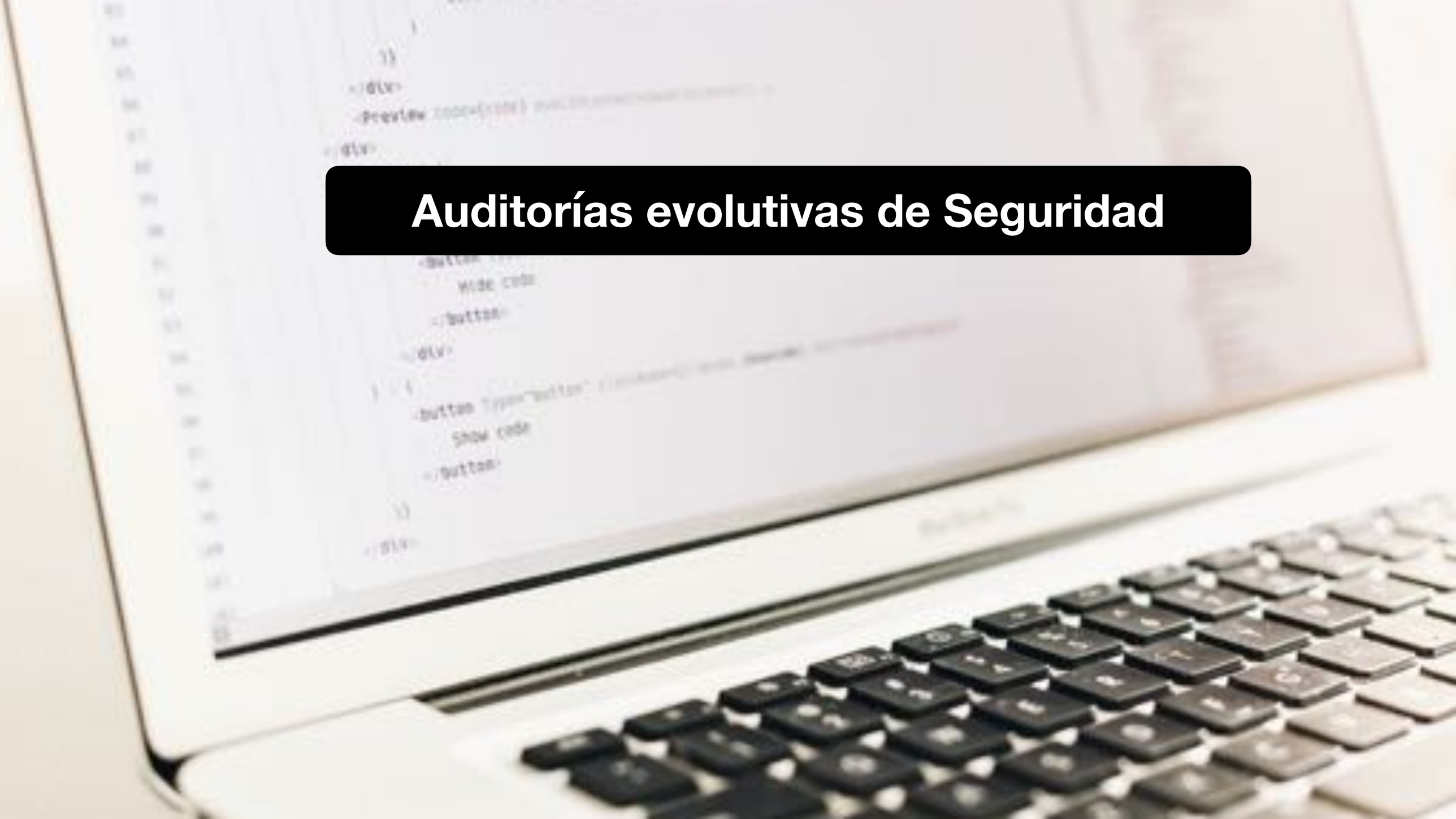

Pedro Xabier Alaña
pedroxabier sarenet .es
Dpto. Comercial



Auditorías evolutivas de Seguridad

AUDITORÍAS EVOLUTIVAS DE SEGURIDAD

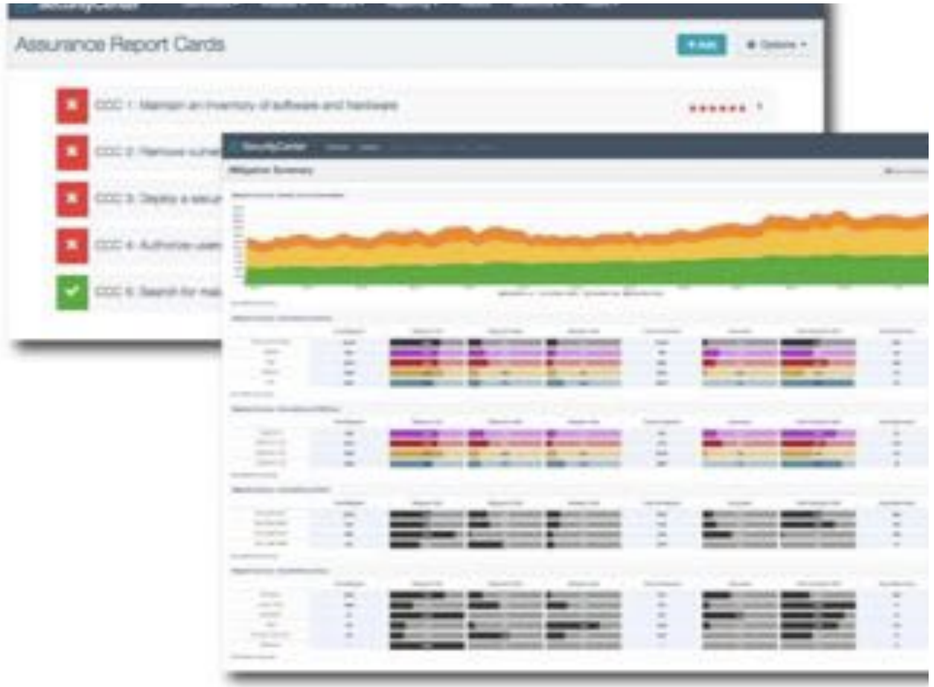
- **Tecnología Security Center de Tenable explotada desde el Data Center de Sarenet en Vizcaya por personal de seguridad propio**
- Acuerdo estratégico entre Tenable y Sarenet
- Complemento ideal de seguridad para aportar contexto global e información completa de ciberexposición (más allá de perímetro, 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

sarenet

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, tendenci informes y flujos de trabajo altamente personalizables para adaptarse a las necesidades de su programa de seguridad

tenable

sarenet

BENEFICIOS CLAVE DE TENABLE SECUTIRY CENTER

Beneficios clave

- 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)

- 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

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

tenable

sarenet

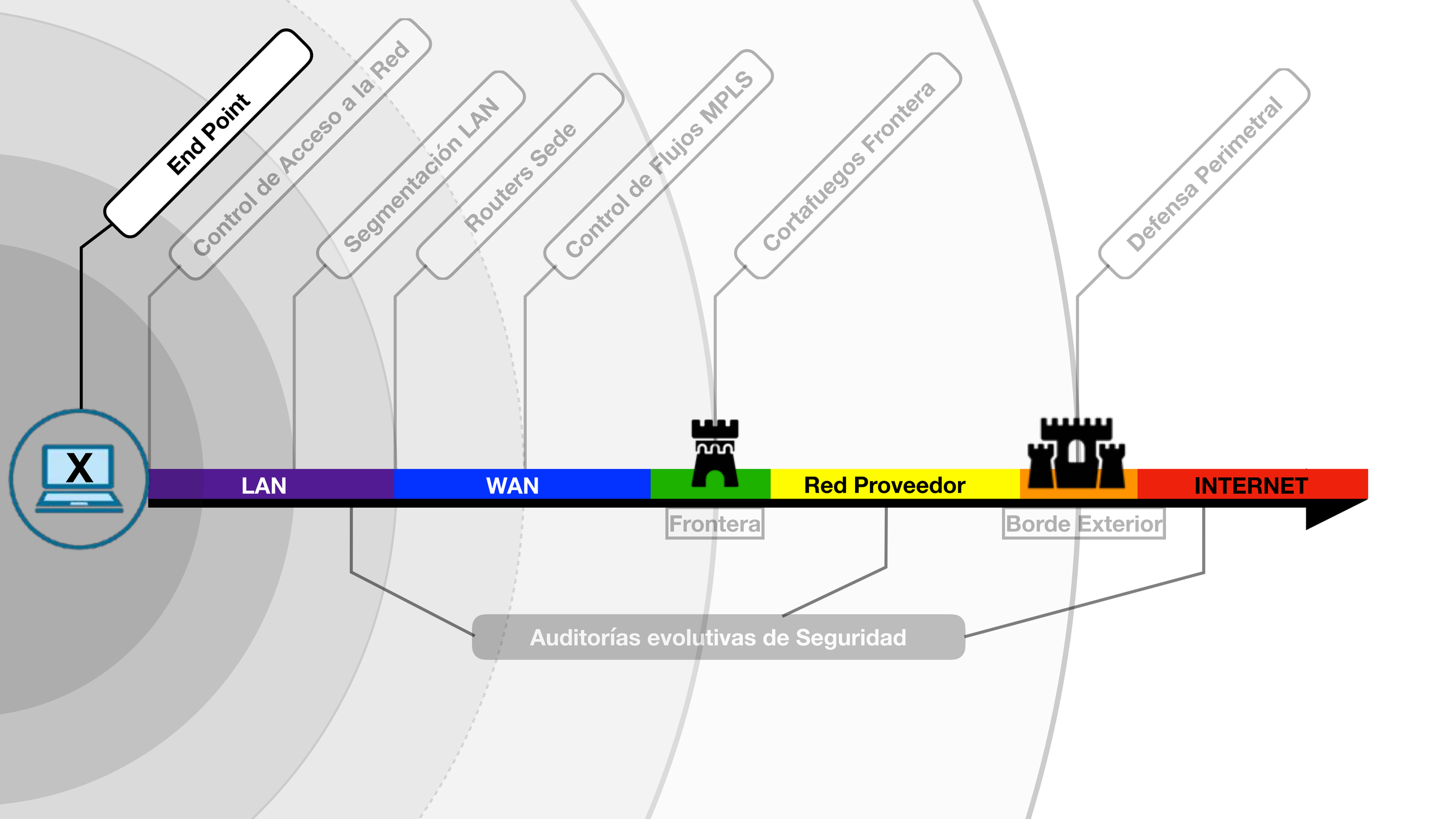
PREGUNTAS CLAVE

¿Dónde estamos expuestos ?

¿Cómo estamos expuestos?

¿Dónde debemos priorizar para remediar esas vulnerabilidades?


tenable.sc
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Users
Security Manager
Executive 30 Day
Switch Dashboard
Options
Executive 30 Day - Current Vulnerability Type Matrix
Executive 30 Day - Exploitable Vulnerability Type Matrix
Executive 30 Day - Mitigated Vulnerability Type Matrix
Executive 30 Day - Current Vulnerability Summary by Severity
Executive 30 Day - Mitigated Vulnerability Summary by Severity
Critical
High
Medium
Low
Info
Executive 30 Day - Current Vulnerability Trending by Severity
Executive 30 Day - Exploitable Vulnerability Trending by Severity


End Point
Control de Acceso a la Red
Segmentación LAN
Routers Sede
Control de Flujos MPLS
Cortafuegos Frontera
Defensa Perimetral
X
LAN
WAN
Red Proveedor
INTERNET
Frontera
Borde Exterior
Auditorías evolutivas de Seguridad

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

SOPHOS

sarenet

Historia de Sophos

Evolución hacia la protección completa

1985

Founded in Abingdon (Oxford), UK

Peter Lammer c1985

Jan Hruska c1985

1988

First checksum-based antivirus software

1989

First signature-based antivirus software

1996

Voted best small/ medium sized company in UK

US presence established in Boston

2003

Acquired ActiveState

ActiveState
Code to Cloud: Smarter, Safer, Faster

2

SafeGuard Enterprise Encryption

Acquired Utimaco Safeware AG

utimaco safeware

Acquired Astaro

astaro internet security

ired DIALOGS

DIALOGS connecting business

Divested non-core Cyber business

IPO London Stock Exchange

London Stock Exchange

Sophos XG

IPS +40% Optimized IPS Engine
Firewall +50% FastPath Optimization
Anti-Virus +250% Improved Proxy Architecture

Acquired Cyberoam

Cyberoam

Acquired Mojave Networks

mojave

2015

Acquired Reflexion

Reflexion

Launched Synchronized Security with Security Heartbeat

Acquired Surfright

SurfRight

Acquired Invincea

invincea

INTERCEPT X
SOPHOS

Acquired PhishThreat

Acquired Barricade

SOPHOS

sarenet

Leader en Endpoint Security

SOPHOS

sarenet

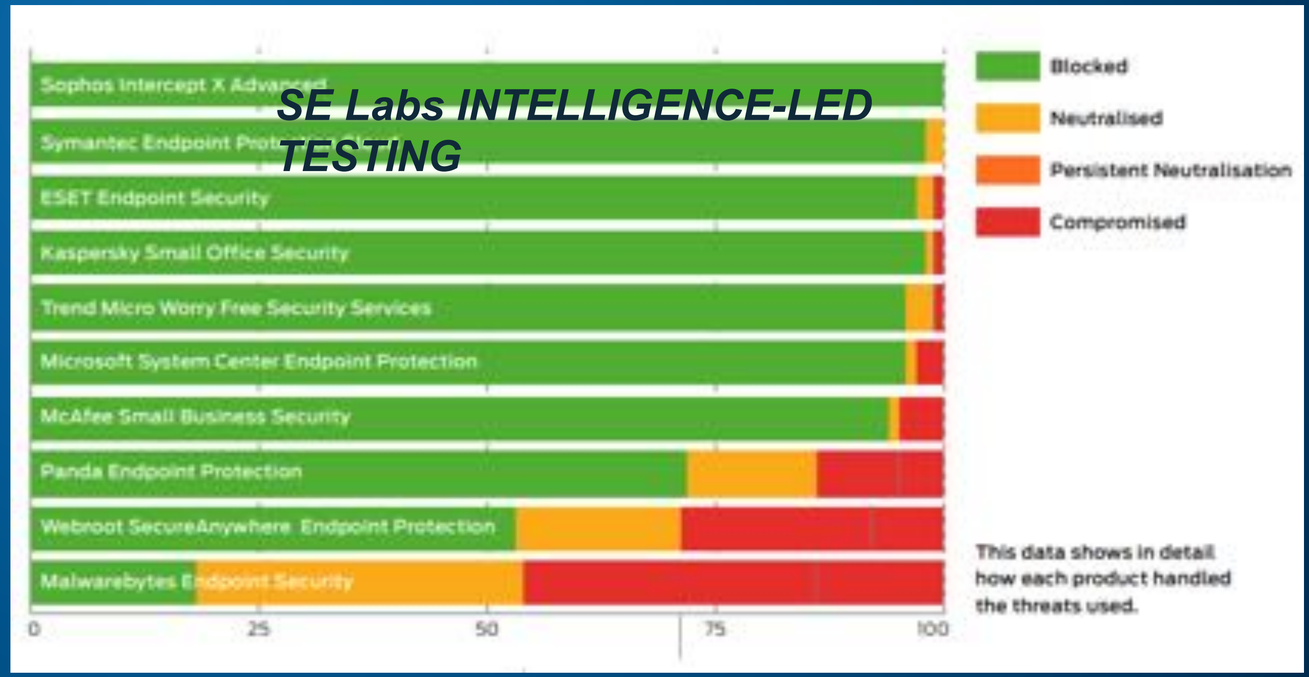
Sophos ranked #1 for enterprise endpoint protection
Sophos ranked #1 for SMB endpoint protection

ENTERPRISE ENDPOINT PROTECTION

SE LABS

SE Labs AAA SMALL BUSINESS ENDPOINT PROTECTION APR-JUN 2018

SMALL BUSINESS ENDPOINT PROTECTION

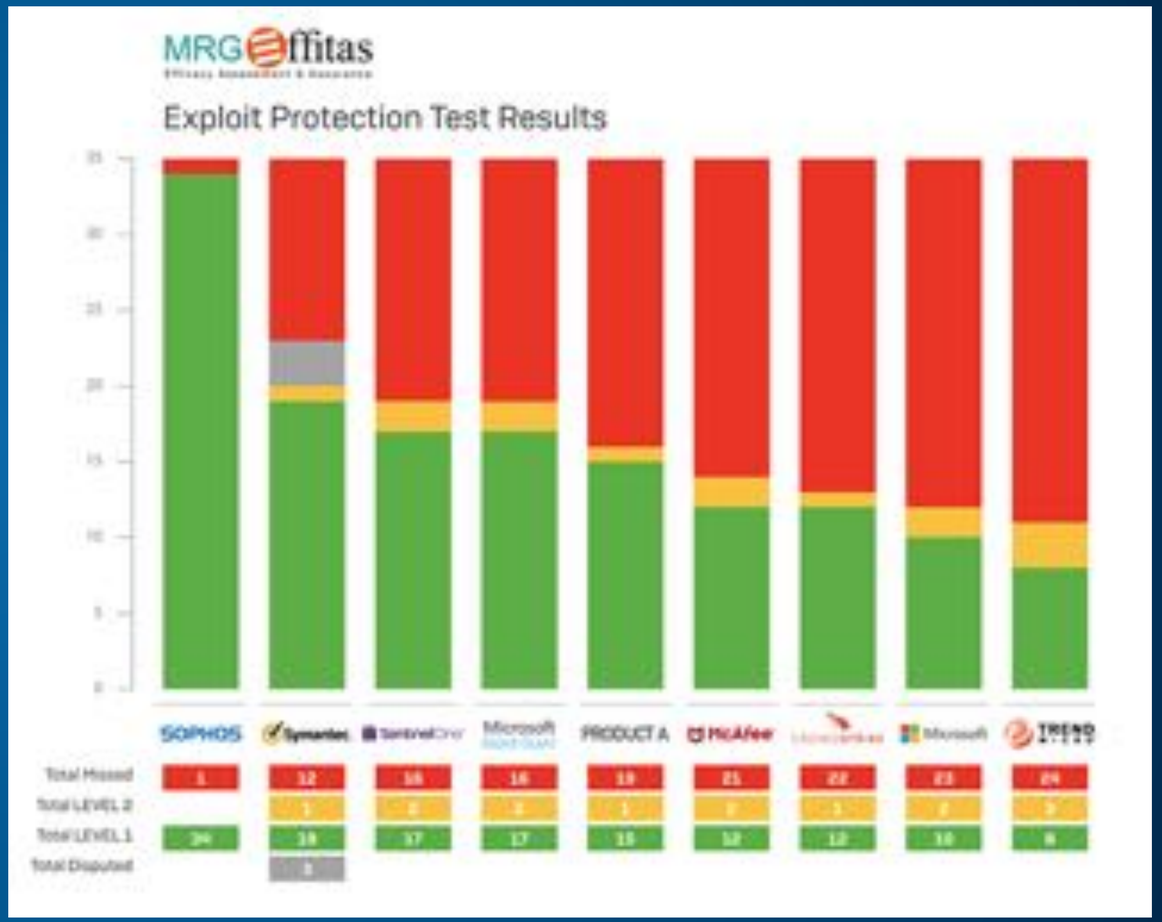


SOPHOS

sarenet

MRG Effitas


MRG Effitas
Comparative Protection Assessment
Malware & PUA
Missed
Behavior Blocked
Auto Blocked
Accuracy / False Positive
False Positive
True Negative
MALWARE
PUA
ACCURACY / FP
SOPHOS
Symantec
McAfee
SentinelOne
CROWDSTRIKE
DISPUTED

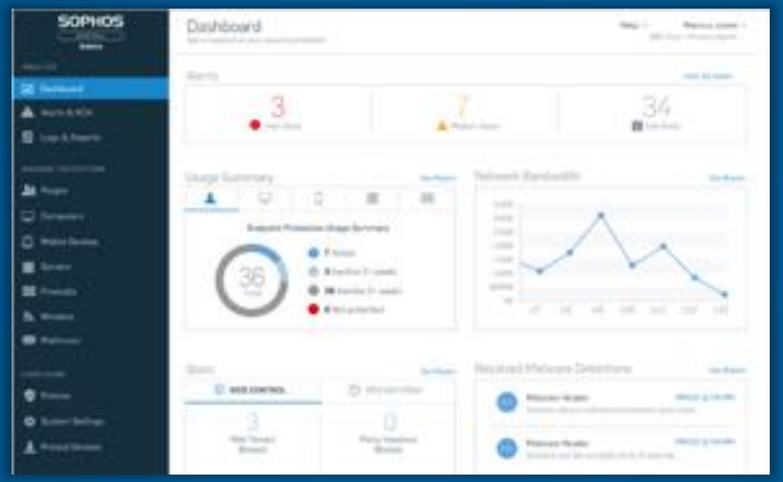

MRG Effitas
Exploit Protection Test Results
SOPHOS
Symantec
SentinelOne
Microsoft
PRODUCT A
McAfee
CROWDSTRIKE
Microsoft
TREND MICRO
Total Missed
Total LEVEL 2
Total LEVEL 1
Total Disputed

Gestion Centralizada

Partner Dashboard

Allows Partners to manage multiple customer installations

Admin



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

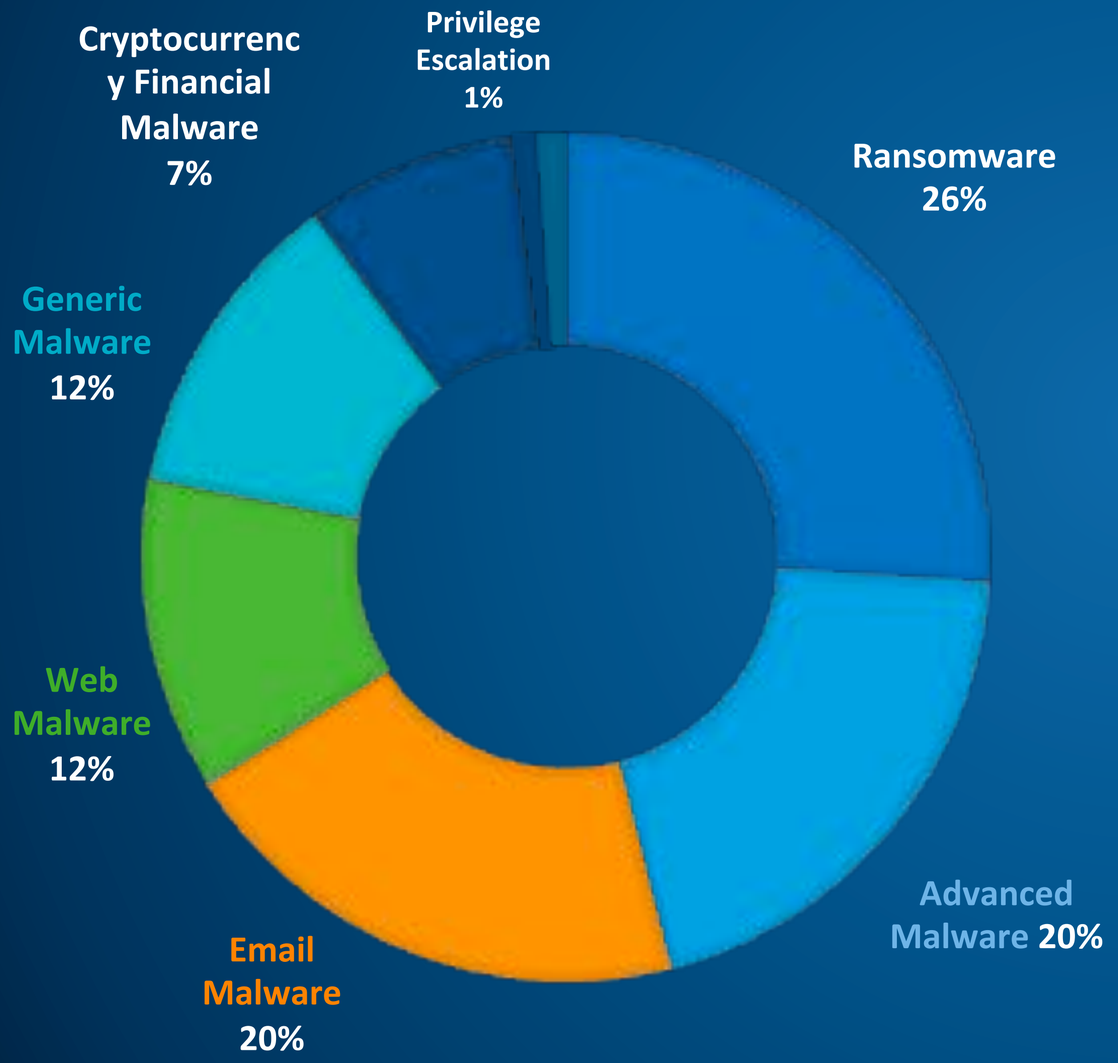
Self Service

Allows Users to customize security status and notifications

SOPHOS

sarenet

EL PANORAMA DE LAS AMENAZAS HA EVOLUCIONADO



Ransomware

54% de las organizaciones ha sufrido ramsomware 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^

SOPHOS

Source: SophosLabs

^Source: The State of Endpoint Security Today Survey

sarenet

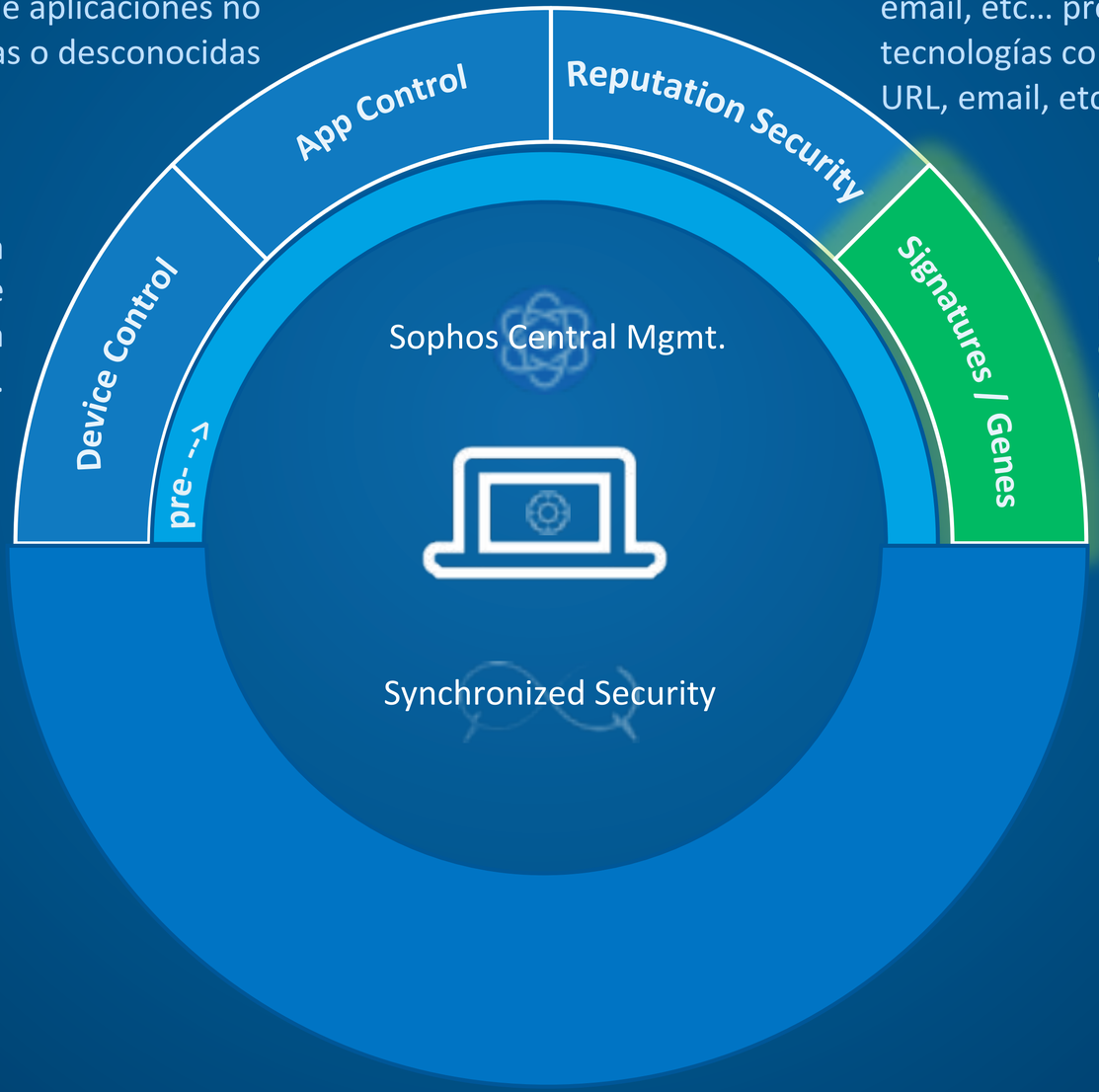
Protección Endpoint Tradicional

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

.doc .xls .pdf

Non-.exe Malware

Script-based Malware

Phishing Attacks

Malicious URLs

Removable Media

Unauthorized Apps

SOPHOS

sarenet

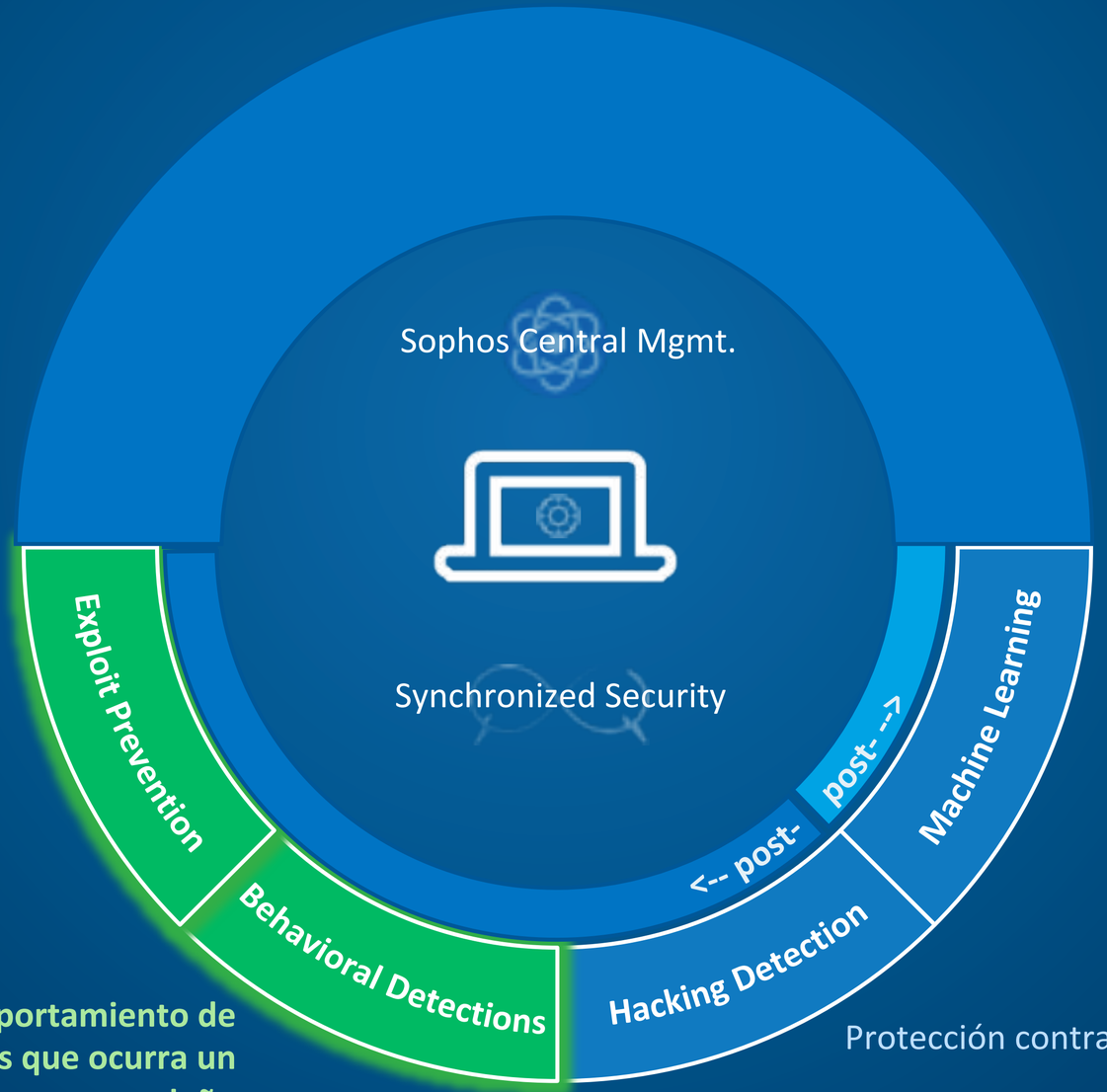
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

Protección contra técnicas post-explotación

SOPHOS

sarenet

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

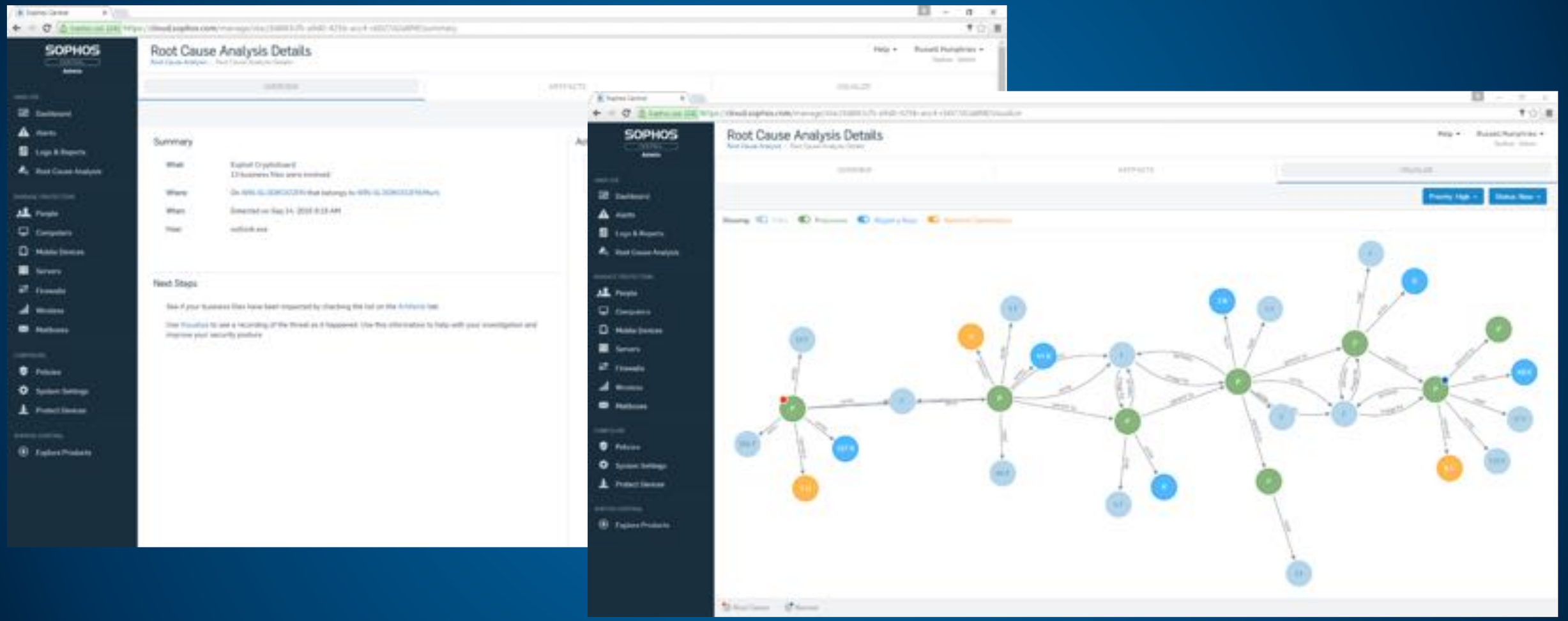
Process Protection
Stops attacks that perform process hijacking or replacement

Network Lockdown
Helps to stop attacks that connect back to C&C

CryptoGuard – Interceptando Ransomware

Analisis de causa raiz

Entendiendo el Quién, Qué, Cuándo, Dónde, Por qué y Cómo



SOPHOS

sarenet

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

SOPHOS

sarenet

CARACTERÍSTICAS PRINCIPALES DE LOS ENDPOINT DE SOPHOS

- Gestión centralizada desde consola en la nube. 3 níveles 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

SOPHOS

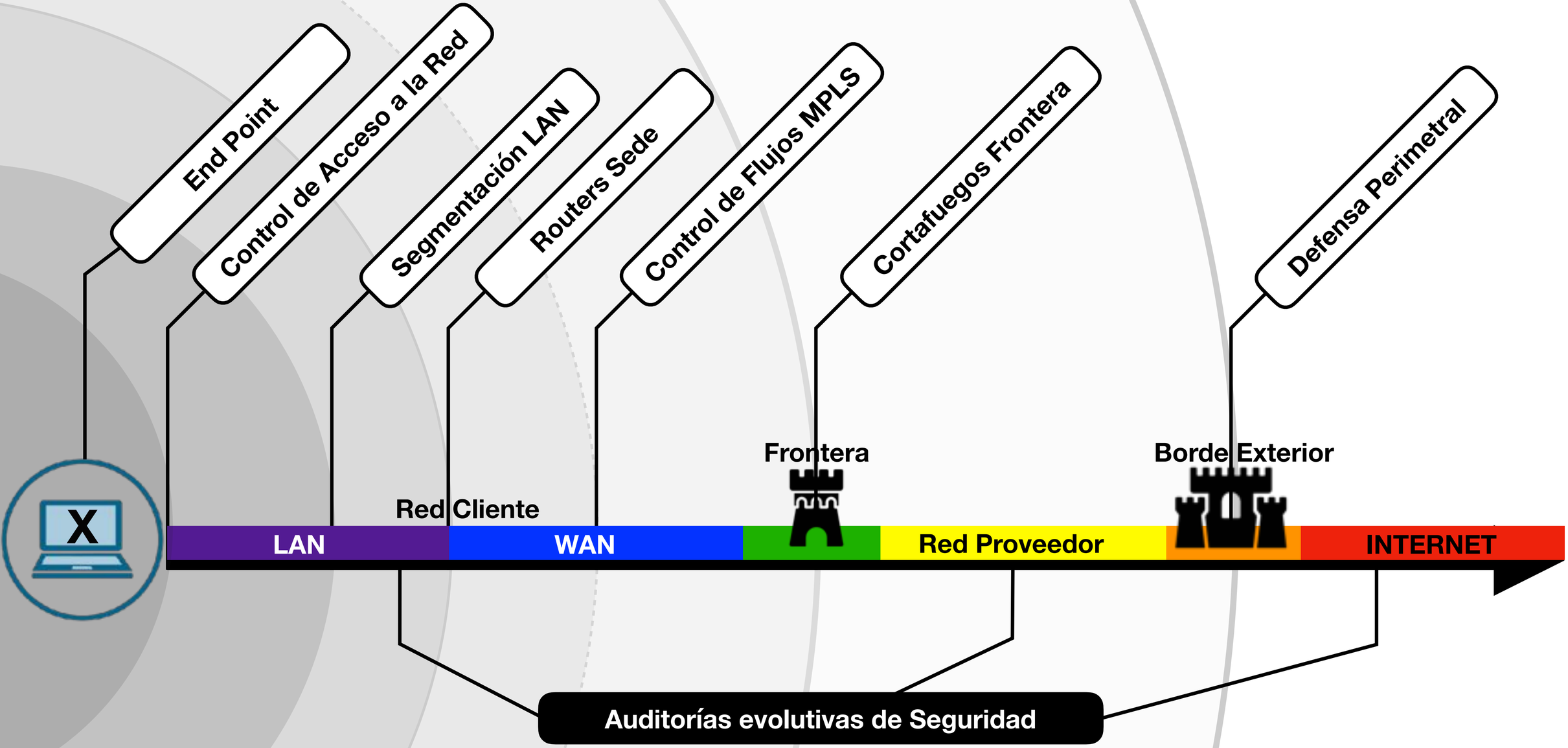
sarenet

¡¡ PRUEBALO SIN COSTE!!

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

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

sarenet


End Point
Control de Acceso a la Red
Segmentación LAN
Routers Sede
Control de Flujos MPLS
Cortafuegos Frontera
Defensa Perimetral
Frontera
Borde Exterior
Red Cliente
LAN
WAN
Red Proveedor
INTERNET
Auditorías evolutivas de Seguridad

Cuando todo falla ...

Plan de Contingencia