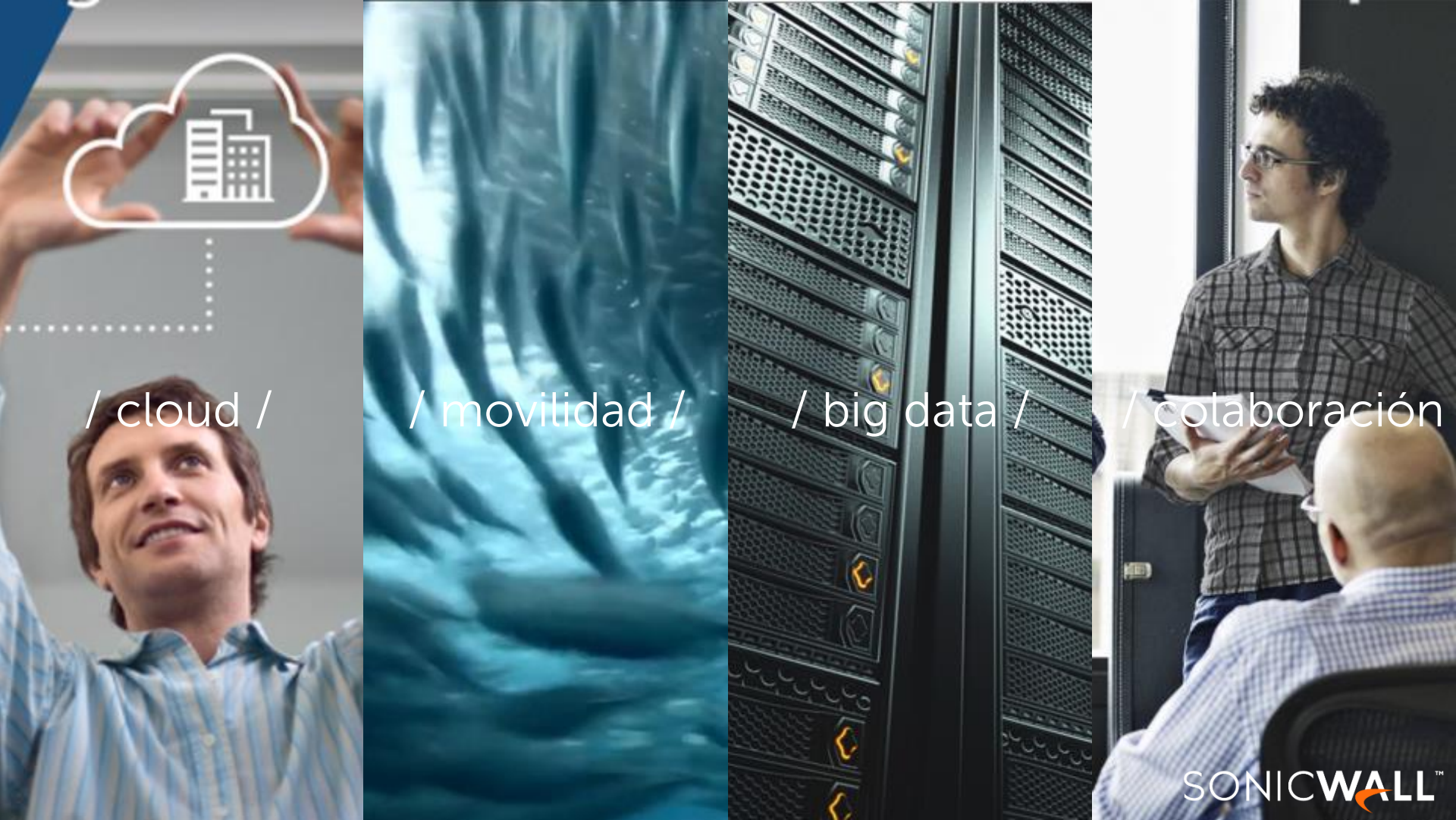
Lic. Marcelo E. Rey
Sales Engineer SoLA
mrey@sonicwall.com

¿En que pensamos cuando escuchamos Ciudades Inteligentes?

SONICWALL™

Ciudades Inteligentes


/ cloud /
/ movilidad /
/ big data /
/ colaboración
SONICWALL™


Actualmente, hay cerca de 9 billones de dispositivos conectados a Internet
En el 2020, Habrá mas de 50 Billones
SONICWALL™

SONICWALL™

THE INTERNET of THINGS

https://www.theguardian.com/technology/2015/mar/11/internet-of-things-hacked-online-perils-future

SONICWALL™

Dispositivos IoT en el hogar – **¿estan seguros?**

Your TV might be watching you

CNNMoney

By Erica Fink and Laurie Segall @CNNTech August 1, 2013: 11:32 AM ET

"Cualquiera que diga que sus sistemas son in-hackeables esta equivocado"

Kashmir Hill, Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide

+ Follow (1,810)

TECH | 8/27/2013 @ 3:47 PM | 23,539 views

'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users

Los consumidores deben segurizar y monitorear las redes hogareñas

CNET › Security › Belkin WeMo smart home networks in danger of hacks

Belkin WeMo smart home networks in danger of hacks

Researchers warn that more than 500,000 home automation devices have vulnerabilities that would allow attackers to remotely take control of thermostats, lighting, sprinkler systems, and more.

by Dara Kerr @darakerr / February 18, 2014 6:10 PM PST

CNET › Security › FTC and TrendNet settle claim over hacked security cameras

FTC and TrendNet settle claim over hacked security cameras

The camera maker settles a claim after hundreds of its home security cameras were hacked and videos of babies sleeping and children playing were published on the Web.

by Dara Kerr @darakerr / September 4, 2013 6:30 PM PDT

Tus Usuarios de IT son usuarios de IoT.
¿Puedes confiar en tus usuarios?

SONICWALL

Dispositivos IoT para llevar – **¿están seguros?**

Google Glass can be hacked via JavaScript code due to security flaw

Posted: 07 Feb 2014, 08:25, by Peter K.

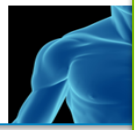
¿Qué tipo de datos recopila su dispositivo móvil (wearable)?

Eric Basu, Contributor
I offer a military perspective on entrepreneurship & govt contracting

ENTREPRENEURS | 8/03/2013 @ 8:08PM | 10,321 views

Hacking Insulin Pumps And Other Medical Devices From Black Hat

One of the briefings at Black Hat this year was a session on how vulnerable medical devices are to cyber attack, given by Jay Radcliff. This was part of our company's coverage of Black Hat and Defcon highlights sent via social media. Although the actual



1/15/2014 5:15 PM ET | By Holly Ellyatt, CNBC

CNBC

Car hacking: The next big cybercrime?

As the in-car computers pick up more steam, keep in mind that more technology often means more ways for crooks to get you.

Fiat Chrysler recalls 1.4 million cars after Jeep hack

Jeep's Grand Cherokee is one of the recalled cars

El WiFi del auto tiene las mismas vulnerabilidades de seguridad que los WiFi tradicionales

News

Pacemaker hack can deliver deadly 830-volt jolt

Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination

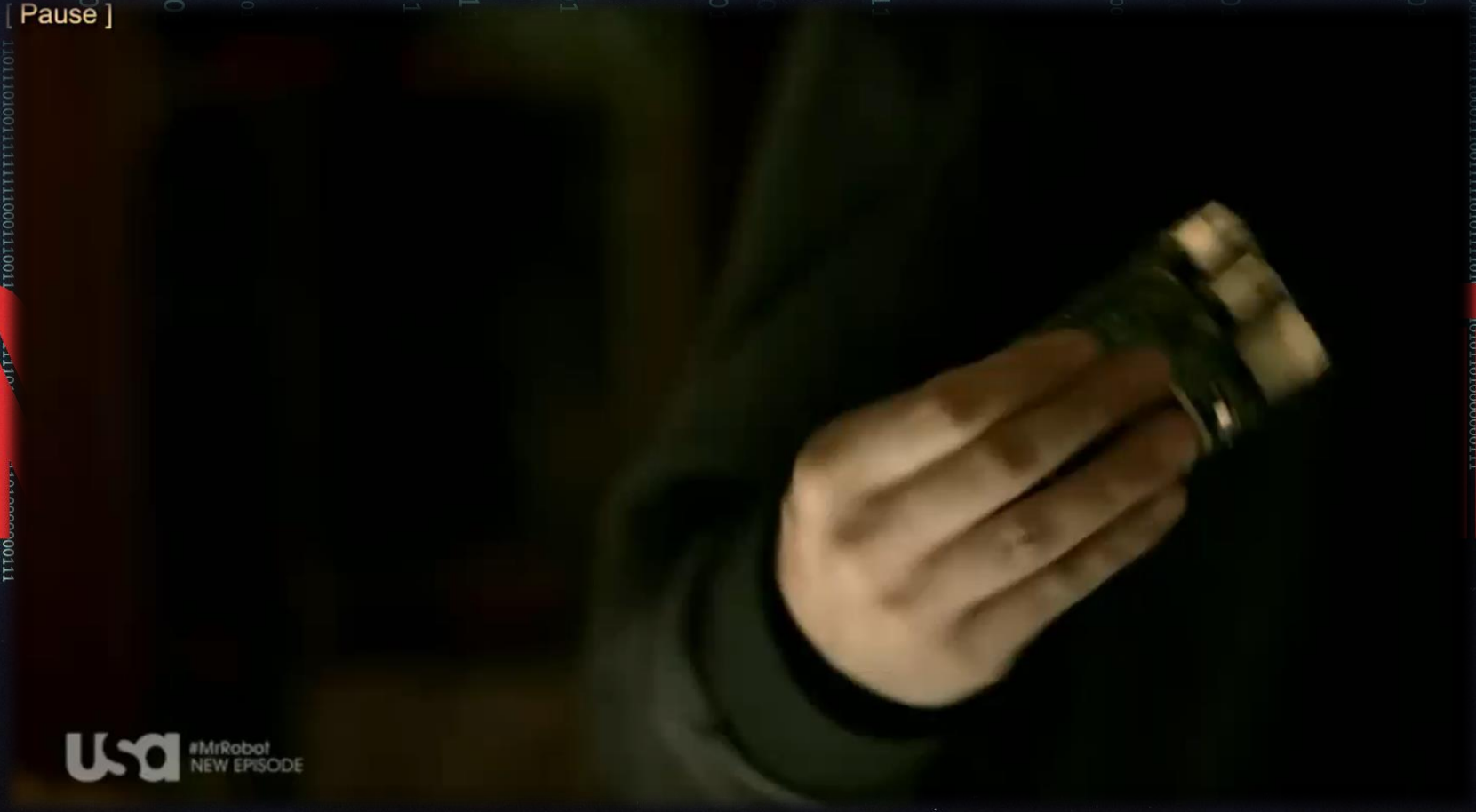
By Jeremy Kirk
October 17, 2012 12:40 AM ET

Los CSOs en las organizaciones con personas que viajan deben estar preocupados a cerca de estas vulnerabilidades ya que un atacante podría usarlos para accede a información de la compañía

SONICWALL

MR. ROBOT

[Pause]



El perímetro se extiende…
Diferentes puntos de entrada a la red

SONICWALL™

1

Modern-day Security

SONICWALL™

Stateful Packet Inspection

Deep Packet Inspection

Pregunta Numero #1

SONICWALL™

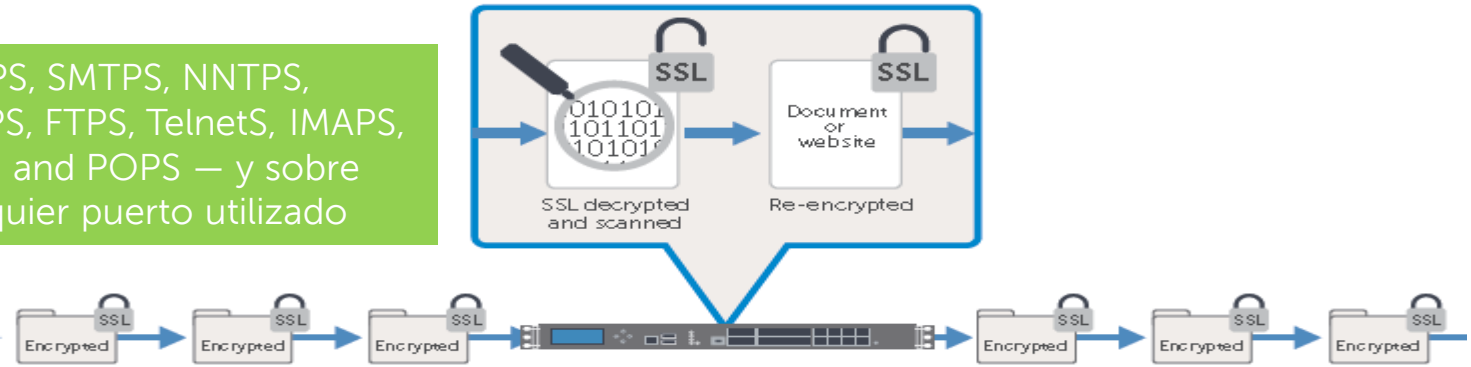
¿Quien esta analizando trafico HTTPS actualmente?

DPI-SSL - Inspección de SSL

Casi el 65% del trafico de las redes corporativas el encriptado usando SSL.

2015 Dell Security Threat Report

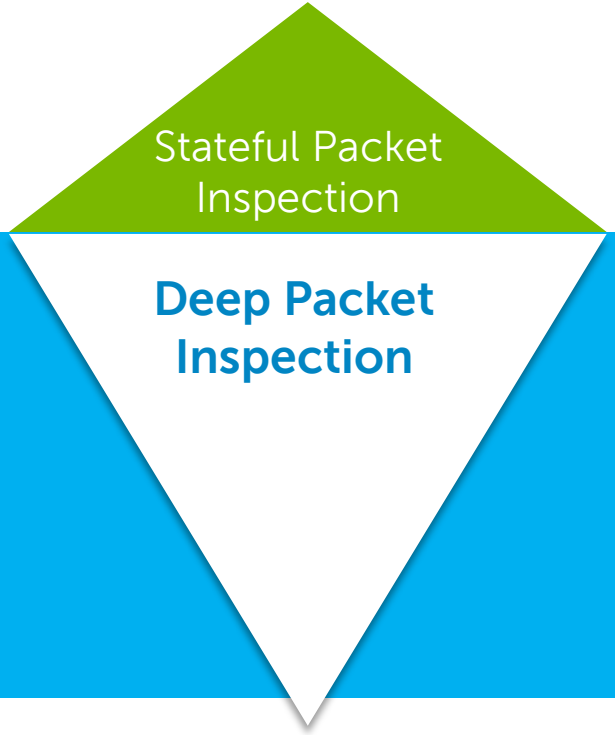
HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS, and POPS — y sobre cualquier puerto utilizado



Organizaciones que no inspeccionen trafico SSL, no pueden analizar aproximadamente 2/3 del trafico de red.

SONICWALL

Defensa-en-profundidad: Seguridad a través de **Deep Packet Inspection**



1. Stateful packet inspection
2. Prevención de Intrusiones (IPS)
3. Prevención de Amenazas (anti-virus/spyware)
4. Des-encripción de SSL
5. Identificación y control de aplicaciones
6. Gestión de anchos de banda (Traffic Shapping)
7. Filtros de Navegación
8. Y mucho mas…

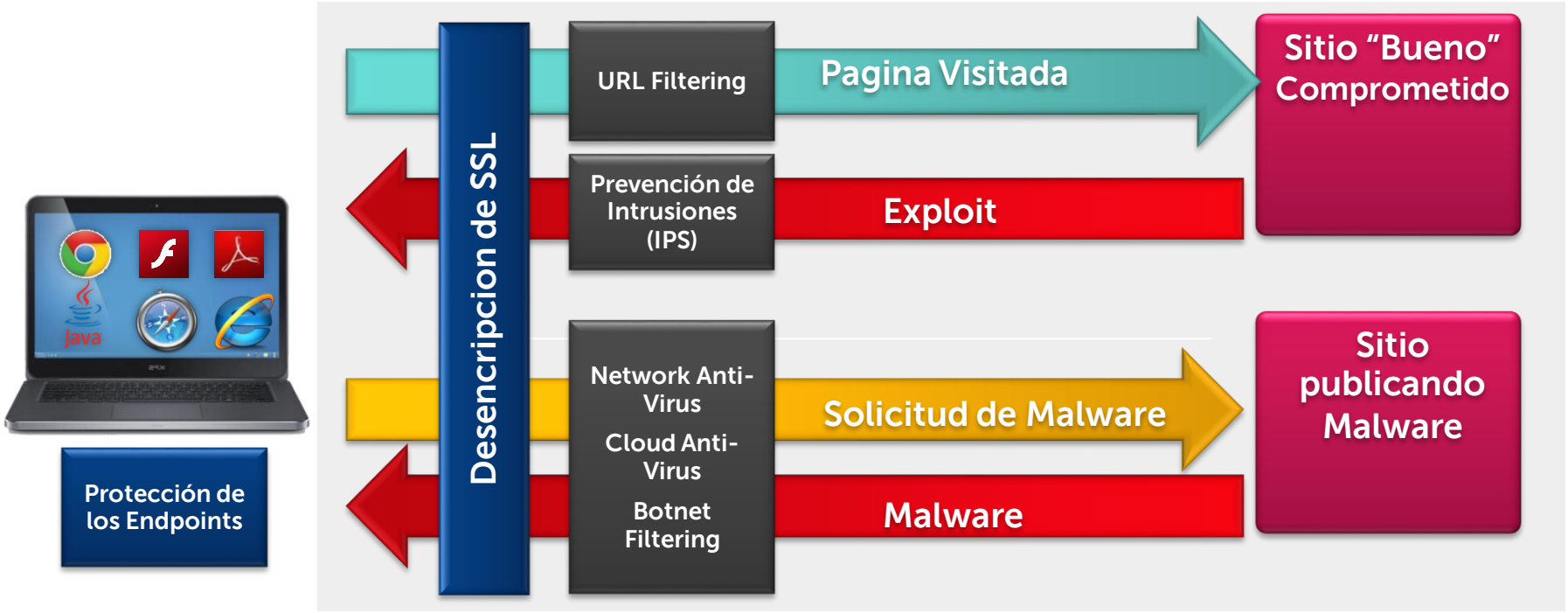
SONICWALL

Prevención de Intrusos, AntiVirus y Anti-spyware

SONICWALL™

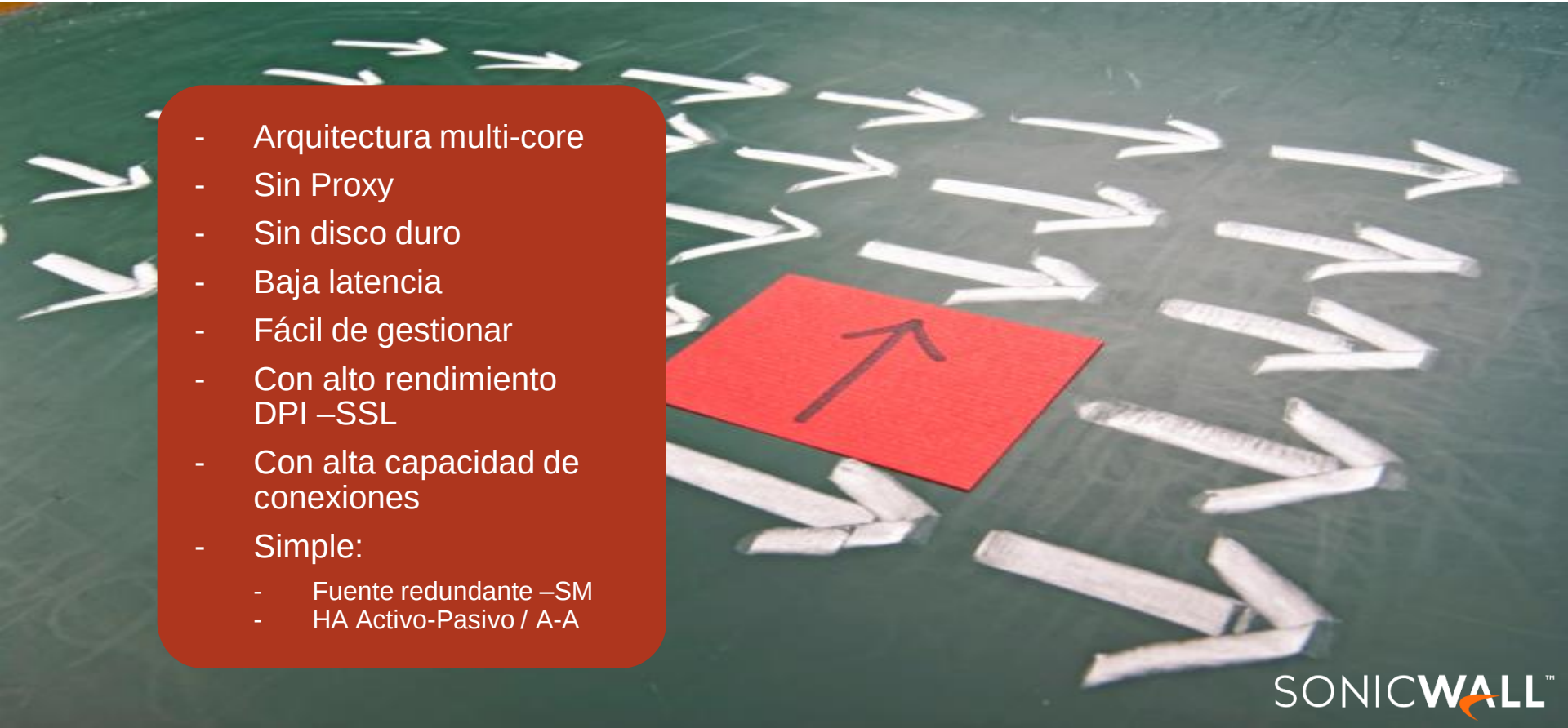
Next Generation Firewall (NGFW)

Interrumpir el ciclo del malware




/ evasión /
/ prevención de intrusiones /
SONICWALL™

Somos muy diferentes



- Arquitectura multi-core
- Sin Proxy
- Sin disco duro
- Baja latencia
- Fácil de gestionar
- Con alto rendimiento DPI –SSL
- Con alta capacidad de conexiones
- Simple:
  - Fuente redundante –SM
  - HA Activo-Pasivo / A-A

SONICWALL™

On Premise + Cloud – Protección Contra Malware

foo.exe

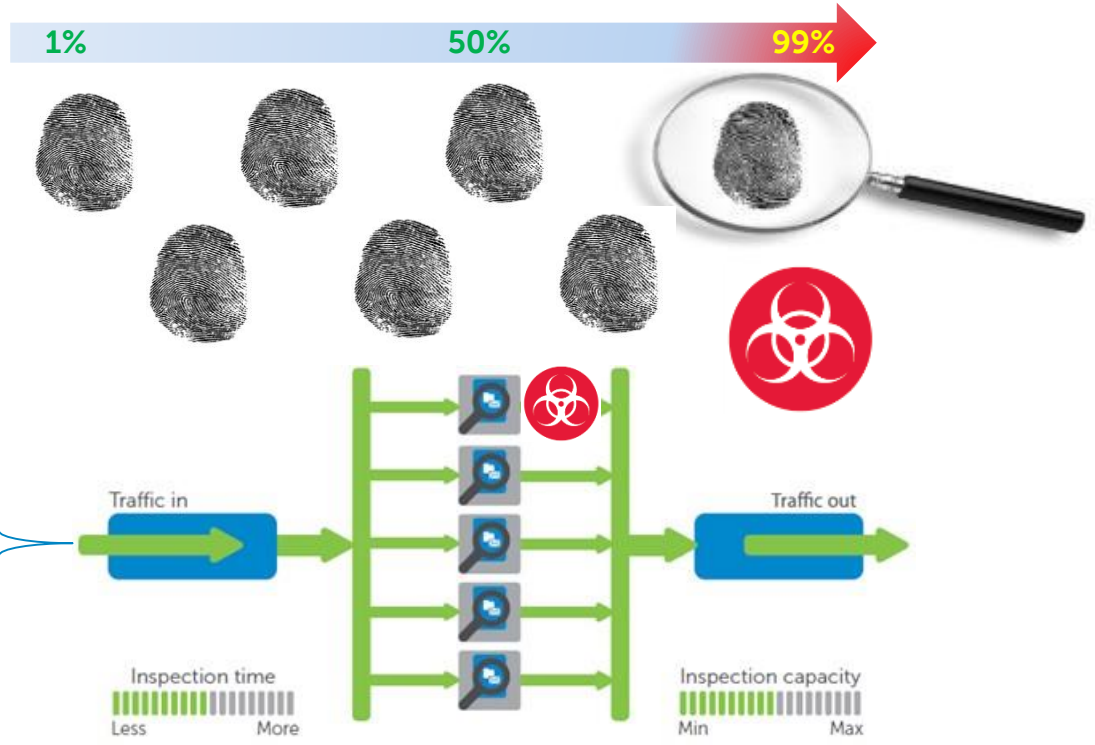
Protección contra malware basado en Red

Descarga Cancelada

99%

DROP

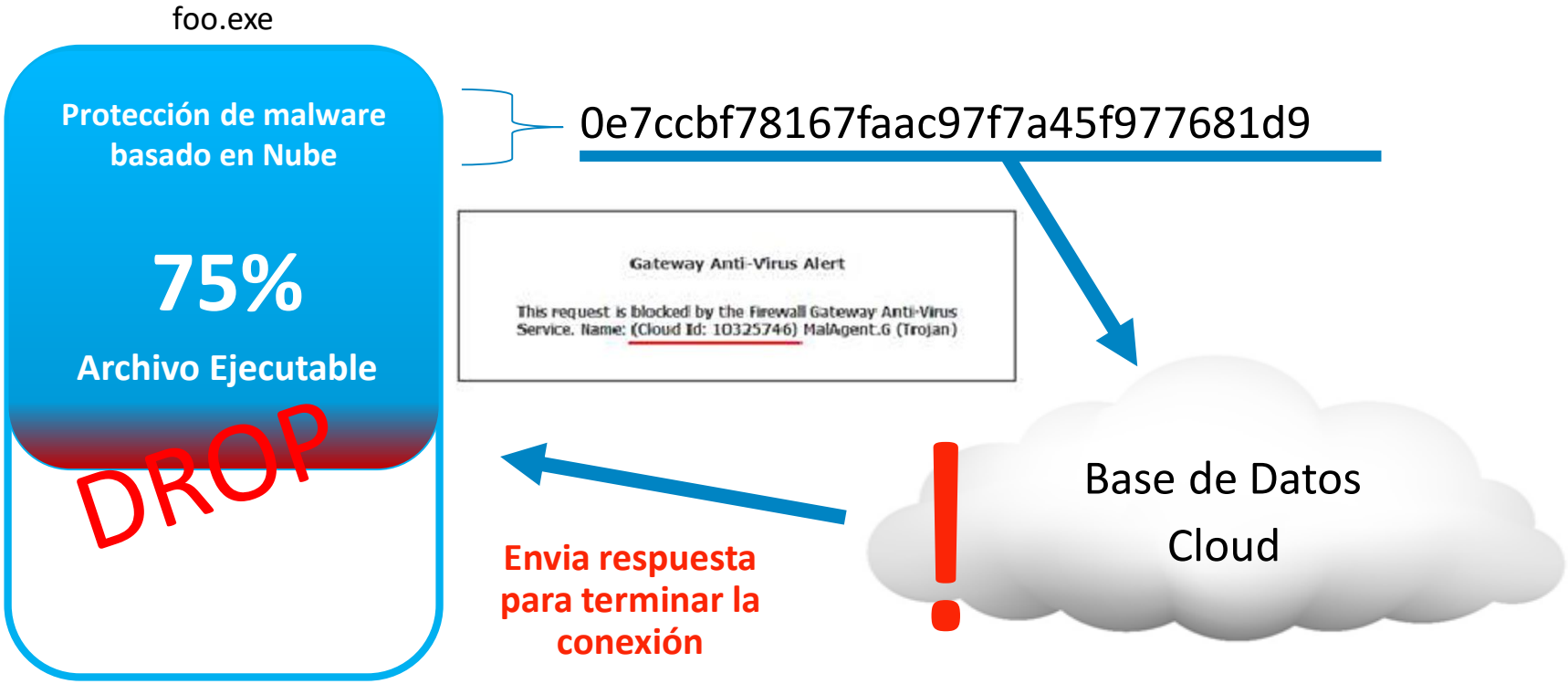
1% Descarga Restante



Envió de Alertas & Descartar Conexiones

SONICWALL

On Premise + Cloud – Protección Contra Malware



SONICWALL


MR. ROBOT
EXECUTIVE PRODUCER
SAM ESMAIL
usa
#MrRobot
NEW EPISODE
SONICWALL

Ransom ware...

SONICWALL™

Ransomware attacks on Hospitals put Patients at Risk

Sunday, April 03, 2016 Rakesh Krishnan

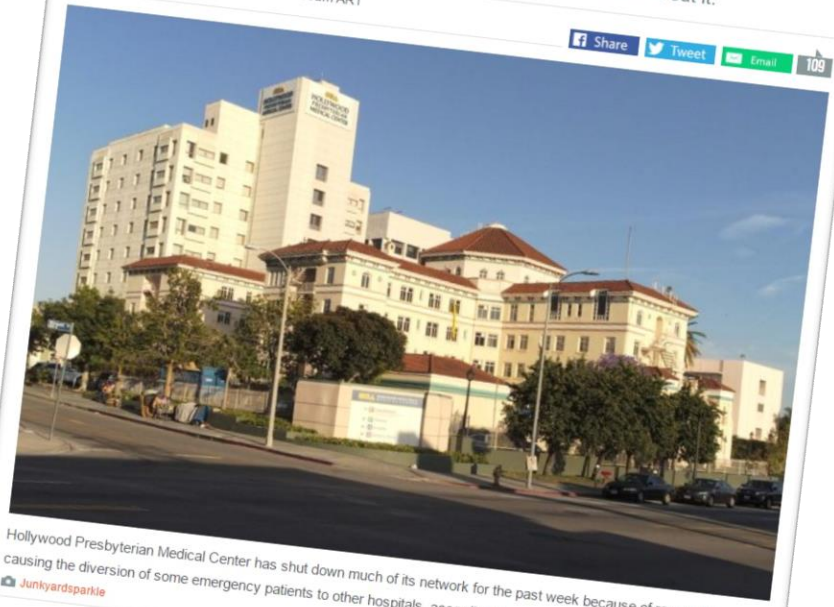
Just last week, the Federal Bureau of Investigation (FBI) issued an urgent "Flash" message to the businesses and organisations about the threat of **Samsam Ransomware**, but the ransomware has already wreaked havoc on some critical infrastructure.

MedStar, a non-profit group that runs 10 hospitals in the Baltimore and Washington area, was attacked with Samsam, also known as **Samas** and **MSIL**, last week, which encrypted sensitive data at the hospitals.

Patients diverted to other hospitals after ransomware locks down key software

Crypto-extortion increasingly targets bigger victims; most stay silent about it.

by **Sean Gallagher** - Feb 17, 2016 11:56am ART



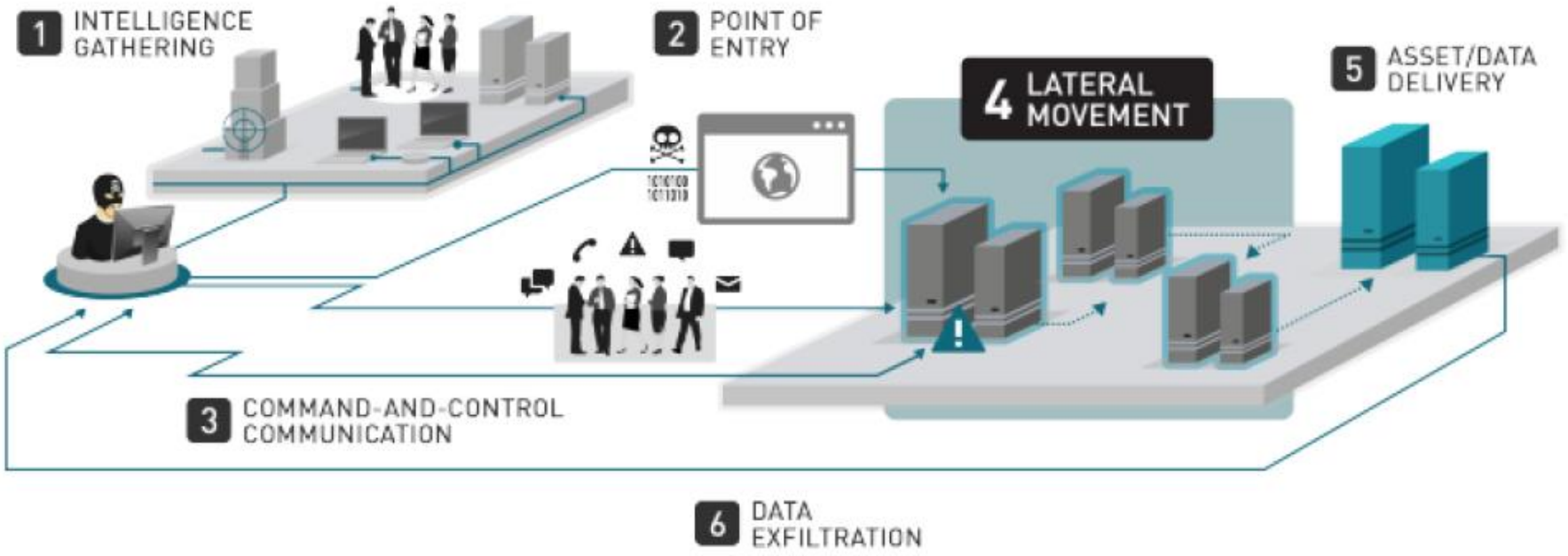
Hollywood Presbyterian Medical Center has shut down much of its network for the past week because of ransomware, causing the diversion of some emergency patients to other hospitals, according to sources at the hospital.

Junkyardsparkle

Hollywood Presbyterian Medical Center, a hospital in Los Angeles, is the victim of what officials describe as an ongoing cyberattack. A hospital spokesperson told Ars in a prepared statement that "patient care has not been affected" by the intrusion. And an executive of the hospital told reporters

http://thehackernews.com/2016/04/hospital-ransomware.html
http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/

Movimiento Lateral



Six Stages of an APT attack

SONICWALL

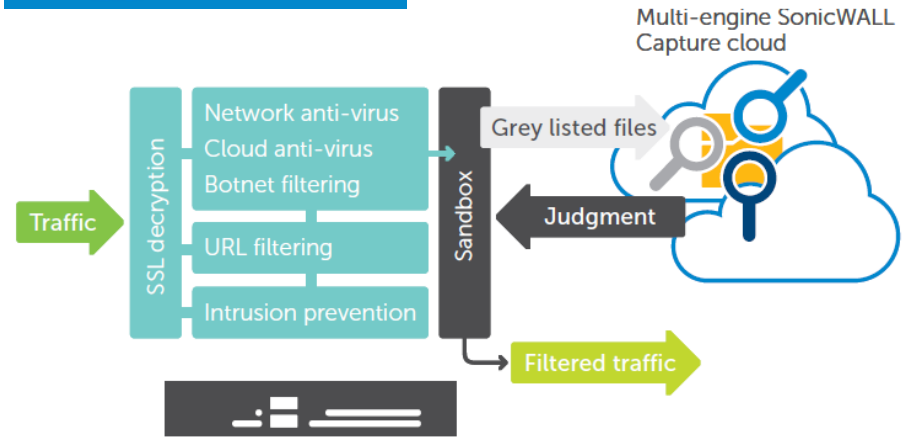
NEW!!! - Introducing SonicWALL Capture Advanced Threat Protection Service

Cloud service detects and blocks zero-day threats at the gateway

VMRAY lastline

SonicWALL

Mac OS X



Multi-engine advanced threat analysis detects more threats, can't be evaded

- Virtualized sandbox
- Full system emulation
- Hypervisor level analysis

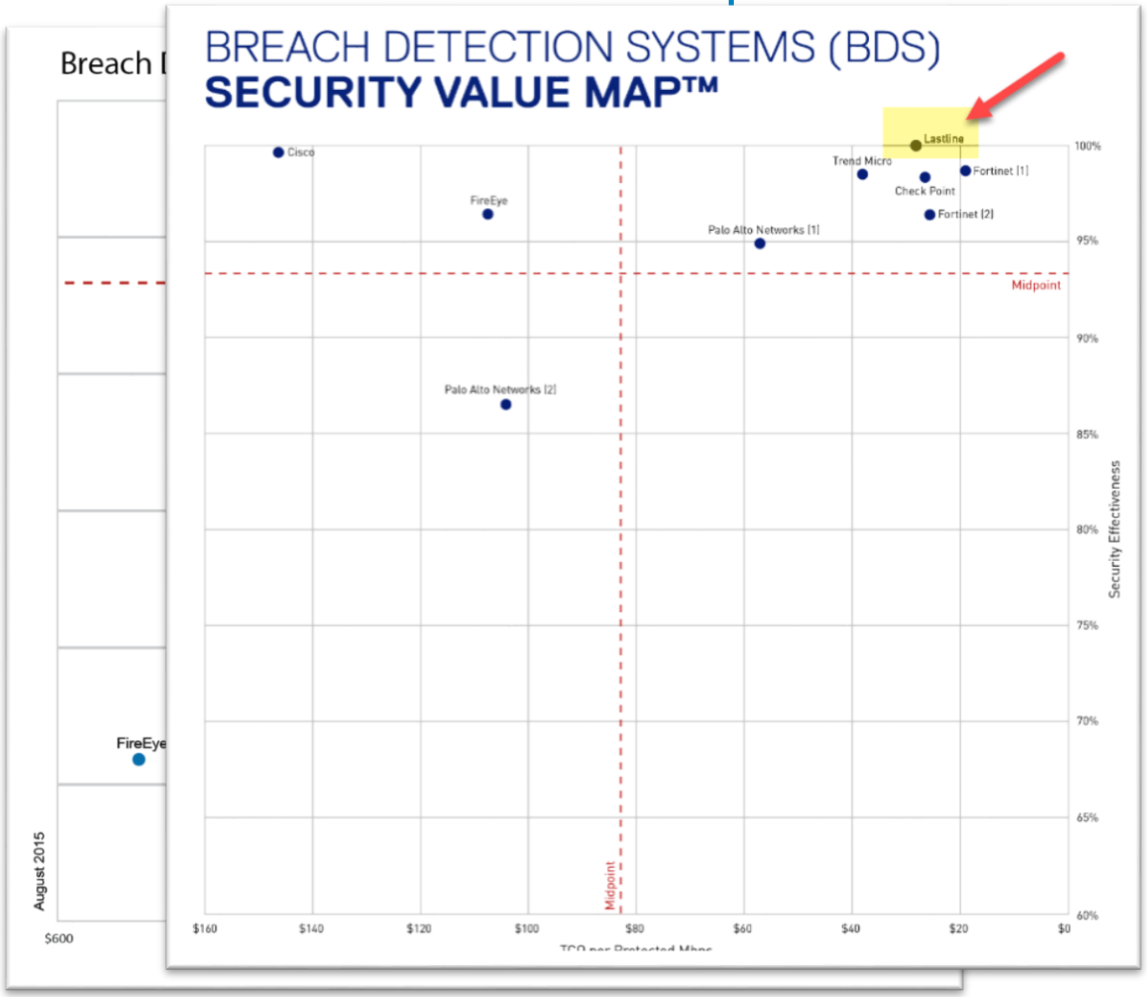
Broad file type and OS environment analysis

- PE, MS Office, PDF, archives, JAR, APK
- Windows, Android and Mac OS

Automated and manual file submission

SONICWALL

Posicionamiento Capture ATP



Sandbox líder en el mercado

NSS Labs RECOMMEND

2015 y 2016

http://landing.lastline.com/nss-2015

http://landing.lastline.com/nss-2016

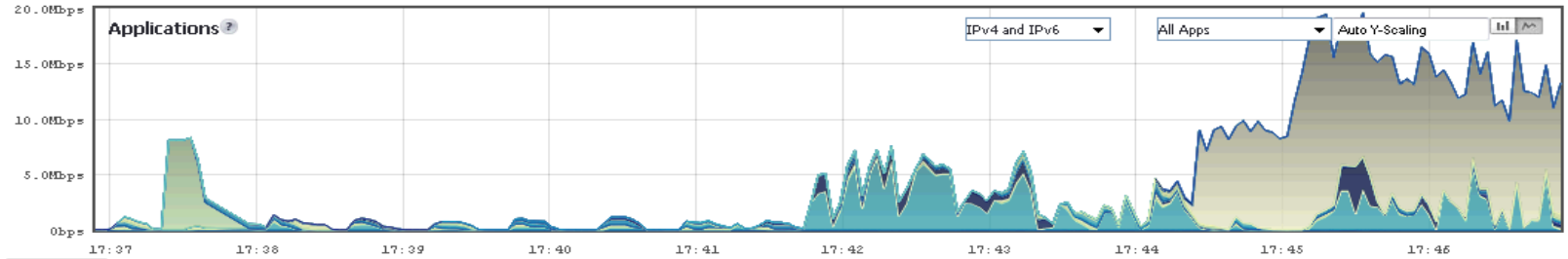
SONICWALL

Control de Aplicaciones

Real-Time Monitor

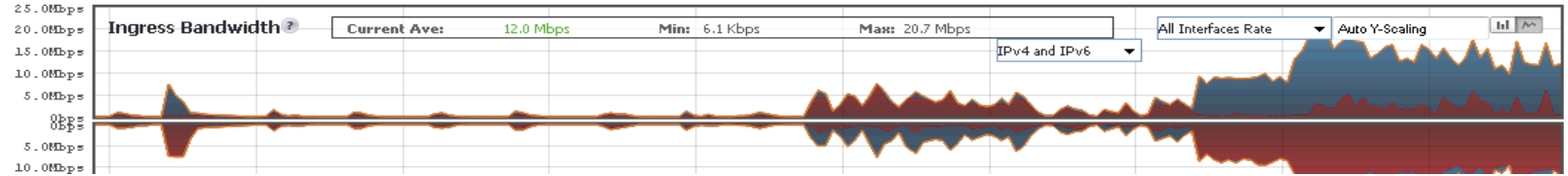
- Dashboard
  - Multi-Core Monitor
  - Real-Time Monitor
  - AppFlow Dash
  - AppFlow Monitor
  - AppFlow Reports
  - Threat Reports
  - User Monitor
  - BWM Monitor
  - Connection Monitor
  - Packet Monitor
  - Log Monitor
- System
- Network
- 3G/4G/Modem
- SonicPoint
- Firewall
- Firewall Settings
- DPI-SSL
- VoIP
- Anti-Spam
- VPN
- SSL VPN
- Virtual Assist
- Users
- High Availability
- Security Services
- WAN Acceleration
- AppFlow
- Log

Refresh every: 3 sec. View Range: 10 minutes Data Source: Local



Legends

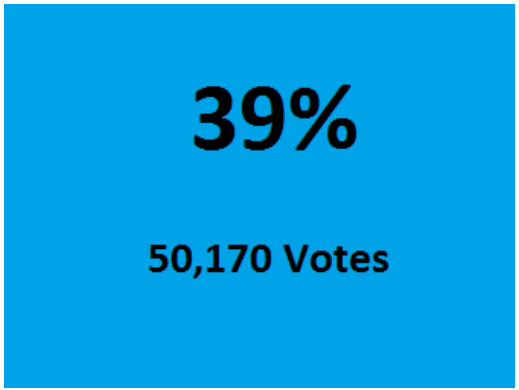
General Multicast	General DNS	Service NTP	General HTTPS MGMT	Microsoft Remote Desktop-436	Chart Beat-3763	Image-4239	HTTP-5147	DoubleClick-6261
SSL-5159	Facebook-6363	Facebook-6921	General HTTPS	General HTTP	Facebook-2822	Google-9379	DoubleClick-7900	DNS-4398
General IKE	Facebook-6985	OCSP-6908	Image-4254	Image-4243	DNS-4395	Site Scout-7883	ScoreCard Research-3990	IMR Worldwide-7023
YouTube-5727	Google Analytics-2226	Others	YouTube-9256	YouTube-9255	Chart Beat-3767	Betr Ad-7871	Shockwave Flash (SWF)-575	HTTP-5148
MediaMath-7892	Adsonar-7867	Facebook-2821	Google Analytics-7885	Google Safe Browsing-707	Google Safe Browsing-708	Adsafe Media-7910	Google-6015	DNS-6818
Service HTTPS Management	Encrypted Key Exchange-5	General LDAP	CIFS-5181	Service SMB	Service Kerberos TCP	Microsoft Netlogon-602	Microsoft RPC End Point Mapper-477	Service RPC Services (IANA)
Service DCE EndPoint	Service Terminal Services TCP	Atlas DMT-2228	Double Verify-7872	Serving-Sys-7864	General NETBIOS	DNS-5183	Google Analytics-5874	Aggregate Knowledge-7907
Google-6011	Image-8682	Google Analytics-704						



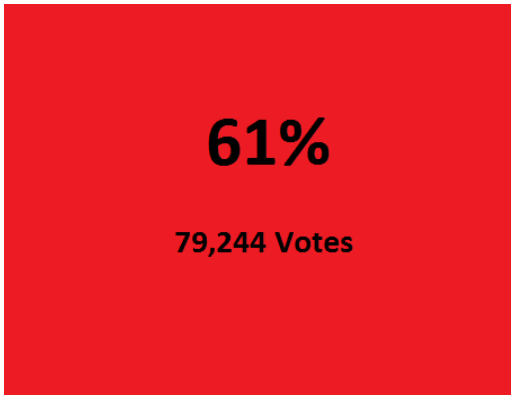
La importancia del control de navegación

- Respondan esta pregunta…. Cuantos de ustedes preferirían….

- Mostrar a sus amigos y familia su Historial de Internet



- Vivir cerca de un volcán activo

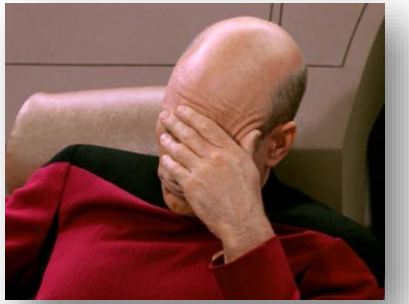


La importancia del control de navegación

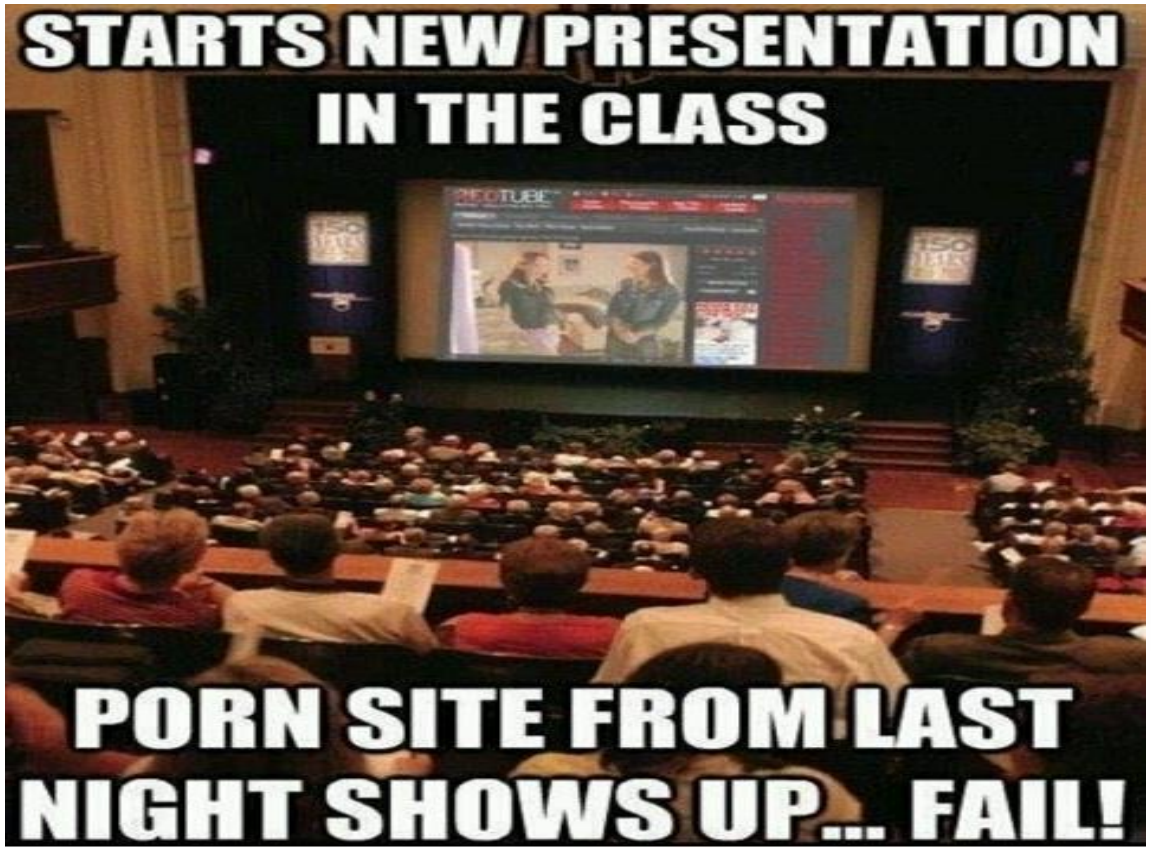
- Alguien esta viendo un sitio que probablemente no debería estar viendo.

La importancia del control de navegación

- Alguien esta viendo un sitio que probablemente no debería estar viendo.
- Alguien se ofende e inicia demandas contra el canal!.



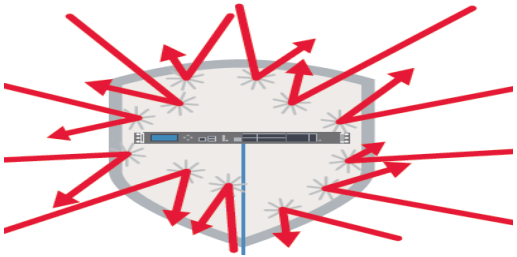
La importancia del control de navegación



Defensa-en-profundidad con múltiples capas de protección de amenazas

Defensa de los endpoints

- Firewall enforced Content Filtering
- Firewall enforced Anti-Virus & Anti-Spyware
- Secure Mobile Access
- Endpoint threat protection



Defensa del Perímetro

- Prevención de Intrusiones (IPS)
- Inspección de SSL
- Gateway + Cloud Malware Protection
- Content Filtering Service
- Application Intelligence, Control and Visualization
- Email Security

Continuous Countermeasure updates

- Threat Counter-intelligence

- Active participant in leading research organizations

SONICWALL™

Firewall Sandwich Design

Maximum DPI Connections

40M+
2.5M – 10M
375K – 1.25M
4K –200K

SMB / Distributed Enterprise

TZ Series

NSA Series

Branch/Campus

SuperMassive 9000 Series

Enterprise / Data Center

Carrier / ISP

SuperMassive E10000 Series

50 - 3000 Mbps

3,500 - 12,000 Mbps

40,000 – 100,000+ Mbps

Deep Packet Inspection Performance

SONICWALL

Convergencia de la seguridad y networking

Dell SonicWALL GMS

Gestion centralizada multi-sucursal

Dell NG-FW SonicWALL

Dell Networking X-Series

Access Points

Dell SonicWALL

Gestión Centralizada multi-punto

SONICWALL

Dell Secure Mobile Access (SMA)

Detección

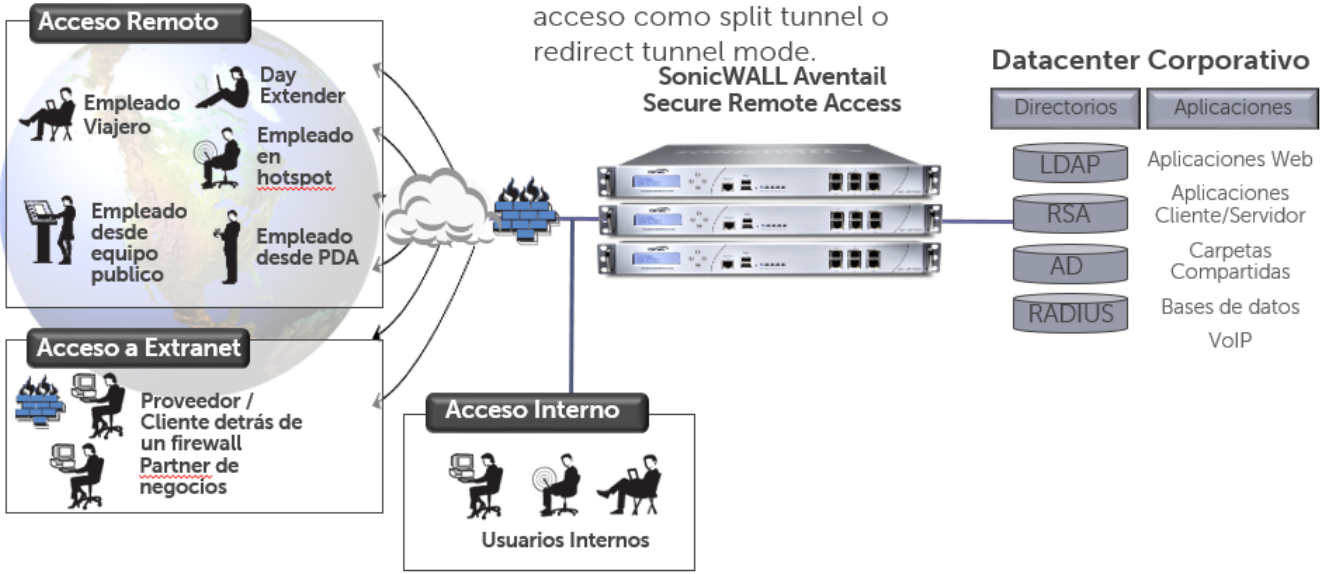
Control de seguridad en punto final.
Detecta la identidad y el estado de seguridad del dispositivo remoto

Conexión

Acceso a redes de forma segura.
Garantiza el acceso seguro y sencillo a todos los recursos de la red, definiendo perfiles de acceso como split tunnel o redirect tunnel mode.

Protección

Gestión Centralizada.
Refuerza el control del acceso de los equipos, permitiendo a los usuarios acceder únicamente a las aplicaciones autorizadas.



Multi-plataforma:

- Windows
- Linux
- Mac
- Dispositivos Móviles

SONICWALL

SMA - Acceso remoto desde equipos móviles

(BYOD - Bring Your Own Device)

Mobile Connect for iOS

Mobile connect for Android

- Cliente nativo para acceso remoto a través de túnel
- **Endpoint control**: Capacidad de validar al equipo remoto de acuerdo a:
  - Numero de IMEI
  - Detección de Jailbreak en Apple (IOS)
  - Detección de Rooted device (Android)
  - Control de Applicaciones
  - Per-App VPN

SONICWALL

SonicWALL Email Security

Protection

Spam, Virus, Phishing

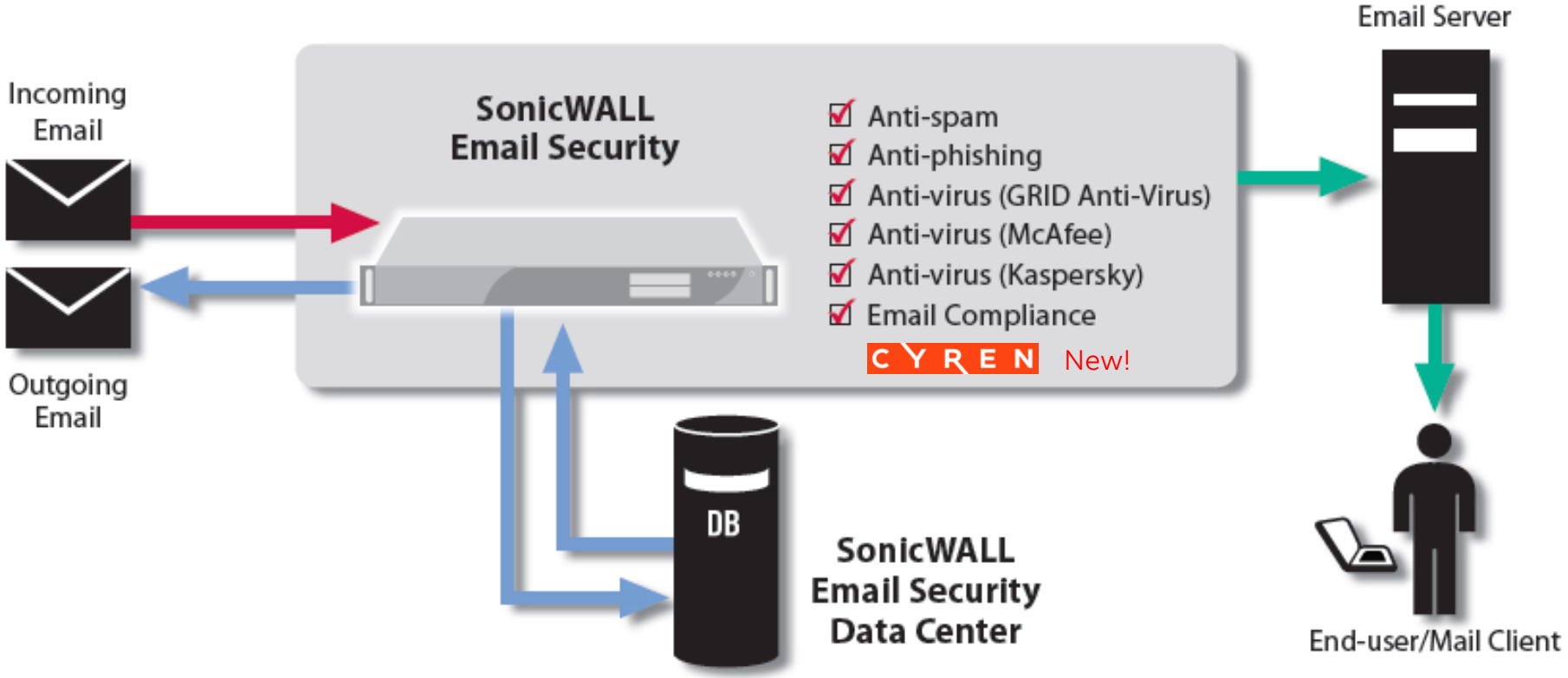
Compliance & Encryption

DMARC

Brand Protection

SONICWALL

SonicWall Email Security



¡¡¡Gracias!!!

¿Preguntas?

SONICWALL™

Lic. Marcelo E. Rey
Sales Engineer SoLA
mrey@sonicwall.com