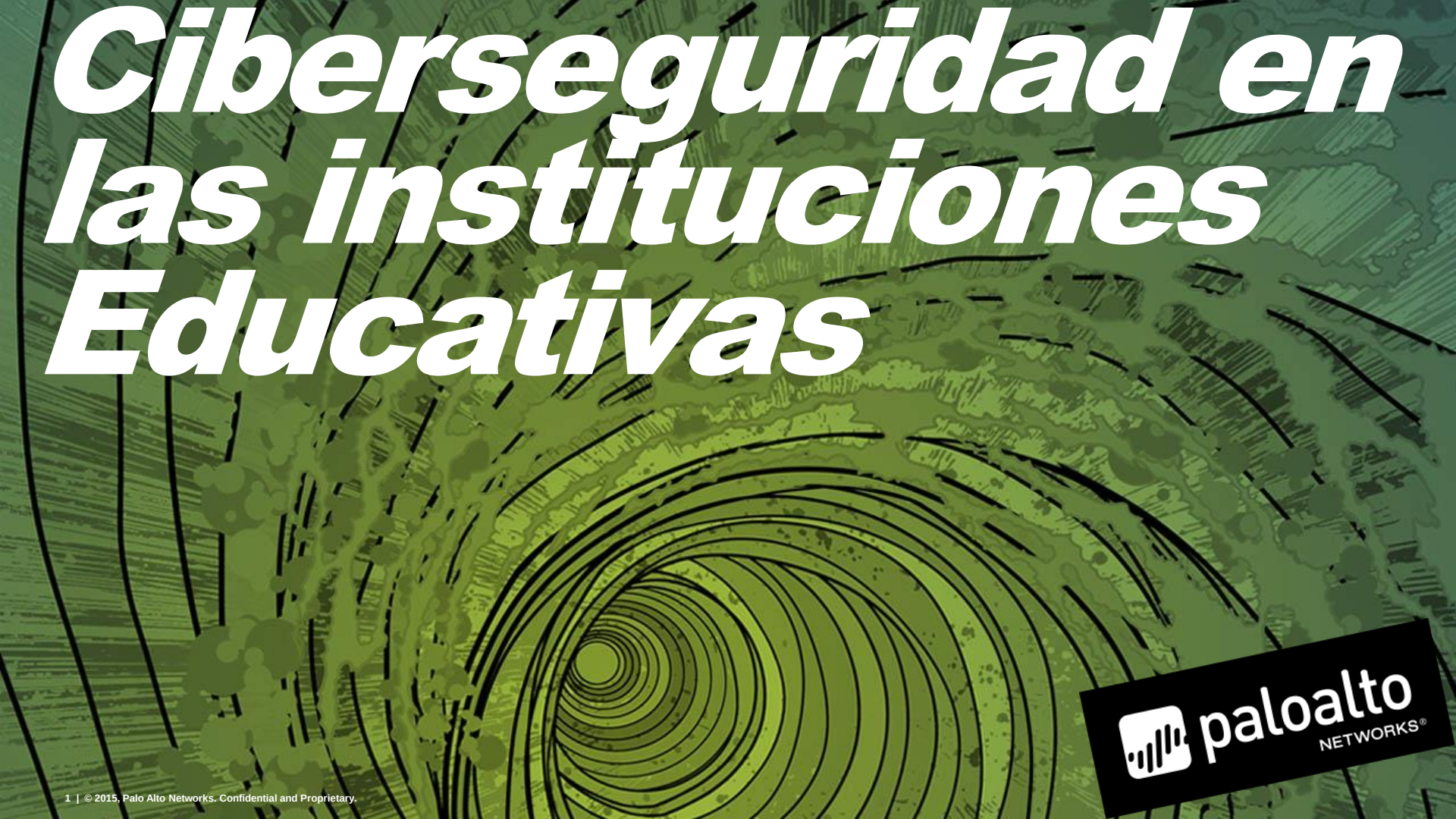
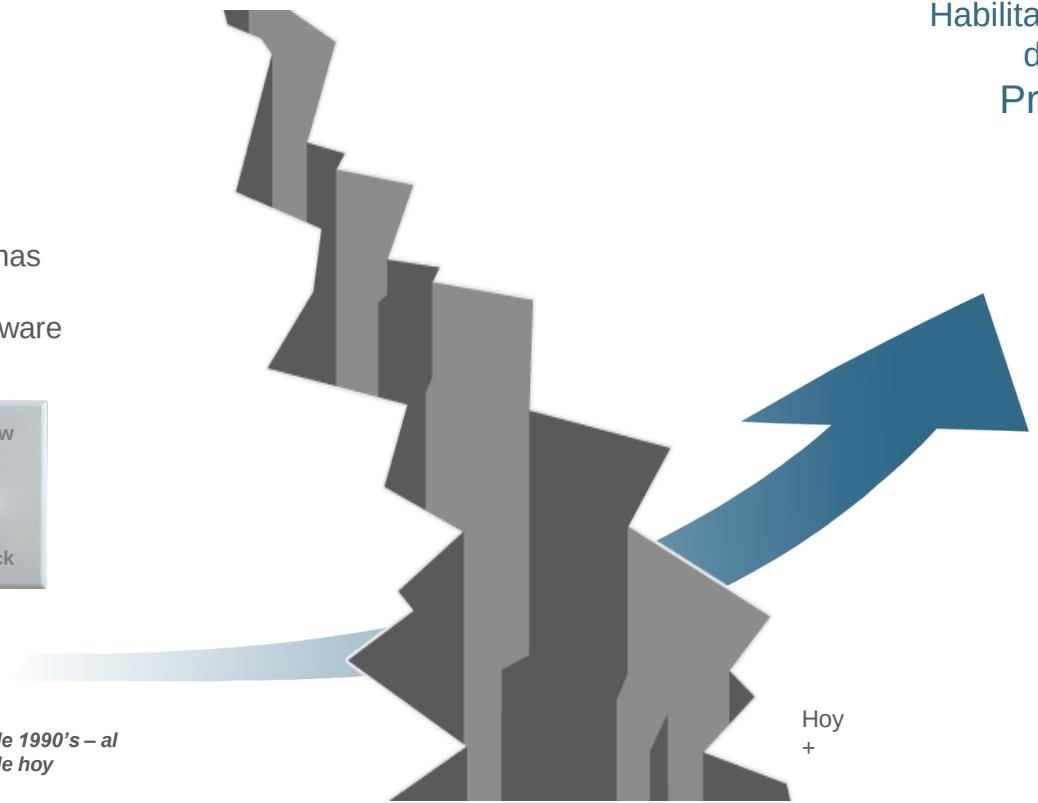
Ciberseguridad en las instituciones Educativas



Pioneros en la próxima generación de seguridad

Nueva Seguridad :
Habilitar todas las aplicaciones de manera segura
Prevenir todas las amenazas

Seguridad Legacy:
Permitir o bloquear algunas apps
Detección de algunos malware



Mediados de 1990's – al día de hoy

Hoy
+

Agenda

Retos de Ciberseguridad en el sector educativo.

Evolución de los firewalls

Plataforma de Seguridad Palo Alto Networks

Mejores Prácticas

Call to Action

Agenda

Retos de Ciberseguridad En el Sector Educativo




	Estudiantes	Profesores e investigadores	Personal Administrativo	IT
Conectividad	• Alta	• Alta	• Alta	• Alta
Movilidad	• Alta	• Alta	• Media a baja	• Media a baja
Tipo de Contenidos	• Educativos • Safesearch • Internet Seguro • Plataformas Educativas	• Educativos • Internet más abierto • Internet Seguro • Plataformas Educativas	• Acceso a sistemas de nóminas, recursos humanos e intranet, contables y de trámites gubernamentales. • Internet Seguro • Acceso a internet restringido a productividad	• Acceso a administración de recursos de redes y sistemas en general. • Internet Seguro • Acceso a internet en general
Riesgos	• Ver contenidos inapropiados para el alumno • Dispositivos propios o de la escuela comprometidos • Consumo de ancho de banda.	• Querer tener acceso a los recursos de la escuela sin permiso (shadow IT) RDP, Teamviewer. • Perdida de propiedad intelectual de la escuela • Dispositivos propios o de la escuela comprometidos	• Baja productividad por redes sociales, streaming, y exfiltracion de datos criticos • Dispositivos propios o de la escuela comprometidos • Consumo excesivo de ancho de banda	• Permitir el acceso a todos los demás usuarios asumiendo que todos dentro de la red son usuarios confiables. • No tener registro de quien accedio a que sistema. • Sistemas enteros comprometidos (Web, DB, Red)

Las reglas son para romperse

- Uso de VPNs, proxies y DNS externos para evitar la seguridad. (Usar DNS 8.8.8.8 o 4.2.2.2) SSH a sitios externos, OpenVPN, Hola, etc.
- Uso de Aplicaciones Shadow IT para compartir archivos que están en casa. Dropbox, Slideshare.
- Uso de anonymizers para evasión (HTTP proxies).
- Uso de buscadores en internet para ver contenido inapropiado.
- Además la mayoría de los usuarios tienen tiempo y curiosidad para buscar una evasión creativa.

El ciclo de vida de un ciberataque de seguridad

- La **Prevención** de un Ataque en la etapa más temprana es **Crítica.**

Inteligencia de un ataque	Aprovechar el Exploit	Ejecución de Malware	Controlar el canal de comunicación	Robar los datos
Planificación Del Ataque	Infección Silenciosa	Ejecución de archivo Malicioso	El Malware se comunica con el atacante	Robo de información, Sabotaje, Destrucción

Controles Preventivos **Controles reactivos**

Agenda

Evolución de los firewalls

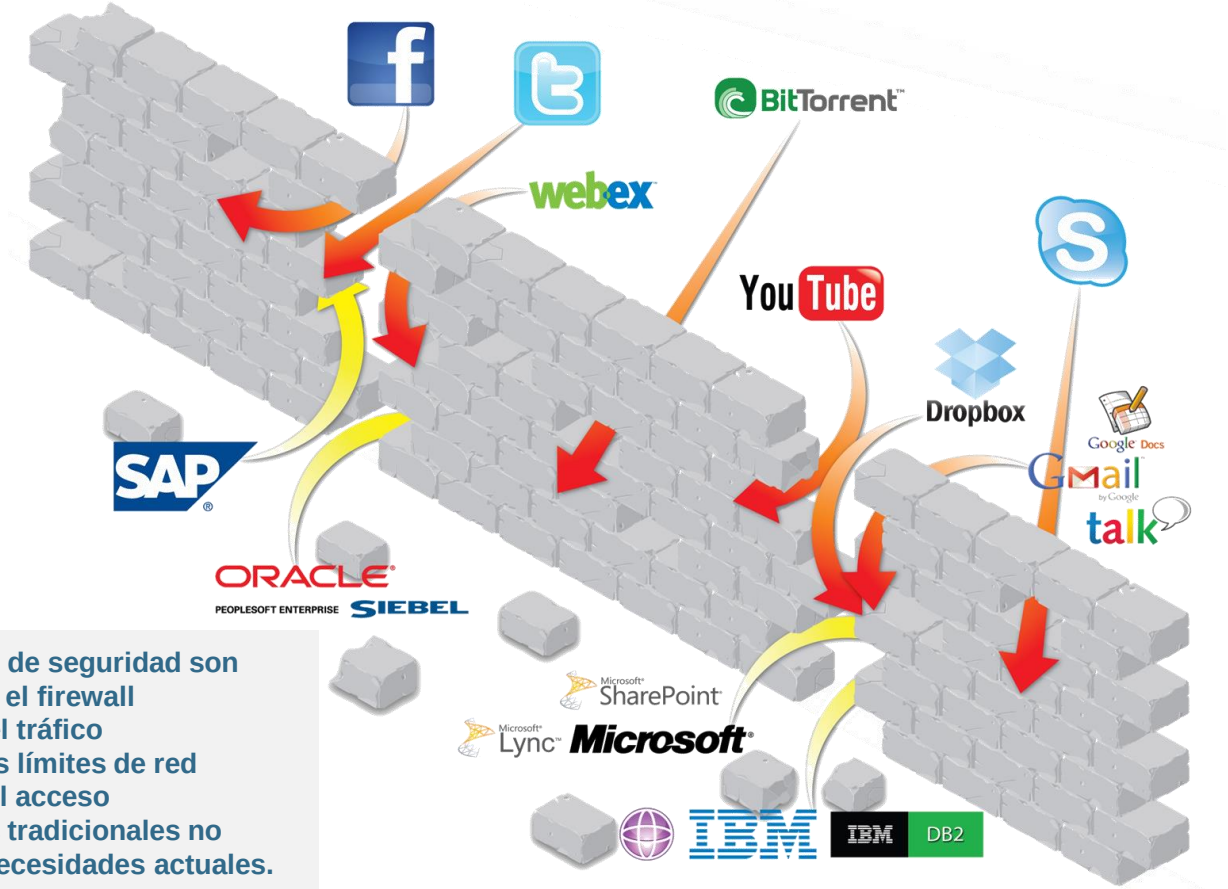
Retos en el sector educativo

Plataforma de Seguridad Palo Alto Networks

Mejores Prácticas

Call to Action

Las aplicaciones han cambiado, los Firewalls no

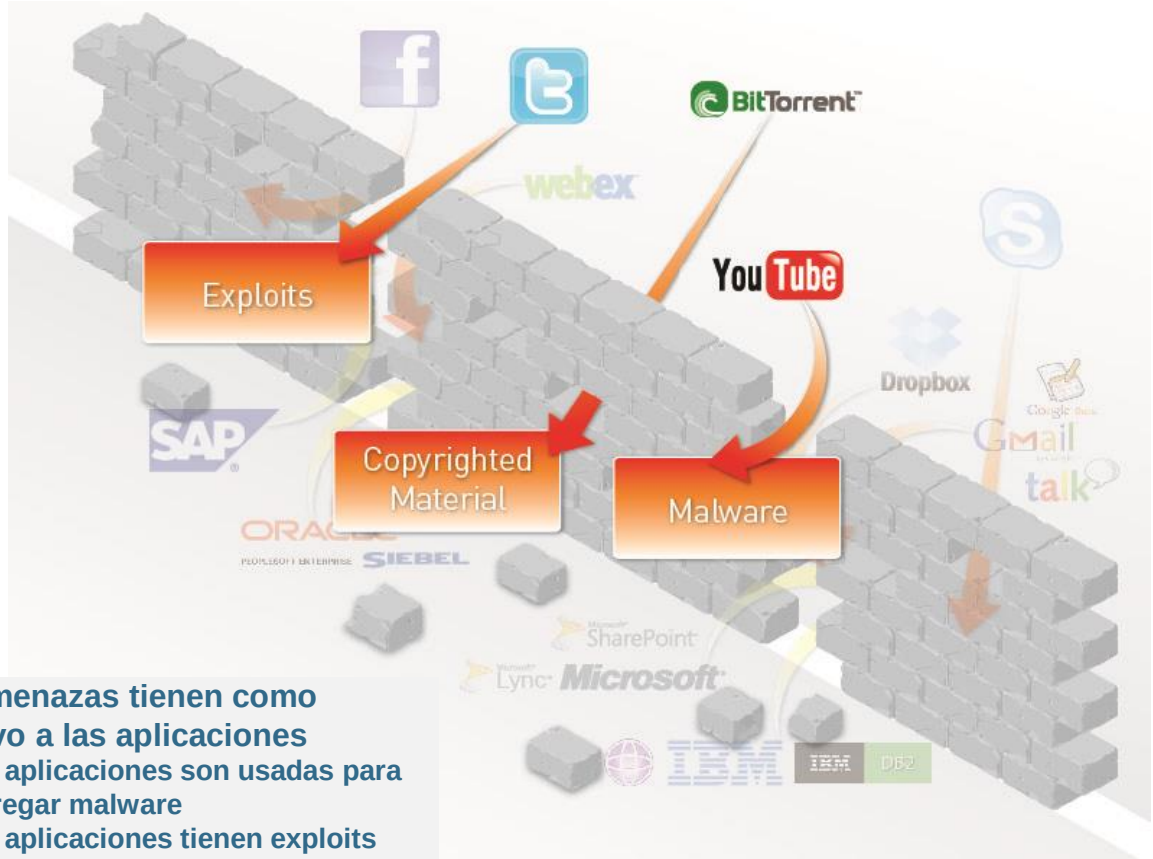


Las políticas de seguridad son aplicadas en el firewall

- Ve todo el tráfico
- Define los límites de red
- Habilita el acceso

Los firewalls tradicionales no cubren las necesidades actuales.

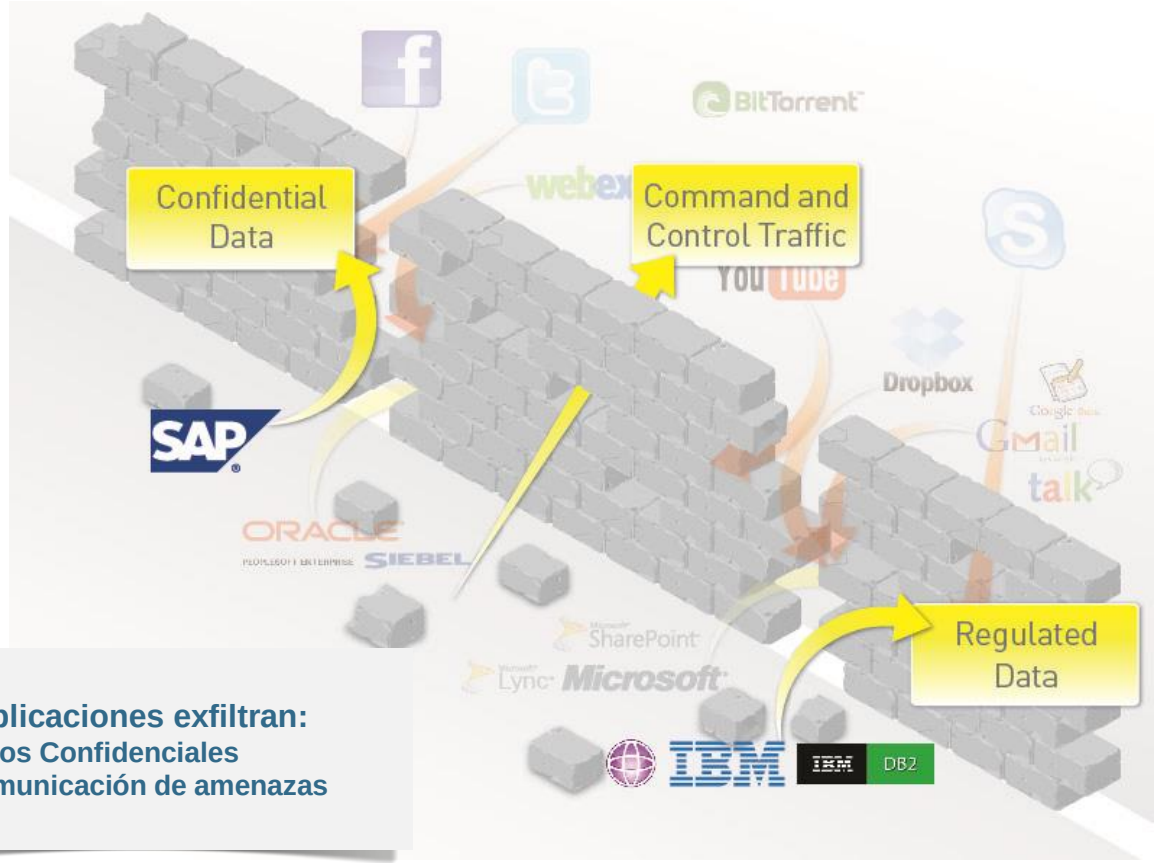
Aplicaciones: Vector de Ataque y Objetivo



Las amenazas tienen como objetivo a las aplicaciones

- **Las aplicaciones son usadas para entregar malware**
- **Las aplicaciones tienen exploits específicos**

Aplicaciones: Entrega de Payload / Command & Control



Las aplicaciones exfiltran:

- **Datos Confidenciales**
- **Comunicación de amenazas**

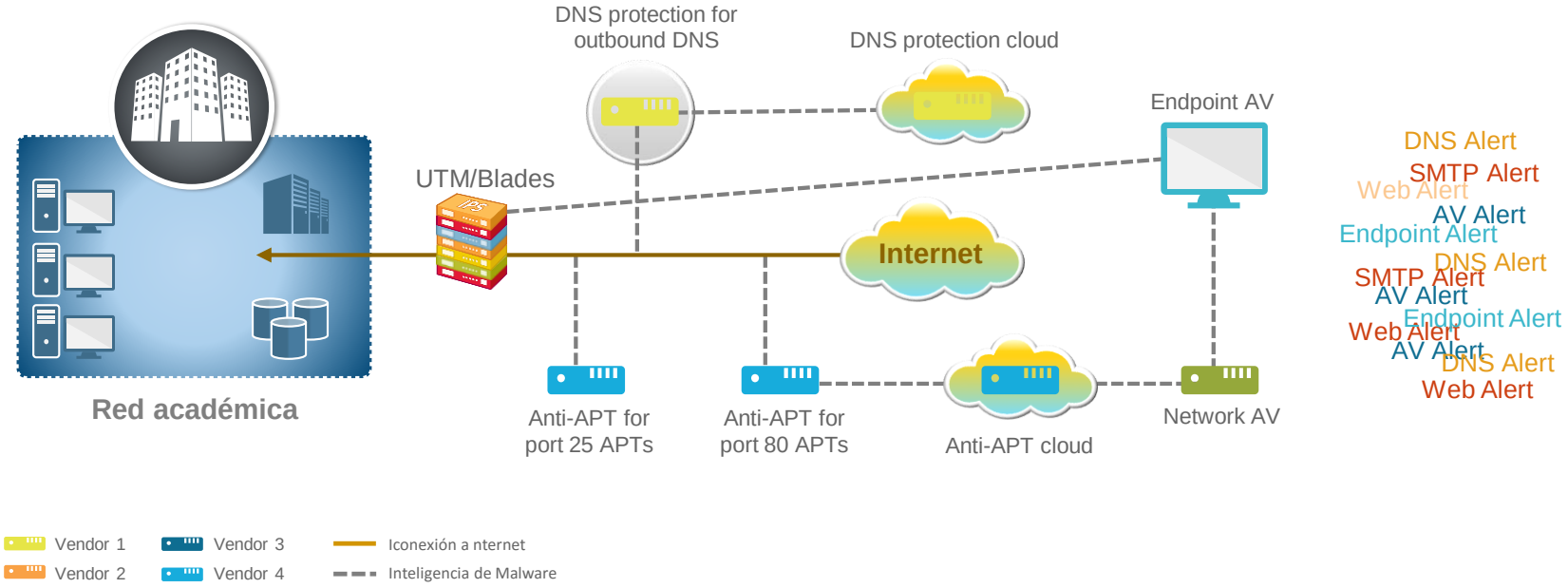
paloalto NETWORKS

Fallas en las arquitecturas legacy

Visibilidad limitada

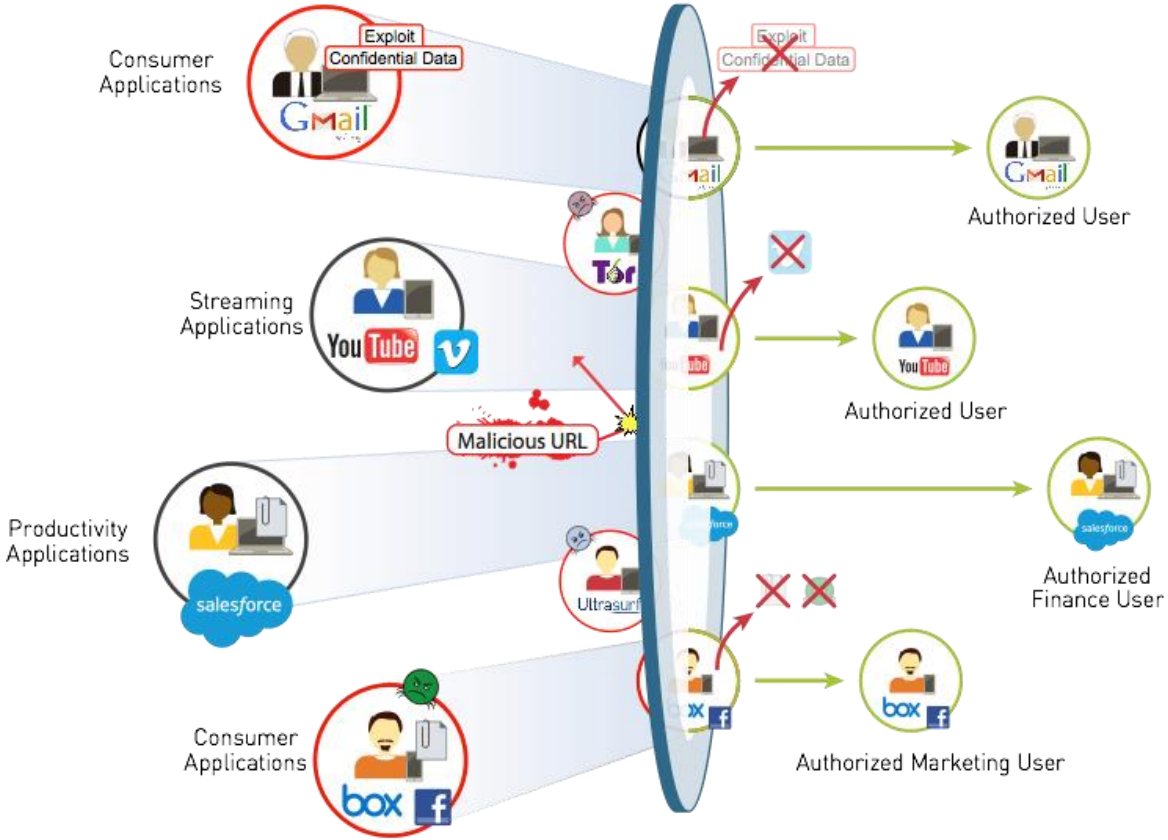
Eventos no correlacionados

Respuesta Manual



Habilitar todas las aplicaciones de manera segura

Habilitar aplicaciones, usuarios y filtrar contenido



Agenda

Evolución de los firewalls

Retos en el sector educativo

Plataforma de Seguridad Palo Alto Networks

Mejores Prácticas

Call to Action

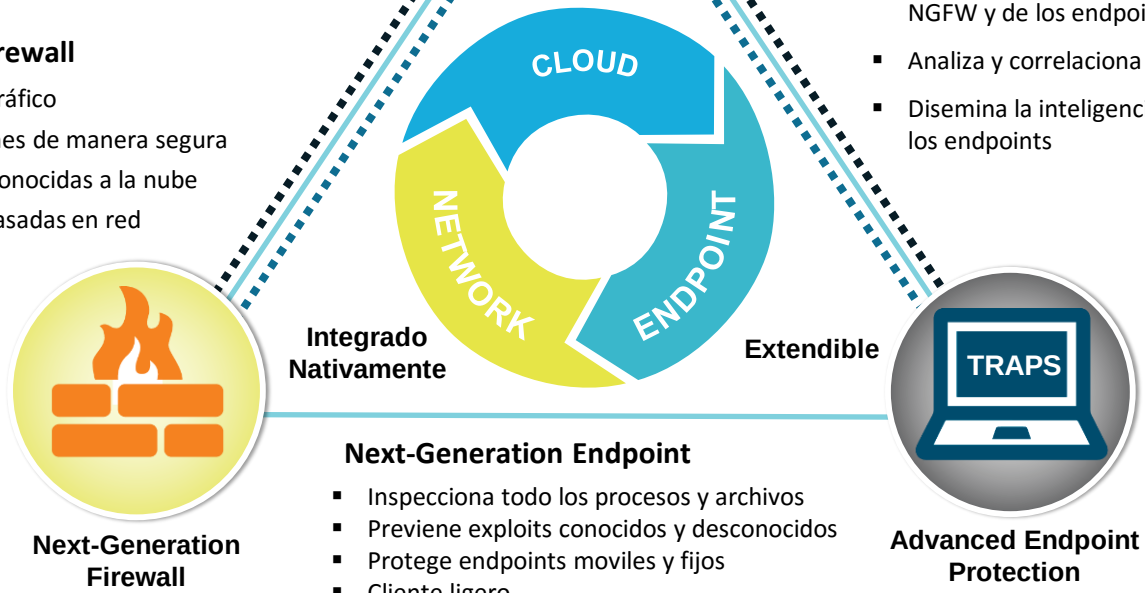
Delivering the Next-Generation Security Platform

Next-Generation Threat Cloud

- Acumula amenazas potenciales provenientes del NGFW y de los endpoints
- Analiza y correlaciona inteligencia de amenazas
- Disemina la inteligencia de amenazas a los NGFW y a los endpoints

Next-Generation Firewall

- Inspecciona todo el tráfico
- Habilita las aplicaciones de manera segura
- Envia amenazas desconocidas a la nube
- Bloquea amenazas basadas en red



Next-Generation Endpoint

- Inspecciona todo los procesos y archivos
- Previene exploits conocidos y desconocidos
- Protege endpoints moviles y fijos
- Cliente ligero

Single Pass Architecture – Planos separados

Cloud Network Endpoint

App-ID

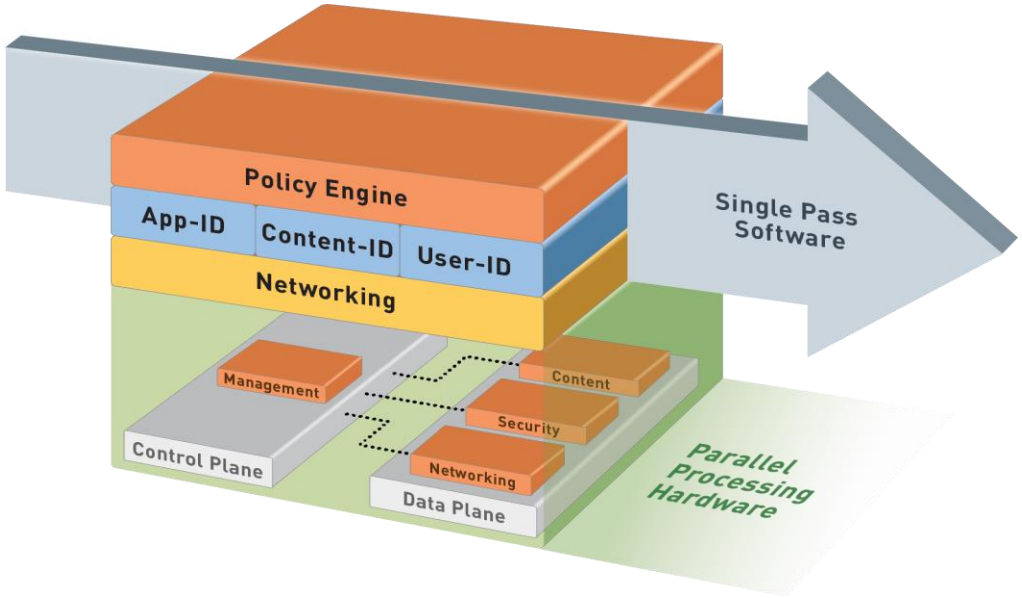
Identifica la aplicación

Content-ID

Escanea el contenido

User-ID

Identifica al usuario



Unit 42 : Advanced Threat Research Team

unit42 THREAT RESEARCH
THE NEXT STEP IN THREAT INTELLIGENCE

Palo Alto Networks threat intelligence team

- Expertos en Ciberseguridad
- Reune, investiga, analiza, y provee las últimas tendencias en ciber amenazas
- Comparte la investigación con los clientes, partners y toda la comunidad de Palo Alto Networks para proteger mejor los ambientes de computo de las empresas, escuelas, proveedores de servicio y agencias gubernamentales.
- Descubre grupos adversarios analizando información recolectada de las plataformas de Palo Alto Networks. Da un contexto de los métodos y motivaciones de los atacantes.

Agenda

Evolución de los firewalls
Retos en el sector educativo
Plataforma de Seguridad Palo Alto Networks
Mejores Prácticas
Call to Action

Mejores Practicas

- Zero-Trust
- SafeSearch
- Contexto
- Prevención más que Detección

Mejores Practicas

- Zero-Trust
- SafeSearch
- Contexto
- Prevención más que Detección

Zero-Trust – Reduciendo errores sin intención….

No se debe confiar en que los usuarios serán:

- Cuidadosos con los attachments
- Cuidadosos con los links desconocidos

La mayoría de los empleados son buenos para:

- No dar click a links
- No abrir archivos
- No Visitar sitios

Pero, si una sola persona lo hace ¡Todos los sistemas están en riesgo!

Los candados hacen honesta a la gente honesta… La segmentación lógica reduce el riesgo de que el personal u otros recursos accedan recursos y sistemas privados…

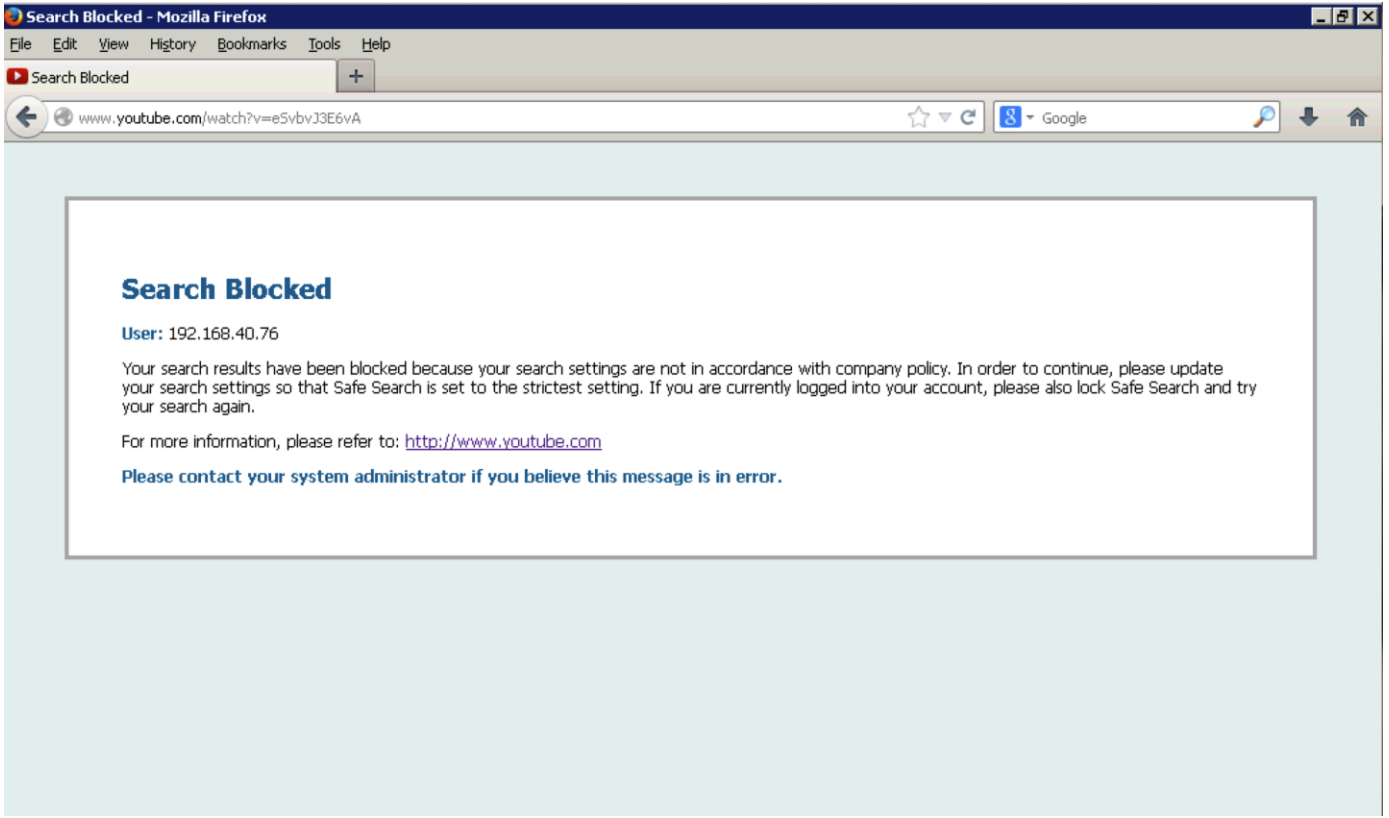
Aproximación progresiva de seguridad- Zero Trust

- Evaluar cuales son los riesgos financieros y los sistemas de alto valor (ejemplos: repositorios compartidos, software propietario, datos de alumnos)
- Enfocarse en la visibilidad primero, y después en habilitamiento seguro de aplicaciones y control

Mejores Practicas

- Zero-Trust
- SafeSearch
- Contexto
- Prevención más que Detección

Safesearch enforcement



Mejores Practicas

- Zero-Trust
- SafeSearch
- Contexto
- Prevención más que Detección

Context

slideshare-uploading
application function

slideshare
application

roadmap.pdf
file name

prodmgmt
group

HTTP
protocol

file-sharing
URL category

344 KB

mjacobsen
user

SSL
protocol

Canada
destination country

172.16.1.10
source IP

TCP/443
destination port

64.81.2.23
destination IP

Perfilar por grupo de usuarios y aplicaciones

- ***EJEMPLOS:***
- Si el alumnado es menor de edad es de gran interés evitar aplicaciones para adultos como Snapchat o Tinder
- Si los investigadores y profesores necesitan acceder a recursos en el DC o a sus computadoras de trabajo, una VPN ayuda a extender las políticas de seguridad
- A los empleados administrativos, se les puede dar una serie de aplicaciones dependiendo de su departamento, ejemplo, comunicación y marketing (Facebook) tiene diferentes aplicaciones a finanzas (SAP)
- Segmentar a cada grupo y verificar que solo los administradores tienen acceso a la red de administración.
- Hacer una política de QoS por aplicación, tal vez no quiero que Netflix se acabe mi ancho de banda en temporada de inscripciones o de exámenes online.

Mejores Practicas

- Zero-Trust
- SafeSearch
- Contexto
- Prevención más que Detección

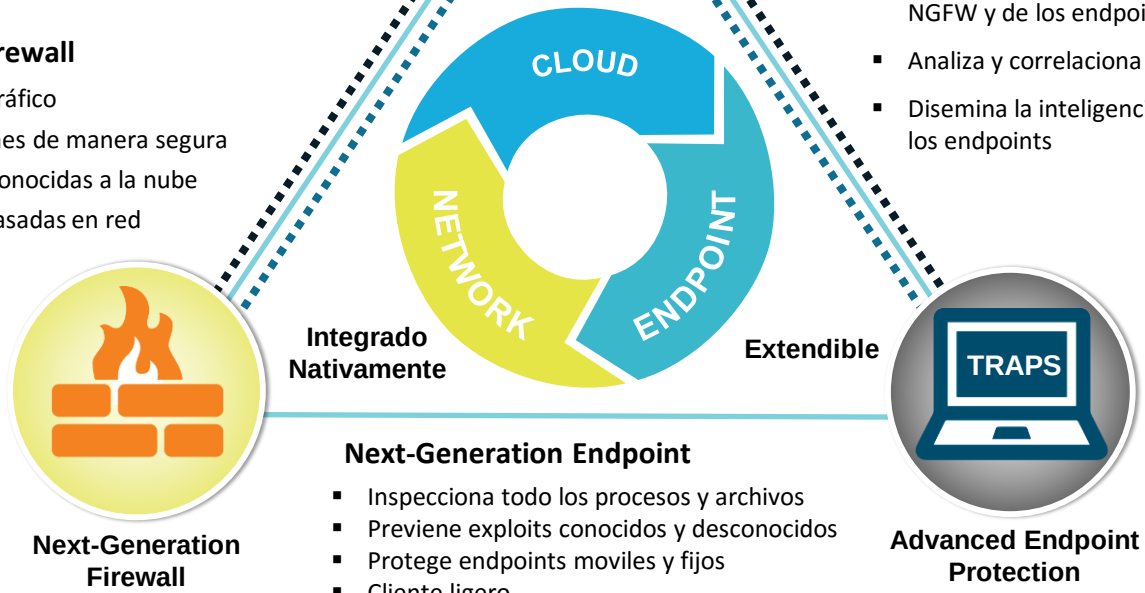
Delivering the Next-Generation Security Platform

Next-Generation Threat Cloud

- Acumula amenazas potenciales provenientes del NGFW y de los endpoints
- Analiza y correlaciona inteligencia de amenazas
- Disemina la inteligencia de amenazas a los NGFW y a los endpoints

Next-Generation Firewall

- Inspecciona todo el tráfico
- Habilita las aplicaciones de manera segura
- Envia amenazas desconocidas a la nube
- Bloquea amenazas basadas en red



Next-Generation Endpoint

- Inspecciona todo los procesos y archivos
- Previene exploits conocidos y desconocidos
- Protege endpoints moviles y fijos
- Cliente ligero

Threat Prevention Mejores Prácticas (también aplica para Ransomware)

Crear Protecciones

1 *Reducir la superficie de ataque*

- Hacer listas blancas de aplicaciones o bloquear aplicaciones de alto riesgo con APP-ID
- Bloquear IPs y regiones que sabemos son riesgosas
- Bloquear tipos de archivos peligrosos.
- Dar visibilidad al tráfico cifrado – SSL Decryption
- Bloqueo de sitios Web Peligrosos – URL Filtering

2 *Prevenir amenazas conocidas*

- Bloquear vulnerabilidades conocidas, malware y exploits con Threat Prevention
- Prevenir tráfico C&C (anti-spyware)
- Prevenir tráfico DNS C&C (anti-spyware)
- Localizar con precisión usuarios infectados User-ID

3 *Detectar/Prevenir Amenazas Desconocidas*

- Prevenir ataques de día cero con WildFire
- Prevenir exploits 0-day con Advanced Endpoint Protection
- Descubre sistemas infectados con el reporte de Botnet
- Bloqueo de tráfico desconocido (TCP/UDP)
- Detectar exfiltración de datos

Call To Action

Gracias

Agustin Robles
arobles@paloaltonetworks.com

Alejandra Bonilla
abonilla@paloaltonetworks.com

Omar Ochoa
oochoa@paloaltonetworks.com

