“Firewalls de Siguiente Generación Expandiendo la seguridad a Nivel aplicación, usuario y contenido”

Luis F. Fornelli

Country Manager – México

lfornelli@paloaltonetworks.com

Abril 2013

paloalto NETWORKS

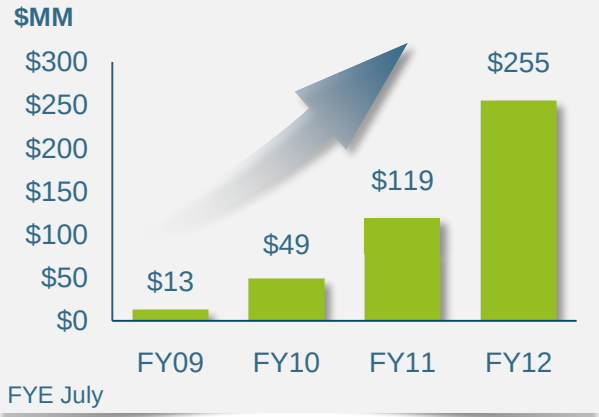
the network security company™

Palo Alto Networks de un vistazo

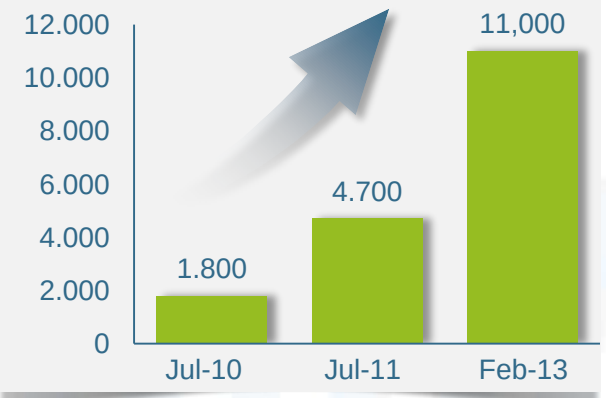
Corporate highlights

- Fundada en 2005; primer cliente en 2007
- Habilitando aplicaciones de manera segura
- Capaz de atender todas las necesidades de seguridad de la red
- Crecimiento excepcional y Presencia Global
- Equipo con gran experiencia en Tecnología y Gestión
- 1,000+ empleados en más de 80 países

Ingresos



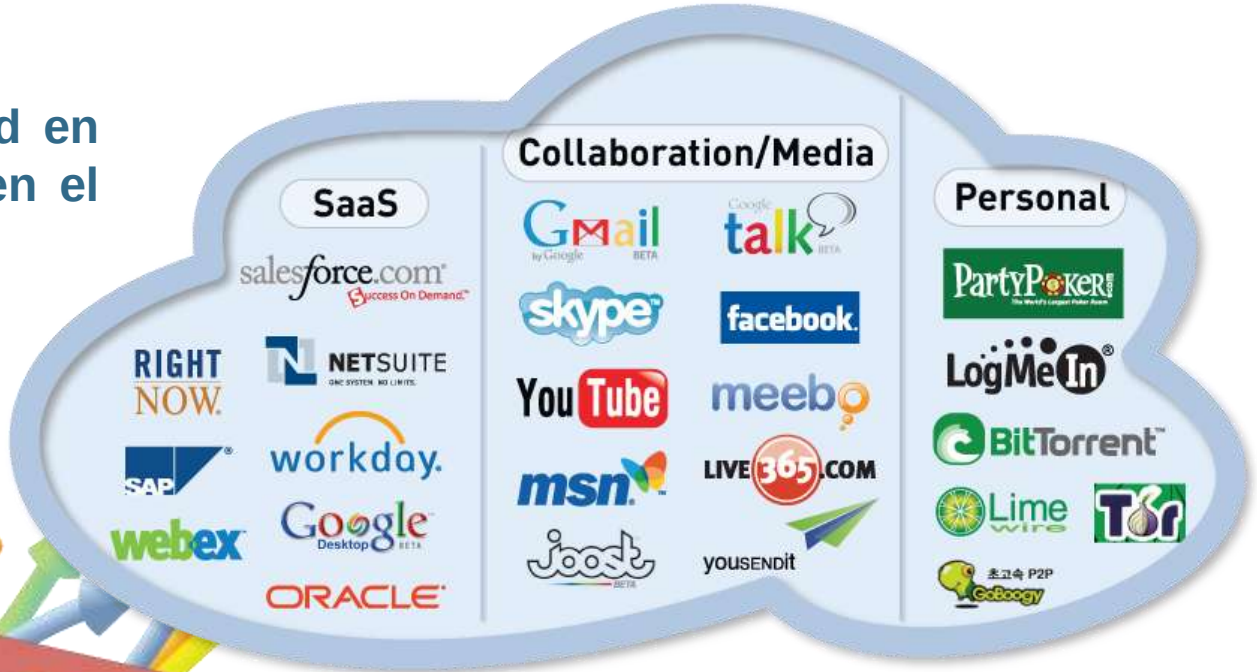
Clientes empresariales

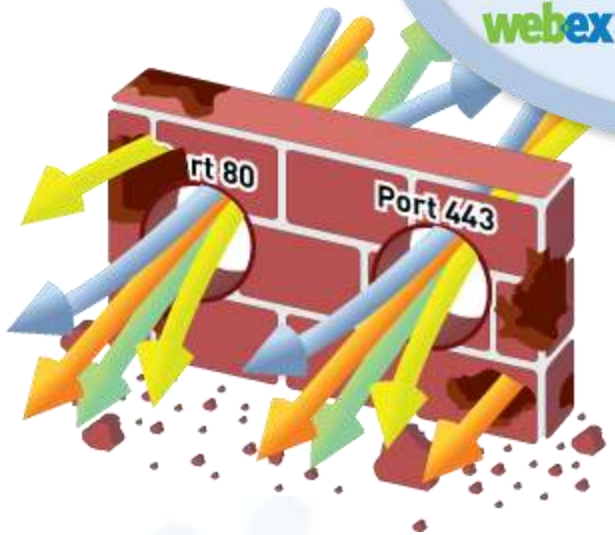


Las Aplicaciones han cambiado, los Firewall NO

Las políticas de seguridad en la red se hacen cumplir en el firewall

- Ve todo el tráfico
- Define los límites de confianza
- Permite el acceso





PERO…Las aplicaciones han cambiado

- **Puertos ≠ Aplicaciones**
- **Direcciones IP ≠ Usuarios**
- **Paquetes ≠ Contenido**

Los firewalls tradicionales ya no cumplen con estas necesidades

Se requiere restaurar la visibilidad y el control en el firewall

paloalto NETWORKS

La Dispersión Tecnológica NO es la respuesta

"Más cajas" no resuelven el problema

Los "ayudantes" para el Firewall tienen visión limitada del tráfico

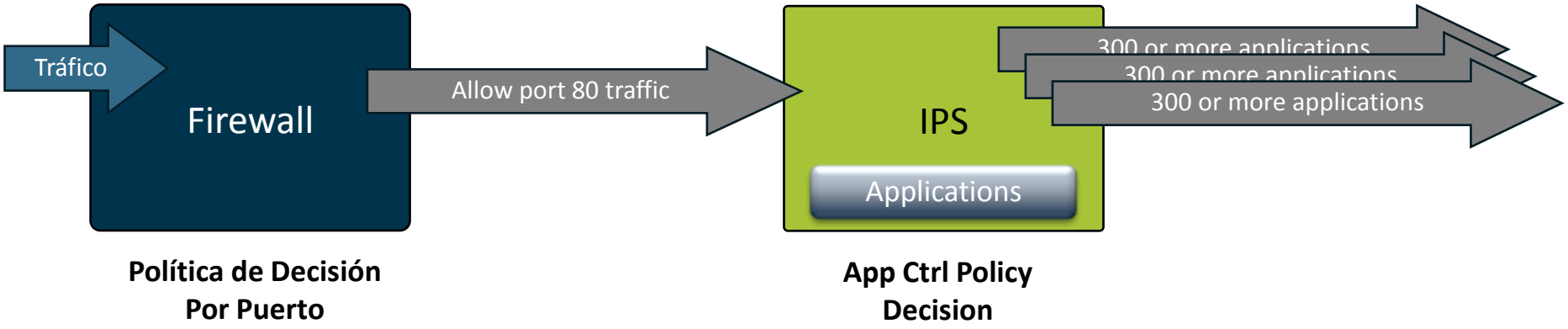
Son complejos y costosos de comprar, operar y mantener

No se ocupan de las aplicaciones

La Respuesta? Hagamos que el Firewall haga su trabajo!

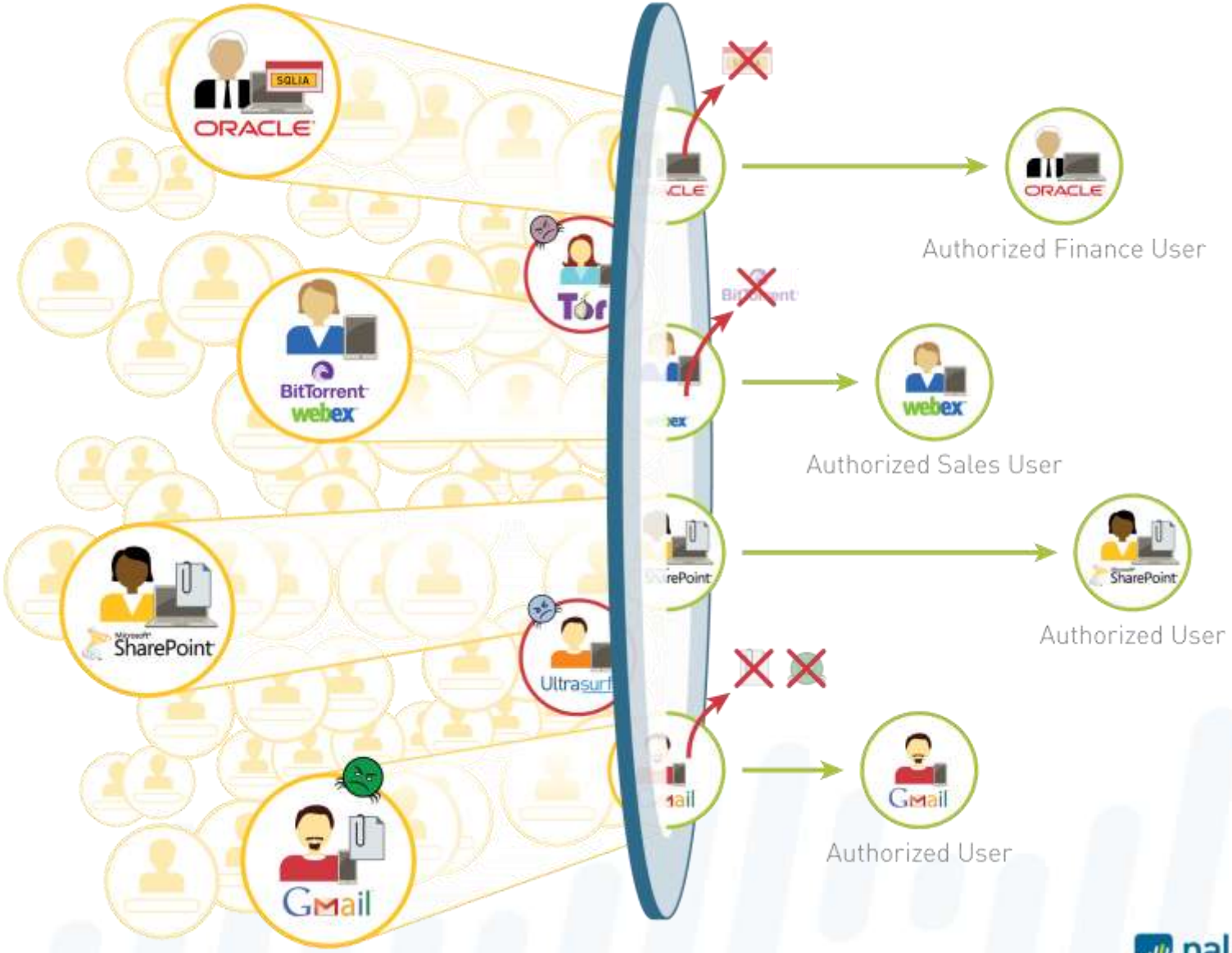
1. Identificar aplicaciones sin importar puerto, protocolo, táctica evasiva o encripción en SSL
2. Identificar y controlar usuarios sin importar la dirección IP, ubicación o dispositivo
3. Proteger contra amenazas conocidas y desconocidas transmitidas por aplicaciones
4. Visibilidad granular y políticas de control sobre el acceso a las aplicaciones y sus funcionalidades
5. Multi-gigabit, baja latencia, implementación en línea

Diferenciando: App-ID vs. Escaneo de dos pasos



- Ramificaciones operacionales del escaneo en dos pasos
  - Dos políticas separadas con información duplicada – imposible de reconciliar
  - Dos bases de datos de logs reducen la visibilidad y la hacen menos efectiva
  - Incapaz de manejar tráfico desconocido sistemáticamente
- Las tecnologías tradicionales de firewalls utilizan escaneo de dos pasos

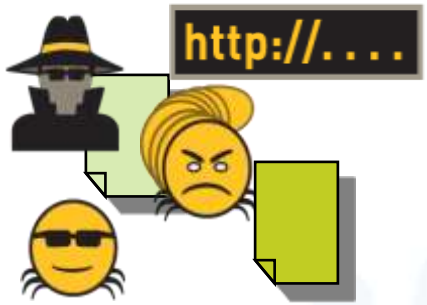
Habilitando Aplicaciones, Usuarios y Contenido



Convirtiendo al Firewall en una Herramienta de habilitación de Negocios

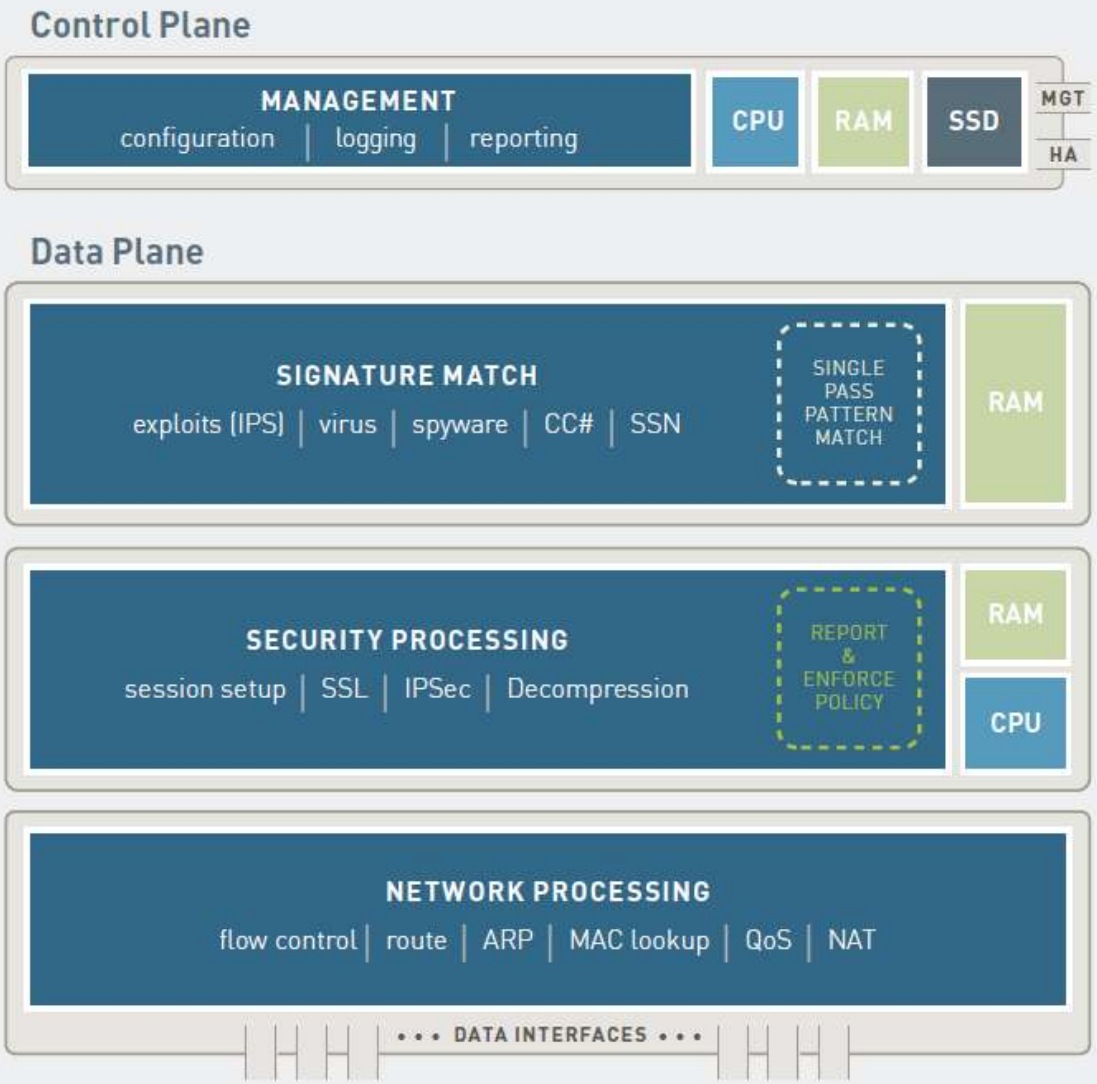
- **Aplicaciones:** La habilitación comienza con la clasificación de aplicaciones por App-ID.

- **Usuarios:** Relacionando usuarios y dispositivos sin importar su ubicación con aplicaciones por medio de User-ID y GlobalProtect.



- **Contenido:** Escaneando el contenido y protegiendo contra todas las amenazas, tanto conocidas como desconocidas, con Content-ID y WildFire.

Arquitectura de Plataforma de Un Solo Paso SP3



Signature Matching
Stream-based, uniform signature match (vulnerability exploits (IPS), virus, spyware, CC#, SSN and more)

Security Processing
High density parallel processing for flexibility, hardware-acceleration for standardized complex functions

Network Processing
Front-end network processing, hardware accelerated per-packet route lookup, MAC lookup and NAT

Enterprise-wide Next-Generation Firewall Security

Perímetro

- **App visibility y control en el firewall**
  - Todas las apps, todos los puertos, todo el tiempo
- **Prevenir Amenazas**
  - Amenazas Conocidas
  - Malware Desconocido/Dirigido
- **Simplicar la infraestructura de seguridad**

Data Center

- **Segmentación de Red**
  - Basada en usuario y aplicación, no en puerto/IP
- **Seguridad de red simple y flexible**
  - Integración con todos los diseños de DC
  - Alta disponibilidad, Alto Desempleño
- **Prevención de Amenazas**

Empresa Distribuída

- **Seguridad de red consistente en todas partes**
- HQ/sucursales/usaurios remotos y móviles
- **Perímetro lógico**
  - Las Políticas corresponden a las aplicaciones y usarios, no a una ubicación física
- **Administración Centralizada**

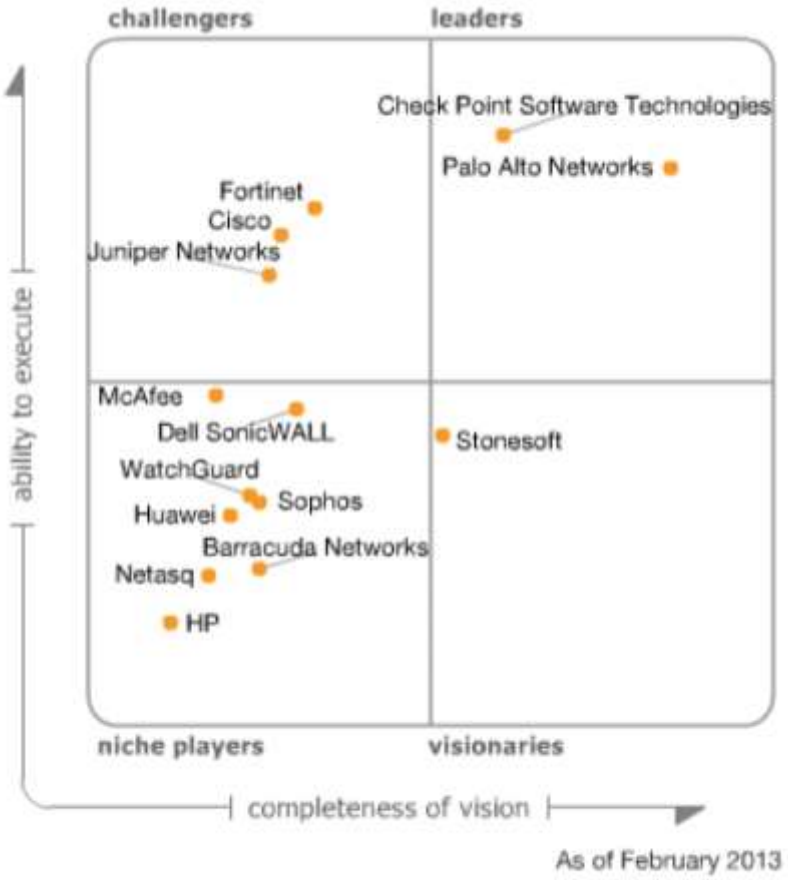
Aborda tres problemas clave del Negocio

- **Habilitar Aplicaciones con Seguridad**
  - Identificar más de 1,600 aplicaciones, sin importar puerto, protocolo, encripción o táctica evasiva
  - Control granular sobre aplicaciones y sus funciones (permitir, negar, limitar, escanear, etc)
  - Aborda las deficiencias claves de la infraestructura de firewall tradicional
  - Manejo sistemático de aplicaciones desconocidad
- **Prevención de Amenazas**
  - Detiene una gran variedad de amenazas conocidas – exploits (por vulderabilidad), viruses, spyware, etc.
  - Detecta y detiene amenazas desconocidas con WildFire
  - Detiene fuga de información confidencial (e.g., # de T de C, # de SS, tipo de archivo, etc)
  - Fuerza la aplicación de políticas de uso aceptable para navegación web en general
- **Simplifica la Infraestructura de Seguridad**
  - Colocando al firewall como el centro de la infraestructura de seguridad de la red
  - Reduce la complejidad en arquitectura y operación

2013 Gartner 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."

Gartner, February 2013



Source: Gartner (February 2013)

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

the network security company™