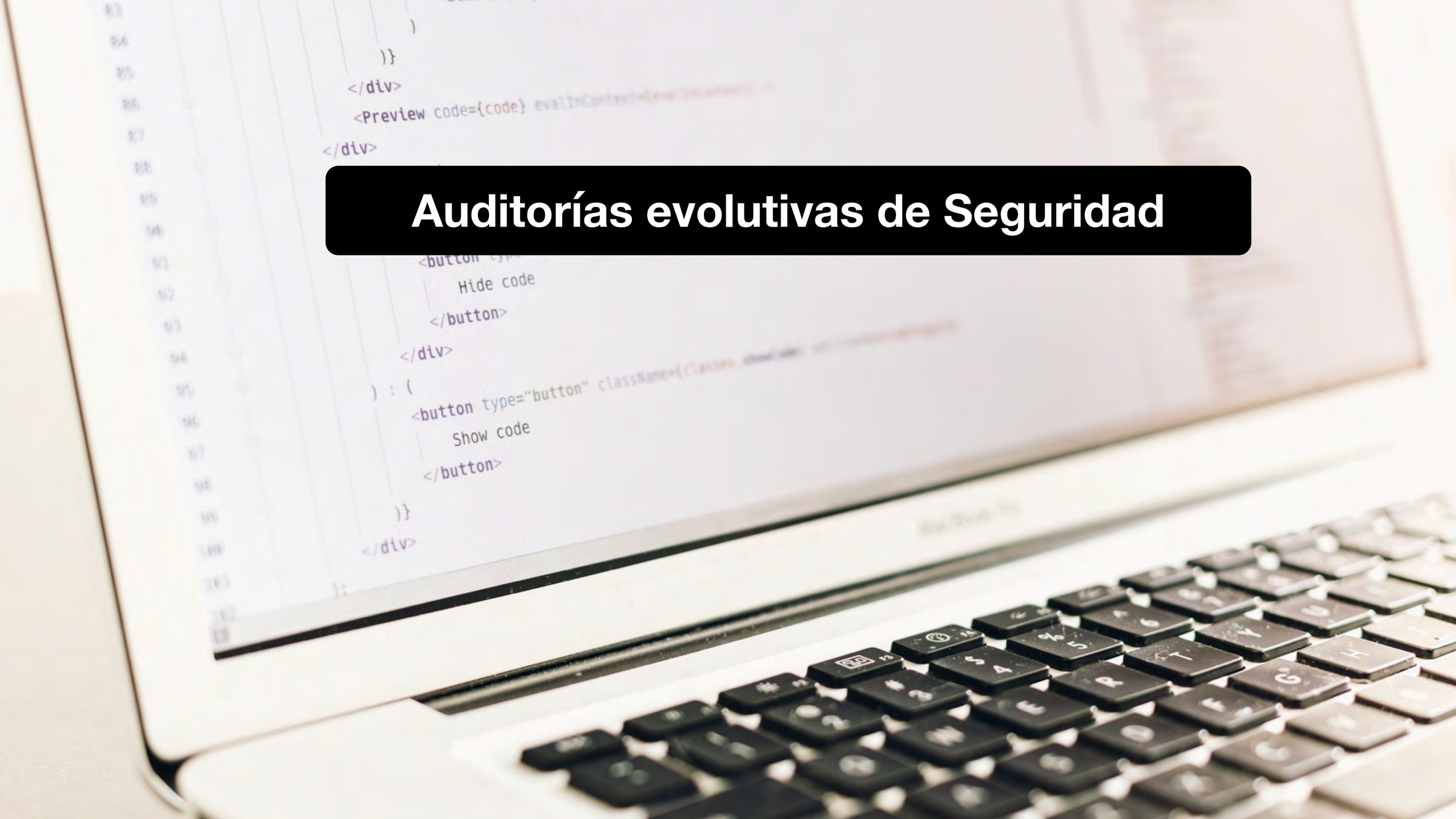
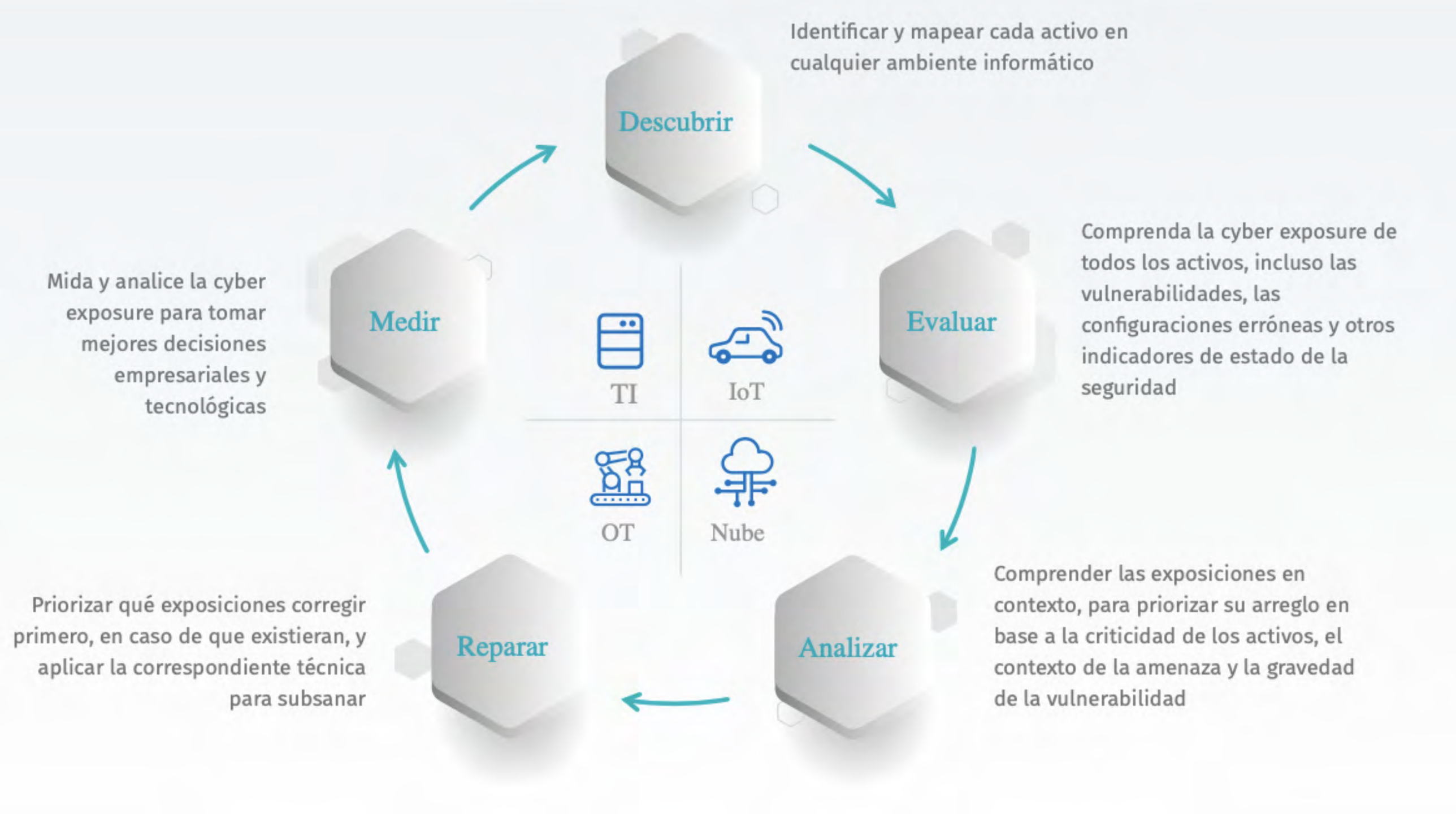

Aitor Jerez
aitor sarenet
Director comercial


Auditorías evolutivas de Seguridad

tenable

sarenet


Descubrir
Identificar y mapear cada activo en cualquier ambiente informático
Evaluar
Comprenda la cyber exposure de todos los activos, incluso las vulnerabilidades, las configuraciones erróneas y otros indicadores de estado de la seguridad
Analizar
Comprender las exposiciones en contexto, para priorizar su arreglo en base a la criticidad de los activos, el contexto de la amenaza y la gravedad de la vulnerabilidad
Reparar
Priorizar qué exposiciones corregir primero, en caso de que existieran, y aplicar la correspondiente técnica para subsanar
Medir
Mida y analice la cyber exposure para tomar mejores decisiones empresariales y tecnológicas
TI
IoT
OT
Nube

tenable.sc™

Identifique, investigue y priorice vulnerabilidades de forma precisa.

Cada organización, sin importar su tamaño, podrá responder con certeza las preguntas siguientes:

1. *¿Dónde estamos expuestos?*
2. *¿Dónde debemos dar prioridad en función del riesgo?*
3. *¿Estamos reduciendo la exposición con el tiempo?*
4. *¿Qué resultado obtenemos si nos comparamos con nuestros pares?*

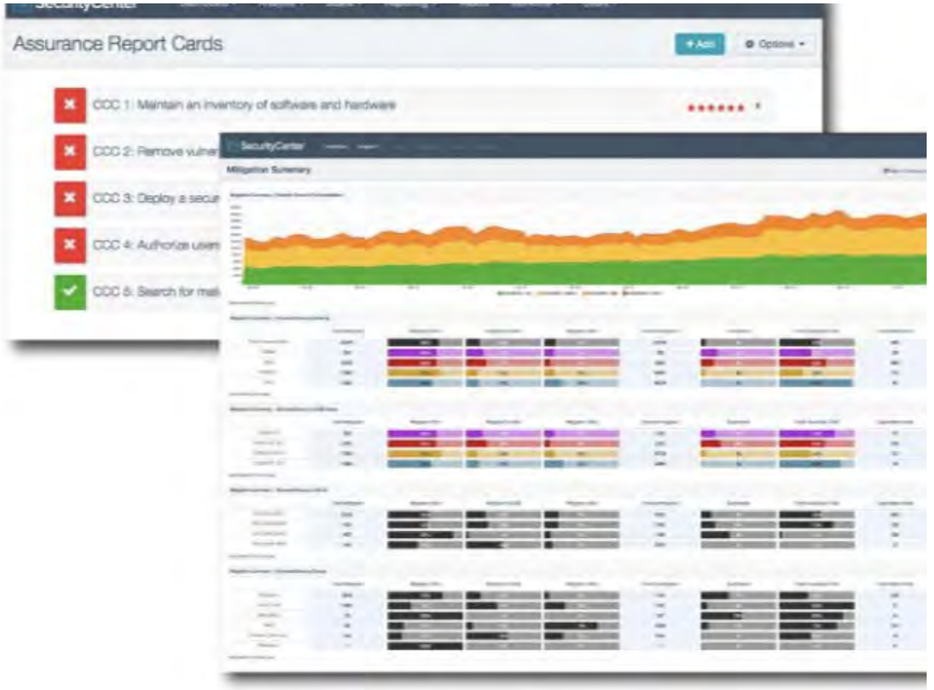
tenable

sarenet

tenable.sc™

Identifique, investigue y priorice vulnerabilidades de forma precisa.

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

tenable.sc™

Identifique, investigue y priorice
vulnerabilidades de forma precisa.

- **Tecnología Security Center de Tenable explotada desde el Data Center de Sarenet por personal de seguridad propio gracias a un acuerdo estratégico**
- Complemento ideal de seguridad para aportar **contexto global e información completa de ciberexposición** (más allá de perímetro, red y puesto de trabajo o servidores)
- **Nessus** cuenta con **más de 130000 plugins** implementados
- 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.sc™

Identifique, investigue y priorice
vulnerabilidades de forma precisa.

Common Vulnerability Scoring System

CVSS es un sistema de puntuación que proporciona un método estándar y abierto para estimar el impacto de una vulnerabilidad y que se compone tres grupos principales de métricas: Base, Temporal y de Entorno (Environmental). Cada uno de estos grupos se compone a su vez de un conjunto de métricas.

Grupo Base: Engloba las cualidades intrínsecas de una vulnerabilidad y que son independientes del tiempo y el entorno. Las métricas evaluadas en este grupo son:

- **Access Vector (AV)**. Valores: [L,A,N] (Local, Adjacent, Network
- **Access Complexity (AC)**. Valores [H,M,L] (High, Medium, Low)
- **Authentication (Au)**. Valores [M,S,N] (Multiple, Single, None)
- **Confidenciality Impact (C)** . Valores [N,P,C] (None, Partial, Complete)
- **Integrity Impact (I)**. Valores [N,P,C] (None, Partial, Complete)
- **Availability Impact (A).** Valores [N,P,C] (None, Partial, Complete)

Grupo Temporal: Características de la vulnerabilidad que cambian en el tiempo. Se aplican tres métricas::

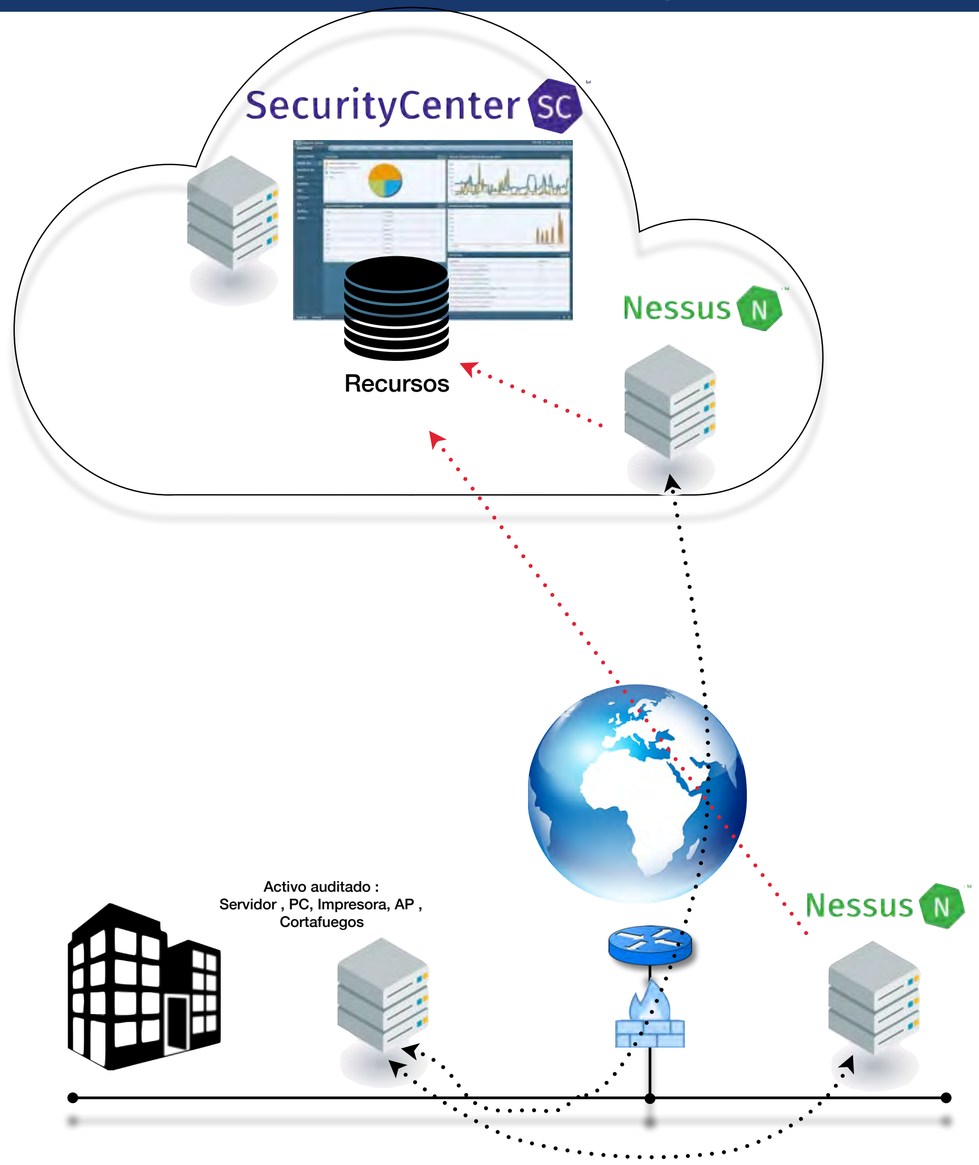
- **Exploitability (E).** Valores: [U,POC,F,H,ND] (Unproven, Proof-of-Concept, Functional Exploit, High, Not Defined)
- **Remediation Level (RL).** Valores: [OF,TF,W,U,ND] (Official Fix, Temporary Fix, Workaround, Unavailable, Not Defined)
- **Report Confidence (RC).** Valores: [UC,UR,C,ND] (Unconfirmed, Uncorroborated, Confirmed, Not Defined)

Grupo Environmental: Las características de la vulnerabilidad relacionadas con el entorno del usuario. En este caso los factores que se evalúan son:

- **Collateral Damage Potential (CDP).** Valores: [N,L,LM,MH,H,ND] (None, Low, Low Medium, Medium High, High, Not Defined)
- **Target Distribution (TD).** Valores: :[N,L,M,H,ND] (None, Low, Medium, High, Not Defined)
- **Security Requirements (CR, IR, AR).** Valores: [L,M,H,ND] (Low, Medium, High, Not Defined)

tenable.sc™

Identifique, investigue y priorice vulnerabilidades de forma precisa.



tenable

sarenet

tenable.sc™

Identifique, investigue y priorice
vulnerabilidades de forma precisa.

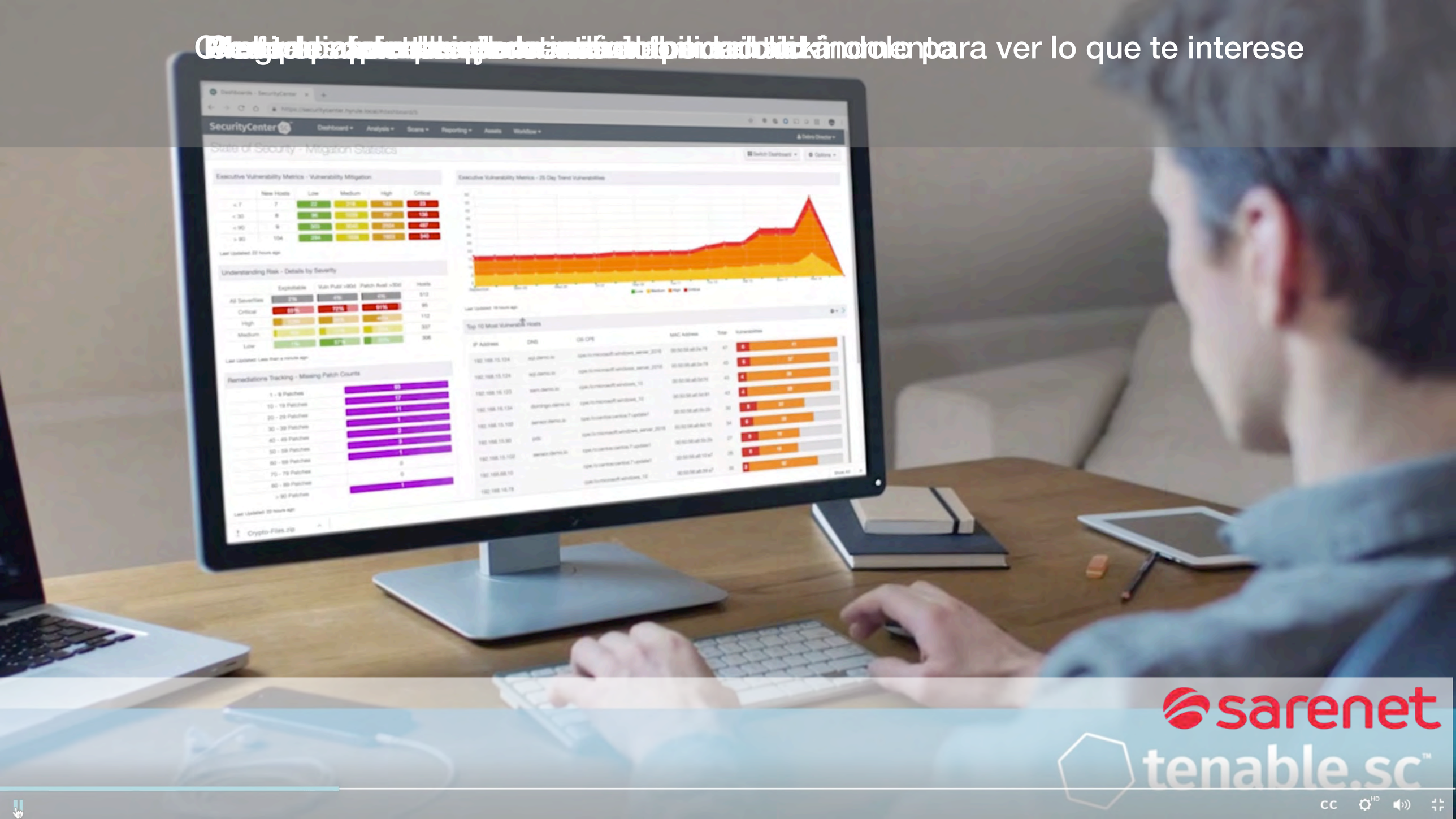
Beneficios clave

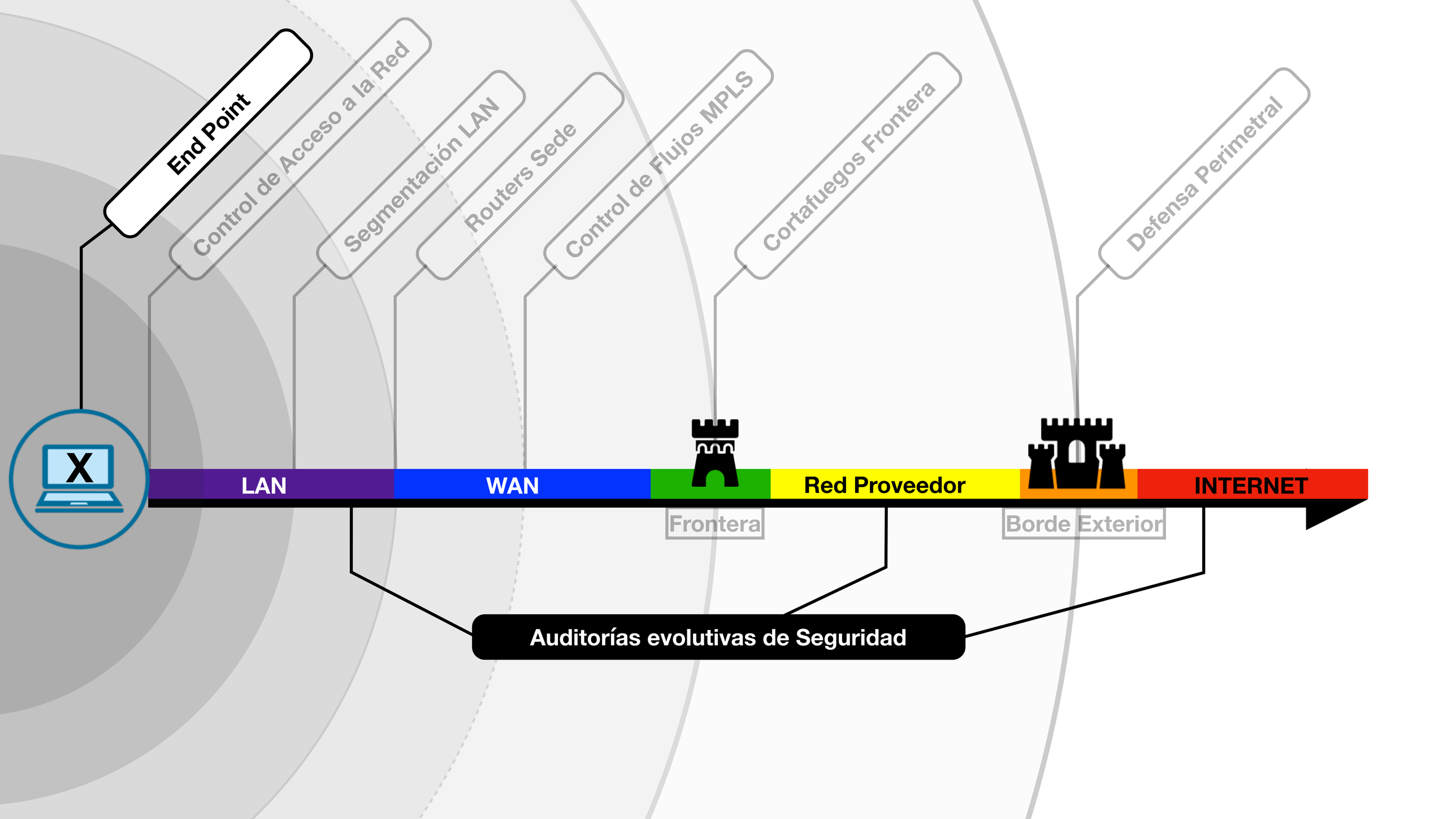
- **Identifica las debilidades** al escanear los activos conectados a la red en busca de vulnerabilidades conocidas, configuraciones erróneas y malware
- Nos da una medida objetiva del grado de ciberexposición del activo **CVSS**
- Permite un seguimiento efectivo del **cumplimiento de la política de 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 automatizada

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

tenable

sarenet


SecurityCenter
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Executive Vulnerability Metrics - Vulnerability Mitigation
Executive Vulnerability Metrics - 25 Day Trend Vulnerabilities
Understanding Risk - Details by Severity
Remediations Tracking - Missing Patch Counts
Top 10 Most Vulnerable Hosts
sarenet
tenable.sc


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

Hito

1985

Founded in Abingdon (Oxford), UK

Peter Lammer c1985

Jan Hruska c1985

1988

First checksum-based antivirus software

Inicio

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

Acquired Utimaco Safeware AG

utimaco safeware

SafeGuard Enterprise Encryption

Acquired Astaro

astaro internet security

Acquired DIALOGS

DIALOGS connecting business

Divested non-core Cyber business

Acquired Cyberoam

Cyberoam

Acquired Mojave Networks

mojave

IPO London Stock Exchange

London Stock Exchange

Sophos XG

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

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

400,000

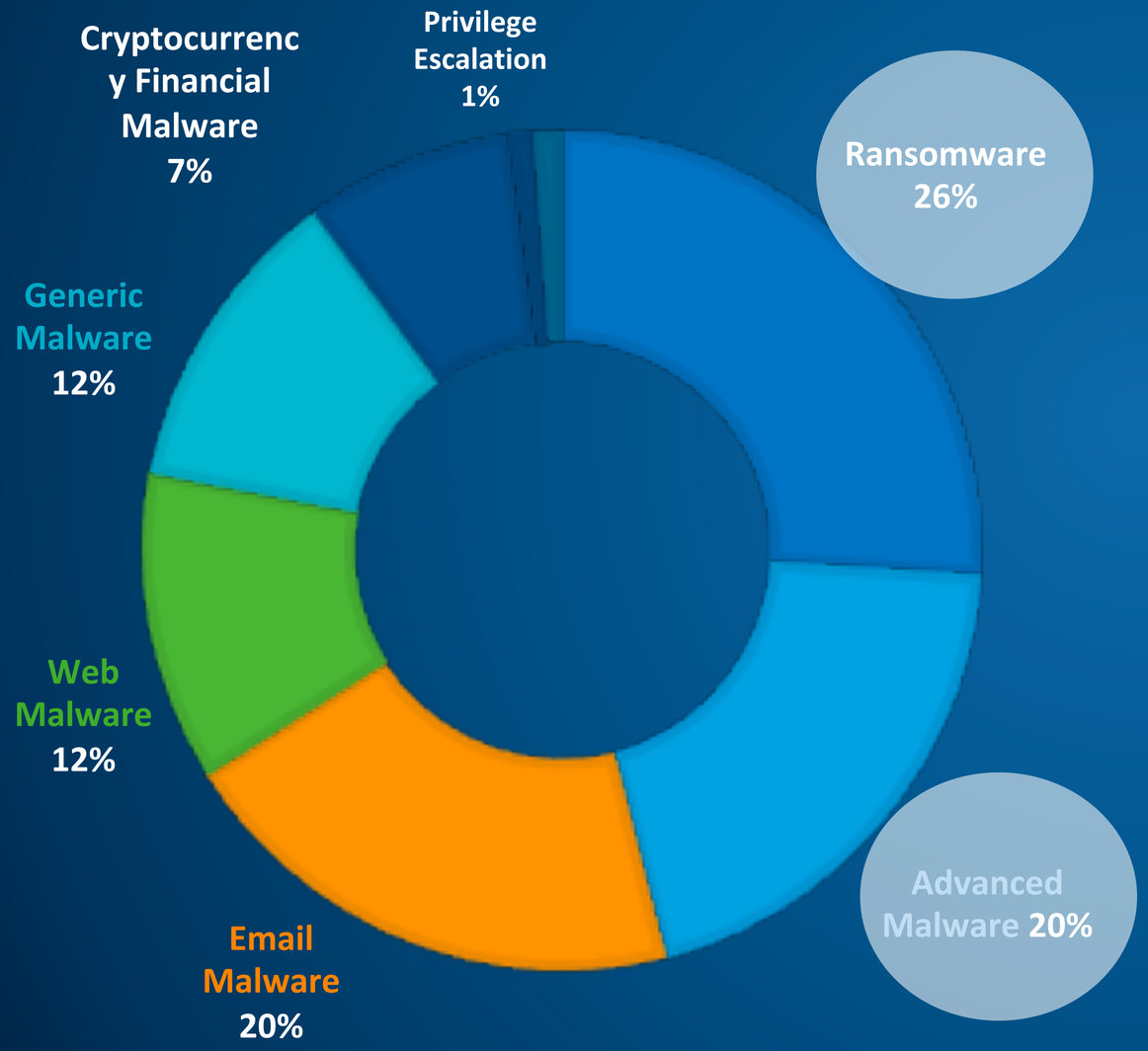
SophosLabs receives and processes 400,000 previously unseen malware samples each day.

75% of the malicious files SophosLabs detects are found only within a single organization.

SOPHOS

Source: SophosLabs

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

Yo lo compraría sólo por el nombre .....

Ransomware - Wannacry (ficheros)
Petya - MBR (registro de arranque maestro)

Gartner®

“Leader”

2018 Endpoint Protection Platform Magic Quadrant
Leader in all ten reports since it was first published
One of only 3 leaders

Winner
Security Innovation
of the Year

FORRESTER®

“Leader”

The Forrester Wave: Endpoint Security Suites
Off the charts strategy rating

Winner
Innovation Award
Endpoint Security

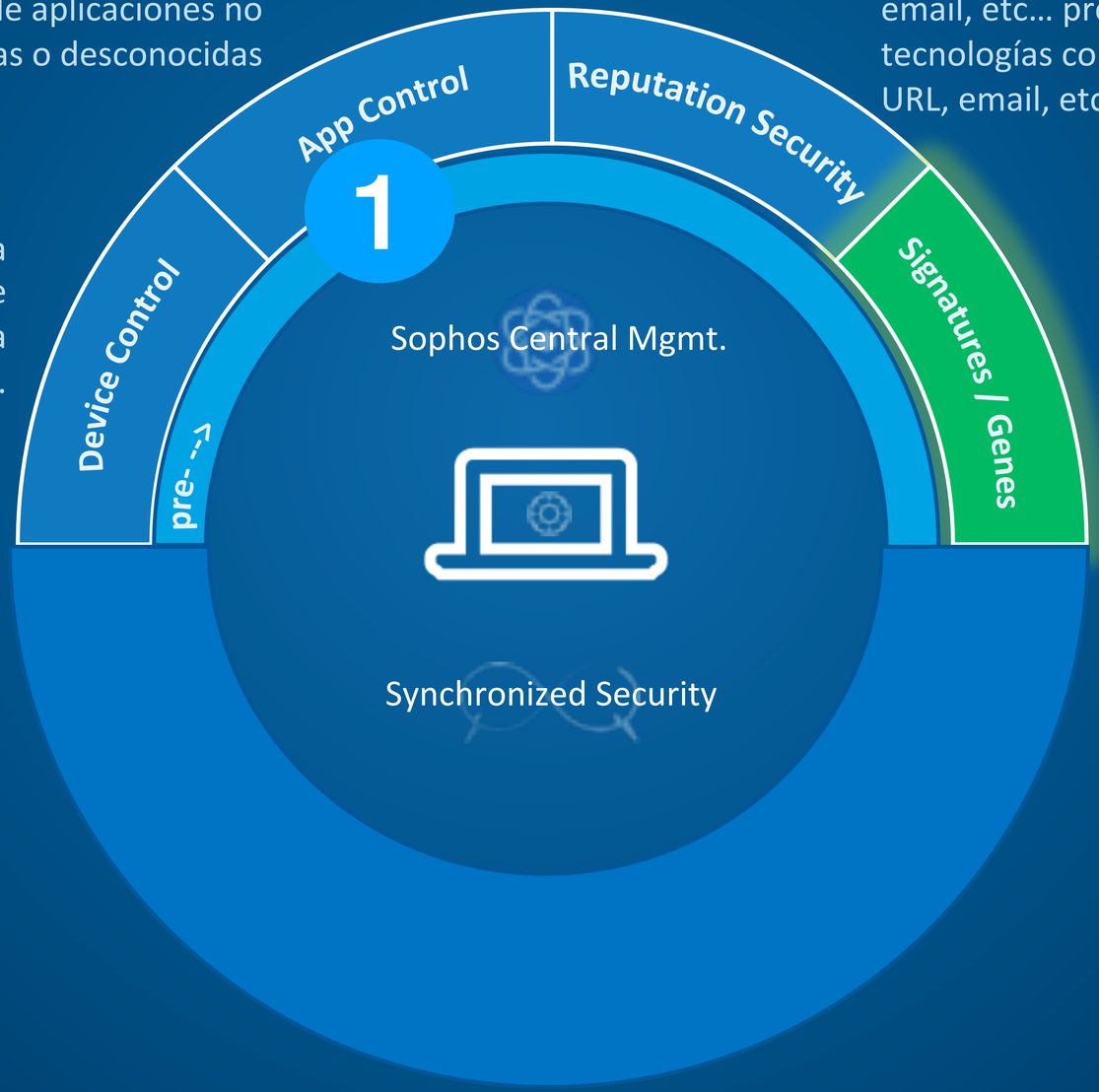
Protección Endpoint Tradicional

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

SOPHOS

sarenet

Gestion Centralizada

1

Control total

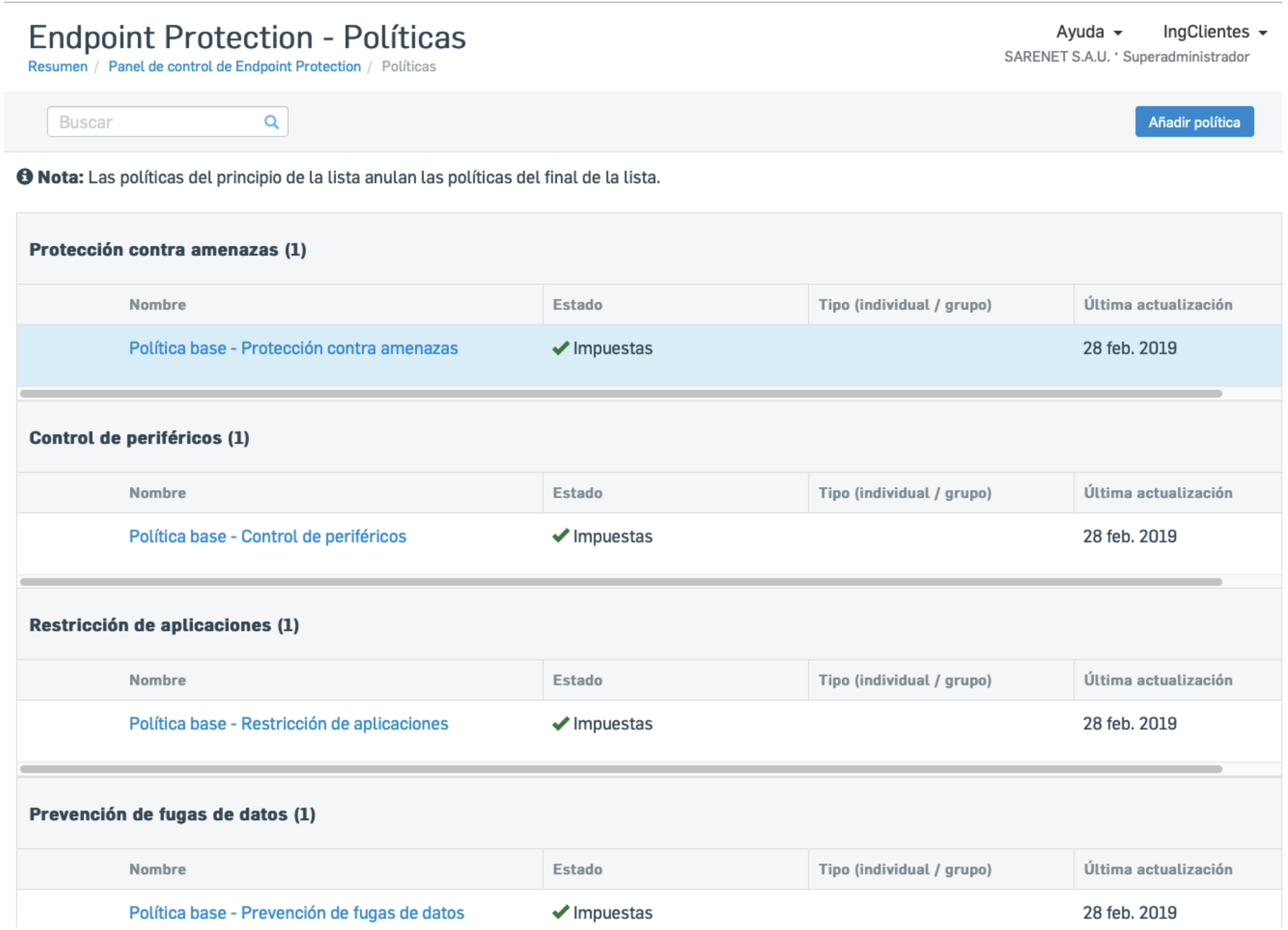
Aplique sus políticas de datos, dispositivo, aplicación y web con facilidad, gracias a la perfecta integración en el agente para estaciones y en la consola de administración.

- **Control web** Filtrado web basado en categorías aplicado dentro y fuera de la red corporativa
- **Control de la aplicación** Bloqueo de aplicaciones por categoría o por nombre con solo un clic
- **Control del dispositivo** Acceso controlado a medios extraíbles y dispositivos móviles
- **Control de datos** Prevención de pérdida de datos (DLP) que utiliza reglas preintegradas o personalizadas

Simplicidad sofisticada

Al igual que su aplicación favorita para web o teléfonos inteligentes, Sophos Endpoint Protection ofrece una funcionalidad sofisticada junto con una experiencia de usuario sencilla e intuitiva.

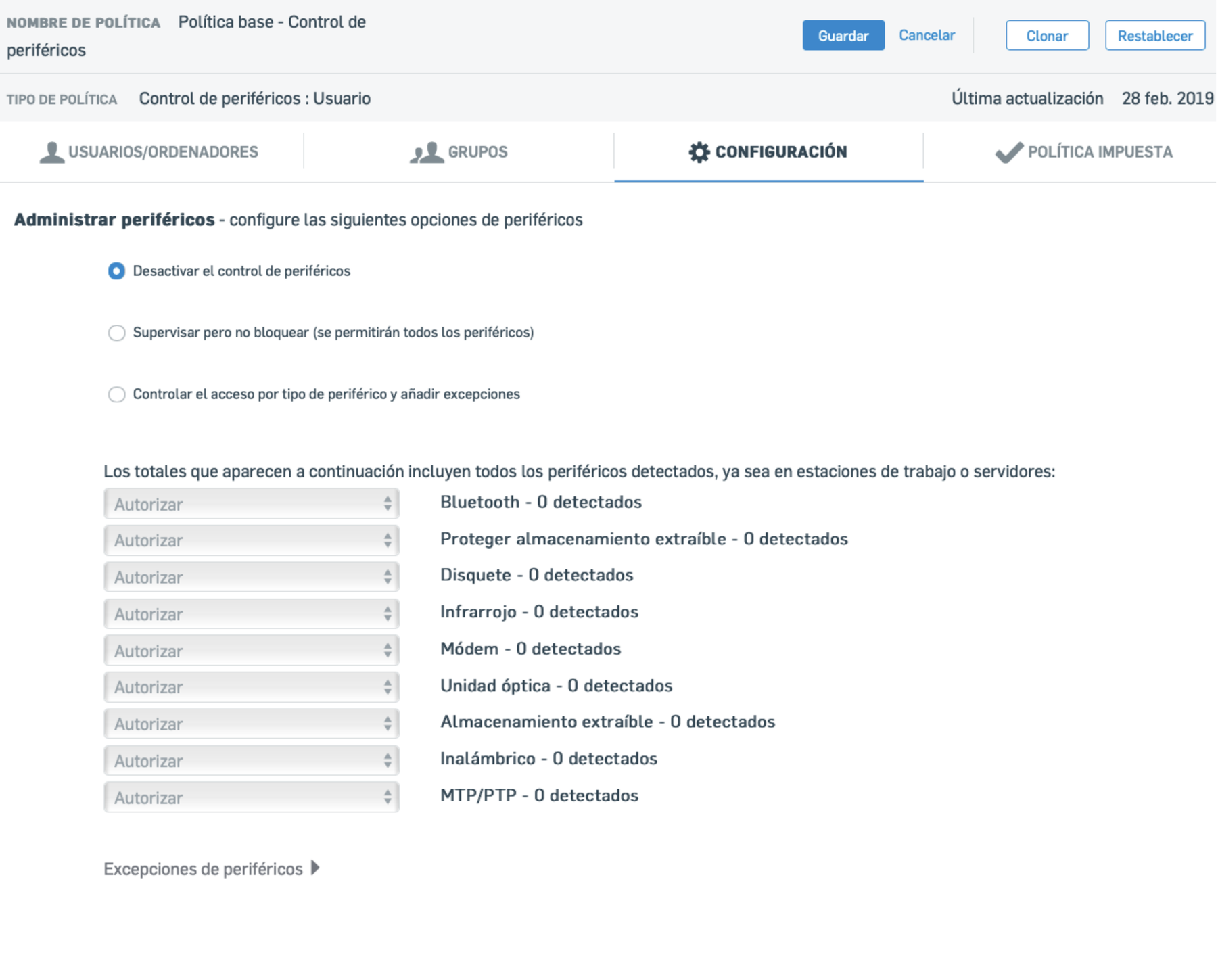
- Despliegue rápido y sencillo desde la nube o de forma local
- Políticas predeterminadas que se configuran para equilibrar la protección, usabilidad y rendimiento
- Eliminación automática de productos de seguridad para estaciones de terceros
- Configuración sencilla de funciones avanzadas tales como HIPS y control de dispositivo, gracias a los datos continuamente actualizados de SophosLabs



1

Gestión de políticas de diferentes naturalezas que aplicamos a usuarios o grupos

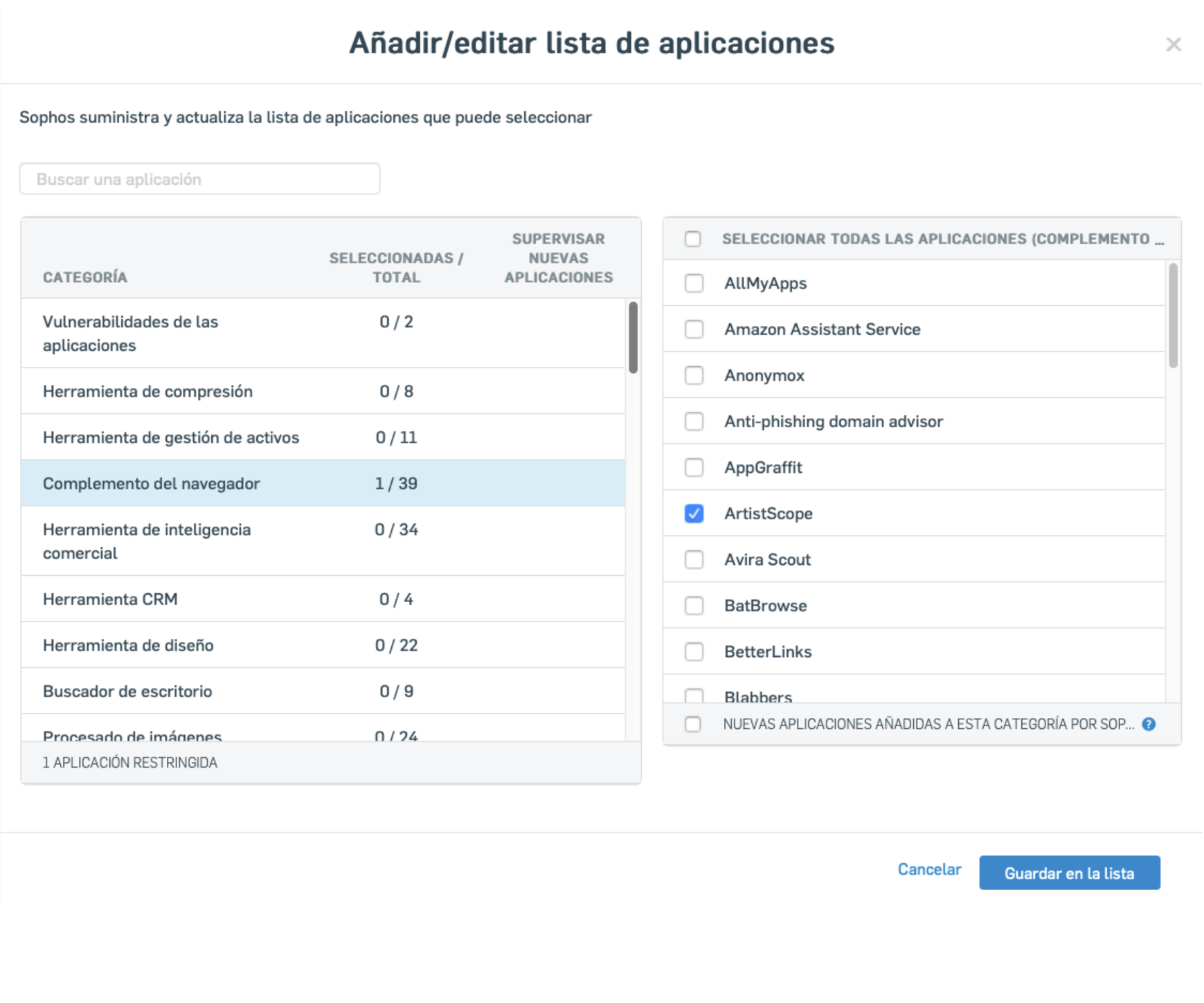
sarenet



1

Por ejemplo, podemos crear una política sobre los periféricos autorizados

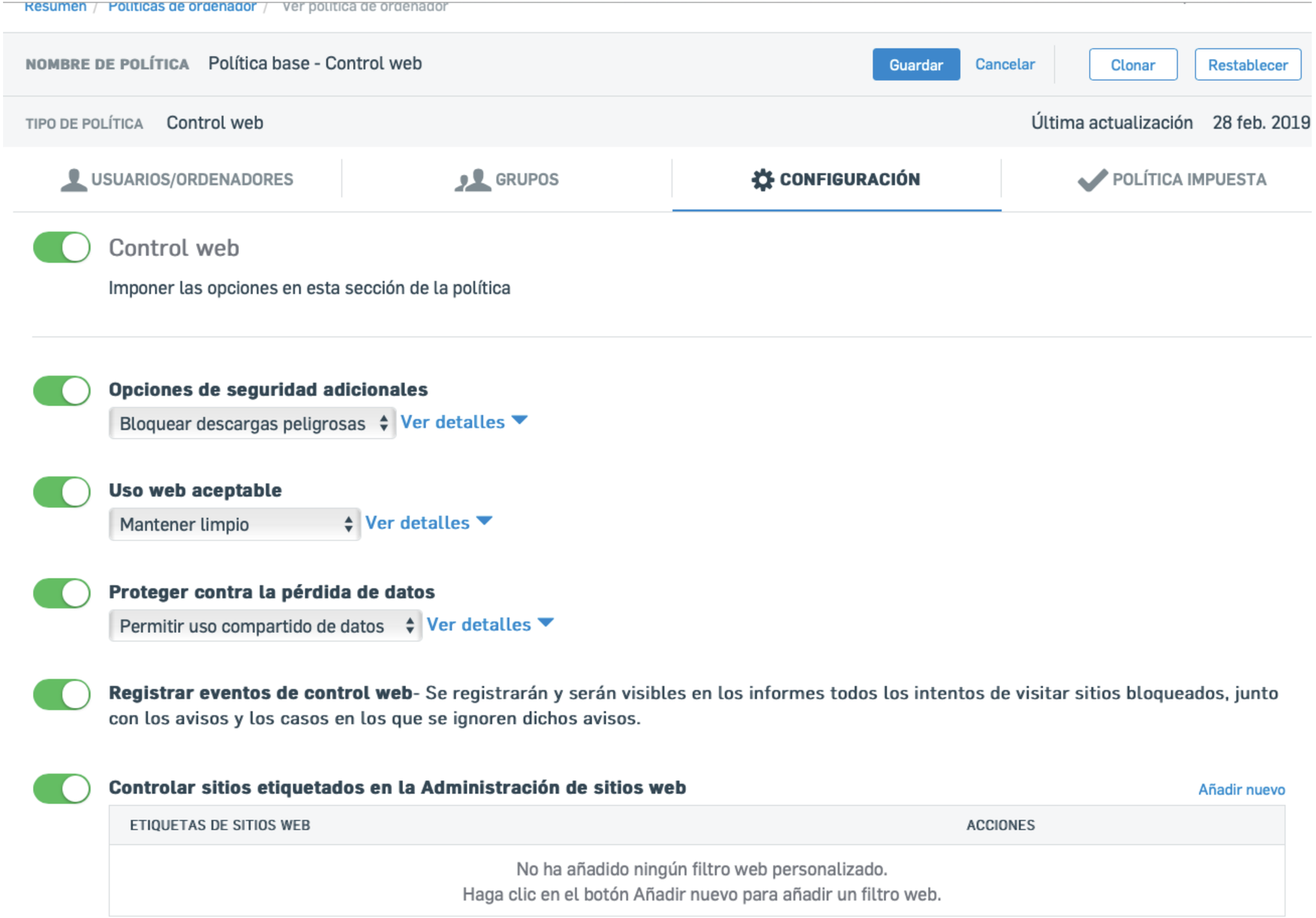
sarenet



1

O … las aplicaciones que dejamos , o no , utilizar

sarenet



1

O … controlar las acciones dentro de la navegación…

sarenet

1

O … el grado de protección…

Live Protection

Use Live Protection para comprobar la información sobre amenazas más reciente de SophosLabs online

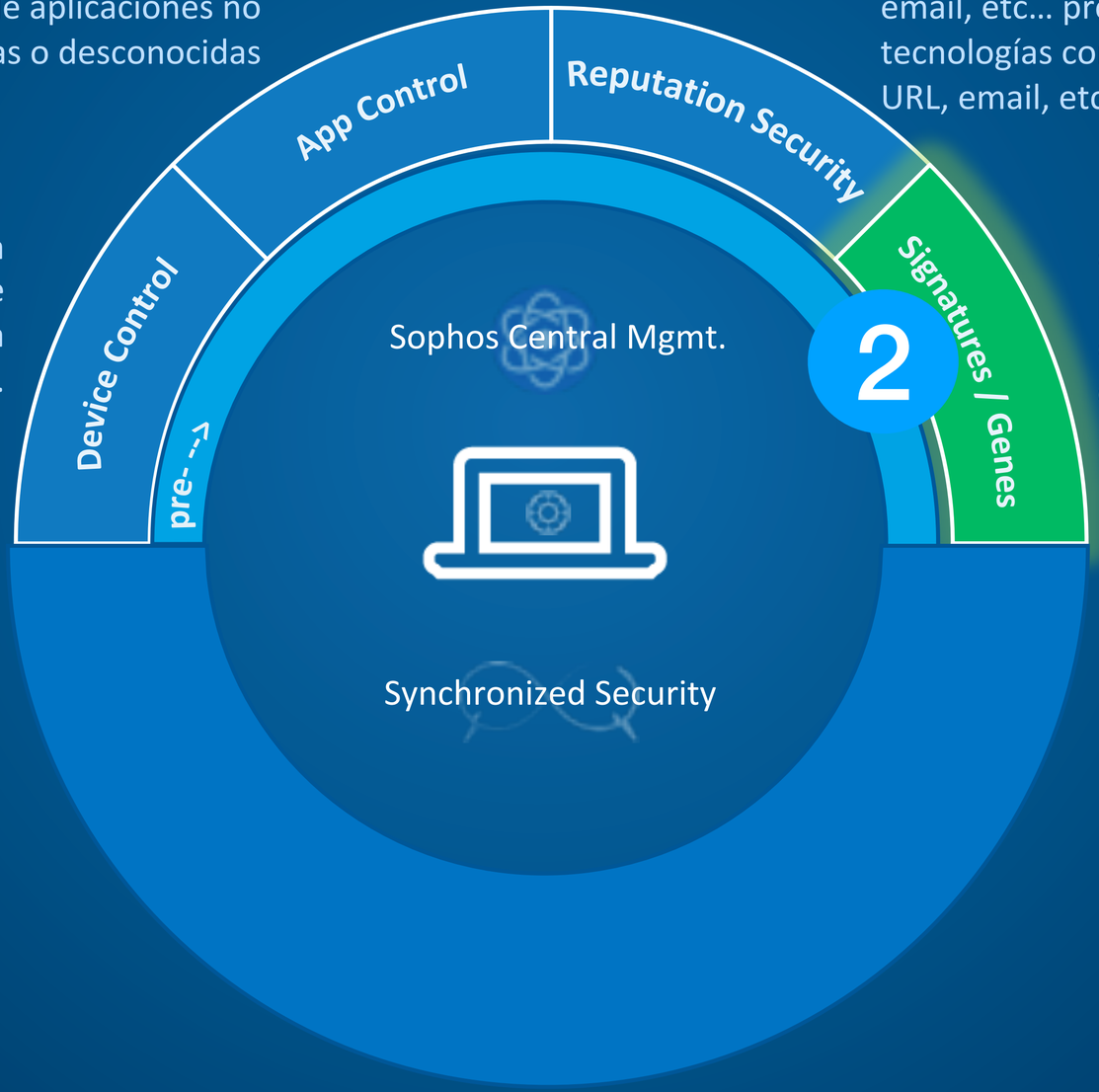
- **Usar Live Protection durante los escaneados programados**
- **Enviar automáticamente muestras de archivos a SophosLabs**

Nota: Es posible que los datos salgan de su región geográfica y se compartan con los ingenieros de Sophos.

Protección Endpoint Tradicional

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

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



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…

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

Machine Learning With Feature Selection Using Principal Component Analysis for Malware Detection: A Case Study

SophosLabs Matrix Report

SophosLabs 2019 Threat Report

MLPdf: An Effective Machine Learning-Based Approach for PDF Malware Detection

Today's Malware

Real-time data on the top malware threats from our award-winning SophosLabs Team. More

DocDl ▼ JSDldr ▼ Agent ▼ DrodZp ▼
Equatio ▲ Zbot ▼ Phish ▼ Upatre ▼

Today's Spam Threats

We monitor spam from all sources, every day. View our spam dashboard for real-time data. More

PdfUri ▼ 20180802 FareitVB ▲ RtfExp ▼
▲ DrodGzip ▲ Iframe ▲
BredoZp ▲ DrodZp ▼

Tweets by @SophosLabs

SophosLabs
@SophosLabs

More about #OldPhantomCrypter... The license for this kit can be purchased via the main distribution web page for $199 per month, which positions it in the league of the most expensive builders in the market.

See more in our technical paper: news.sophos.com/en-us/2019/02/...

Adware and PUAs

Controlled Applications

sarenet

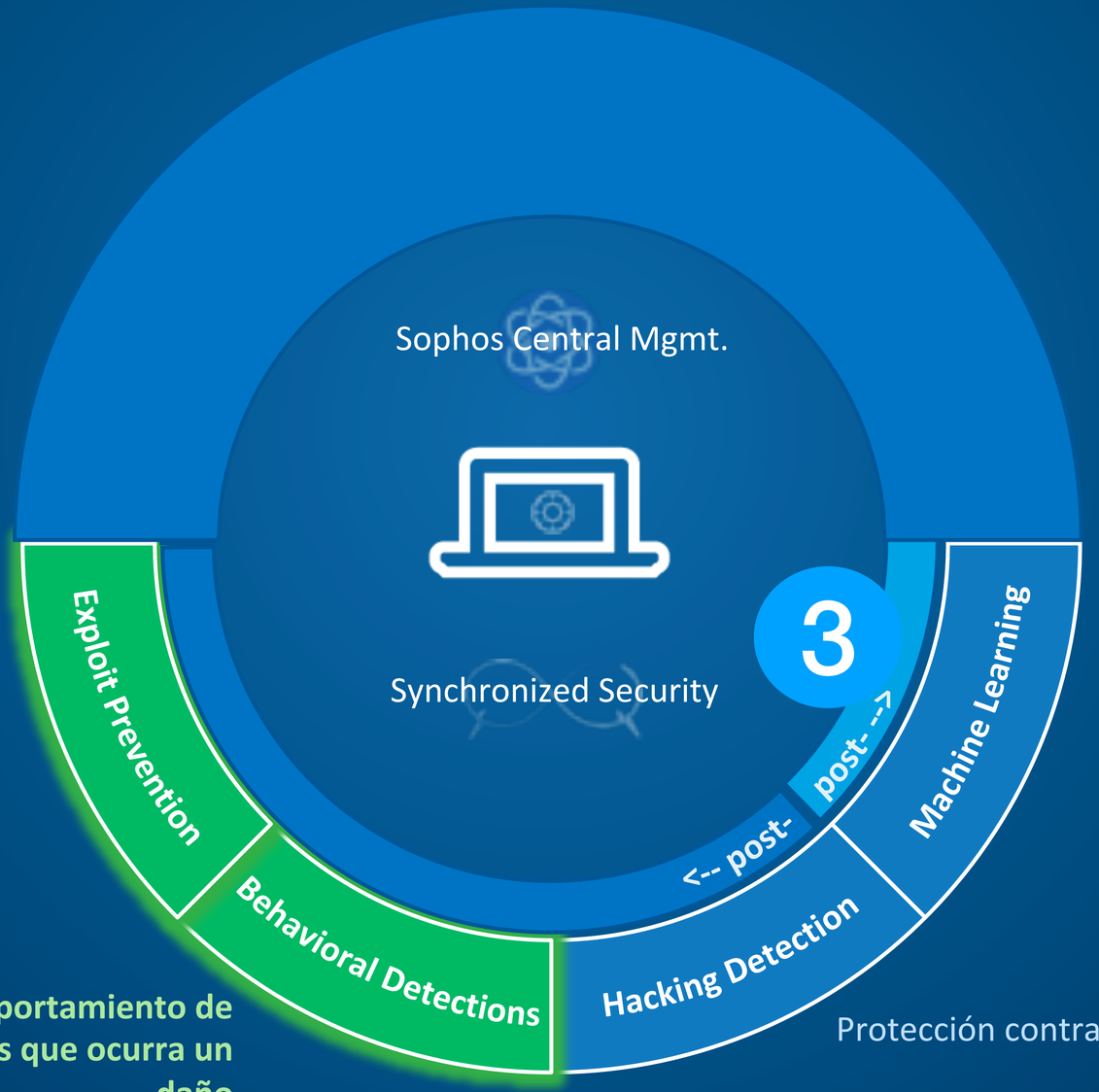
Protección EndPoint de Nueva Generación

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

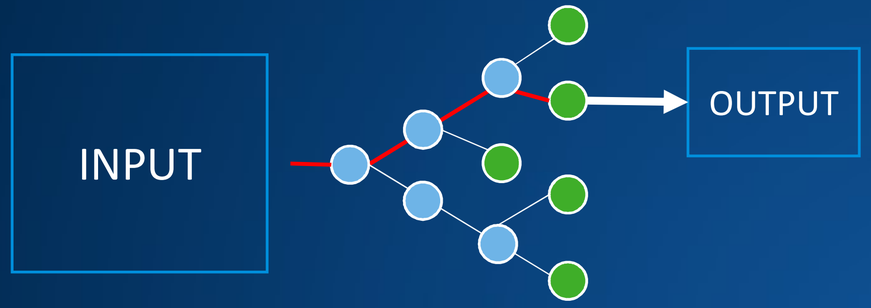
Protección contra técnicas post-explotación

SOPHOS

sarenet

Machine Learning Vs. Deep Learning

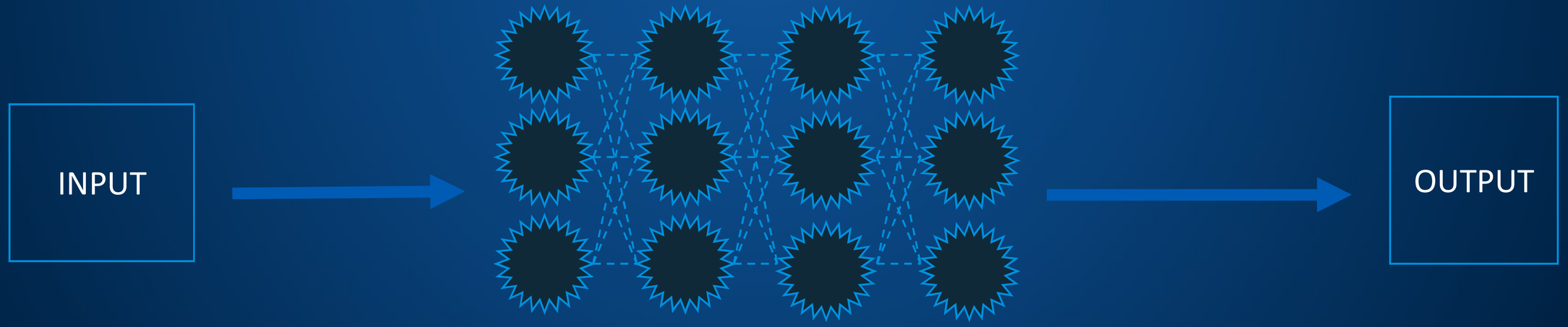
MACHINE LEARNING



Decision Tree

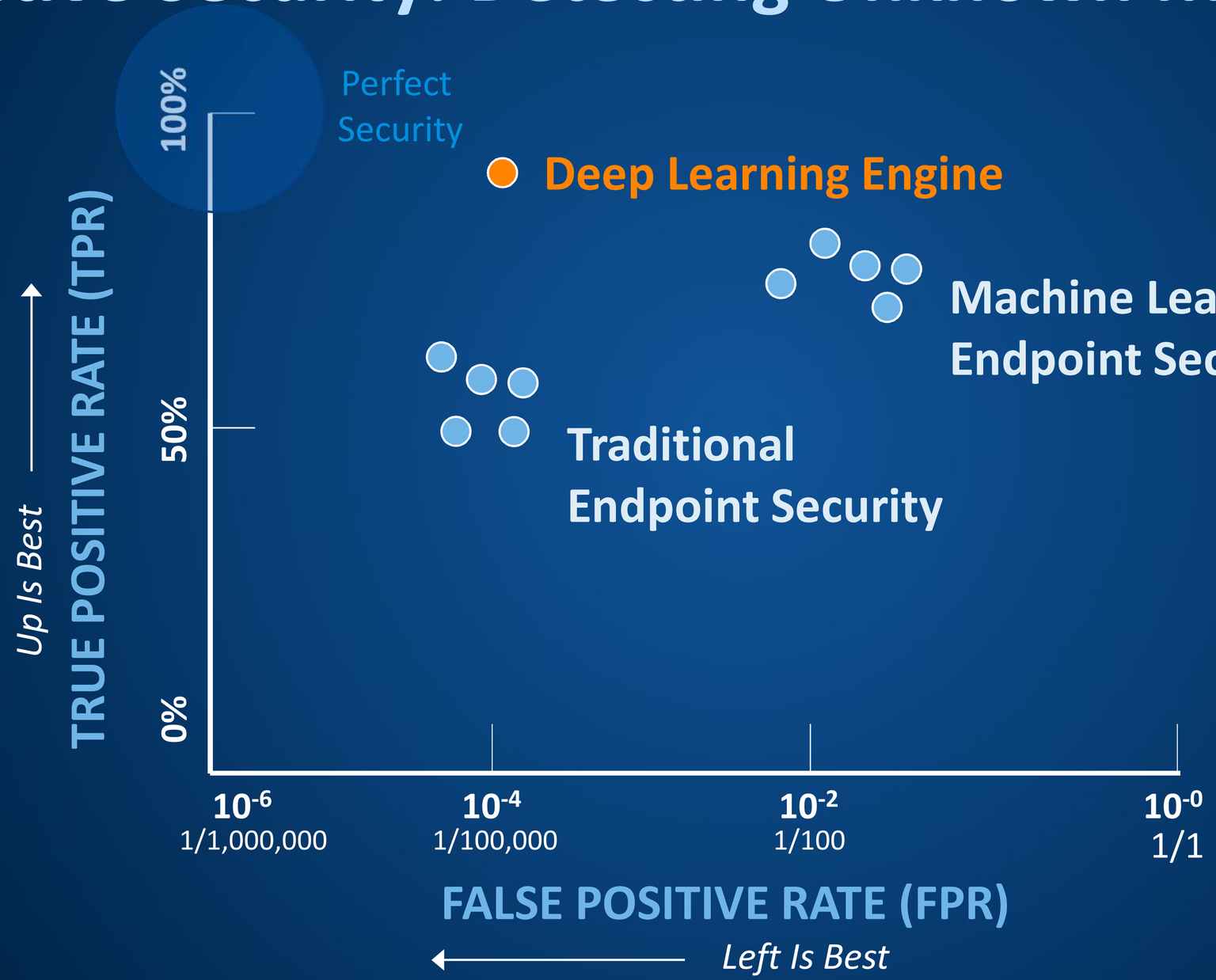
Random Forest

DEEP LEARNING



Interconnected Layers of Neurons, Each Identifying More Complex Features

Predictive Security: Detecting Unknown Malware



Source: SophosLabs analysis of malware found in the wild

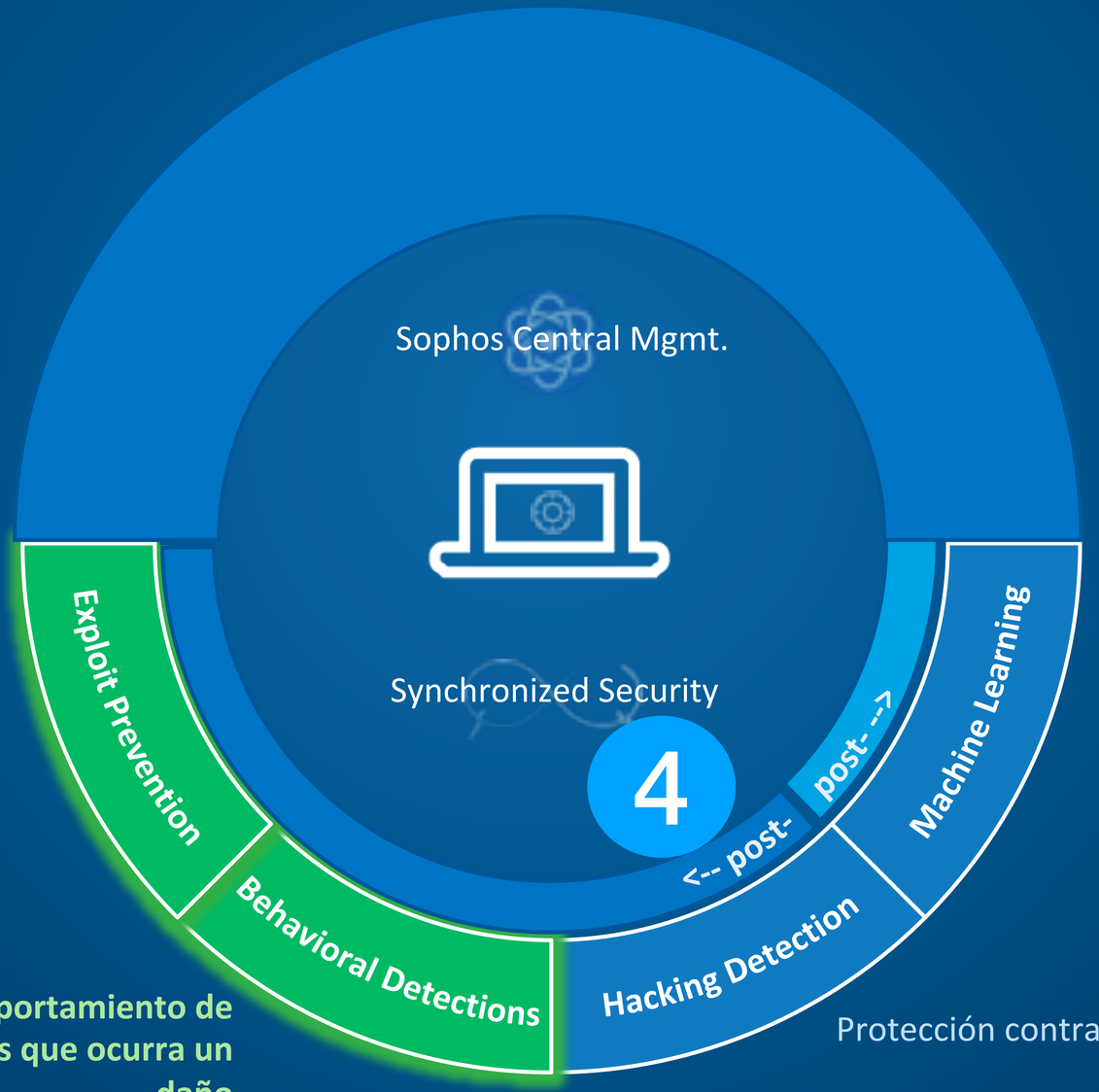
Protección EndPoint de Nueva Generación

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

Protección incluso cuando ya se ha vulnerado

4

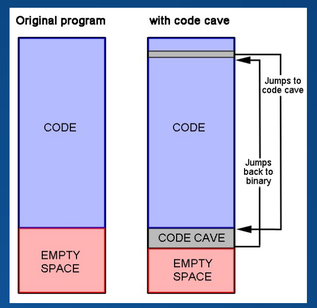
Credential Theft Protection

- Prevent dumping of credentials from memory
- Protect the credential database on Disk and Registry

Additional Registry Protections

- Sticky Key Mitigation
- Application Verifier Protection (Double Agent)

Active Adversary protections



- Code Cave prevention
- Malicious Process Migration
- Process privilege escalation
- APC Filter (prevent Atom Bombing exploit variants)
- Improved Application Lockdown
  - Powershell abuse from browsers
  - HTA apps

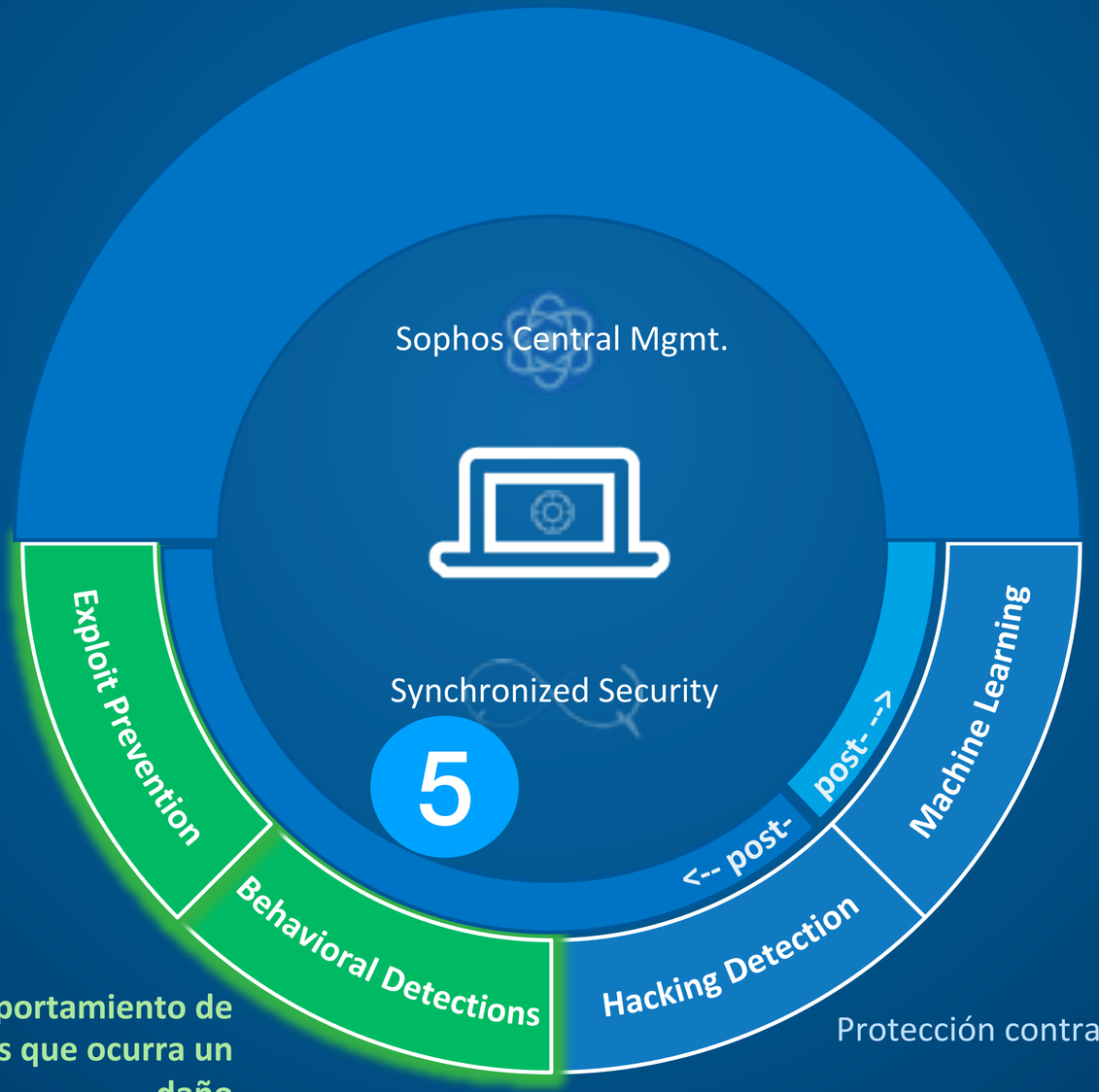
Protección EndPoint de Nueva Generación

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

InterceptX vs Ransomware = CryptoGuard + WipeGuard

File Protection

Stops Techniques That Encrypt or Compress Files

Disk and Boot Record Protection

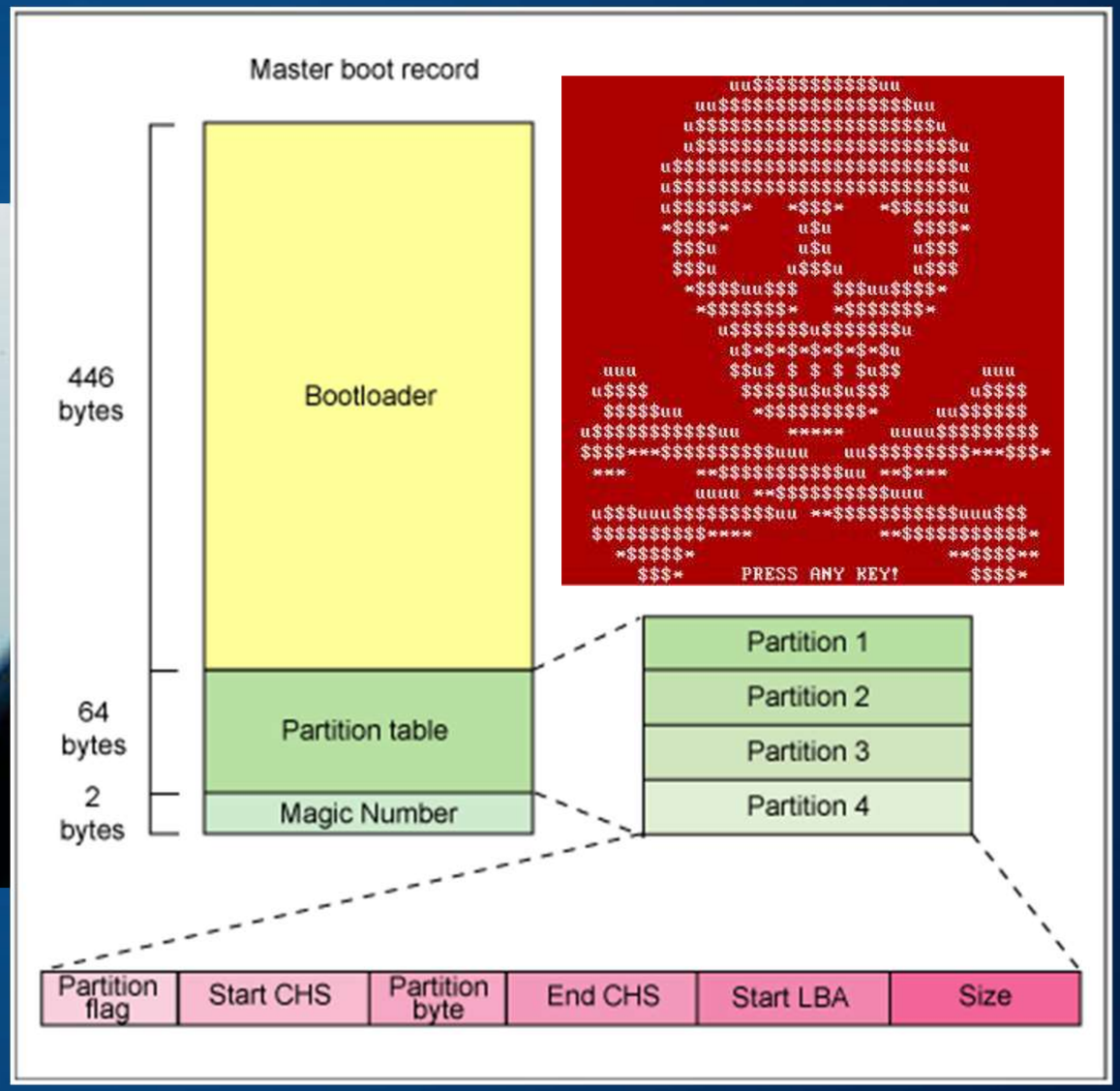
Stops Advanced Attacks that attempt to Lock a device pre-OS

Memory Protection

Stops Memory Exploits From Starting an Encryption Process

CryptoGuard – Interceptando Ransomware

WipeGuard: Modificación MBR



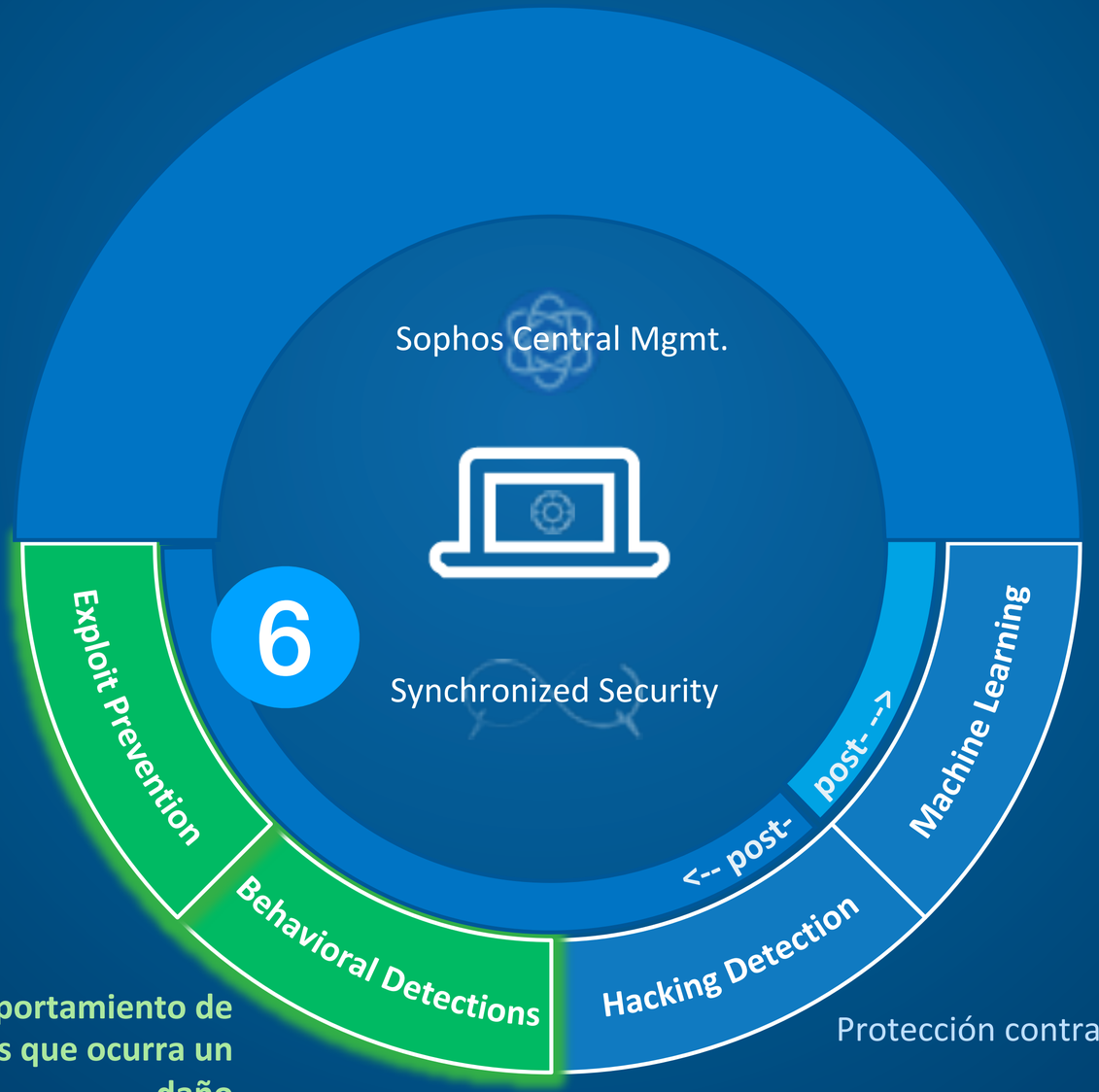
Protección EndPoint de Nueva Generación

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

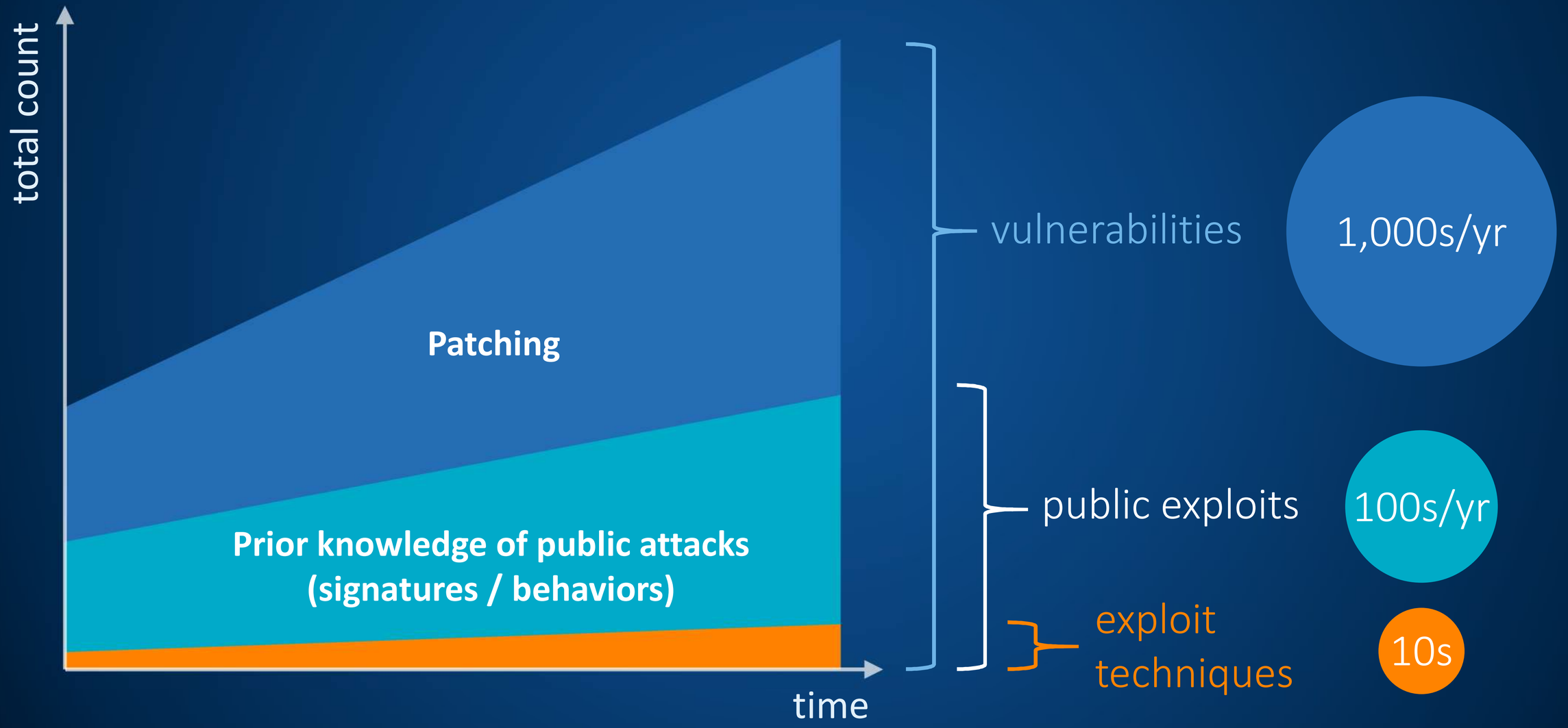
Protección contra técnicas post-explotación

SOPHOS

sarenet

Cómo podemos interceptar un Exploit

Vulnerabilities vs Exploits vs Exploit Techniques



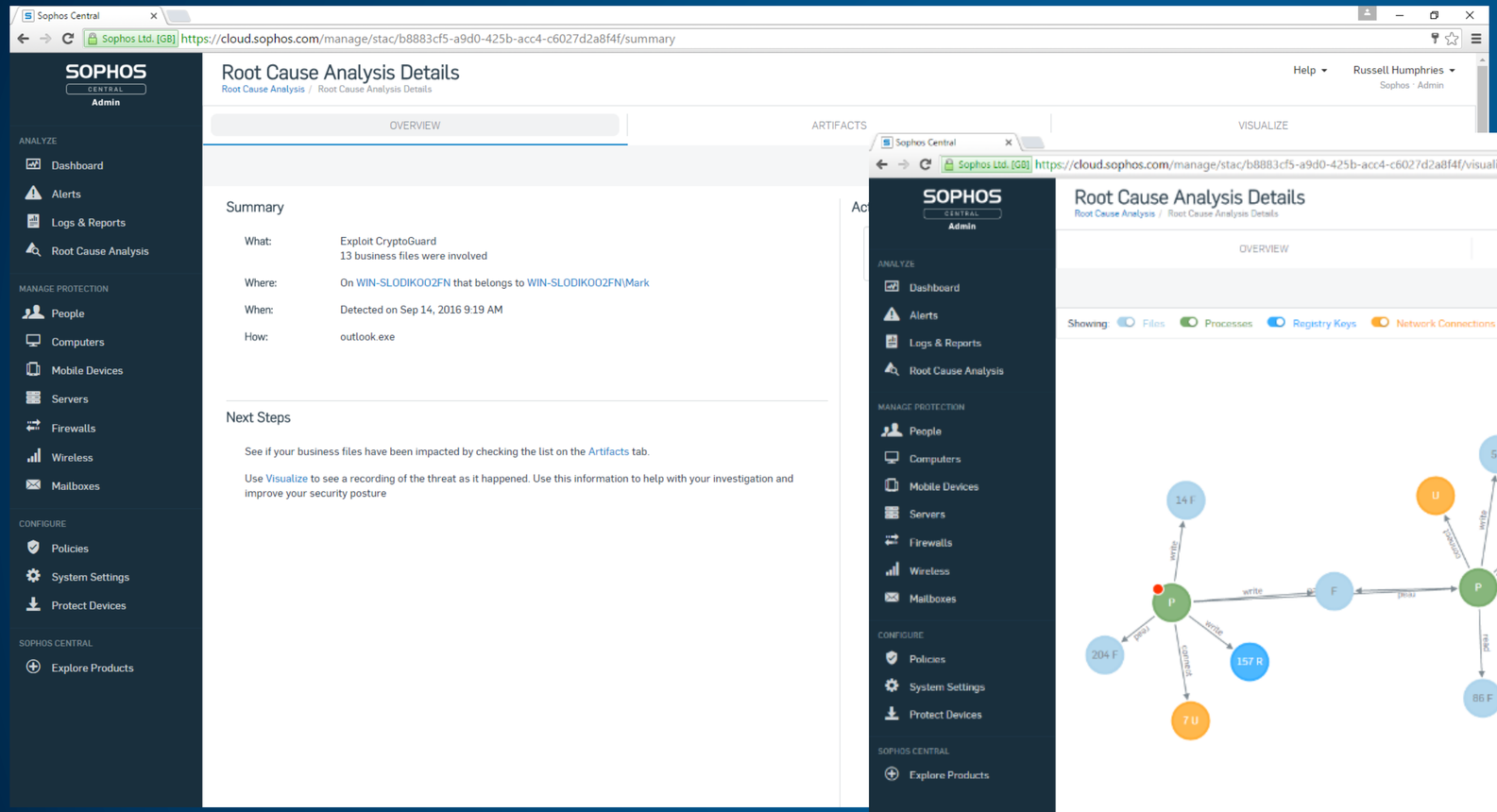
Some of the Exploit and Active Adversary Techniques Stopped by Intercept X

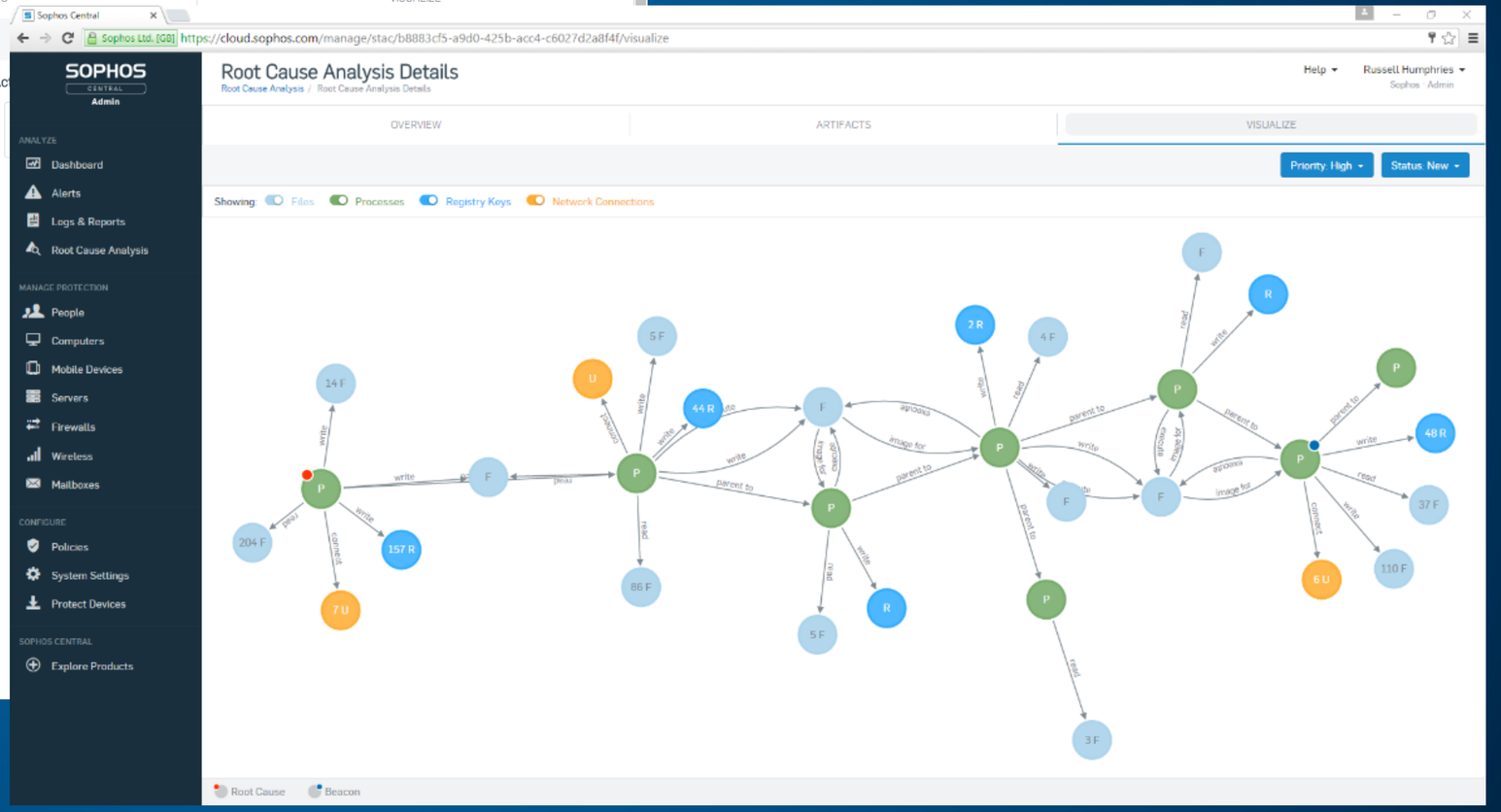
Enforce data execution prevention	Mandatory address space layout randomization	Bottom-up ASLR	Null page deference	Heap spray allocation	Dynamic heap spray	Stack pivot and stack exec (memory protection)
Stack-based ROP (caller)	Structured exception handling overwrite (SEHOP)	Import address table faltering (IAF)	Load library	Reflective DLL injection	Malicious shellcode	VBScript god mode
WOW64	Syscall	Hollow process	DLL hijacking	Squiblydoo Applocker bypass	APC protection (Double Pulsar / Atom Bombing)	Process privilege escalation
	Credential theft protection	Code cave mitigation	MITB protection (Safe Browsing)	Malicious traffic detection	Meterpreter shell detection	

Analisis de causa raiz

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

6





SOPHOS

sarenet

Protección EndPoint de Nueva Generación

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…

.exe Malware

Non-.exe Malware

Script-based Malware

Phishing Attacks

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

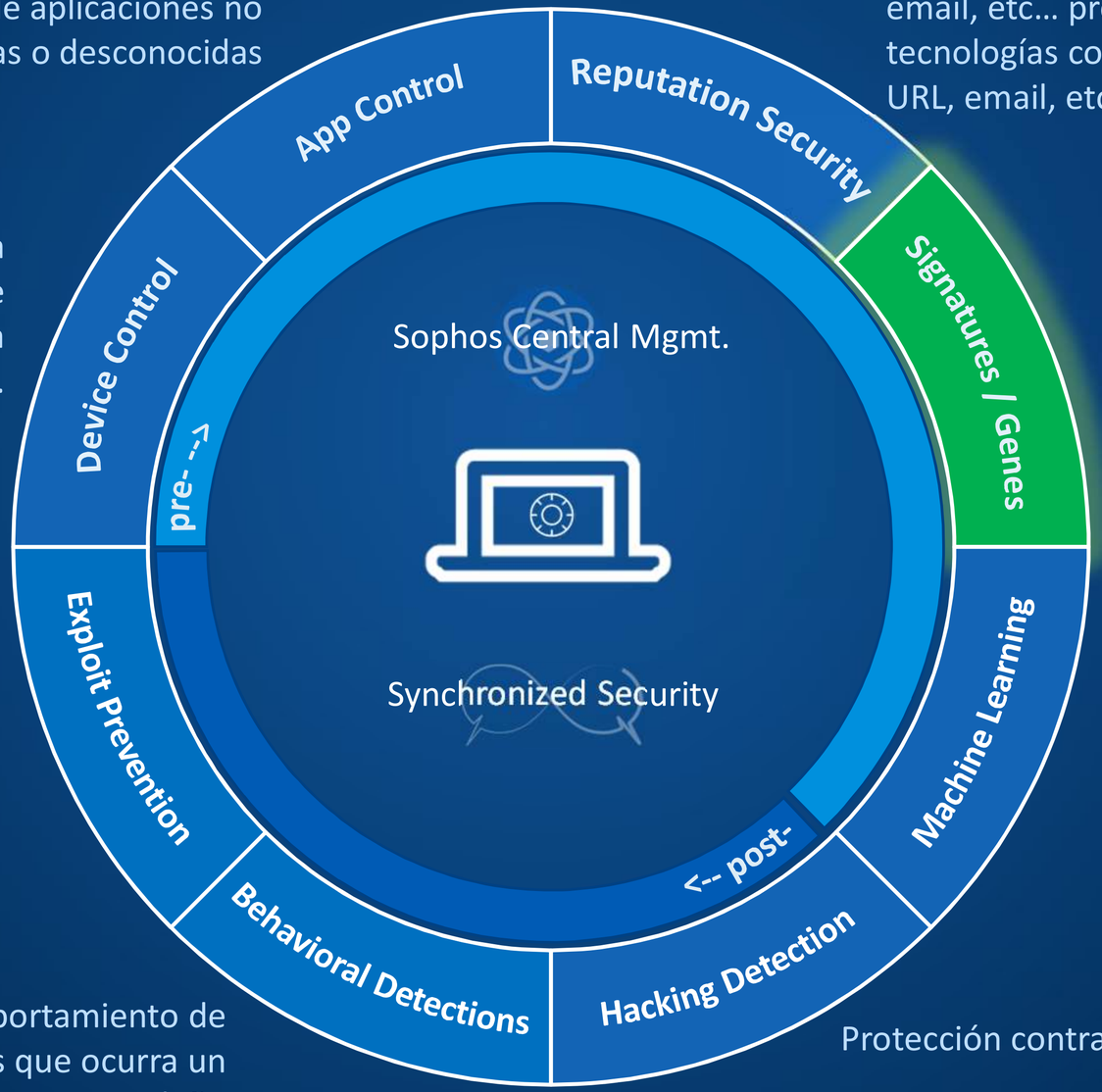
Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,

Malicious URLs

Exploits

Removable Media

Unauthorized Apps



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

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 malware basado en memoria.

SOPHOS

sarenet

PROTECCIÓN AVANZADA CON APRENDIZAJE MEDIANTE DEEP LEARNING DE TÉCNICAS Y COMPORTAMIENTOS DE ATAQUE				PROTECCIÓN TRADICIONAL CON FICHEROS POR FIRMAS
	Sophos Intercept X Advanced with EDR	**Sophos Intercept X Advanced**	**Sophos Intercept X**	**Sophos Endpoint Protection**
Técnicas base	✔	✔		✔
Deep Learning	✔	✔	✔	
Antiexploits	✔	✔	✔	
Antiransomware de CryptoGuard	✔	✔	✔	
Detección y respuesta para endpoints (EDR)	✔			

SOPHOS

sarenet

RESUMEN DE LAS 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**
- **Multiplataforma : 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

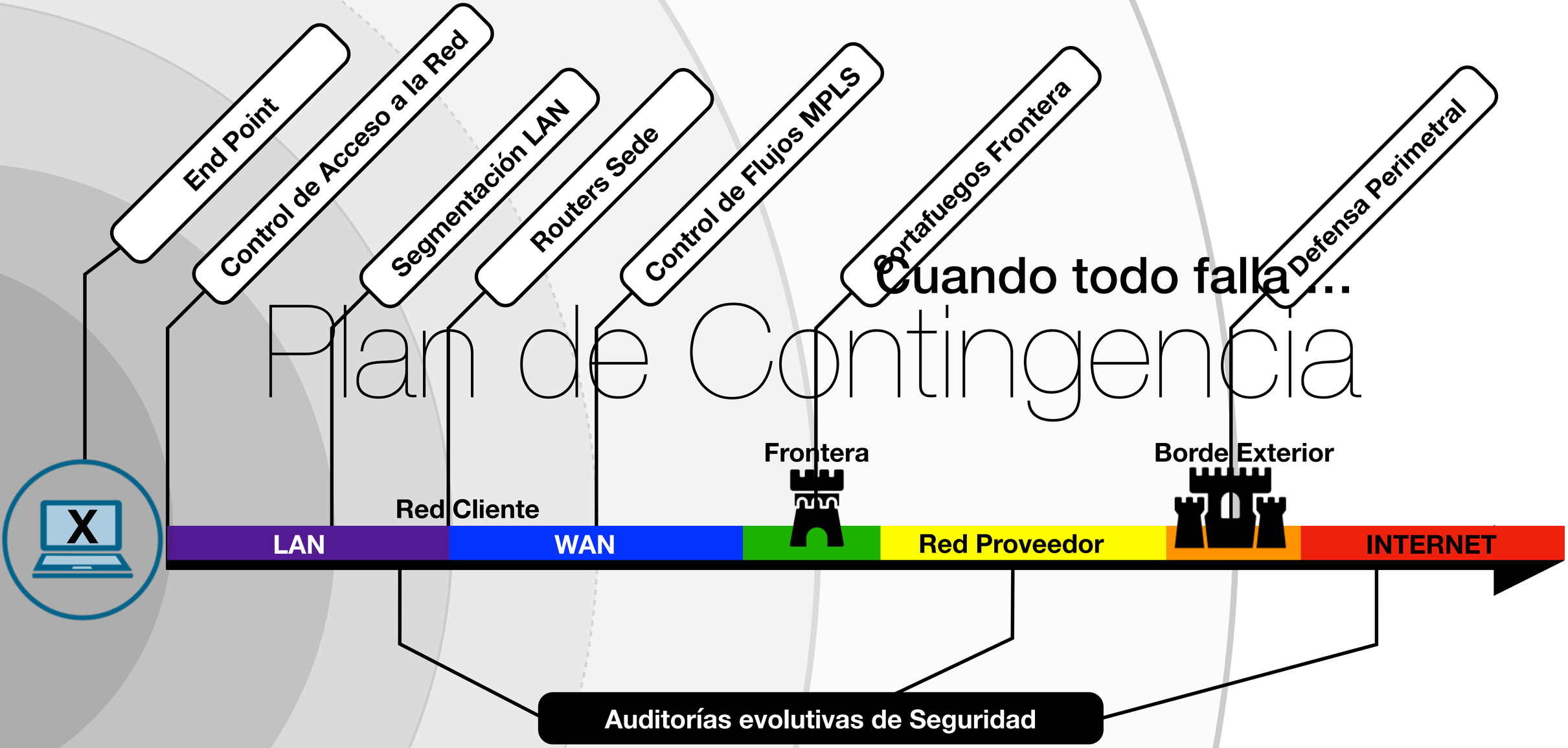
sarenet

¡¡ PRUEBALO SIN COSTE!!

Envía un mail a ingenieriaclientes@sarenet.es poniendo en el asunto “Demo Sophos Valencia” 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
Cuando todo falla...
Plan de Contingencia
Frontera
Borde Exterior
Red Cliente
LAN
WAN
Red Proveedor
INTERNET
Auditorías evolutivas de Seguridad

Plan de Contingencia

Veeam Cloud Connect

sarenet

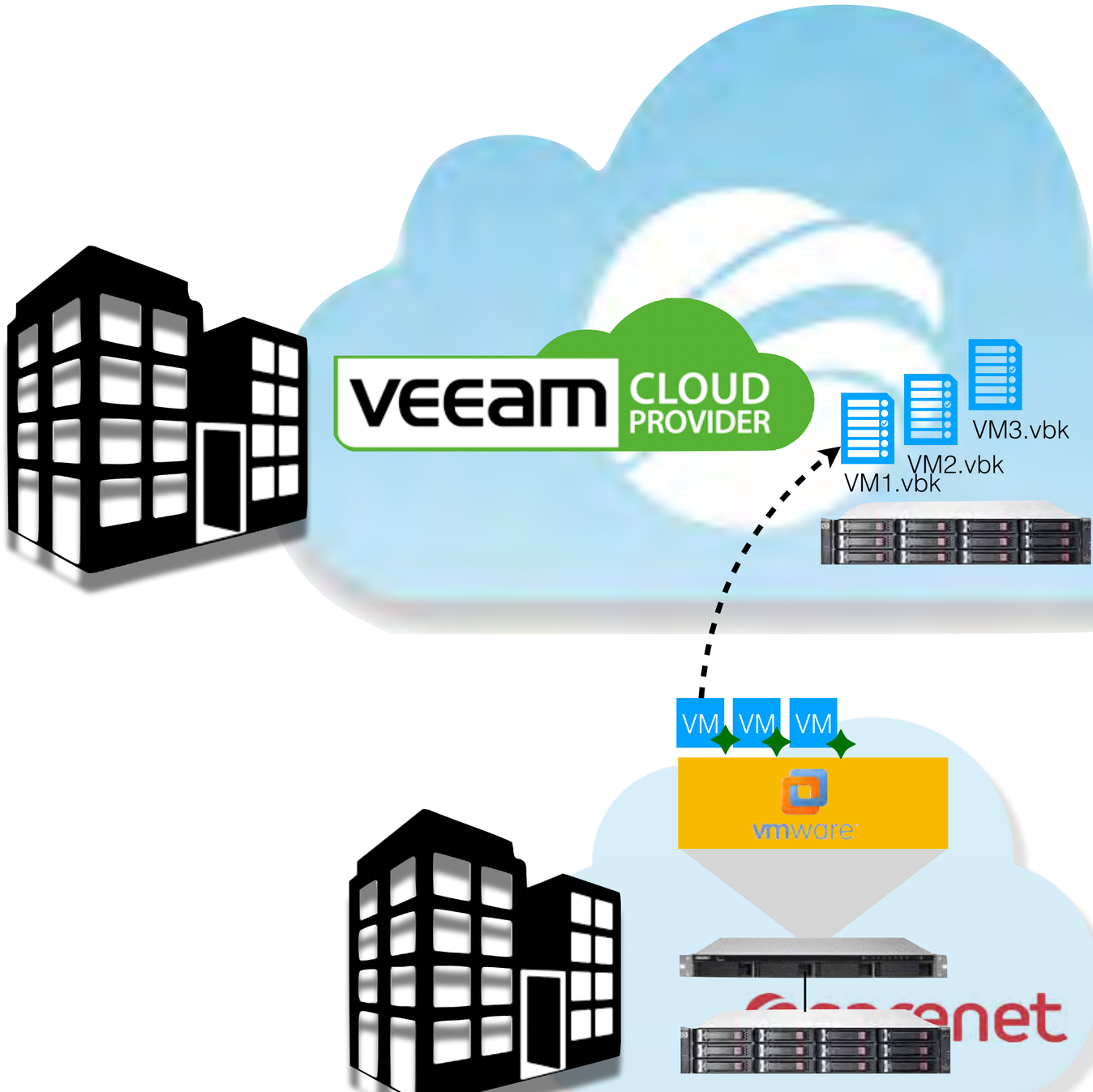
Plan de Contingencia

Veeam Cloud Connect

Veeam Cloud Connect **Backup**

Ahora, además de tener las copias generadas con Veeam en local , puedes almacenarlas fuera de tus instalaciones de forma totalmente segura

Gestiona tu conexión con este almacenamiento desde el propio Veeam y accede a tus copias y restáuralas en local cuando quieras



Plan de Contingencia

Veeam Cloud Connect

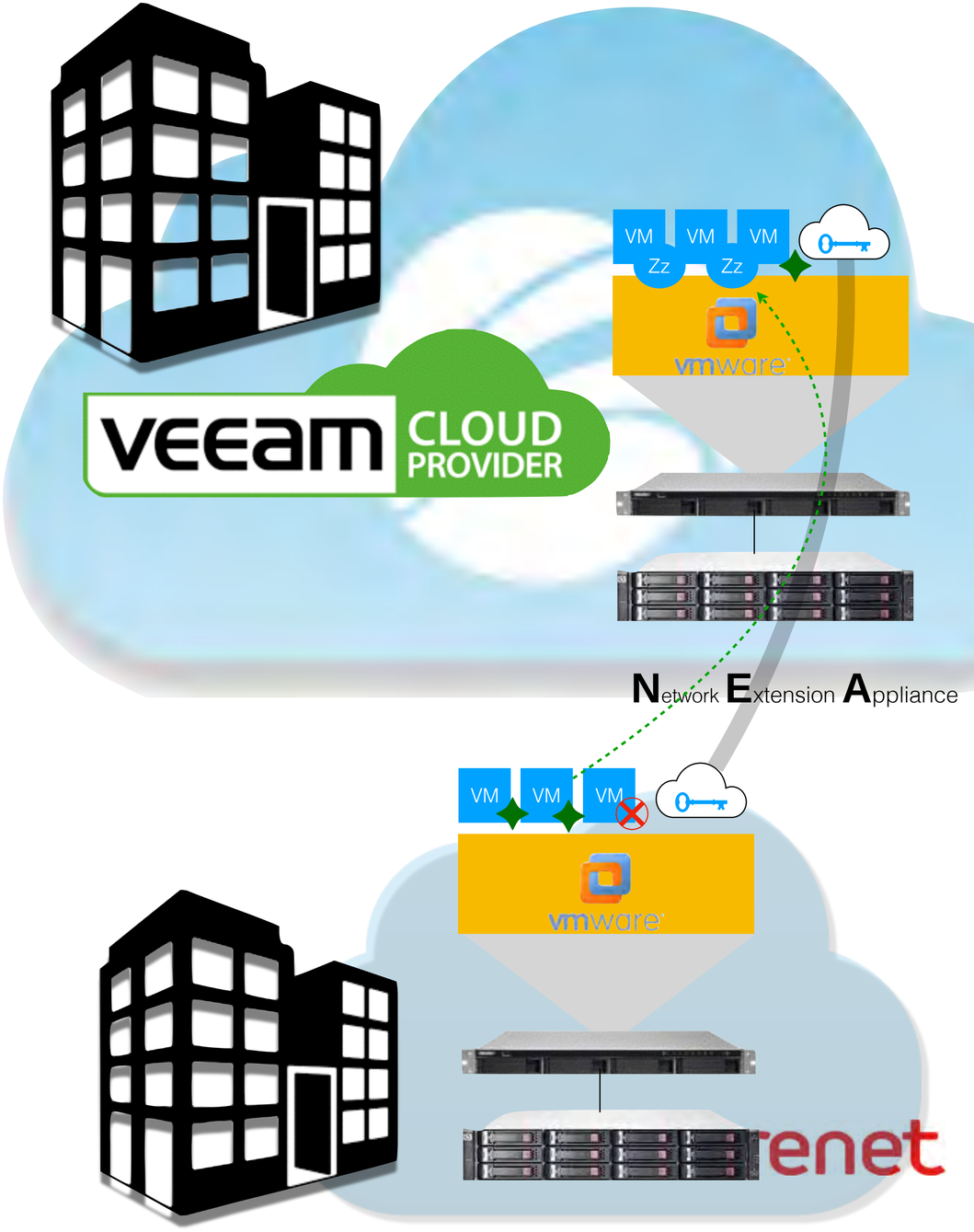
Veeam Cloud Connect **Replication**

Replica tus máquinas virtuales en un entorno externo de forma segura.

Actívalas siempre que lo necesites de forma transparente como si estuvieran en tus instalaciones con el mismo direccionamiento gracias al la tecnología NEA

Gestiona todo este proceso desde el propio Veeam

Nota: Versión vmware 5.5 o sup. , Veeam 9 ó sup.



Plan de Contingencia

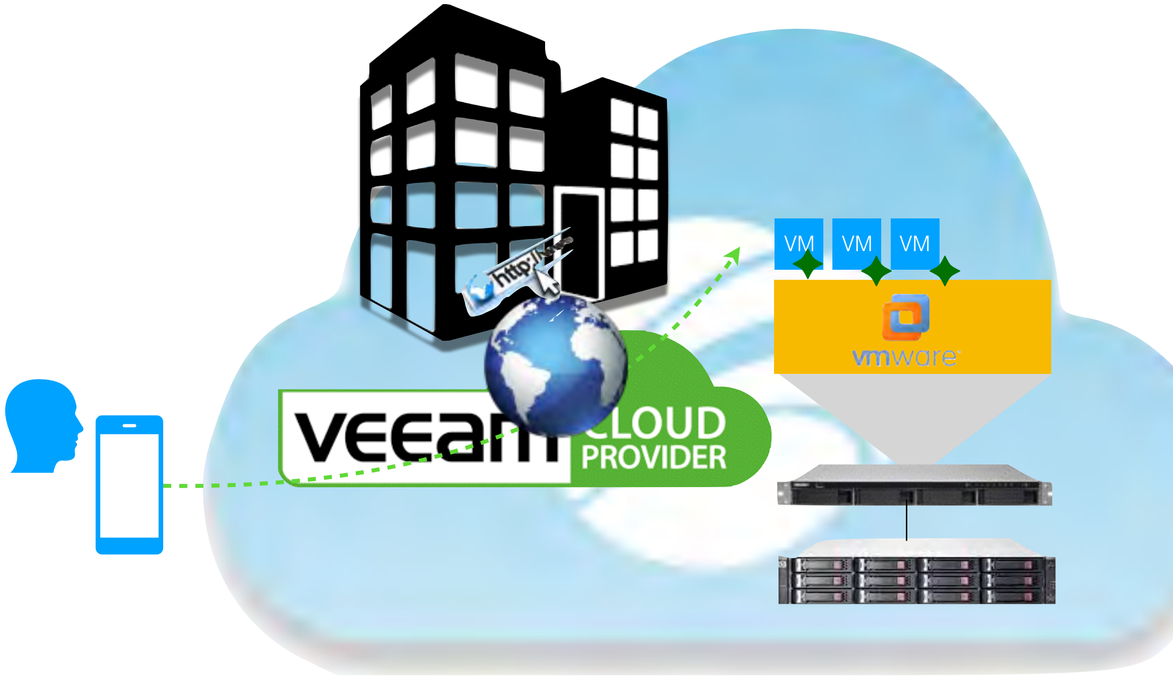
Veeam Cloud Connect

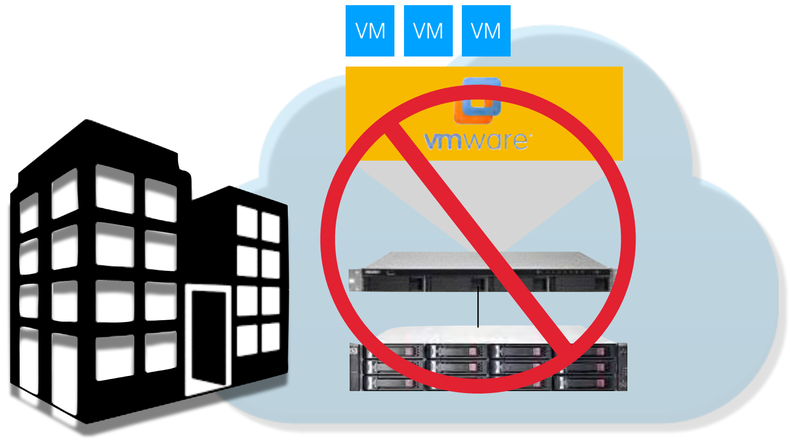
Veeam Cloud Connect Failover Plan

Replica tus máquinas virtuales en un entorno externo de forma segura.

Si tu entorno de virtualización te falla puedes tener un plan alternativo para acceder a tus máquinas por Internet

Gestiona todo este proceso desde un portal que puedes activar desde un smartphone en caso de emergencia





sarenet

Failover Plan

Recomendaciones generales

- Para velocidad < 100 Mbps ==> Acelerador WAN
- Versiones de Veeam y VMWare actualizadas
- Ciclos GFS con Backup Copy
- Regla 3-2-1
- Pruebas Failover Plan

Plan de Contingencia

Veeam Cloud Connect

Recuerda que independientemente del tamaño de tu empresa…..

Grandes Empresas

Veeam Availability Suite™

Empresas Medianas

Veeam Backup & Replication™

Pequeña Empresa (Por Debajo De 250 Empleados)

Veeam Backup Essentials™

sarenet

Sistemas Seguros de Almacenamiento

Plan de Contingencia

Veam Cloud Connect

Sistemas Seguros de Almacenamiento

Backups tradicionales

- Periodicidad. ¿Diario? ¿Semanal? ¿Aleatorio?
- ¿Mecanismo? ¿Cómo es de fiable? ¿Cómo es de costoso?
- ¿Mantengo copia *off-site*?
- ¿Cuánto cuesta recuperarlo?

Plan de Contingencia

Sistemas Seguros de Almacenamiento

Ramsomware, cryptolocker …

Podemos hacerlo mejor

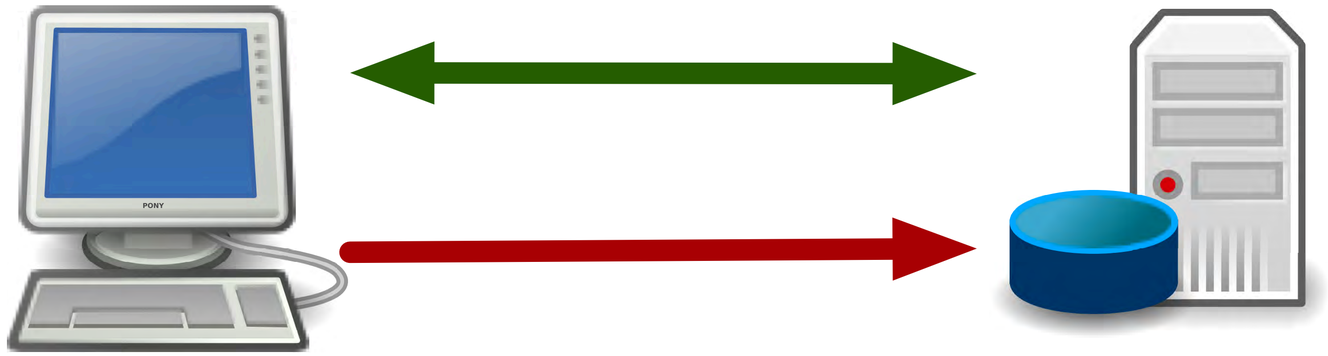
- Mejor periodicidad
- Mecanismo integrado en el almacenamiento
- Retroceso instantáneo (¿1 minuto?)
- Replicación *off-site*
- **Proteger la copia del *hacker* en**

Plan de Contingencia

Sistemas Seguros de Almacenamiento

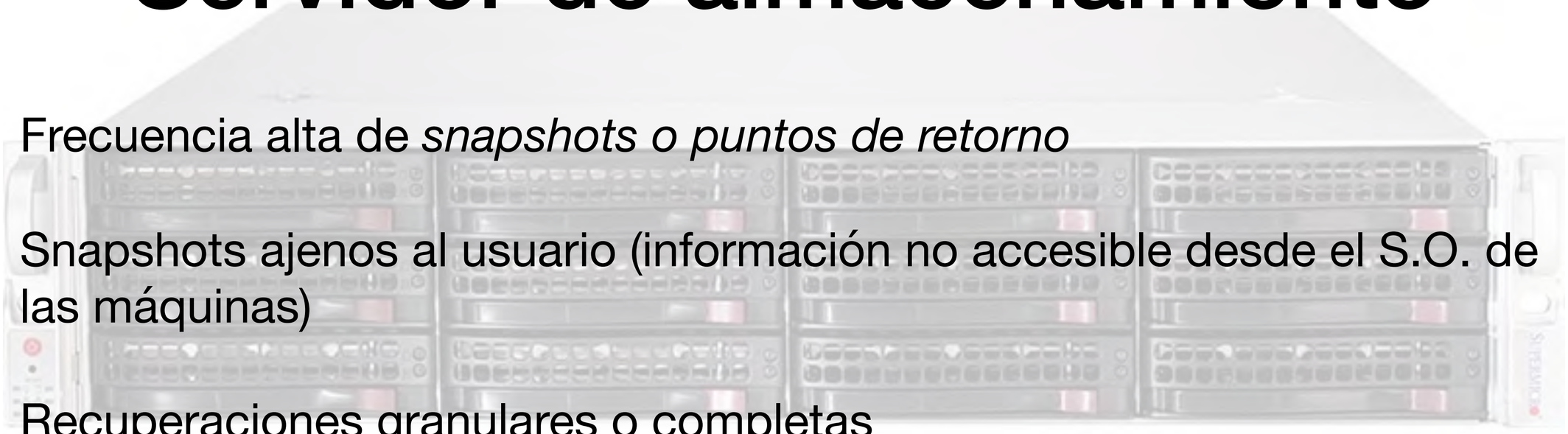
¿Qué proponemos?

- No es necesario un experto en almacenamiento seguro
- Montamos equipo en domicilio de clientes
- Diseñamos estrategia de almacenamiento y de replicaciones y copias de seguridad



sarenet

Servidor de almacenamiento



- Frecuencia alta de *snapshots o puntos de retorno*
- Snapshots ajenos al usuario (información no accesible desde el S.O. de las máquinas)
- Recuperaciones granulares o completas
- Replicación *off-site*

Resumen

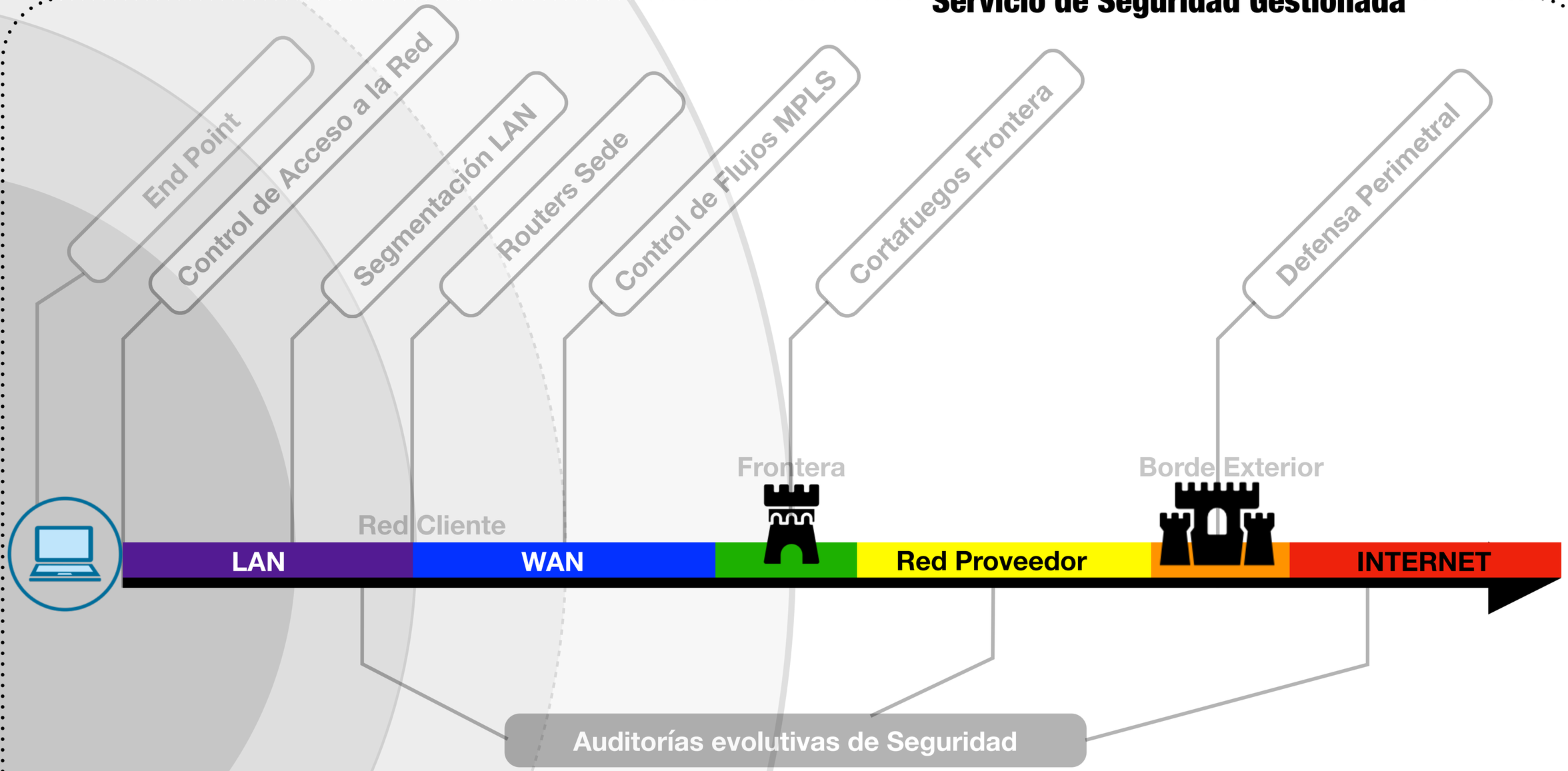
- El backup tradicional sigue siendo necesario pero insuficiente
- Los sistemas de almacenamiento modernos también sirven para grupos de trabajo
- En un incidente perdemos datos desde última copia. ¿Cuánto?
- ¿Medimos el tiempo de recuperación en días, horas o minutos?

Sistemas Seguros de Almacenamiento

Plan de Contingencia

Veam Cloud Connect

Servicio de Seguridad Gestionada



Plan de Contingencia

Cuando todo falla ...

Parque Tecnológico de Valencia
[IMPORTANTE] Se busca propietario de vehículo
Para: XXXX@radgestion.com
Responder a: info@ptvalencia.es

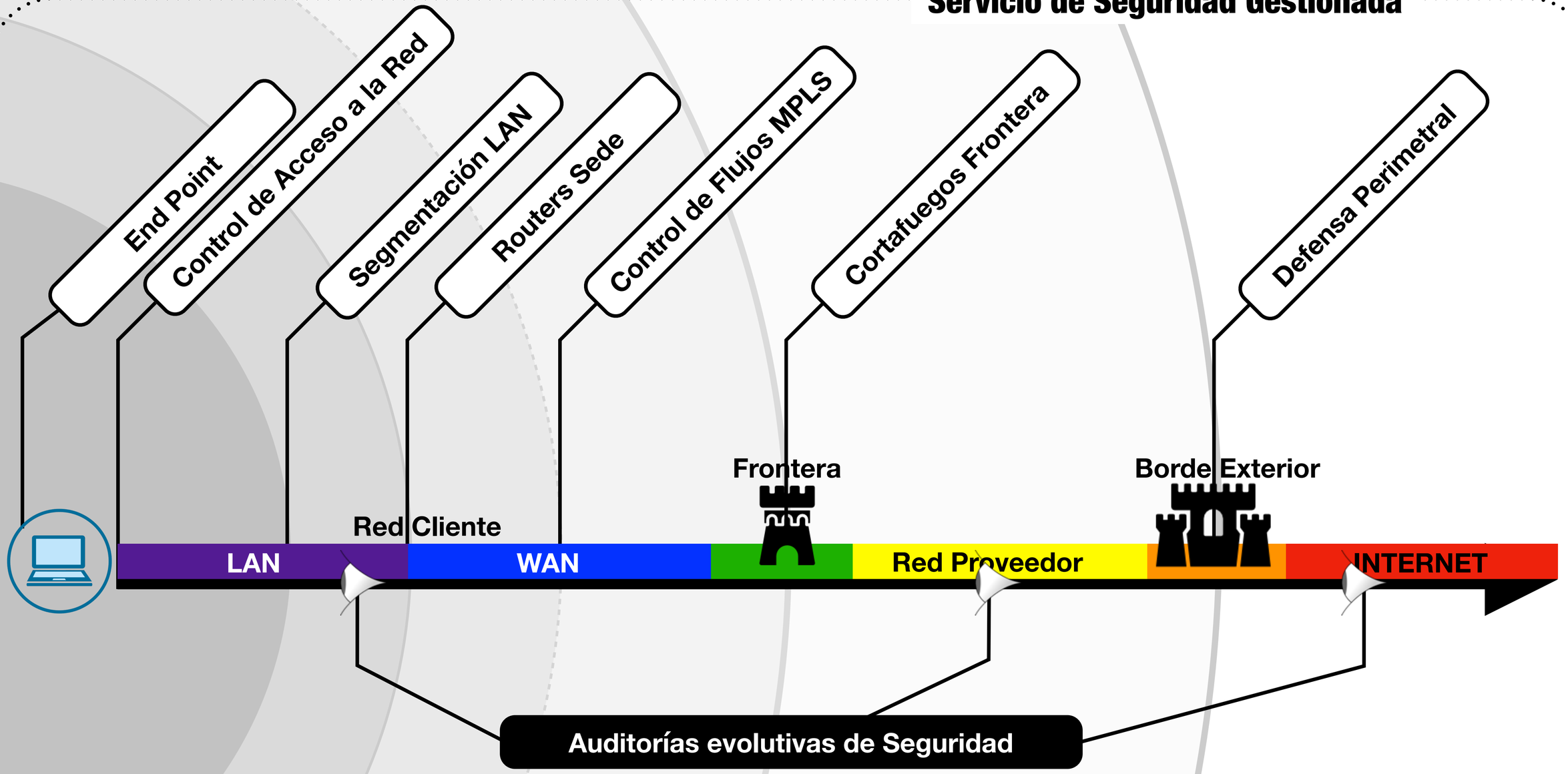
ATENCIÓN:

Se ha producido un pequeño accidente en Carrer Vila de Madrid , a la altura del número 44. Estamos intentando localizar al propietario del vehículo que se ha visto afectado.

Un empleado ha hecho una foto del coche que he adjuntado a este correo electrónico. Si el coche es tuyo, comunícanoslo de inmediato.

Administradores del Parque Tecnológico de Valencia

Servicio de Seguridad Gestionada



Plan de Contingencia

Cuando todo falla ...

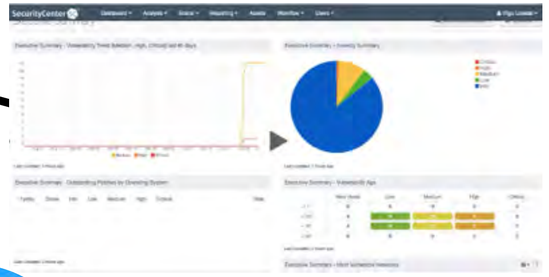
Servicio de Seguridad Gestionada

Generación
de informes

Monitorización
de la MPLS

Cortafuegos

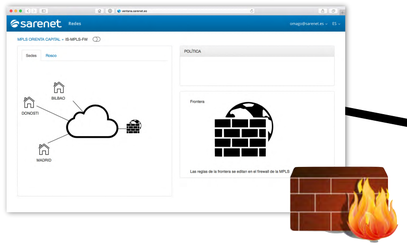
Vigilancia
de alertas



Sistema
de análisis de
vulnerabilidades
Security Center

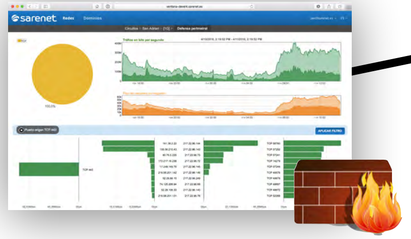
Frontera

Control de flujos



Gestión de
redes Wifi

Perimetral DDoS

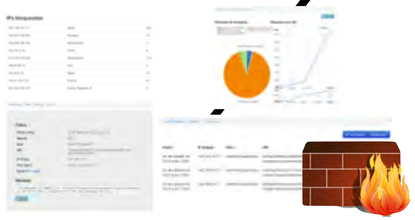


Actuaciones
sobre activos

Segmentación y
segregación de la red

Vulnerabilidades
en servidores

Aplicaciones

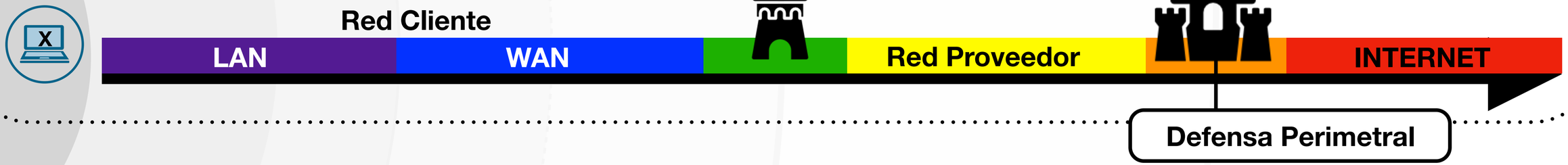


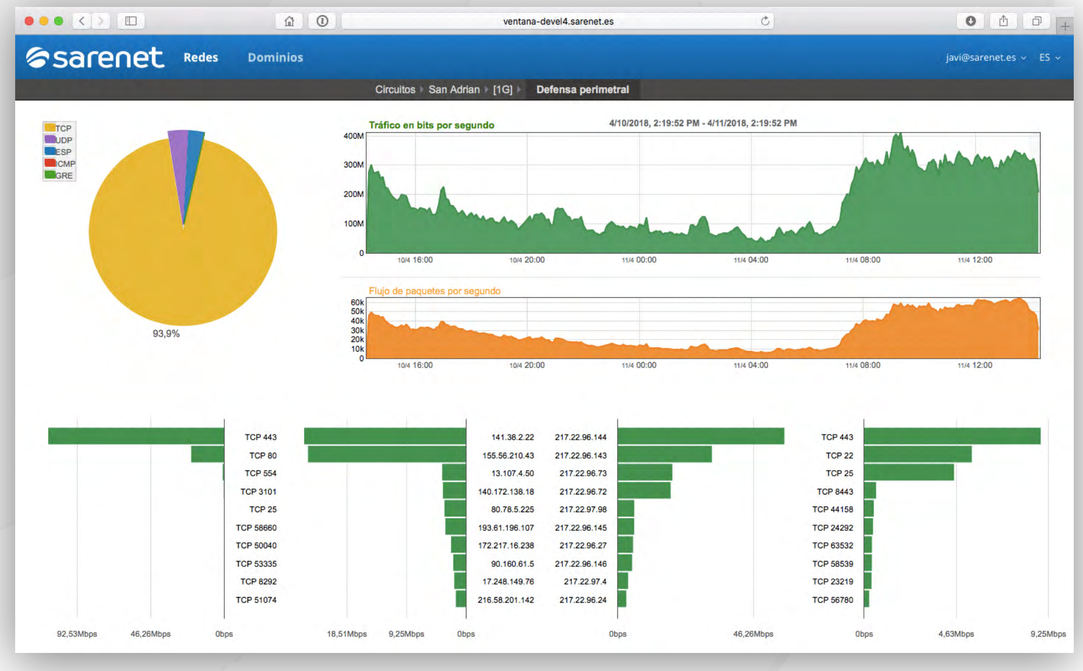
NAC Auth

SSL Portal

Gestión de los
dispositivos NAC y
control de accesos

Servicio de Seguridad Gestionada





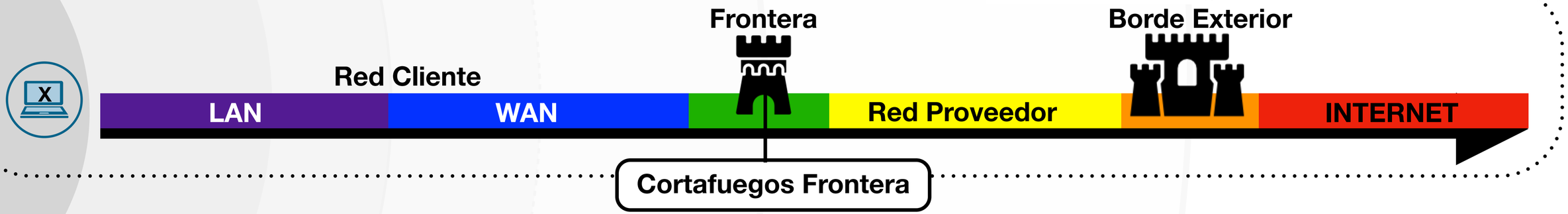
Aplicación Web

Gestión : cliente o Sarenet

Por IP o rango protegido

Desde **150 €/mes**

Servicio de Seguridad Gestionada



Alquiler y alojamiento de cortafuegos gestionado

Actualizaciones del Firmware

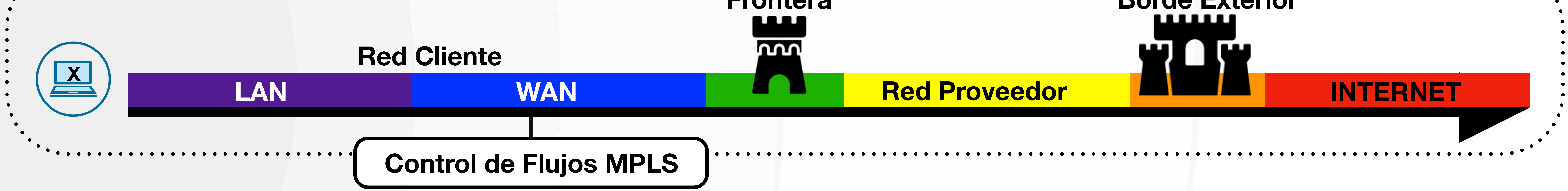
Creación de las políticas de seguridad

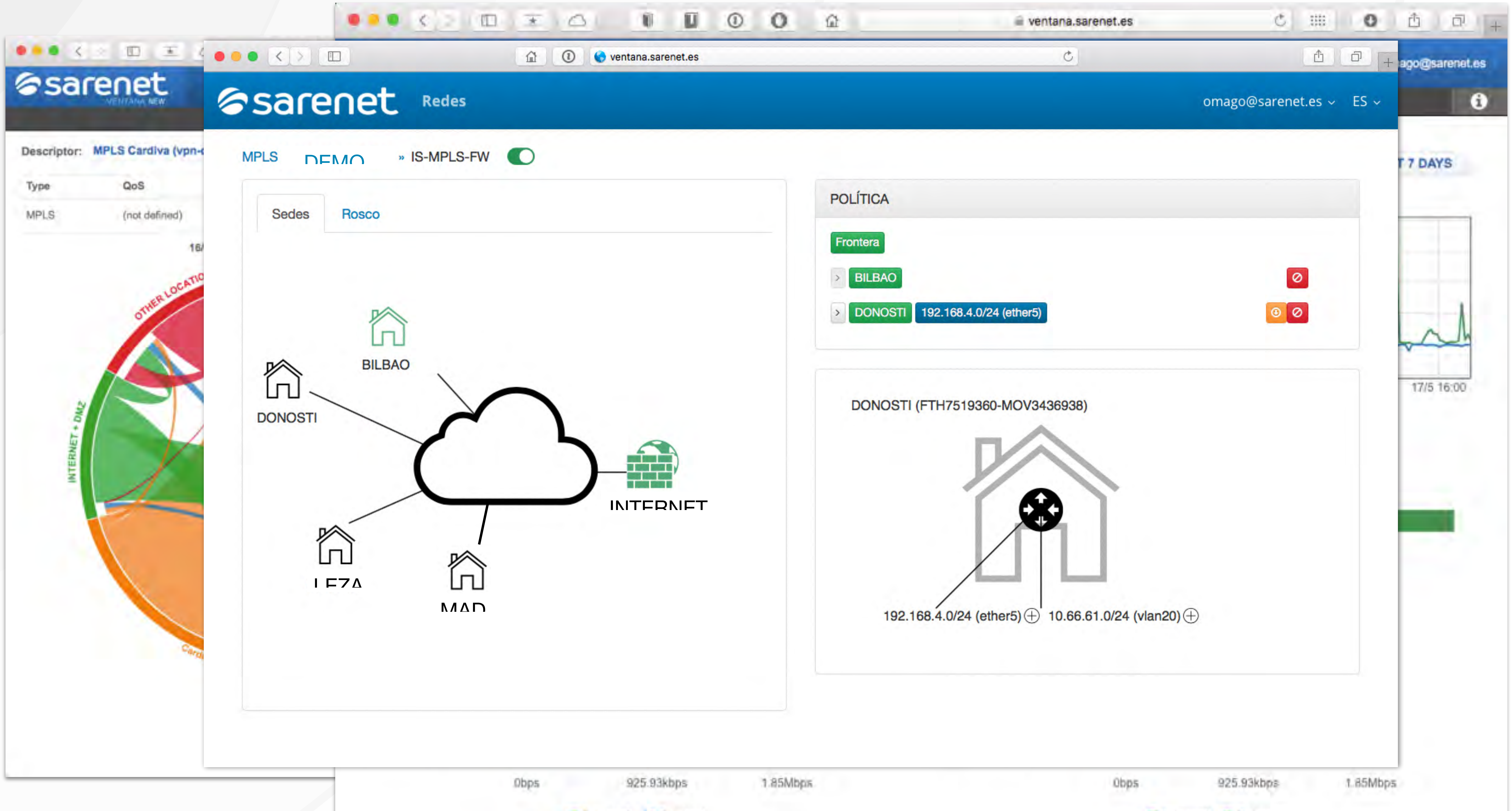
Gestión de accesos externos

Atención de las incidencias de seguridad : IPS/IDS, Botnets, virus

Gestión de sistemas de informes : fortianalyzer FAZ

Servicio de Seguridad Gestionada





Servicio de Seguridad Gestionada

Red Cliente

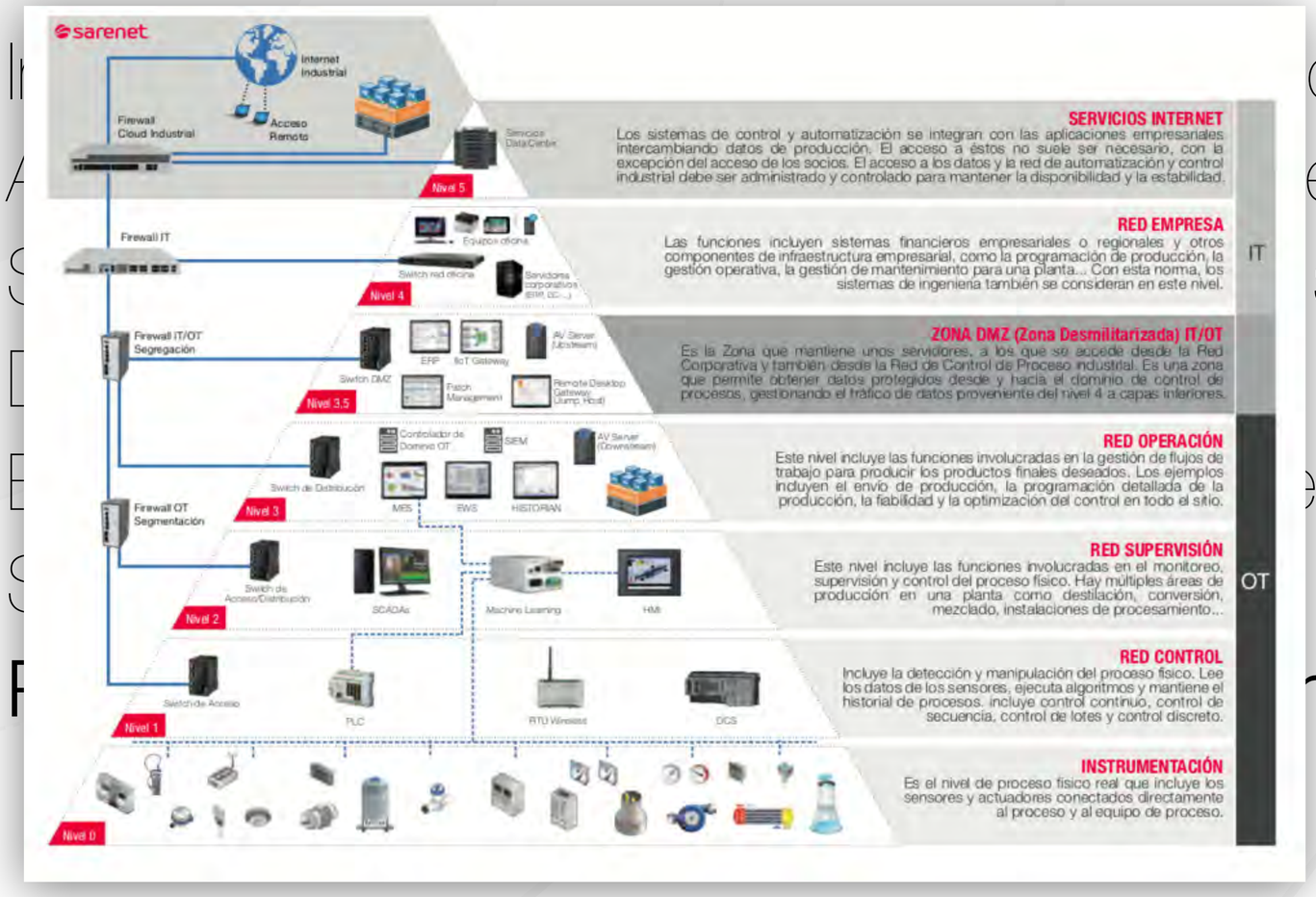
Frontera

Borde Exterior

LAN | WAN | Red Proveedor | INTERNET

Segmentación LAN

Control de Acceso



NAC Auth

SSL Portal

Gestión de los dispositivos NAC y control de accesos

de cliente

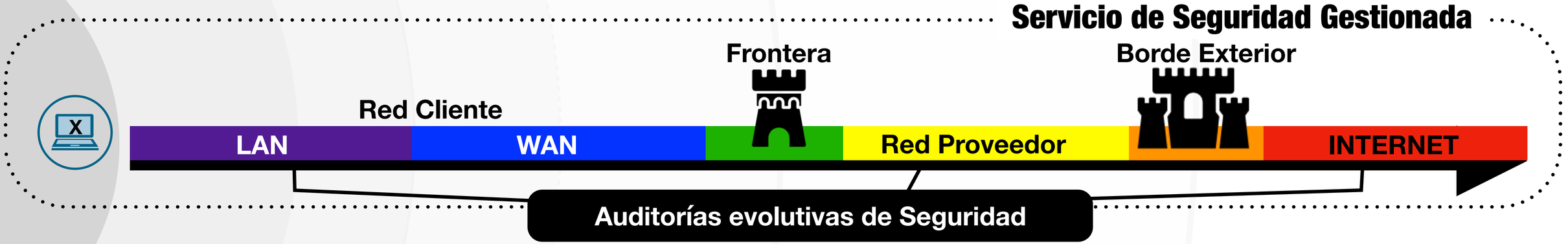
egmentar y segregar las redes

switches y cortafuegos

control de acceso a la LAN

te poste

Gestión de redes Wifi



Contratación de la herramienta de auditoría evolutiva: 10 IPs, 500 €/año

Detección infraestructura crítica

Monitorización continua

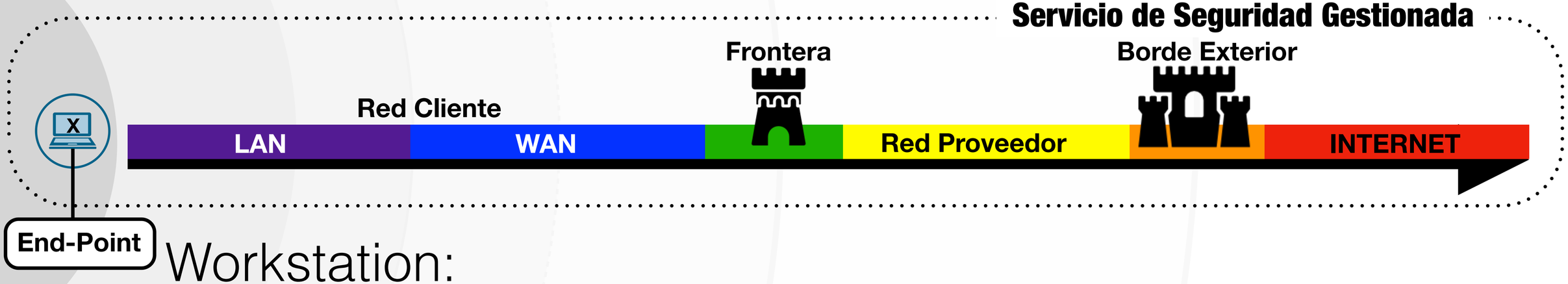
Soporte correctivo

- Alertas y vulnerabilidades

Soporte evolutivo

- Seguimiento continuo : reuniones periódicas y elaboración de informes con recomendaciones de acciones correctoras y de mejoras

Presupuestos a medida en base a fijo mensual : Desde 114 €/mes



Workstation:

Endpoint tradicional - 25 €/año
Intercept X - 35 €/año
Intercept X advanced con EDR - 70 €/año

Servers:

Central Server Protection - 59 €/año
Central Intercept X advanced - 120 €/año

Soporte en base a fijo mensual : Desde 57 €/mes

Plan de Contingencia

Sistemas Seguros de Almacenamiento **Veeam Cloud Connect**

Back-Up:

10€/mes por MV + espacio (ej.: 35€/mes -1TB)

Replication:

MV inactiva: 10€/mes + licencias de MS + almacenamiento

MV activa: 10€/mes + licencias de MS + almacenamiento + CPU + RAM

Failoverplan:

Estudio inicial + Costes de Replicación + IPs (10€/mes por IP)

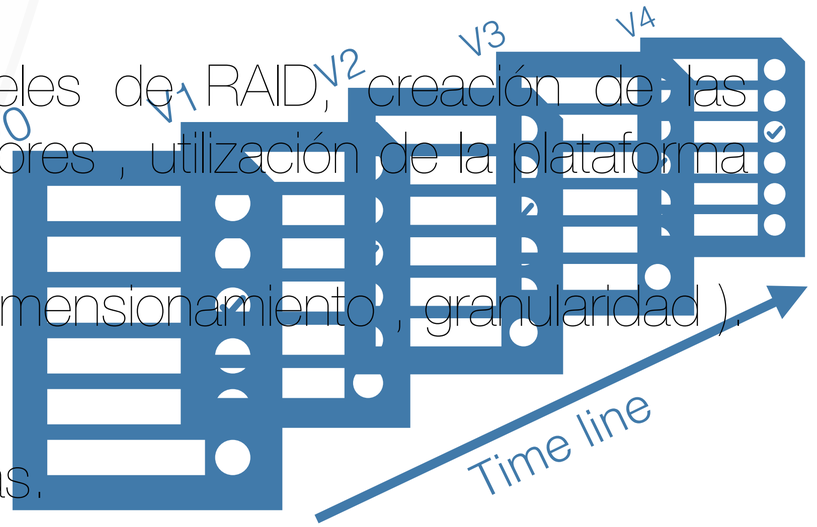
Plan de Contingencia

Sistemas Seguros de Almacenamiento **Veeam Cloud Connect**

Sistemas de almacenamiento seguro

El servicio incluye el hardware en alquiler y su gestión, cubriendo los siguientes puntos:

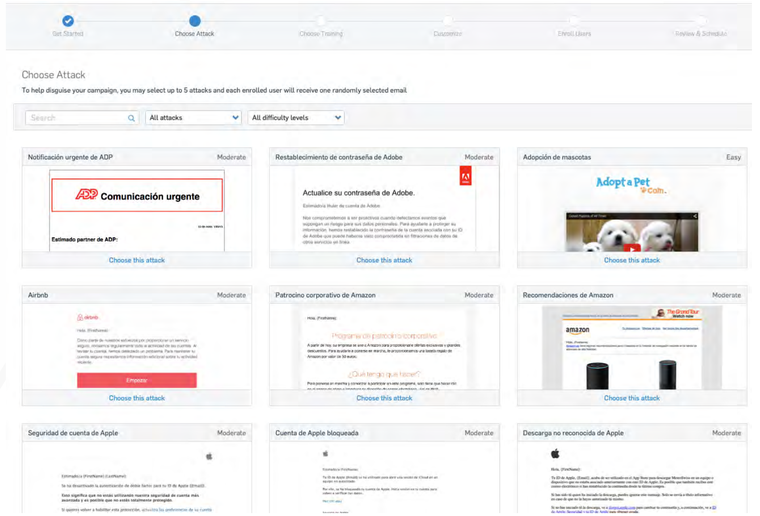
- Instalación en casa del cliente con 2 horas de formación in-situ
- Soporte continuo: recuperaciones en caso de incidentes, gestión de la configuración , vigilancia de la plataforma, informes periódicos de mantenimiento.
- Diseño de la estrategia almacenamiento (configuración de niveles de RAID, creación de las unidades lógicas LUNs , unidades de disco para usuarios o servidores , utilización de la plataforma como almacenamiento de sistemas de virtualización)
- Estrategias de replicación, Back-Ups y snapshots (periodicidad , dimensionamiento , granularidad).
- Monitorización de la plataforma, sistemas de alarmas.
- Reposición Chasis NBD y stock de discos para reposiciones rápidas.
- Ejemplo: 280 €/mes - 12 TB



Portal de concienciación: pishing

Alquiler de la herramienta : 100 usuarios, 19 €/año)
Soporte Sarenet : desde 57 €/mes

- Elaboración y análisis de campañas
- Reuniones de seguimiento e informes



SOC gestionado 24x7

Security Center + SOC Sarenet

- Atención y comunicación de incidentes de seguridad.
- Administración de cambios en elementos de seguridad.
- Administración de respaldo de configuraciones
- Administratición y monitorización de eventos en cortafuegos y FAZ
- Monitorización de la red y de los equipos involucrados
- Monitorización de vulnerabilidades
- Hacking ético : test periódico de robustez de claves, simulación de ataques , etc..
- Generación mensual de informes ejecutivos
- SLA en base a tiempos de respuesta y calidad del soporte.