

Pedro Xabier Alaña
pedroxabier  **sarenet**.es

Dpto. Comercial

Auditorías evolutivas de Seguridad

```
</div>
```

```
</div>
```

```
<Preview code={code} evalInContext={evalContext} />
```

```
</div>
```

```
<button type="button" />
```

```
Hide code
```

```
</button>
```

```
</div>
```

```
) : (
```

```
<button type="button" className={classes.showCode} />
```

```
Show code
```

```
</button>
```

```
)}
```

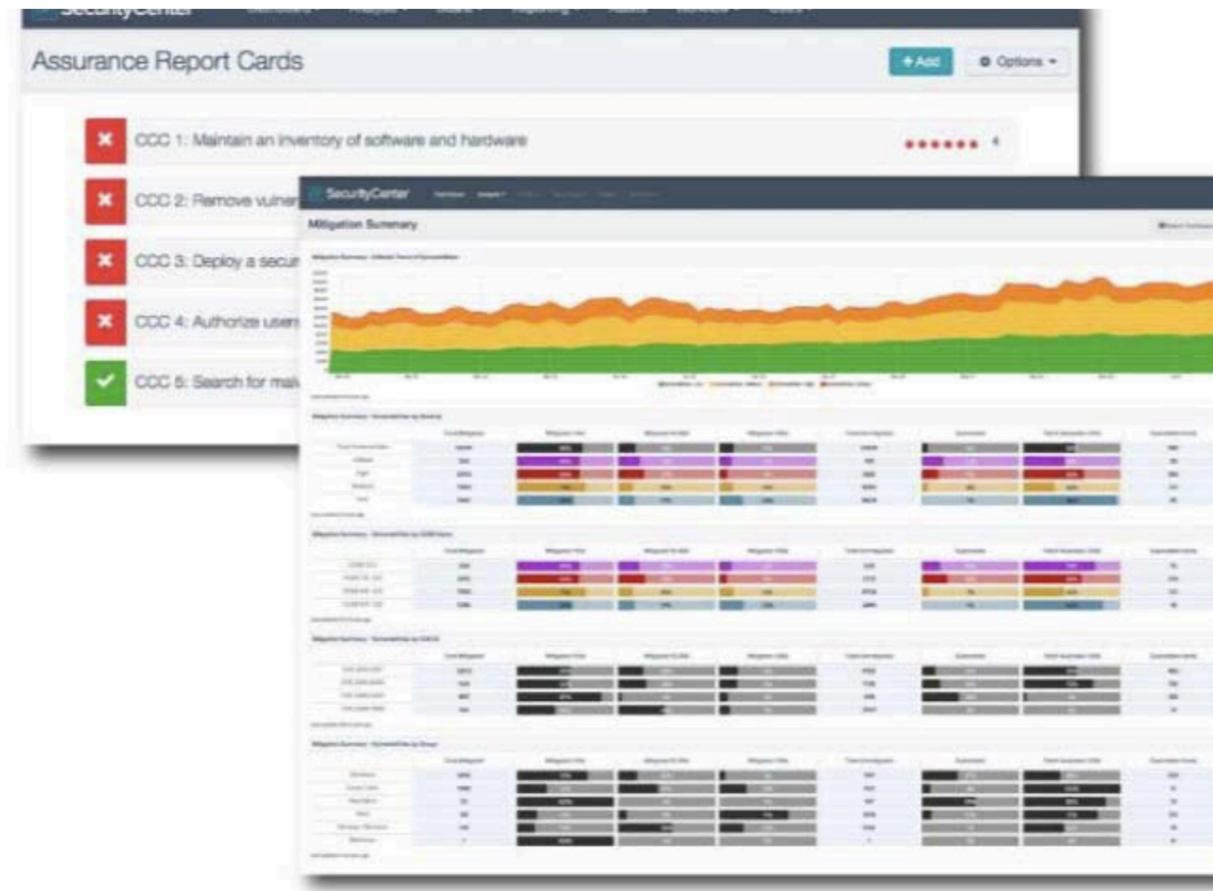
```
</div>
```

AUDITORÍAS EVOLUTIVAS DE SEGURIDAD

- **Tecnología Security Center de Tenable explotada desde el Data Center de Sarenet en Vizcaya por personal de seguridad propio**
- Acuerdo estratégico entre Tenable y Sarenet
- Complemento ideal de seguridad para aportar contexto global e información completa de ciberexposición (más allá de perímetro, red y puesto de trabajo o servidores)
- Más de 130000 plugins implementados
- Desarrollo amplio de API propia
- Control de vulnerabilidades y configuraciones (compliances con fabricantes)
- Sistema de escaneo continuo con histórico evolutivo de la reputación total de la infraestructura IT
- Escaneo publico desde el CPD de Sarenet y escaneo interno desde la red
- Escaneo masivos VS escaneo dirigidos
- Licencia anual por número de direcciones IP
- Permite rastreos pasivos o escaneo intrusivos

TENABLE SECUTIRY CENTER

Capacidades	
Gestión de vulnerabilidades centralizada con múltiples escáneres	✓
Clasificación dinámica de activos (servidor de correo, servidor web, etc.)	✓
Auditoría de configuración basada en políticas	✓
Detección de malware con inteligencia de amenazas integrada	✓
Paneles/informes predefinidos con alimentación automática de Tenable	✓
Respuesta ante incidentes con alertas, notificaciones y tickets configurables	✓
Assurance Report Cards (ARC)	✓



Tenable.sc proporciona análisis de vulnerabilidades, tendencias, informes y flujos de trabajo altamente personalizables para adaptarse a las necesidades de su programa de seguridad

BENEFICIOS PREGUNTAS CLAVE SUSTENTABLE SECURITY CENTER

Beneficios clave

¿Dónde estamos expuestos ?

- Identifica las debilidades al escanear los activos conectados a la red en busca de vulnerabilidades conocidas, configuraciones erróneas y malware
- Permite un seguimiento efectivo del cumplimiento de la política de seguridad implantada en la organización - "Assurance Report Cards" (ARC)

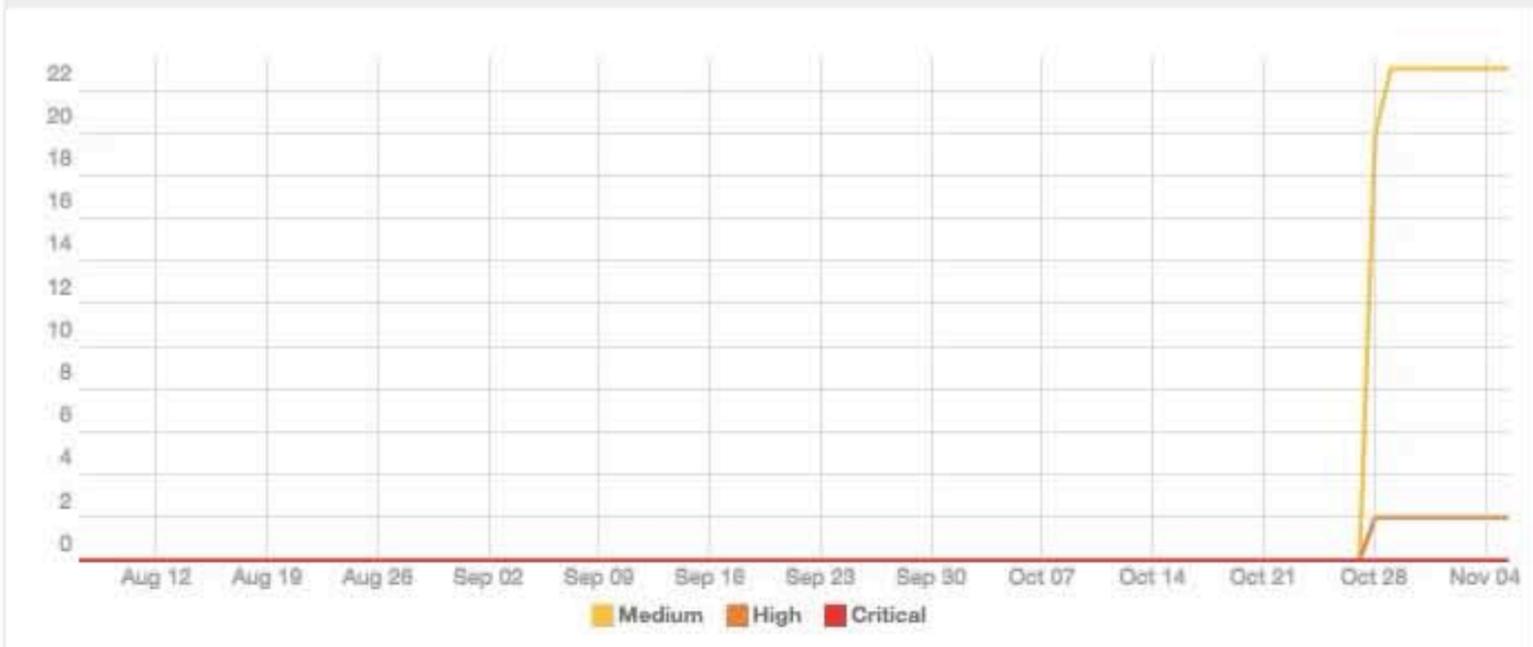
¿Cómo estamos expuestos?

- Evalúa cómo está funcionando la administración de parches según las tendencias de las vulnerabilidades a lo largo del tiempo
- Permite responder rápidamente a los cambios con alertas configurables, notificaciones y acciones automatizadas

¿Dónde debemos priorizar para remediar esas vulnerabilidades?

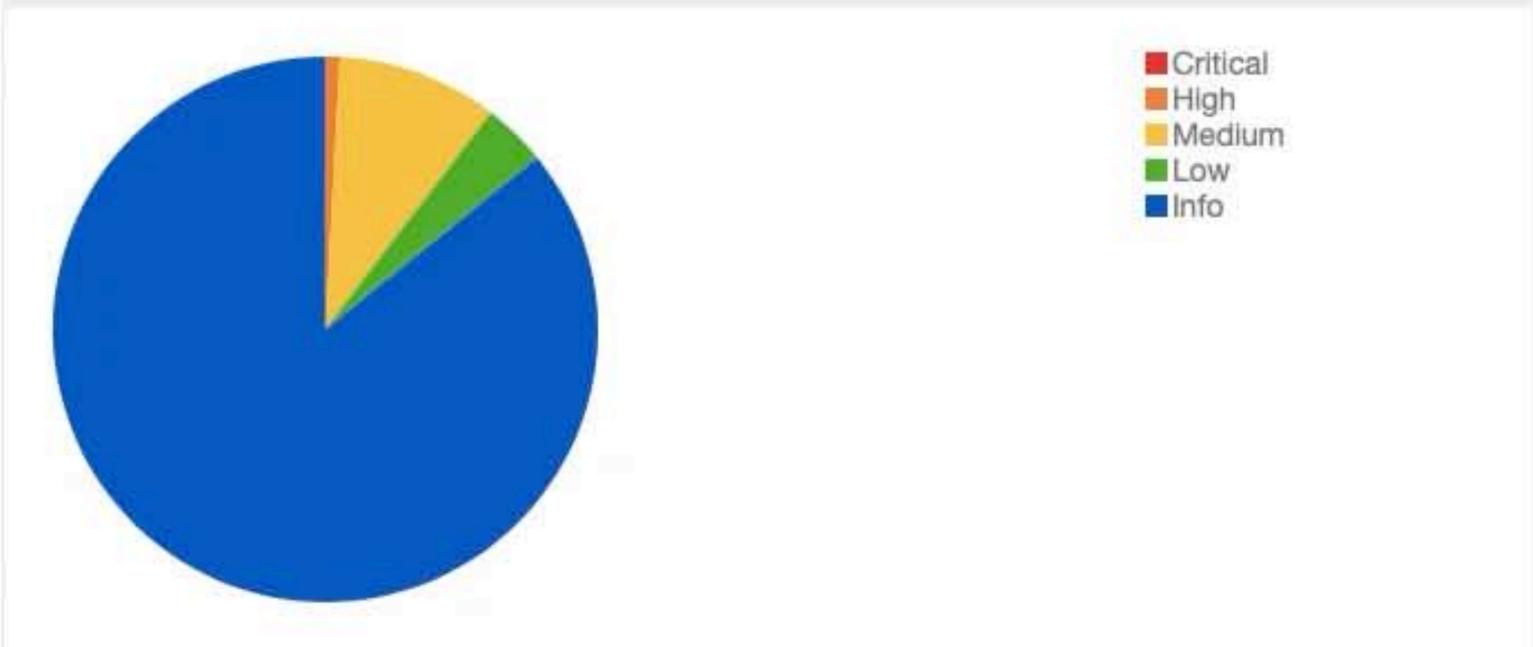
- Optimiza el cumplimiento para la más amplia gama de reglamentos estándares de TI así como las mejores prácticas recomendadas por los principales fabricantes

Executive Summary - Vulnerability Trend (Medium, High, Critical) last 90 days



Last Updated: 5 hours ago

Executive Summary - Severity Summary



Last Updated: 5 hours ago

Executive Summary - Outstanding Patches by Operating System

Family	Score	Info	Low	Medium	High	Critical	Total

Last Updated: 5 hours ago

Executive Summary - Vulnerability Age

	New Hosts	Low	Medium	High	Critical
< 7	0	0	0	0	0
< 30	4	9	23	2	0
< 90	4	9	23	2	0
> 90	0	0	0	0	0

Last Updated: 5 hours ago

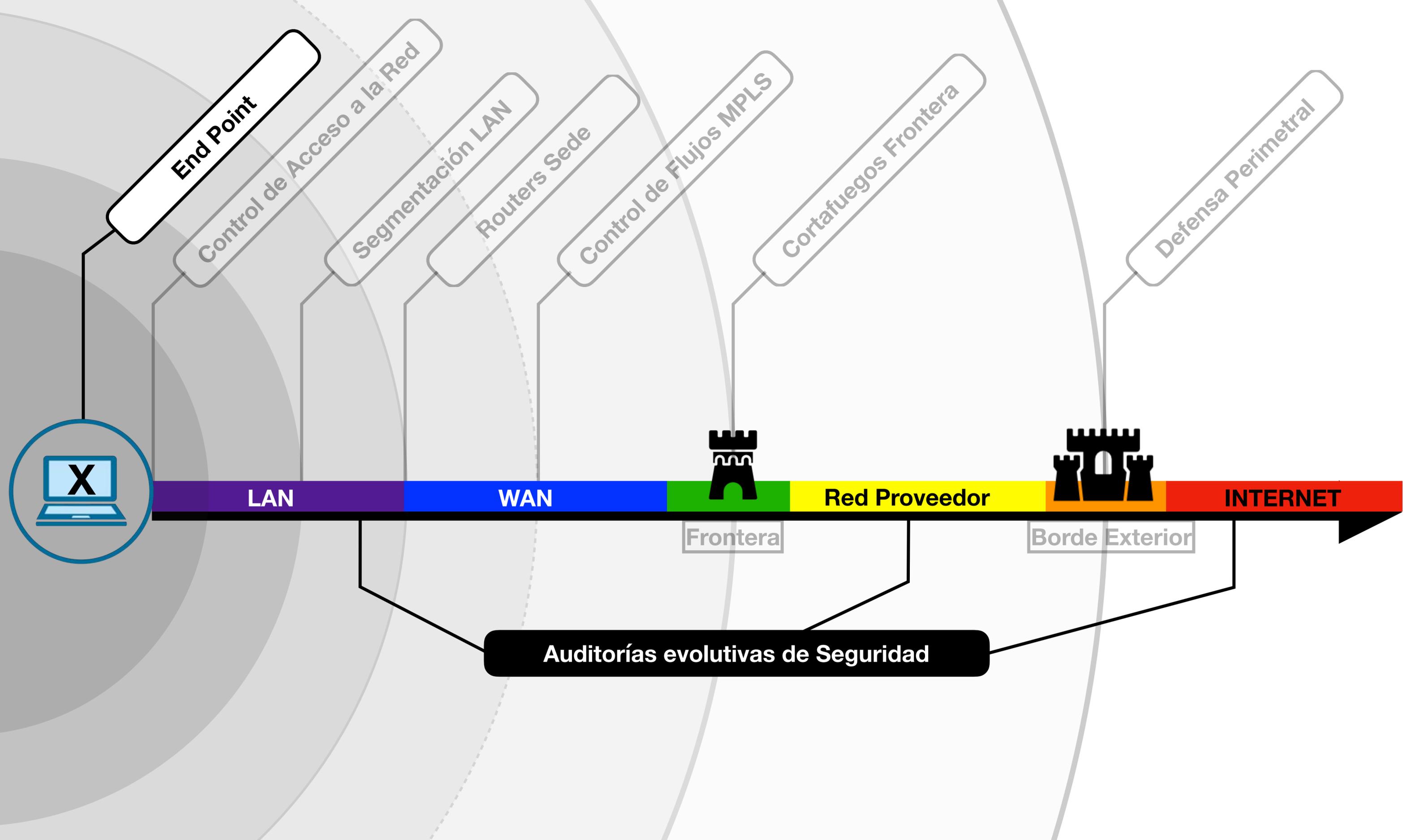
Executive Summary - Most Vulnerable Networks



Executive Summary - Most Vulnerable Hosts

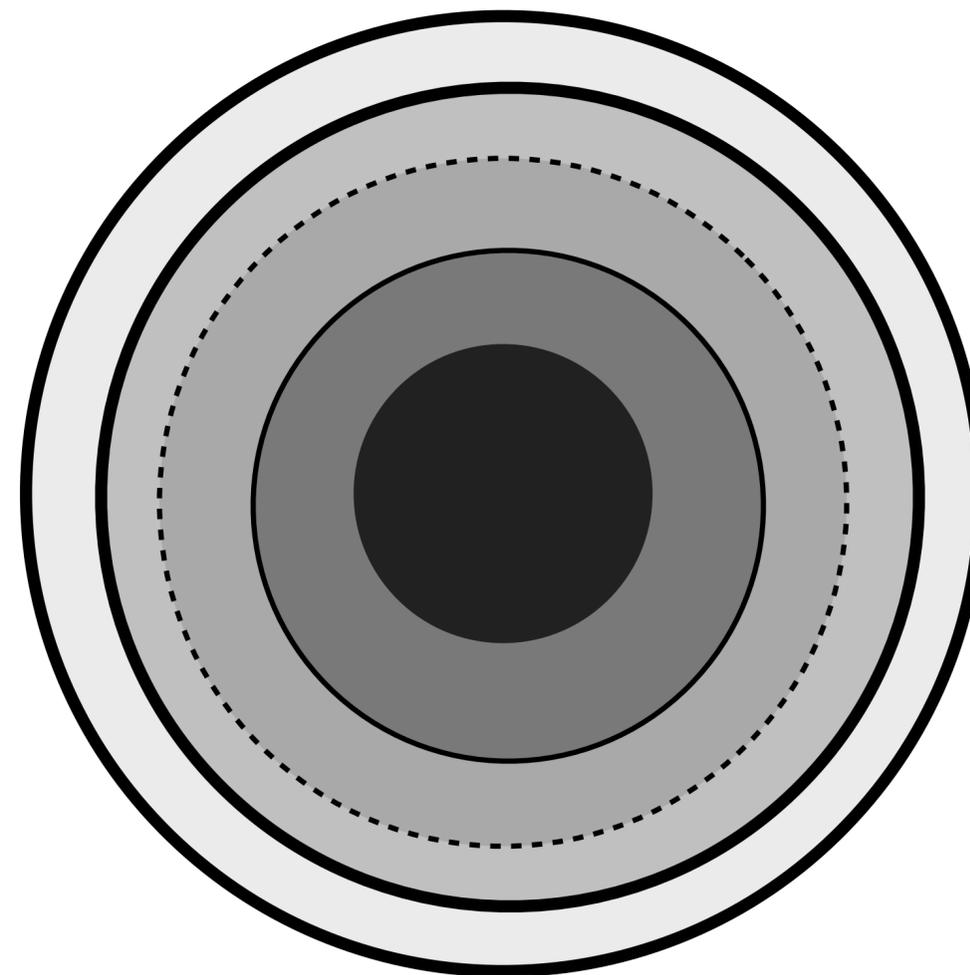


Un
paréntesis (10_{min})
para
respirar



Seguridad Gestionada

Solución de seguridad integral
para nuestros clientes



Sophos

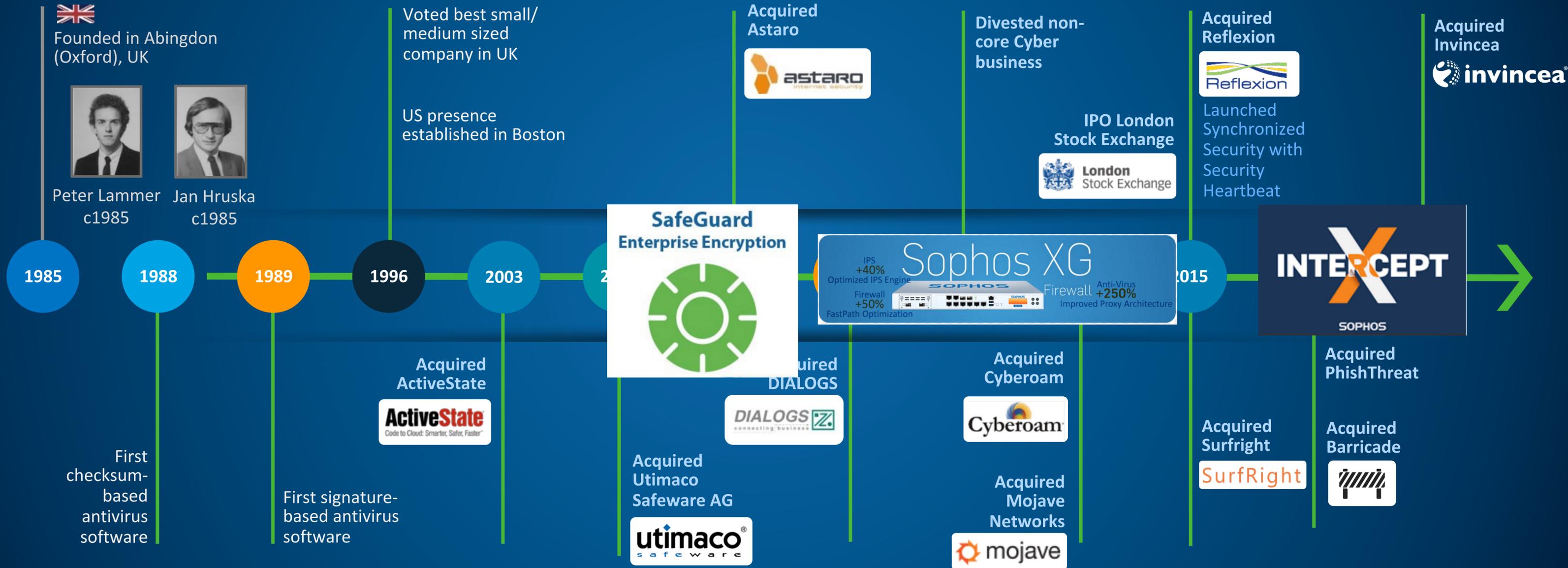
- Fundada en 1985 en Oxford, UK
- 769M\$ de facturación en FY18, **22% YoY**
- 46,1M\$ Beneficio Operativo
- Net Cash Flow 147,7M\$
- 3,000 employees
- 300.000+ Clientes a finales de FY18, **10.000 nuevos Clientes por Trimestre**
- Crecimiento orgánico y por adquisiciones (11 empresas en 10 años)
- SophosLabs
- **Iberia: Crecimiento >40%, 25 empleados, 7.000 Clientes, Soporte local en Castellano**



Sophos Headquarters, Abingdon, UK

Historia de Sophos

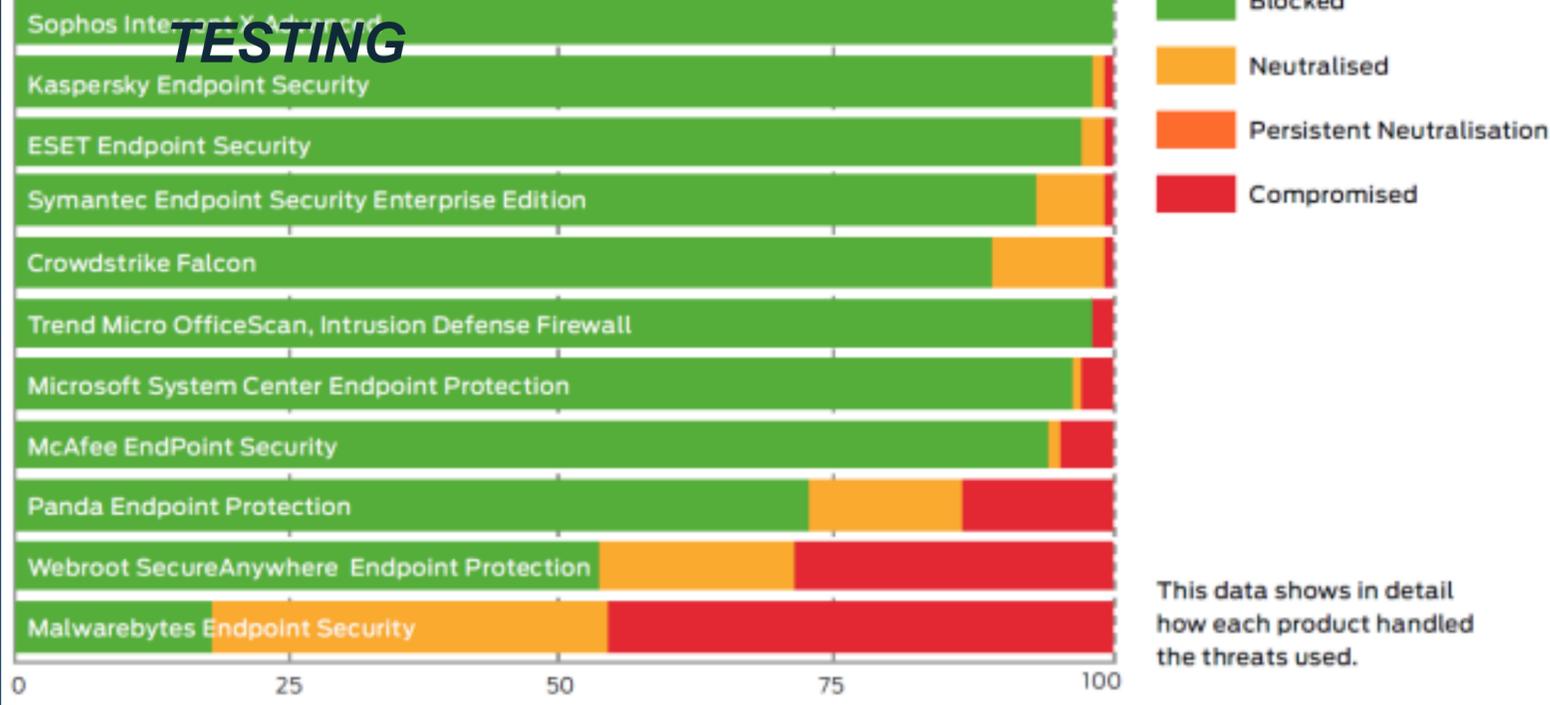
Evolución hacia la protección completa



Leader en Endpoint Security



SE Labs INTELLIGENCE-LED TESTING



Sophos ranked #1 for enterprise endpoint protection
 Sophos ranked #1 for SMB endpoint protection

ENTERPRISE ENDPOINT PROTECTION

SE LABS



SMALL BUSINESS ENDPOINT PROTECTION

SE Labs INTELLIGENCE-LED TESTING



MRG Effitas



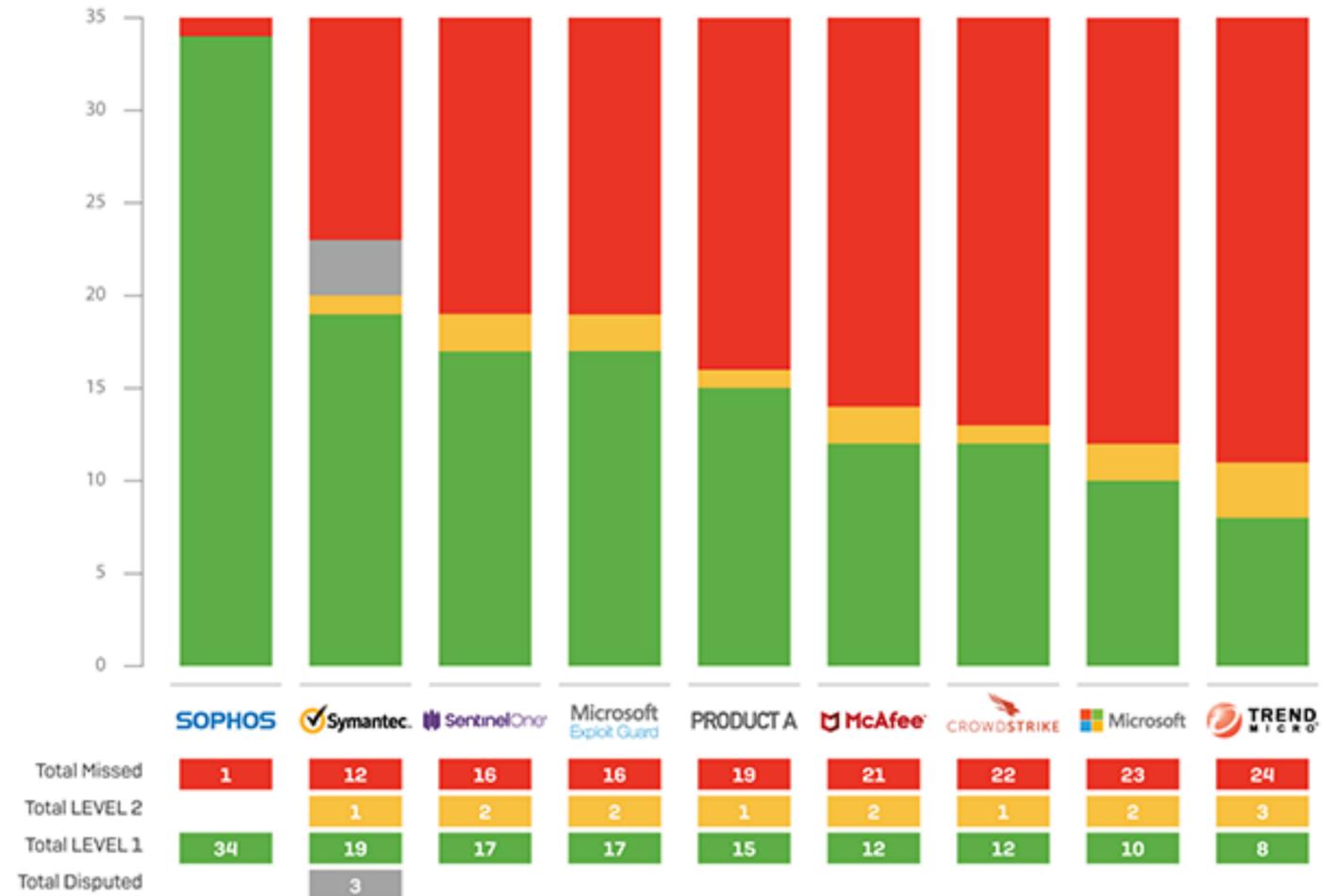
Comparative Protection Assessment



Source: https://www.mrg-effitas.com/wp-content/uploads/2018/02/MRG_Comparative_2018_February_report.pdf



Exploit Protection Test Results

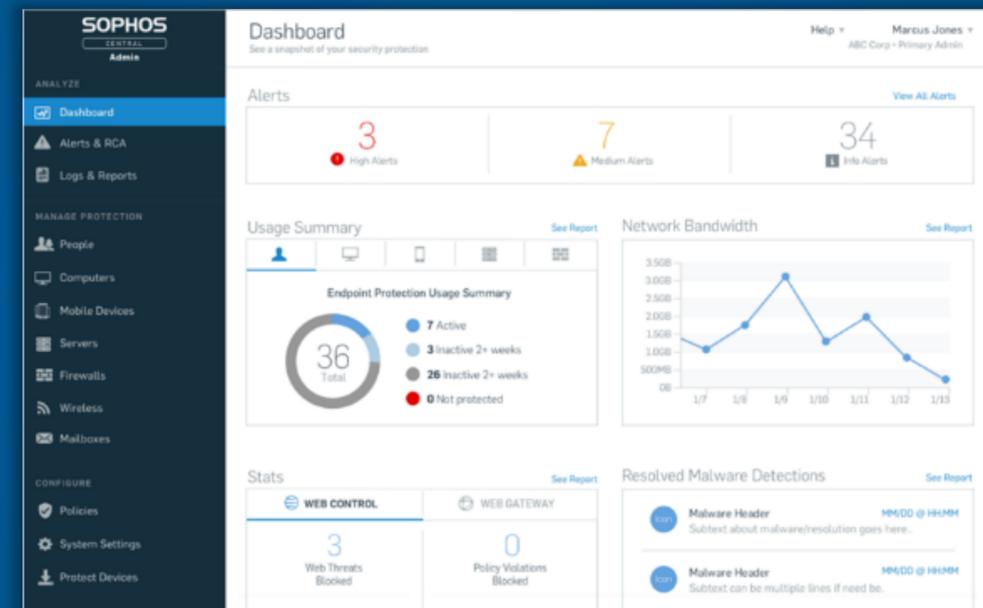


Gestion Centralizada

Partner Dashboard

Admin

Self Service



Allows Partners to manage multiple customer installations

- Endpoint Protection
- Mobile Protection
- Server Protection
- Encryption
- Wireless
- Web Gateway
- Email Security
- Firewall Management

Allows Users to customize security status and notifications

EL PANORAMA DE LAS AMENAZAS HA EVOLUCIONADO



Ransomware

54% de las organizaciones ha sufrido ransomware al menos 2 veces en 2017[^]



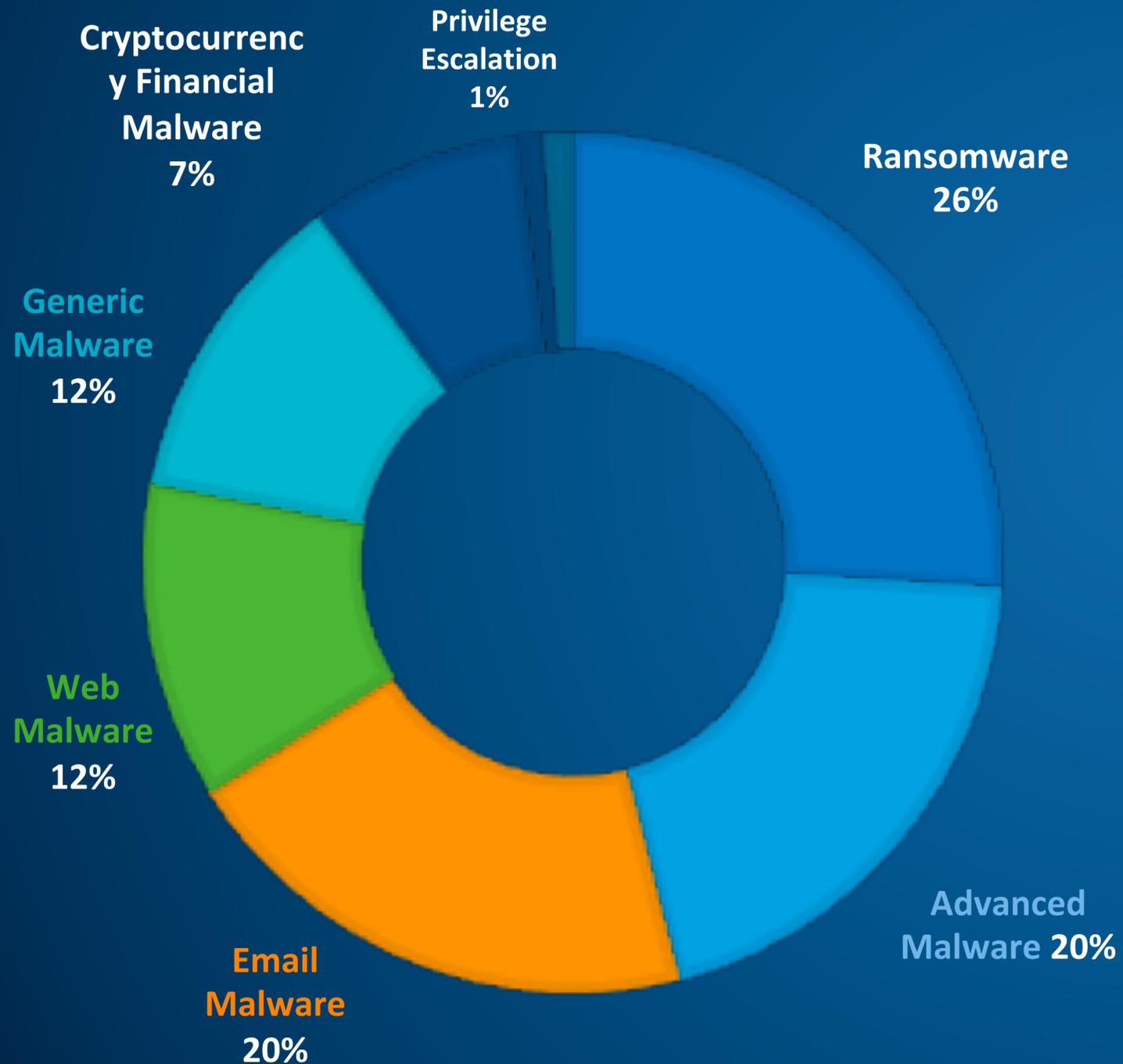
Advanced Threats

83% está de acuerdo en que es muy difícil detener estas amenazas[^]



Exploits

La mayor parte de las empresas no cuenta con protección contra exploits[^]



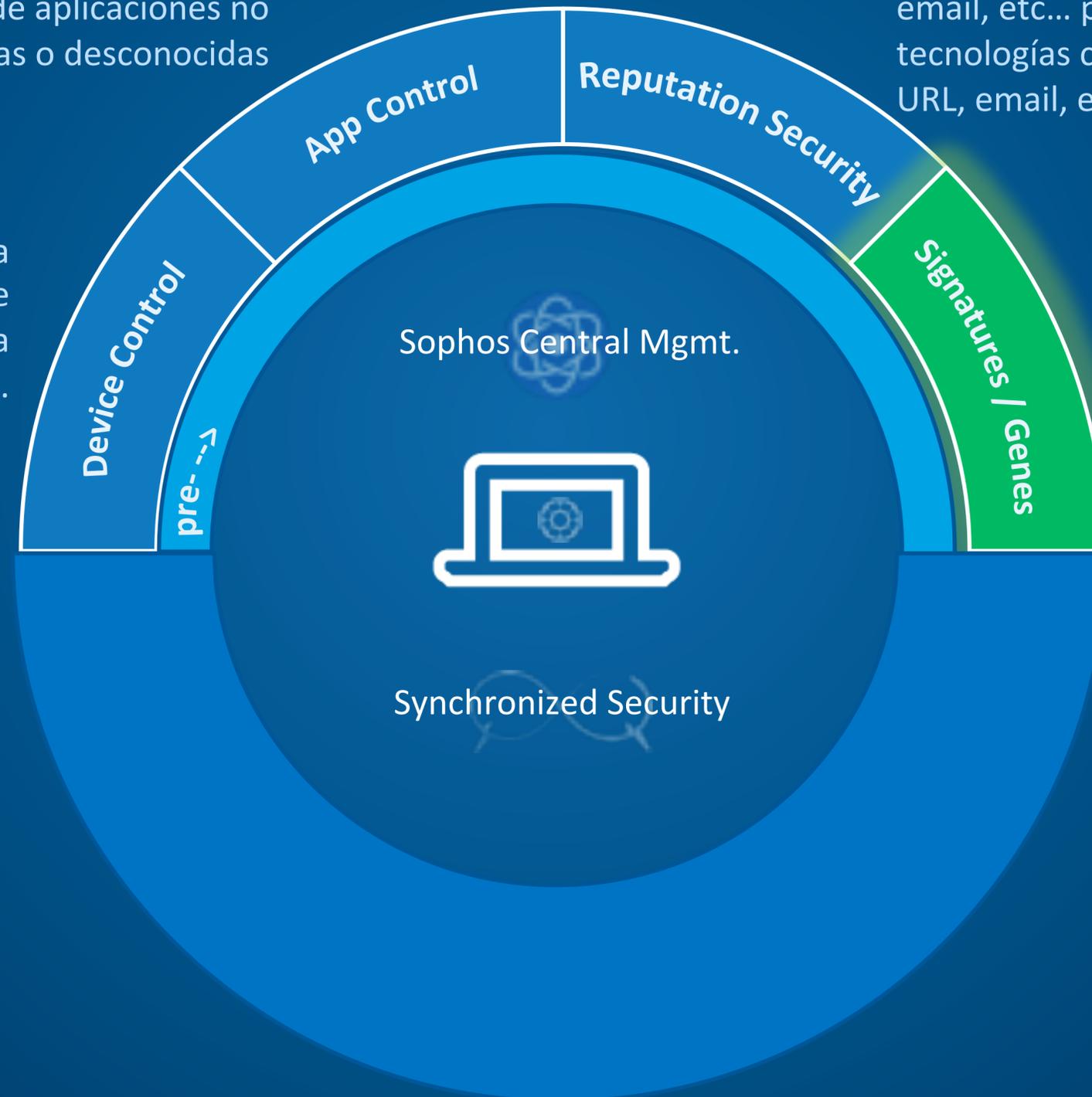
Protección Endpoint Tradicional

Para servidores o puestos, App Control previene de la ejecución de aplicaciones no deseadas o desconocidas

Conociendo el origen/reputación de un fichero, URL, email, etc... previene ataques antes que sucedan. Incluye tecnologías como MTD, reputación de descarga, filtrado URL, email, etc...

Control de políticas para dispositivos extraíbles para que éstos no pongan en riesgo la corporación.

Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,



.exe
Malware



Non-.exe
Malware



Script-based
Malware



Phishing
Attacks



Malicious
URLs

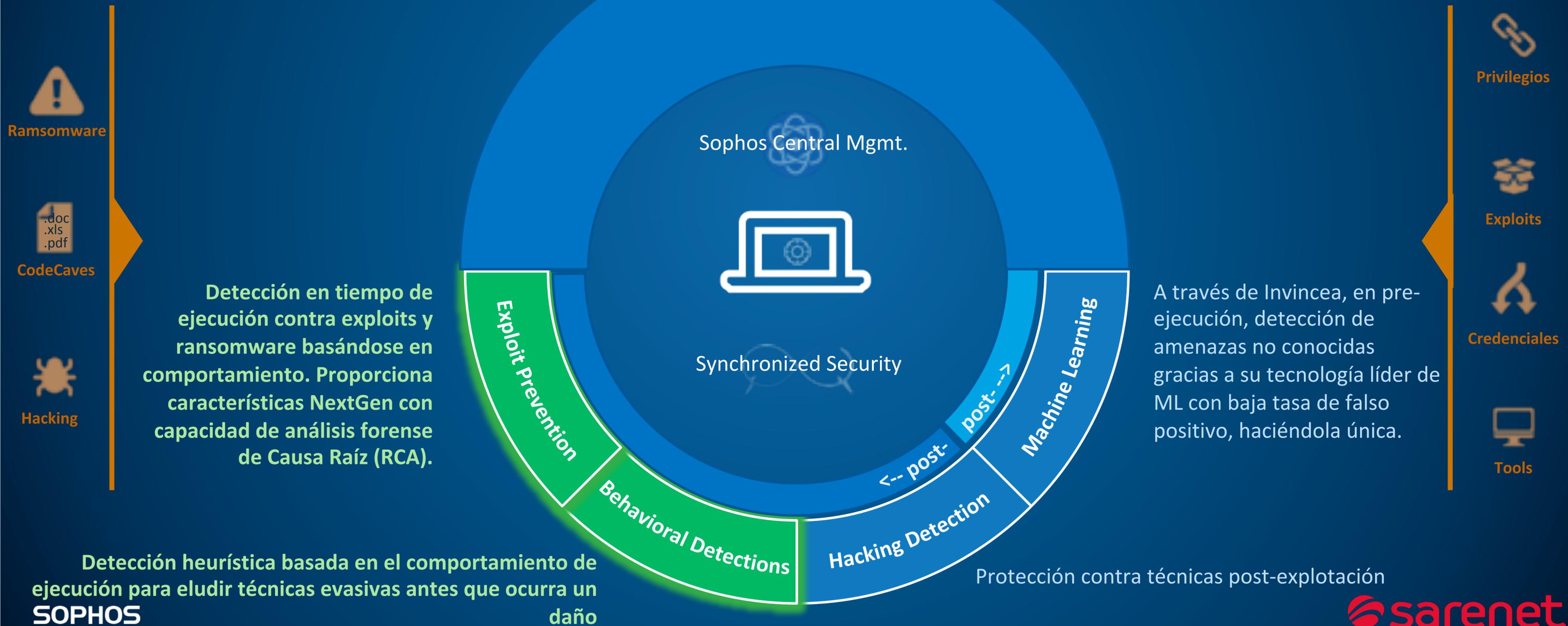


Removable
Media



Unauthorized
Apps

Protección EndPoint de Nueva Generación



Enforce Data Execution Prevention (DEP)

Prevents exploit code running from data memory

Mandatory Address Space Layout Randomization (ASLR)

Prevents predictable code locations

Bottom Up ASLR

Improves code location randomization

Null Page

Prevents exploits that jump via page 0

Anti-HeapSpraying

Pre-allocates common memory areas to block standard attacks

Dynamic Heap Spray

Stops attacks that spray suspicious sequences on the heap

Import Address Table Filtering (IAF)

Stops attackers that lookup API addresses in the IAT

VTable Hijacking

Helps to stop attacks that exploit virtual tables in Adobe Flash

Stack Pivot

Stops abuse of the stack pointer

Stack Exec

Stops attacker code on the stack

SEHOP

Stops abuse of the structured exception handler

Stack-based ROP gadget detection

Stops standard Return-Oriented Programming attacks

Control-Flow Integrity (CFI) assisted by hardware

Stops advanced Return-Oriented Programming attacks

Syscall

Stops attackers that attempt to bypass security hooks

WOW64

Stops attacks that address a 64-bit function from Wow64

Load Library

Blocks libraries that load reflectively or from UNC paths

Shellcode

Stops code execution in the presence of exploit shellcode

VBScript God Mode

Prevents abuse of VBScript in IE to execute malicious code

Block Untrusted Fonts (Windows 10 only)

Stops elevation of privilege (EOP) attacks via untrusted fonts

Application Lockdown

Stops logic-flaw attacks that bypass mitigations

Process Protection

Stops attacks that perform process hijacking or replacement

Network Lockdown

Helps to stop attacks that connect back to C&C

CryptoGuard – Interceptando Ransomware

Monitorización de acceso a ficheros

- Creación de copias ante modificaciones sospechosas

Detección de Ataque

- Paralización del proceso malicioso e investigación

Rollback

- Restauración de ficheros originales
- Ficheros maliciosos eliminados

Visibilidad forense

- Mensaje al usuario
- Alerta al admin
- Análisis de Causa Raíz

4 NÍVELES DE PROTECCIÓN DEL PUESTO DE TRABAJO

- 
- **Central EndPoint Protection:** El EndPoint tradicional que sigue siendo una protección necesaria pero insuficiente

PROTECCIÓN TRADICIONAL EN BASE A ANÁLISIS DE FICHEROS POR FIRMAS

PROTECCIÓN AVANZADA CON APRENDIZAJE MEDIANTE DEEP LEARNING DE TÉCNICAS Y COMPORTAMIENTOS DE ATAQUE

- 
- **Central Intercept X:** Se trata del módulo de Deep Learning para la detección de comportamientos anómalos. Este producto es combinable con productos antivirus tradicionales de otros fabricantes
 - **Central Intercept X Advanced:** EndPoint + Intercept X, es la solución más extendida, incluye Intercept X y EndPoint Protection. Solución válida para cualquier tipo de organización.
 - **Central Intercept X Advanced con EDR:** Añade la capa de inteligencia y reporting avanzado para automatizar la generación de informes forenses. Este producto está diseñada para organizaciones con personal It dedicado a la seguridad

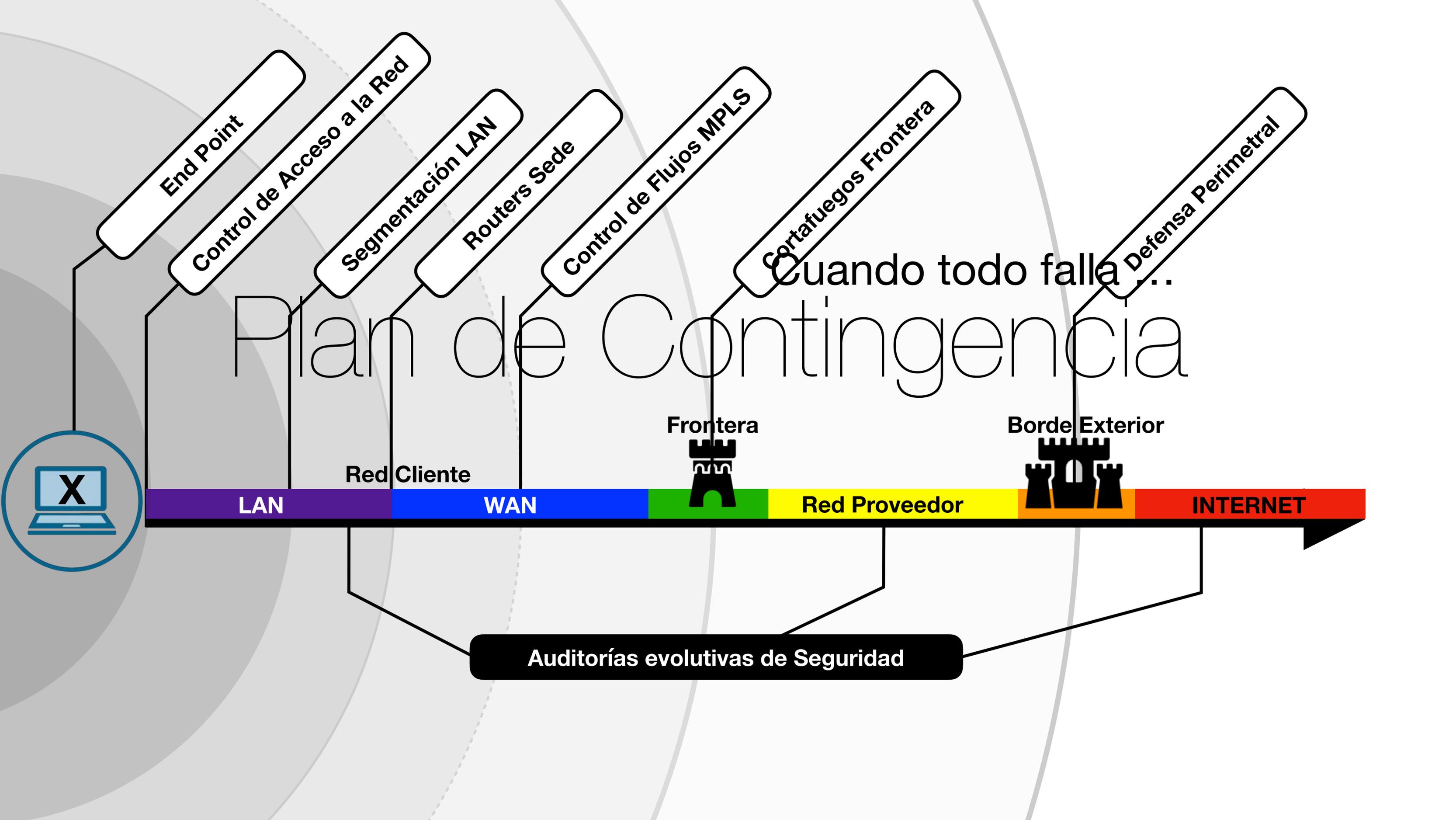
CARACTERÍSTICAS PRINCIPALES DE LOS ENDPOINT DE SOPHOS

- Gestión centralizada desde consola en la nube. 3 niveles de administración (Sarenet, Dpto. IT y usuario)
- Es un cliente ligero en cuanto a consumo local de recursos y sus actualizaciones no son de alto volumen
- Pago por uso en base a licencias. Un usuario es una licencia. Una licencia es válida para todos los PCS y portátiles del mismo usuario, no así con tablet y smartphone donde hay que ir a los productos de movilidad.
- Hay protecciones servidor y protecciones puestos normales
- Los procesos de Deep Learning se ejecutan en local, en el propio equipo, y no se requiere de Internet
- Es un tecnología compatible con otros fabricantes AV
- Tecnología de fabricante global
- Soporta Windows, Linux y MacOS
 - Linux desktop consultar, hay muy poco
 - Linux Server soporta. En server se soporta CentOS, Oracle, Suse, Ubuntu
 - Puestos de trabajo Windows a partir de Windows 7
 - Servidores Windows a partir de Windows 8 R2

¡¡ PRUÉBALO SIN COSTE!!

Envía un mail a ingenieriaclientes@sarenet.es poniendo en el asunto “Demo Sophos Santander” junto a tus datos de contacto

Promoción especial 15% DTO. hasta el 27 de Marzo de 2019



End Point

Control de Acceso a la Red

Segmentación LAN

Routers Sede

Control de Flujos MPLS

Cortafuegos Frontera

Defensa Perimetral

Plan de Contingencia

Quando todo falla ...



Red Cliente

LAN

WAN



Frontera

Red Proveedor



Borde Exterior

INTERNET

Auditorías evolutivas de Seguridad