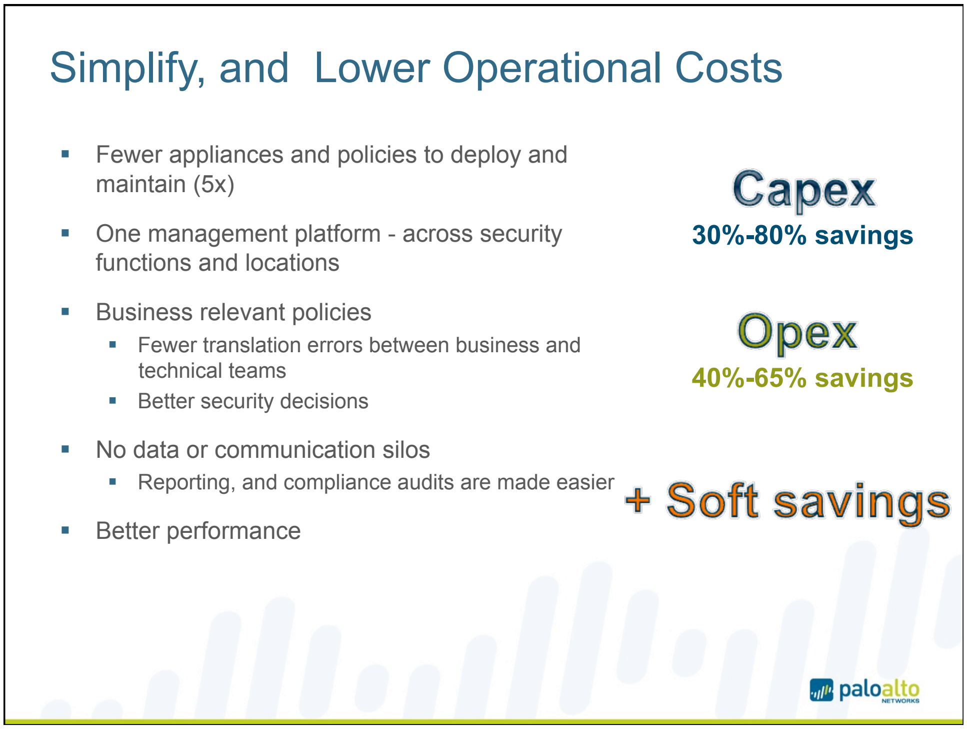
Global Delivery and Scalability, Local Presence

- Technical Assistance Centers World Wide
- Online Self-Help at the Customer's Convenience
- RMA Depots Placed Strategically Around the World for Optimal Delivery
- Professional Services as well as Education Services offerings

Management, Costs

paloalto NETWORKS

the network security company™



Simplify, and Lower Operational Costs

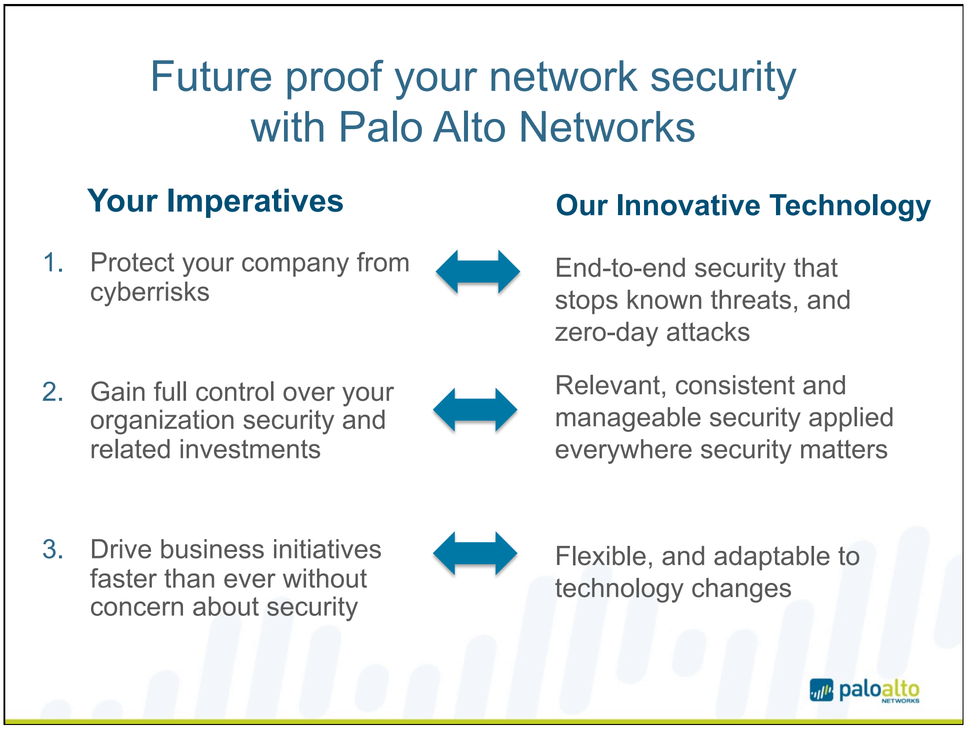
- Fewer appliances and policies to deploy and maintain (5x)
- One management platform - across security functions and locations
- Business relevant policies
  - Fewer translation errors between business and technical teams
  - Better security decisions
- No data or communication silos
  - Reporting, and compliance audits are made easier
- Better performance

Capex
30%-80% savings

Opex
40%-65% savings

+ Soft savings

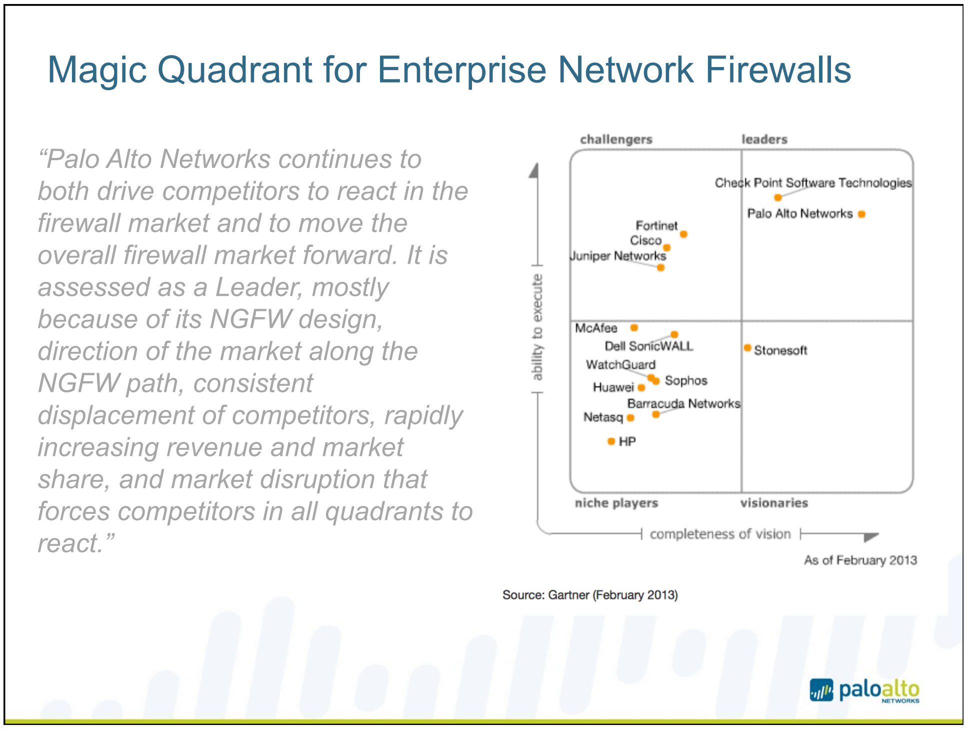
Summary



Future proof your network security with Palo Alto Networks

Your Imperatives		Our Innovative Technology
1. Protect your company from cyberrisks	⟷	End-to-end security that stops known threats, and zero-day attacks
2. Gain full control over your organization security and related investments	⟷	Relevant, consistent and manageable security applied everywhere security matters
3. Drive business initiatives faster than ever without concern about security	⟷	Flexible, and adaptable to technology changes

paloalto NETWORKS



Magic Quadrant for Enterprise Network Firewalls

"Palo Alto Networks continues to both drive competitors to react in the firewall market and to move the overall firewall market forward. It is assessed as a Leader, mostly because of its NGFW design, direction of the market along the NGFW path, consistent displacement of competitors, rapidly increasing revenue and market share, and market disruption that forces competitors in all quadrants to react."

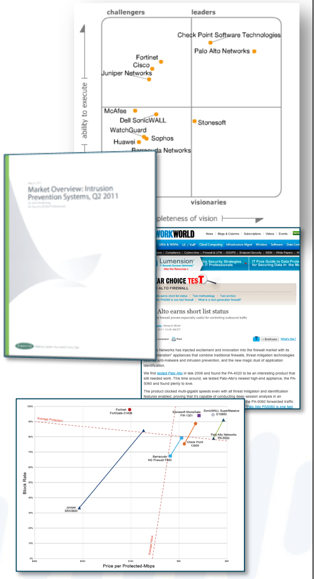
As of February 2013

Source: Gartner (February 2013)

paloalto NETWORKS

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; NSS Recommended
  - NGFW: FW + IPS test; NSS Recommended



paloalto NETWORKS

paloalto NETWORKS

the network security company tm