SONICWALL®

Gestión de vulnerabilidades
IT Digital Security

22 Marzo 2018

INNOVATE **MORE.**
FEAR-**LESS.**

Eduardo Brenes
ebrenes@sonicwall.com

PREGUNTAS PARA HOY

1. Ciberseguridad y ciberesiliencia. ¿Qué ocurre en el mercado de la ciberseguridad?.
2. ¿Cuáles son las principales vulnerabilidades?.
3. ¿Quién es SonicWall y qué ofrece?.

SONICWALL™

© Copyright SonicWall

¿QUÉ OCURRE?

SONICWALL™

Un mundo conectado crea enormes posibilidades…

¿Cómo de seguro es el entorno con todas estas nuevas iniciativas?

El negocio no puede parar y esperar por la ciberseguridad…

Desafortunadamente, los “chicos malos” están también más conectados…

Múltiples amenazas…

Spear-Phishers, BOTnets, DDoS, Zero-Day Threats, Insider threats & former employees

Preparados para atacar…

Herramientas de seguridad, procesos, perfiles de usuario e información separada en silos.

Algunos datos:

- **243** días de media para detectar que datos se han visto comprometidos.
- **84%** incidencias ocurren en las aplicaciones.
- **94%** de las incidencias son reportadas por terceros

El 70% de los ciberataques se dirige contra las pymes

Comentarios

Tweet | Compartir 8 | G+1 2 | Share 20 | Wow! 0

Más noticias sobre: EMPRESAS HACKERS EMPRESA DE SEGURIDAD

Las pymes son un claro foco de vulnerabilidad digital. De hecho, la facilidad con la que los hackers obtienen datos en este tipo de empresas es evidente. La empresa de seguridad ditigal ZeedSecurity advierte que solo el 40% los sistemas de seguridad de las empresas están correctamente asegurados.

La brecha en la seguridad digital en las pymes es aprovechada por los cibercriminales. De hecho, un 70% de los ataques se dirige contra compañías de menos de 100 empelados, según ZeedSecurity. La desprotección en el conjunto de sus infraestructuras digitales es lo que hace que los hackers focalicen sus ataques en este tipo de empresas.

ENLACES RELACIONADOS

- Usuarios estafados y estafadores

SONICWALL™

Expectativas sobre el departamento de IT

innovación | reducir riesgos | despliegues rápidos

mejoras eficiencia | **cumplimiento normativo** | bajo presupuesto

Retos de ciberseguridad

siloed security solutions | BYOD | encrypted everything

ransomware | IOT | unknown, zero day threats

PRINCIPALES VULNERABILIDADES

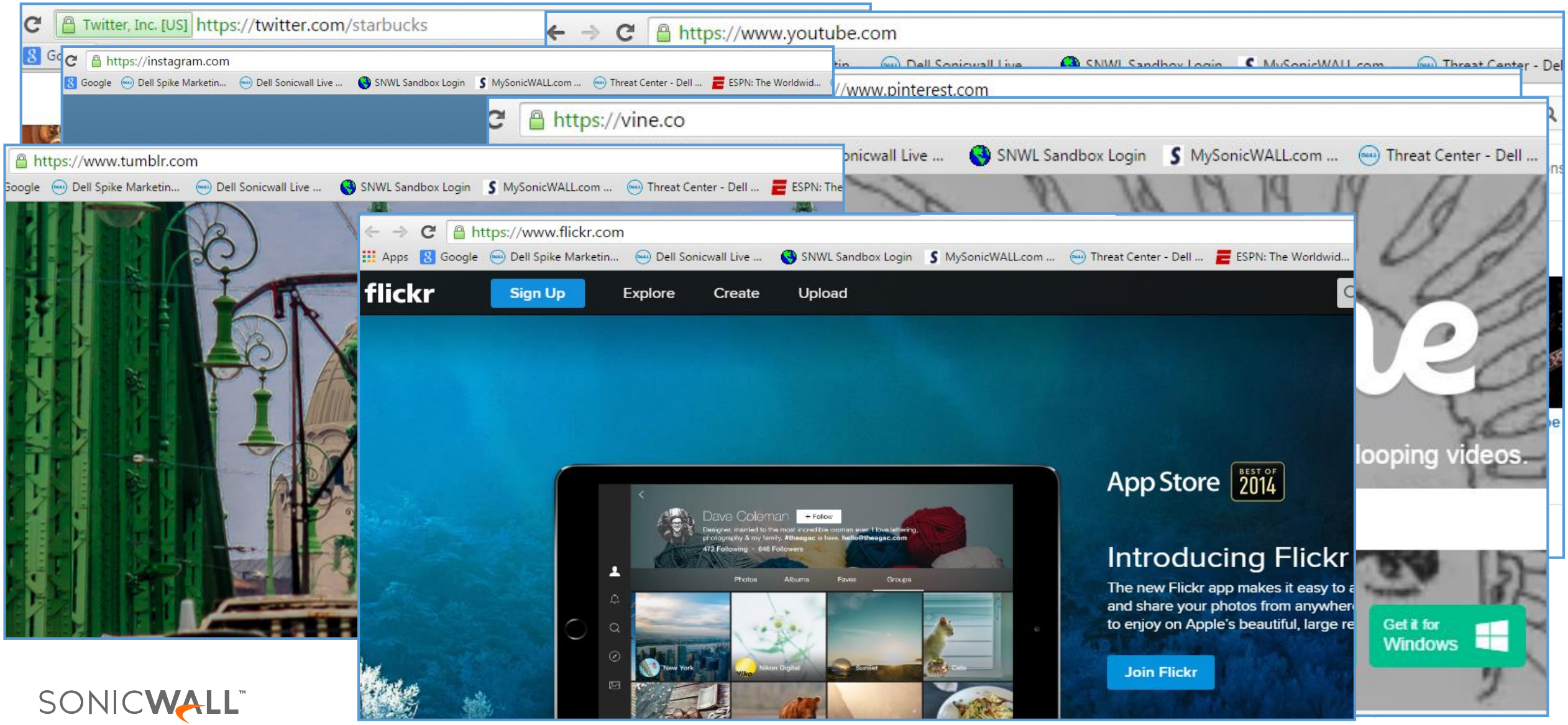
DELL EMC

¿Estás inspeccionando el tráfico HTTPS actualmente?

- ❑ Si
- ❑ No
- ❑ No estoy seguro…

© Copyright SonicWall

USERS' WEB SESSIONS ARE LARGELY ENCRYPTED WITH HTTPS

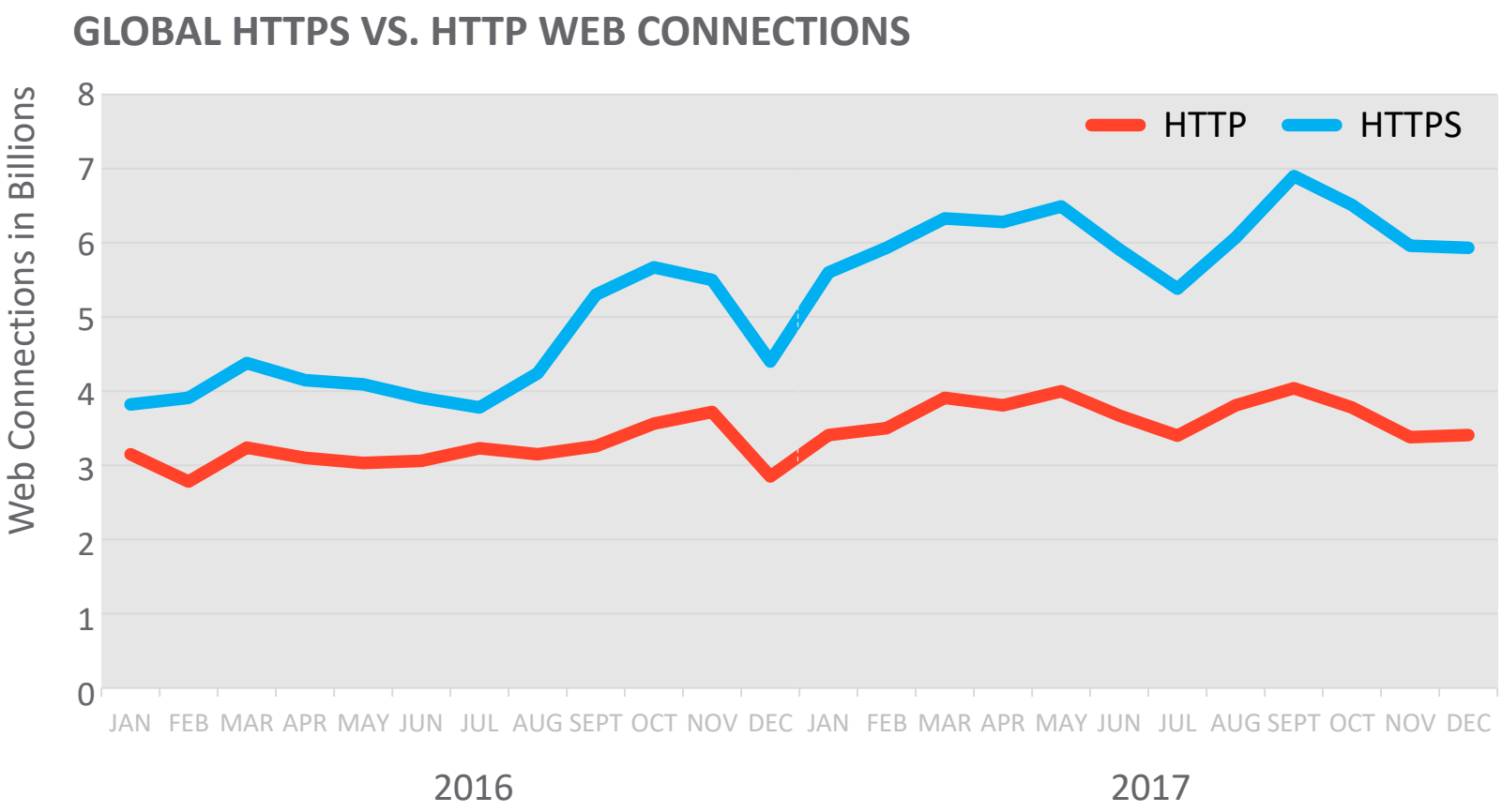


SONICWALL™

INCREMENTO EN EL USO DE SSL/TLS

...de las conexiones web fueron encriptadas con SSL/TLS en 2017.

24%
Crecimiento sobre 2016



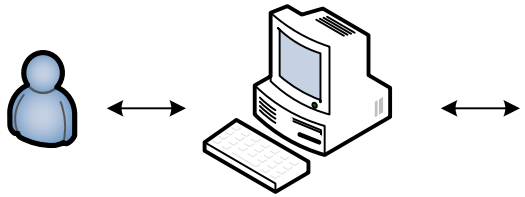
SONICWALL™

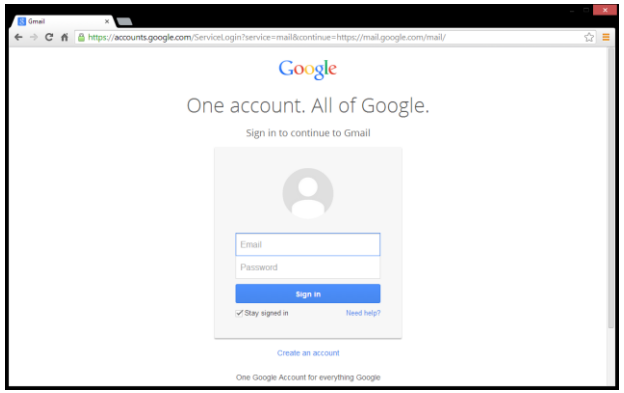
© Copyright SonicWall

DPI-SSL Awareness & Threat Prevention

Imaginemos esto…

Un usuario de la red, utiliza su PC corporativo para chequear su email. Accede a su cuenta de email PRIVADO desde un navegador…

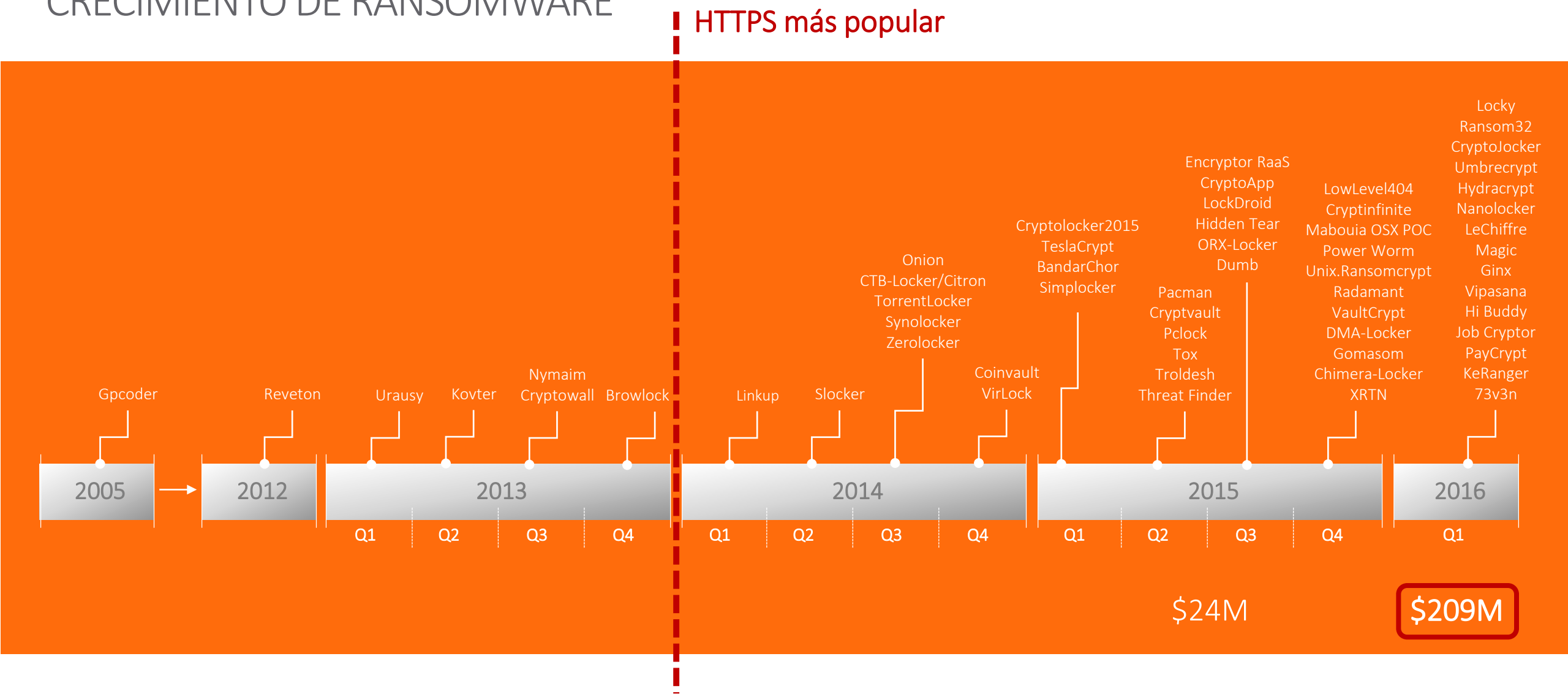




El usuario abre un email de una persona que conoce y en la que confía: un amigo. Ese amigo le remite una serie de bromas en un documento PDF adjunto…El usuario abre el adjunto…

Sin saberlo, accede a un fichero infectado que contiene un Virus Exploit ZeuS que se descarga de Ransomware…

CRECIMIENTO DE RANSOMWARE

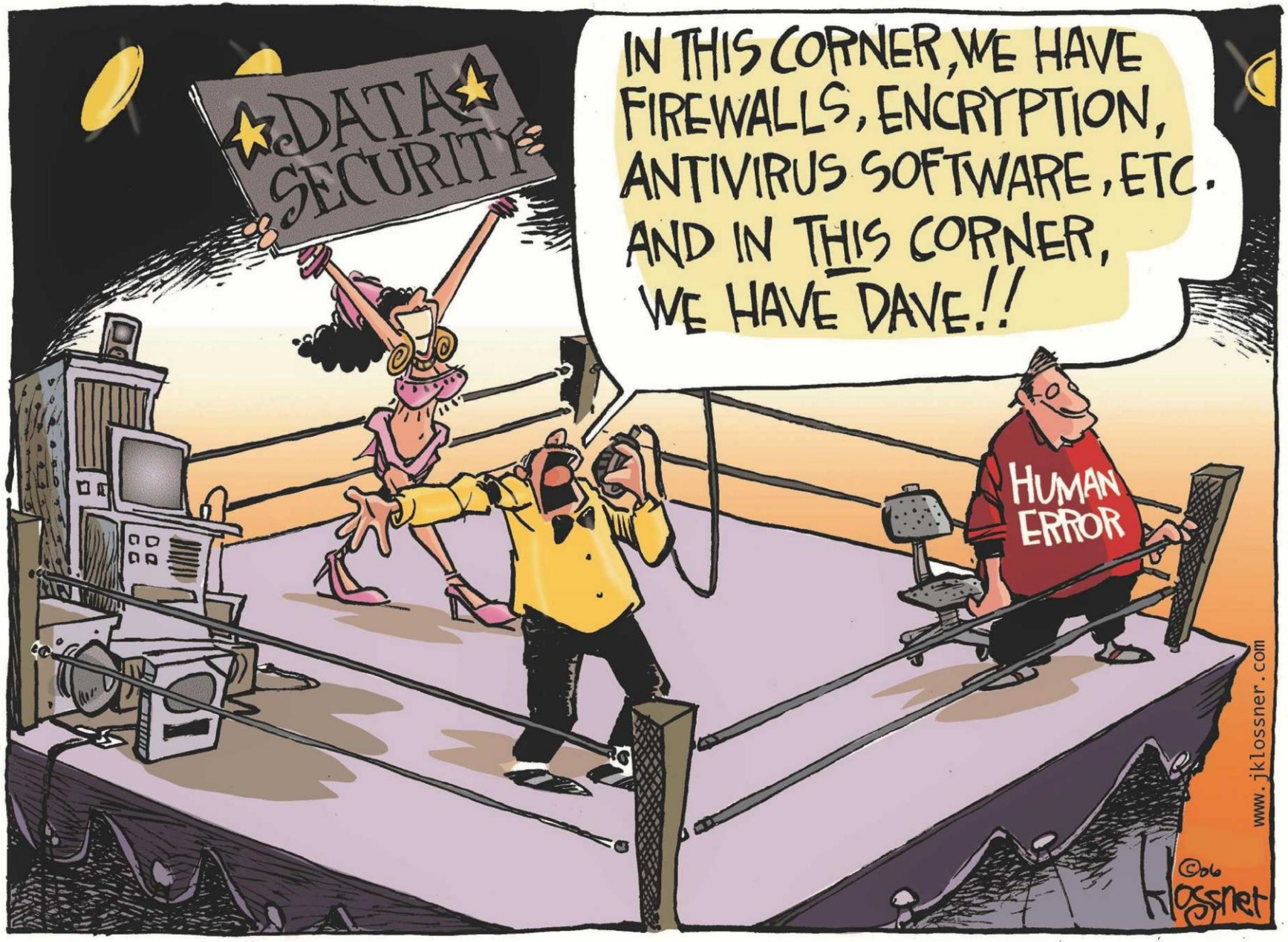


SONICWALL™

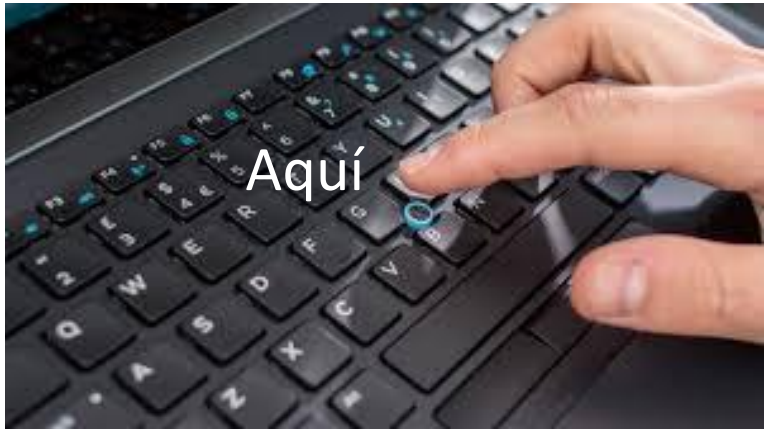
© Copyright SonicWall

Estrategia de defensa de Ransomware

SONICWALL



La ciberseguridad empieza...



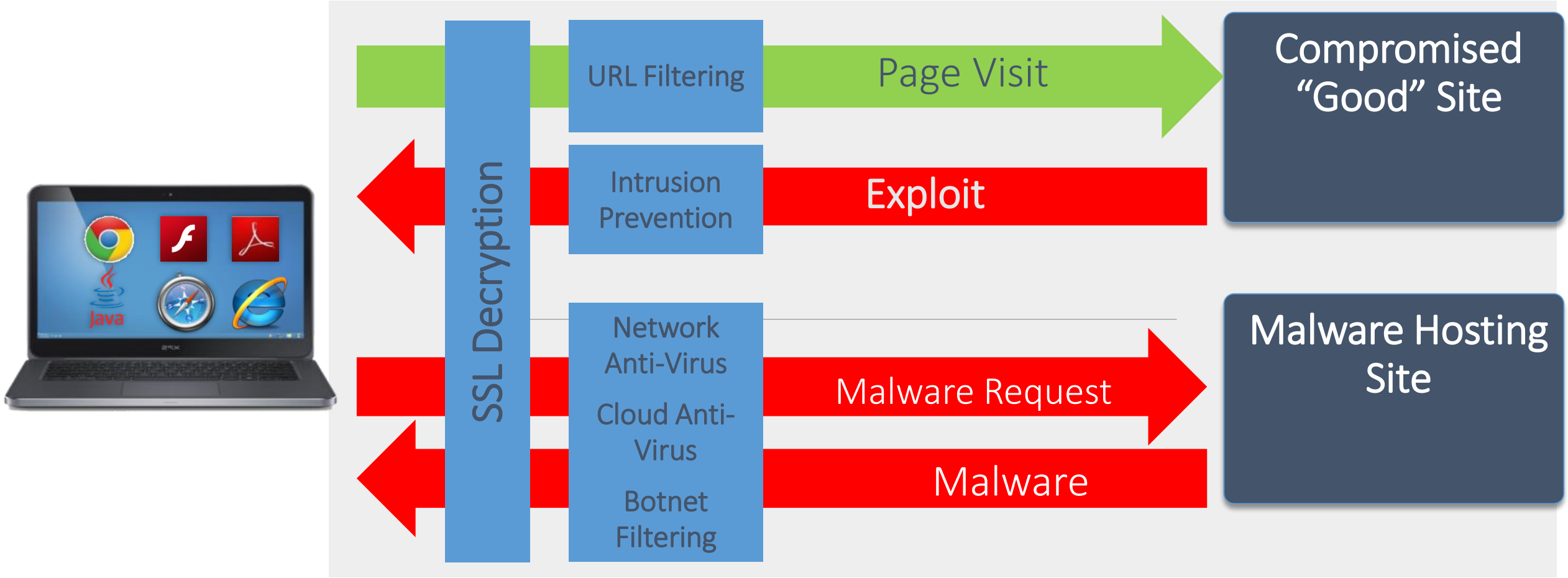
SONICWALL™

Seguridad basada en Capas

- El mejor enfoque es utilizar una defensa de múltiples capas:
  - Antispam
  - User Trust
  - Antivirus
  - IDS/IPS
  - Web Filtering
  - Anti-Botnet
  - DPI-SSL Inspection
  - Application Control
  - Sandboxing

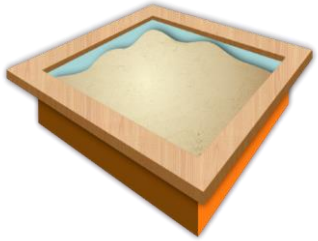
- Cada capa opera en una etapa diferente del ataque.
- Todas las capas deben ser traspasadas para que el ataque tenga éxito.

Cómo ocurre la puesta en peligro…

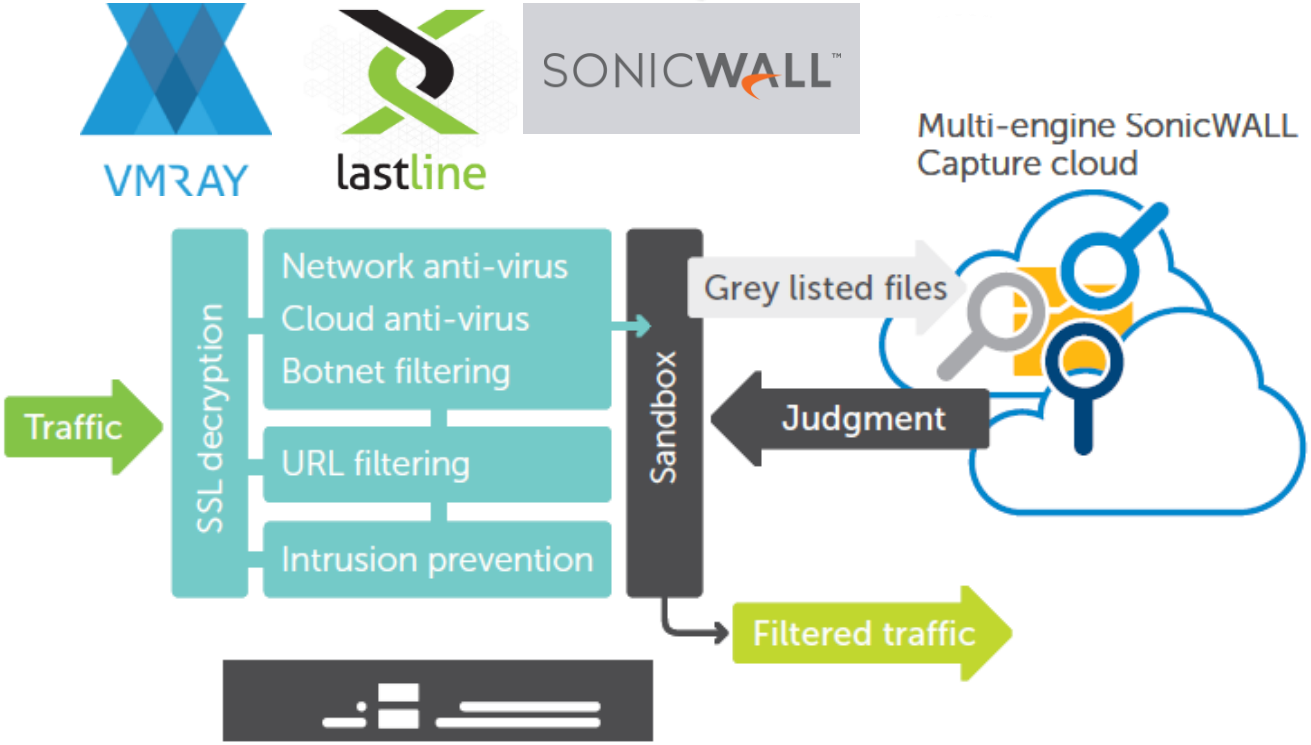


SonicWALL Capture
Advanced Threat Protection Service

Servicio Cloud que detecta y bloquea amenazas zero-day en el gateway



- Motor múltiple de sandbox que detecta más amenazas que una única tecnología
- Amplio análisis de tipos de archivos y Sistemas Operativos soportados
- Bloquea en el gateway hasta tener un veredicto
- Distribuimos firmas de forma rápida en el resto de dispositivos
- Informes y alertas



TZ SOHO – TZ600

NSA 2600 – 6600

SuperMassive 9200-9600

SONICWALL

© Copyright SonicWall

The Capture Client Architecture

SONICWALL | CAPTURE CLOUD PLATFORM

CAPTURE ATP SANDBOX

MANAGEMENT, REPORTING & ANALYTICS

Network Security Platforms

TZ, NSA, SM (NSa)

SonicWall Capture Client Platform					
AV Enforce & Manage	DPI-SSL Mgmt.	Capture ATP lookup	Content Filtering	VPN Client	Future Services
Machine-learning powered Next-Gen AV Technology					

SentinelOne

SONICWALL

¿QUIÉN ES SONICWALL Y QUÉ OFRECE?

Por qué SonicWall…

1 Millón+
redes protegidas

500,000+
organizaciones

3 Million+
Firewalls entregados

SONICWALL™

© Copyright SonicWall

SONICWALL CAPTURE LABS THREAT NETWORK

1M+
Sensors

200+
Countries & Territories

24x7 x365
Monitoring

< 24 Hr.
Response to 0-Day Vulnerabilities

200K+
Malware Samples Collected Daily

200K+
Malicious Events Analyzed Daily

Los datos para el Informe anual de amenazas de SonicWall de 2018 han sido recolectados de la “SonicWall Capture Threat Network”, que recoge información de dispositivos y recursos repartidos por todo el mundo.

SONICWALL™

© Copyright SonicWall

/ clientes /

DELL
RaceTrac
MOVEMENTMORTGAGE
Peter Piper PIZZA
UK UNIVERSITY OF KENTUCKY
USF UNIVERSITY OF SOUTH FLORIDA
SOUTH TEXAS COLLEGE
TEXAS A&M UNIVERSITY
Regio College
ASHRAM COLLEGE
ROC deLeijgraaf
THE SCHOOL DISTRICT PALM BEACH COUNTY
GRAFISCH LYCEUM
ROTTERDAM
PINELLAS COUNTY SCHOOLS
THE PATRÓN SPIRITS COMPANY
Pizza Hut
Radboud Universiteit
ELDE X college
GLENTEL
Wendy's
CARDENAS
LA PERLA
PALM BEACH TAN
SAN BERNARDINO COUNTY SUPERINTENDENT OF SCHOOLS
elzendaalcollege
Manor Lakes College
Walton COUNTY SCHOOL DISTRICT
UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG
Saint Paul PUBLIC SCHOOLS
Dunamare
TUSKEGEE UNIVERSITY
SportClips HAIRCUTS
1800 CONTACTS
LETTUCE ENTERTAIN YOU RESTAURANTS
Onderwijsgroep Noord
Seminole County Public Schools
UNISA
FEED THE DAY corner bakery CAFE
ACE Hardware
Arby's
CAR·TOYS A better way to go.
MARAVEST
Osceola County School District
CEDARVILLE UNIVERSITY
Rythovius College
FLORIDA DEPARTMENT OF EDUCATION fldoe.org
Lauwers College
BURGER KING
Jacksons
Hall County Schools Character · Competency · Rigor
wellantcollege
cog Christelijke Onderwijs Groep
Graafschap College
FASTRIP
Mi Cocina COMIDA TEX-MEX
Sci-Bono Discovery Centre
deKempel Hogeschool
THE COLLEGE AT OLD WESTBURY STATE UNIVERSITY OF NEW YORK
MONASH SOUTH AFRICA
Montessori Scholengemeenschap Amsterdam
DEL TACO
UNITED COLORS OF BENETTON.
Massage Envy
ROSS Medical Education Center
FAU FLORIDA ATLANTIC UNIVERSITY
Vechtdal College
greijdanus
Aventus
USciences University of the Sciences
SONICWALL

Dropbox G Suite Office 365 box

SONICWALL | CAPTURE CLOUD PLATFORM

FW • IPS • ATP • DPI TLS • ANTI-MALWARE • CASB • ANTI-PHISHING • URL FILTERING • WAF

THREAT PREVENTION | MANAGEMENT | REPORTING / ANALYTICS

Network Security Platforms

SMB, DC, MSP, Distributed Enterprise, EDU, Fed

WiFi

SMB, MSSP

Mobile Endpoints

SMB, MSSP

Email

Cloud

IoT

SONICCORE

SONICWALL

SONICWALL

GRACIAS!

Eduardo Brenes

ebrenes@sonicwall.com

Valores diferenciales de SonicWall

- Seguridad Activa: **GRID Capture Network**
- **DPI SSL**
- **Sandboxing Multi motor**
- **Filtrado WEB**
- Consola de Gestión Global: **GMS**
- **Integración con Dell EMC Networking**
- Ratio precio / rendimiento

SONICWALL™