Seguridad Sincronizada en Acción

Juan Alejandro Aguirre
SE Colombia Ecuador Venezuela
SOPHOS

AGENDA

- Estrategia de Ciber-seguridad
- Como está cambiando el entorno actual de amenazas?
- Seguridad Sincronizada: El mejor Sistema de Seguridad Integrado
- Seguridad Sincronizada en Acción
- Historias de Éxito

Estrategia de Ciber-seguridad

SOPHOS

- **SEGURIDAD EN PROFUNDIDAD**

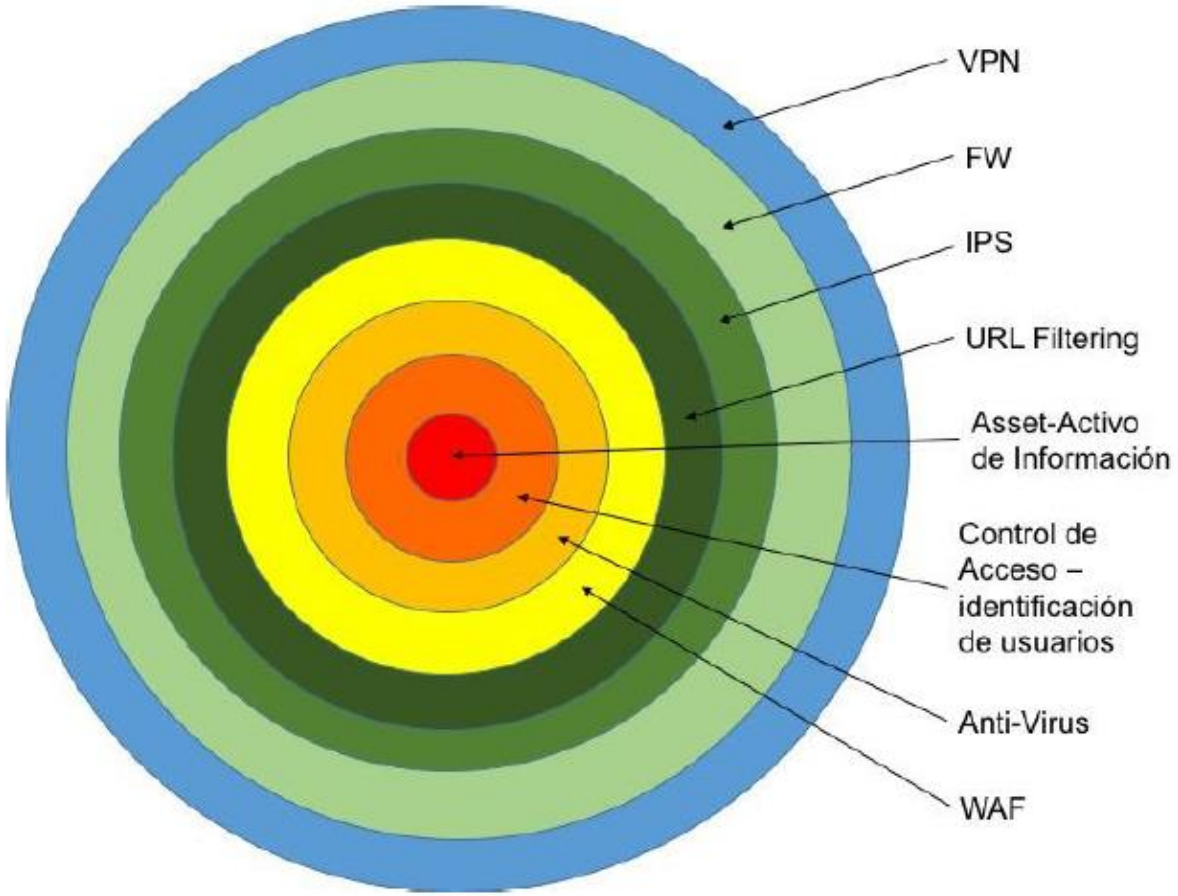
- ISO/IEC 27001 – A.13.1:

Mantener el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en **defensa en profundidad**.

Este enfoque indica que diferentes tipos de controles deben ser ubicados en un lugar específico mediante capas.

Minimiza la probabilidad de una intrusión exitosa que lleve a un compromiso de la disponibilidad, integridad o confidencialidad de la información

- **SEGURIDAD EN PROFUNDIDAD**



- **SEGURIDAD ADAPTATIVA (GARTNER)**

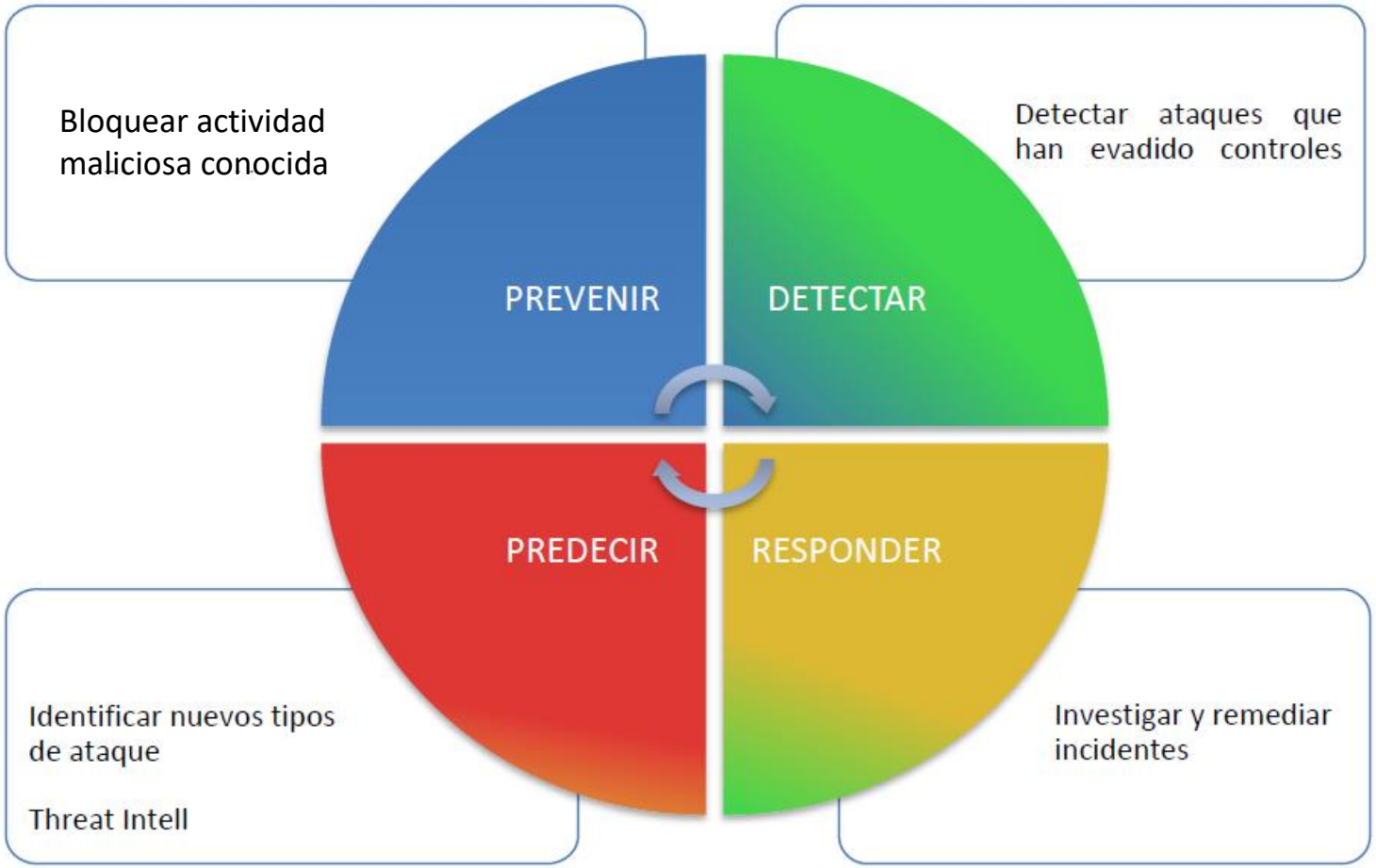
- **PREVENIR**: Describe el set de políticas, productos y procesos que son puestos en lugar para prevenir un ataque exitoso.

- **DETECTAR**: Desarrollar capacidades para encontrar ataques que han evadido los controles preventivos.

- **RESPONDER**: Habilidades y competencias para investigar y remediar incidentes descubiertos por actividades de detección (o por agentes externos) para proveer análisis forense y de la causa raíz.

- **PREDECIR**: Habilitar a las organizaciones para aprender de eventos externos a partir de monitoreo de actividades de hackers en el underground para anticipar proactivamente nuevos tipos de ataques contra los sistemas actuales y la información que estos alojan .

• SEGURIDAD ADAPTATIVA



- **ZERO TRUST – MICROSEGMENTACIÓN (FORRESTER)**

Hoy en día la diferencia competitiva yace en explotar tecnologías digitales para ganar y retener clientes. En este mundo digital no hay fronteras ni perímetro, el negocio de ubica en cualquier lugar desde el cual los clientes se conecten y en cualquier lugar desde el cual los empleados y socios interactúen con la data y los servicios que se prestan.

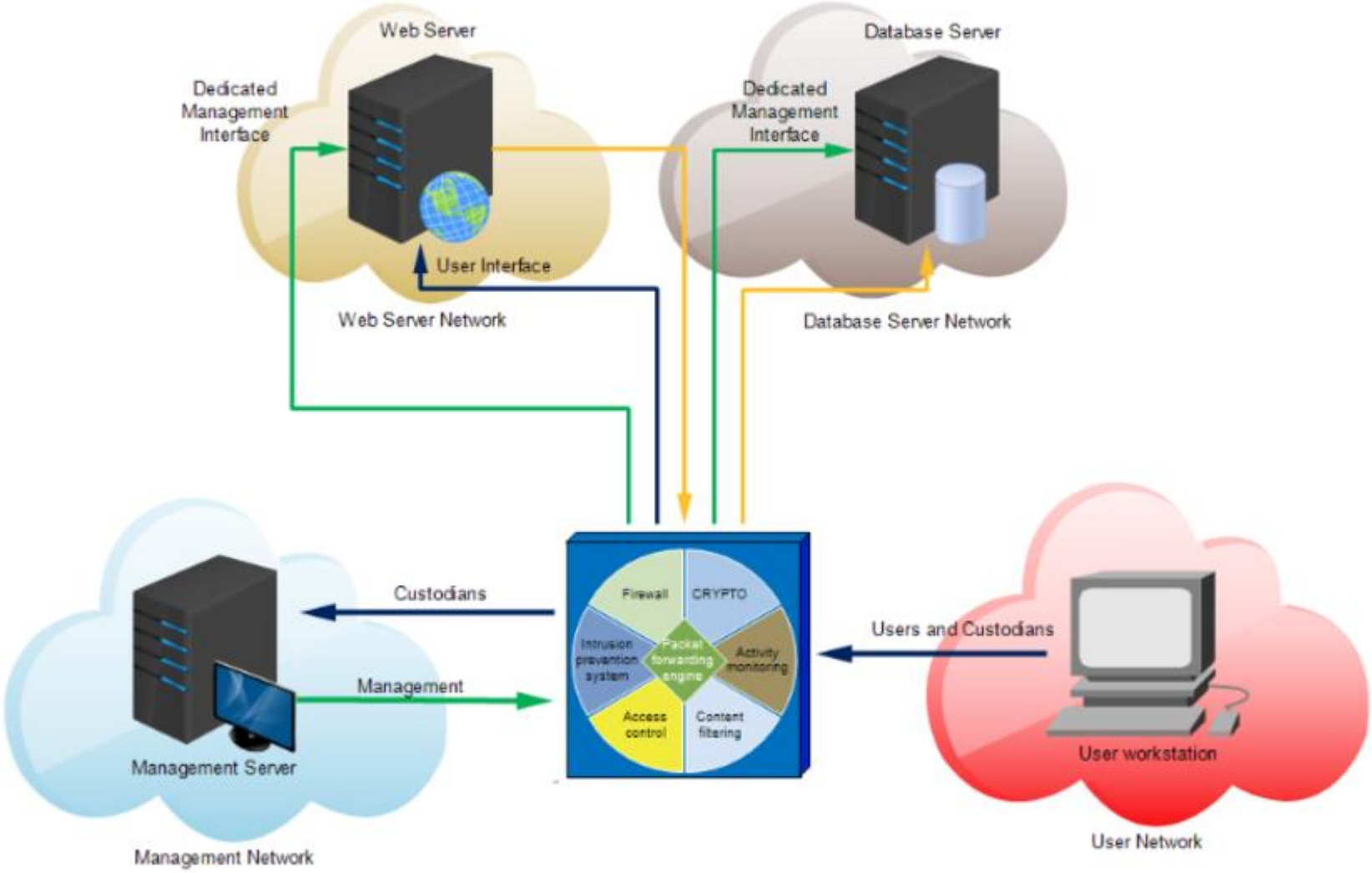
- Nunca da por sentada la noción de confianza. La confianza es continuamente evaluada mediante análisis basado en riesgo de toda la información disponible..

- El foco migra del perímetro al dato.

- Ordena las funciones de diferentes dominios de seguridad como red, identidad y aplicaciones en un enfoque unificado de protección orientada al dato.

- Proteger la propiedad Intelectual de la organización, disminuye las brechas y blinda la reputación.

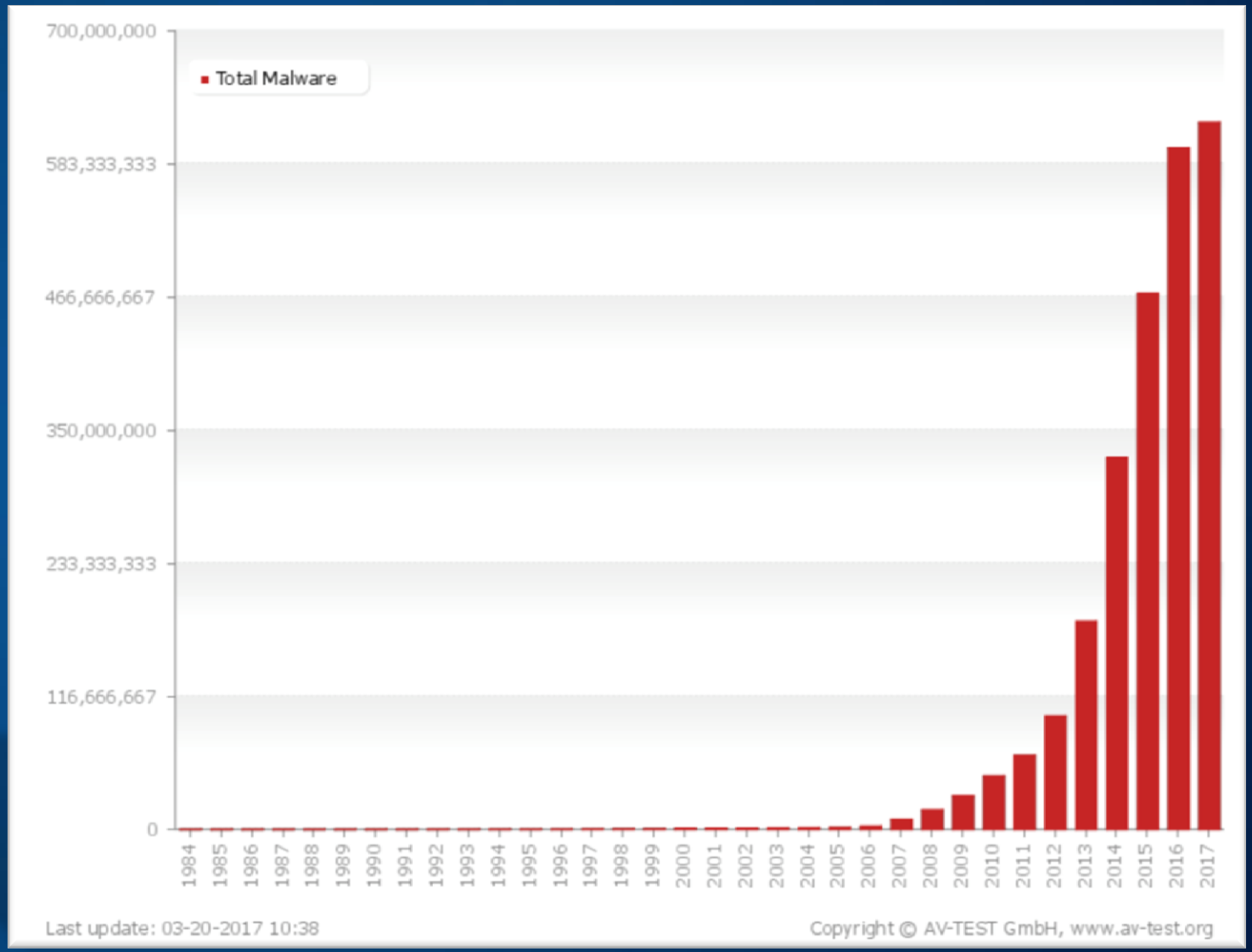
• ZERO TRUST - MICROSEGMENTACIÓN



Entorno Actual de Amenazas

Muestras Únicas de malware

Complejidad de los Ataques



Complejidad de los Ataques

Superficie de Ataque en crecimiento

Complejidad de los Ataques

Superficie de Ataque en crecimiento

Controles no Coordinados

Complejidad de los Ataques

Superficie de Ataque en crecimiento

Controles no Coordinados

Falta de recursos

46%

Organizations believe they have a problematic shortage of cybersecurity skills

ESG Group

Y si pudiéramos simplificar la seguridad e integrar los controles?

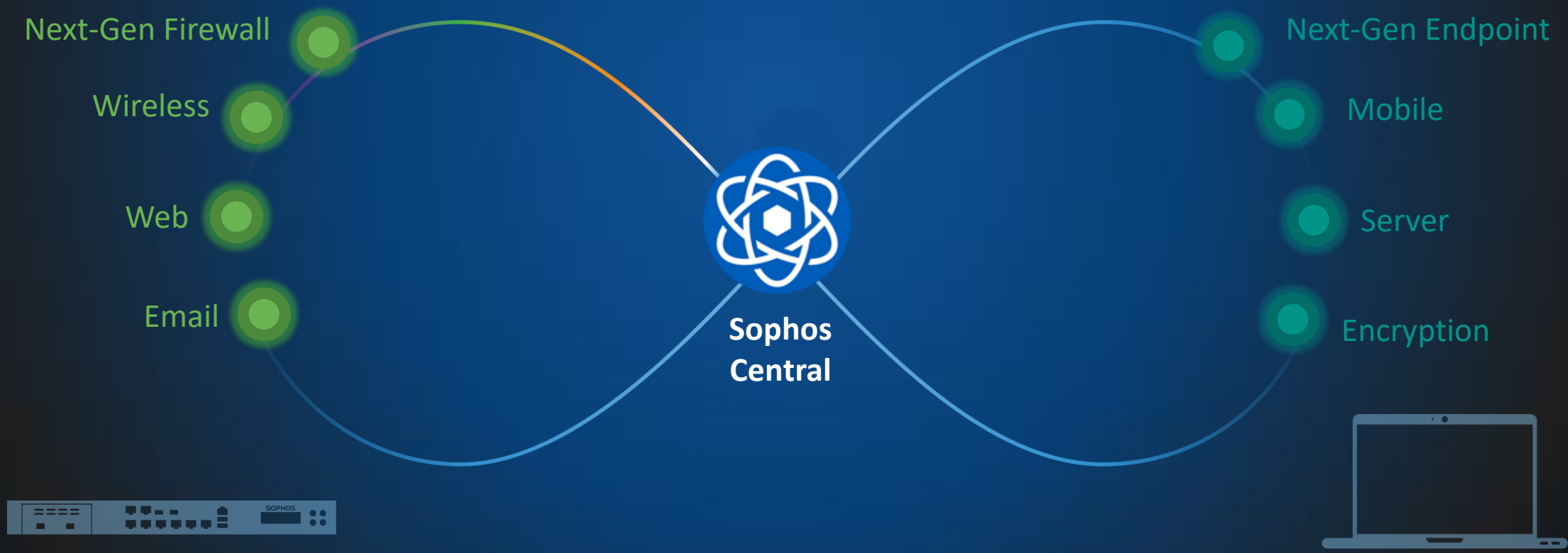
Beneficios de un Sistema Integrado

- Simplifica la administración de IT
- Incrementa la visibilidad a través de toda la infraestructura
- Reduce el riesgo de movimiento de la amenaza
- Responde más rápido a posibles incidentes de seguridad
- Maximiza la operación del equipo de IT apalancado en automatización
- Alcanza un mejor ROI para las inversiones en seguridad

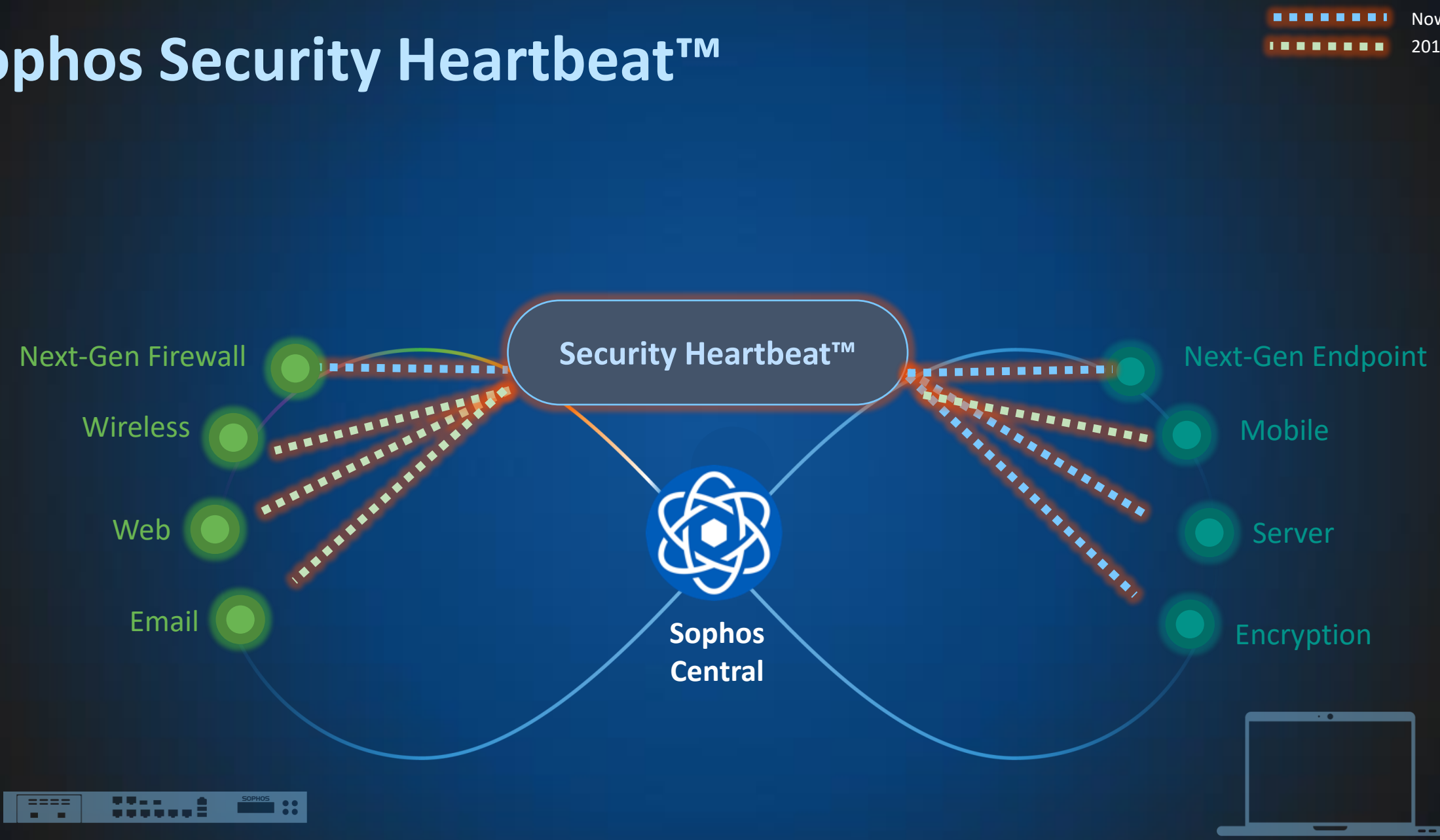
Seguridad Sincronizada

SOPHOS

Seguridad Sincronizada: Mejor Seguridad



Sophos Security Heartbeat™



“**Ningún otro fabricante** esta cerca de entregar este tipo de comunicación entre el Endpoint y los productos de seguridad de Red.”

Chris Christianson, Vice President of Security Programs, **IDC**

Tecnologias Lideres en areas clave

Gartner Magic Quadrant
UNIFIED THREAT MANAGEMENT

Magic Quadrant for Unified Threat Management, , June, 2017

Gartner Magic Quadrant
ENDPOINT PROTECTION

Magic Quadrant for Endpoint Protection Platforms, Eric Ouellet, Ian McShane, Avivah Litan 30 January, 2017

The Forrester Wave™
ENDPOINT ENCRYPTION

The Forrester Wave: Endpoint Encryption, Chris Sherman, 16 Jan 2015

Beneficios de Seguridad Sincronizada

Protección sin paralelos

Productos lideres que integran tecnología de ultima generación activamente trabajan juntos para detector y prevenir ataques avanzados, ransomware, botnets entre otros.

Respuesta a Incidentes Automática

Información de amenazas es compartida y acciones se toman de forma automática a través de la red, aislando el Endpoint antes que la amenaza pueda esparcirse mejorando el tiempo de respuesta a incidentes en un 99.9%.

Visibilidad y Control en Tiempo Real

Visualizar y controlar lo que esta pasando en tiempo real para una administración de seguridad mejor y más simple

Seguridad Sincronizada en Acción

SOPHOS

Respuesta Automática a Incidentes

Antes de Seguridad Sincronizada

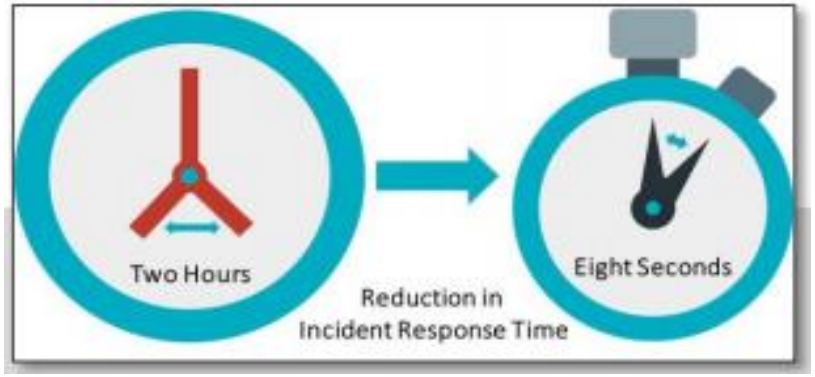
Mínimo 2 horas para identificar usuarios, procesos, maquinas y estimar impacto

Por lo general días, semanas…

Después de Seguridad Sincronizada

Aislamiento automático de Endpoints en la identificación de la amenaza **< 8 s**

Resultados por la firma analista ESG



“Solo tomo 2 minutos encontrar que todo estaba baja control. Sophos XG Firewall detecto la amenaza y el Security Heartbeat permitió que el host infectado fuera inmediatamente identificado, aislado y limpiado. En lugar de ir a modo de emergencia, nos relajamos y terminamos nuestro almuerzo.”

DJ Anderson, CTO, **IronCloud**

Compartiendo Información – Automatizando respuesta.

El Endpoint Se comunica con Sophos Central

El Endpoint automáticamente elimina malware

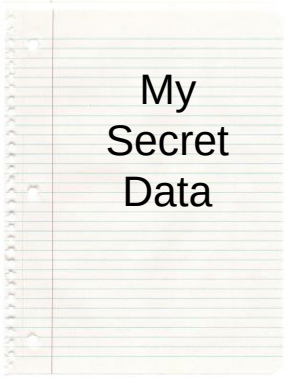
El Endpoint detecta y bloquea malware

El EP se comunica con Sophos central

El Heartbeat regresa a verde

Se recupera acceso

Llaves de cifrado recuperadas

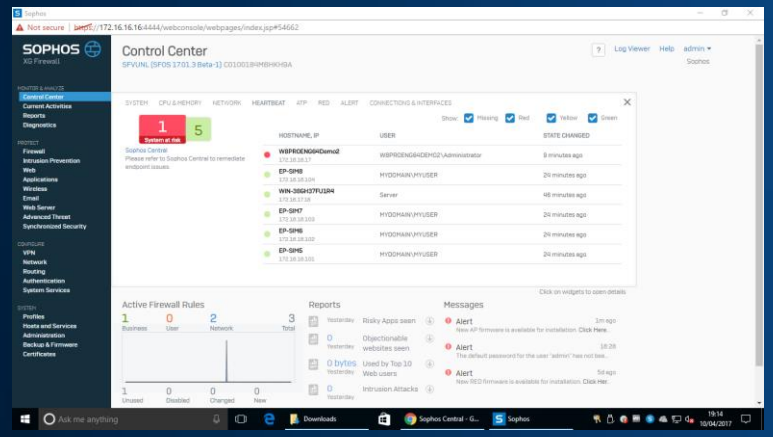


Seguridad Sincronizada: Respuesta coordinada contra Ransomware

SOPHOS

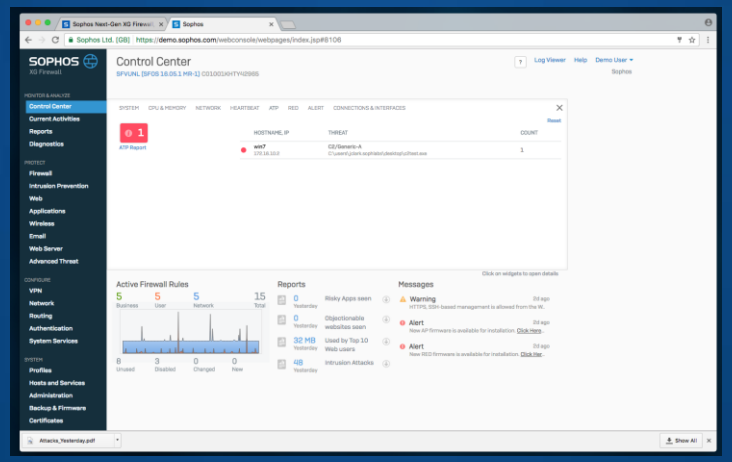
Visibilidad y Control en Tiempo real

Visibilidad de Infraestructura



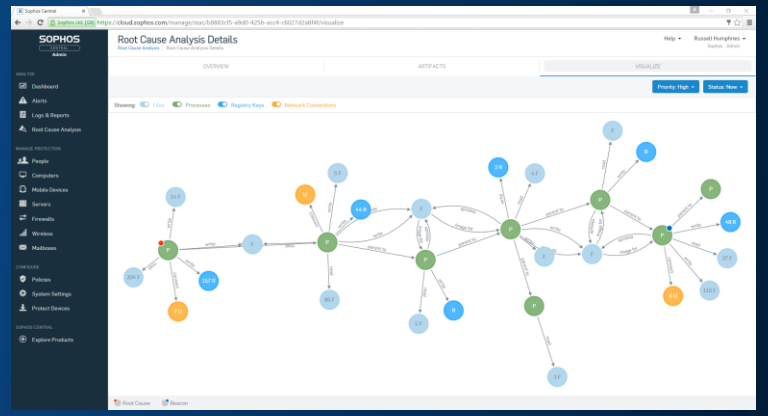
Security Heartbeat

Maquina, Procesos, Usuario



Active Threat ID

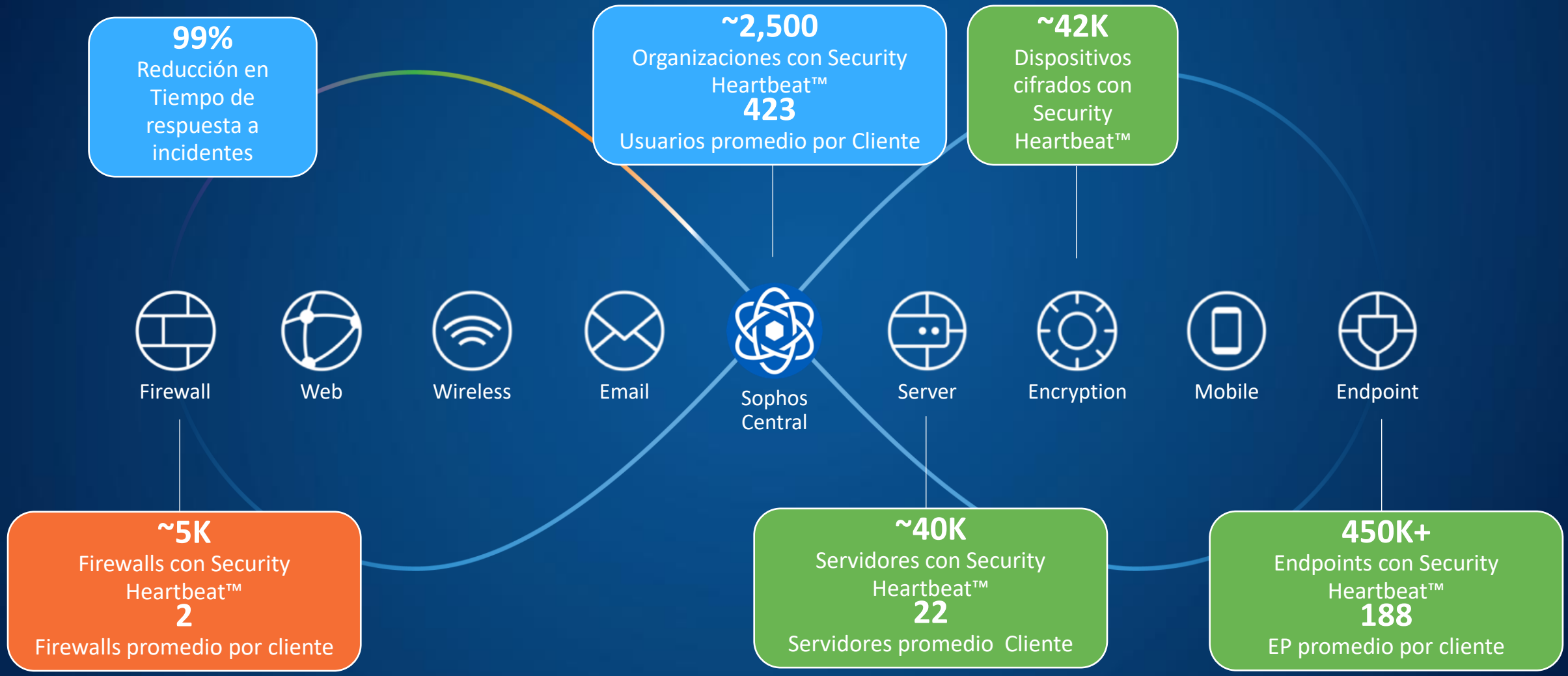
Visibilidad de la Cadena de Amenaza



Root Cause Analysis

Seguridad Sincronizada Casos de Éxito

Seguridad Sincronizada en Acción



DIOCESE OF BROOKLYN

SERVING BROOKLYN AND QUEENS

1.5M Miembros
7000 Empleados
187 Parroquias
90 Colegios
Brooklyn, USA

1000 Computers
- Sophos Central Endpoint Advanced, Intercept X

50 Servers
- Sophos Central Server Advanced

Network
- 3 XG Firewalls, 5 SG UTM
- 2000 Reflexion licenses

Real-time Insight and Control

Visibilidad
A través de múltiples locaciones

Análisis forense de amenazas con RCA es rápida y fácil

Unifica y simplifica
endpoint, FW, y cloud security

Cita

"Sophos ahorra tiempo al identificar amenazas y remediarlas rápidamente. Estimo que ahorra tiempo al identificar amenazas persona de tiempo completo, lo cual es mucho."

Gus Garcia, Senior Project Manager

MIRATO®

Compañía de Cosméticos
400 Empleados
Oficinas remotas WW
€169M Ganancias Anuales

200 Computers
- Sophos Central Endpoint Advanced, Intercept X

40 Servers
- Sophos Central Server Advanced

Network
- 2 XG Firewalls, 1 Web Appliance Sandstorm license

Automated Incident Response

Respuesta en tiempo real a través de la red global

Automatización

Solución que escala la efectividad de la seguridad a nivel mundial

Cita

"Con Sophos Central, plataforma techológica responde a cyber-ataques con un solo click."

"Con Seguridad Sincronizada se fue capaz de responder en tiempo real a amenazas cada vez más agresivas."

Igor Bovio, IT Manager

90 Empleados
4 Locaciones
Orlando, USA

100 Computers
- Sophos Central Endpoint Advanced, Intercept X

Servers
- Sophos Central Server Advanced

Network
- 4 XG Firewalls (210, 310)

Automated Incident Response

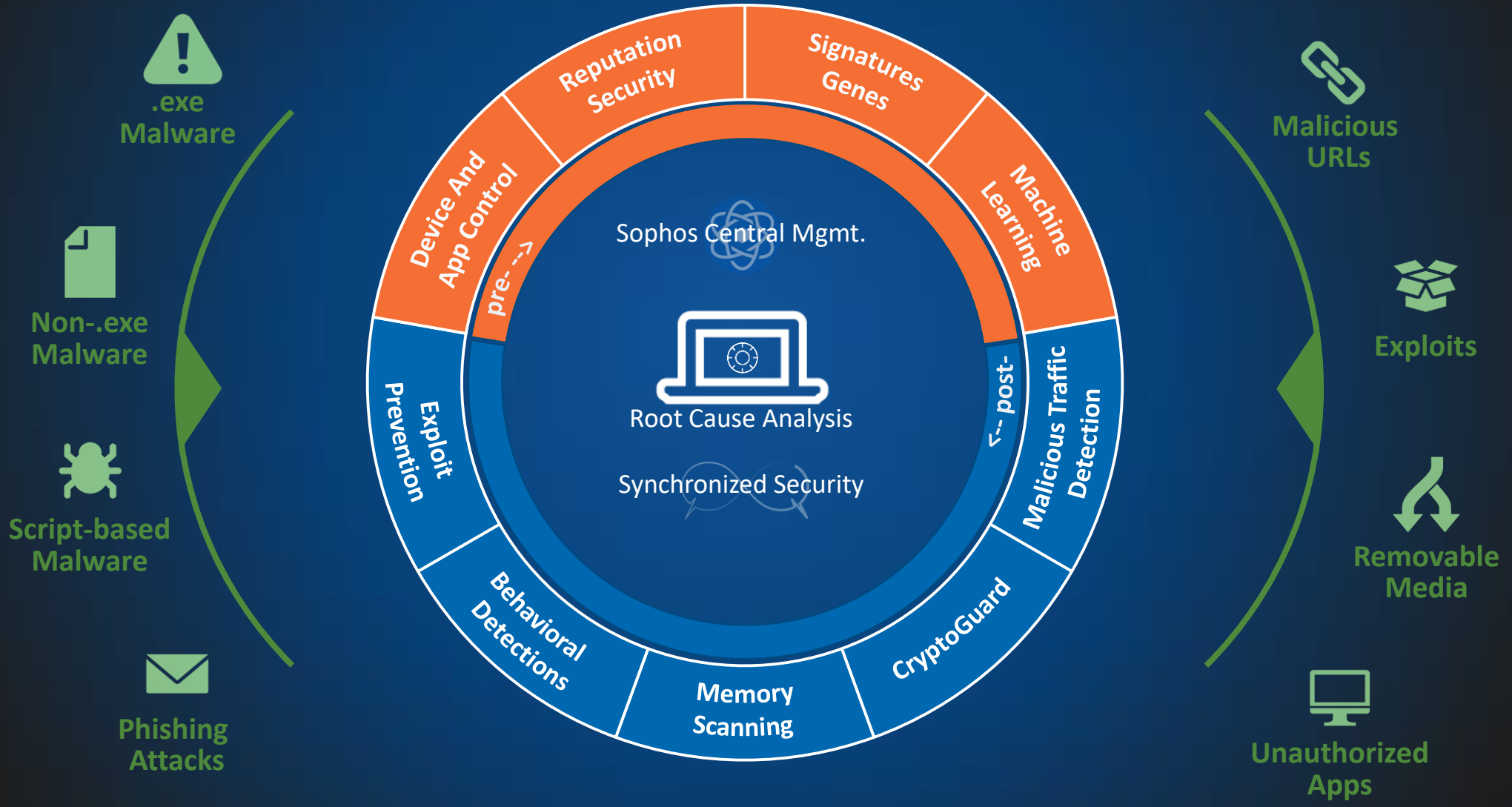
Necesidad de automatizar para mejorar efectividad

XG Firewall
Automáticamente aísla Endpoints diariamente

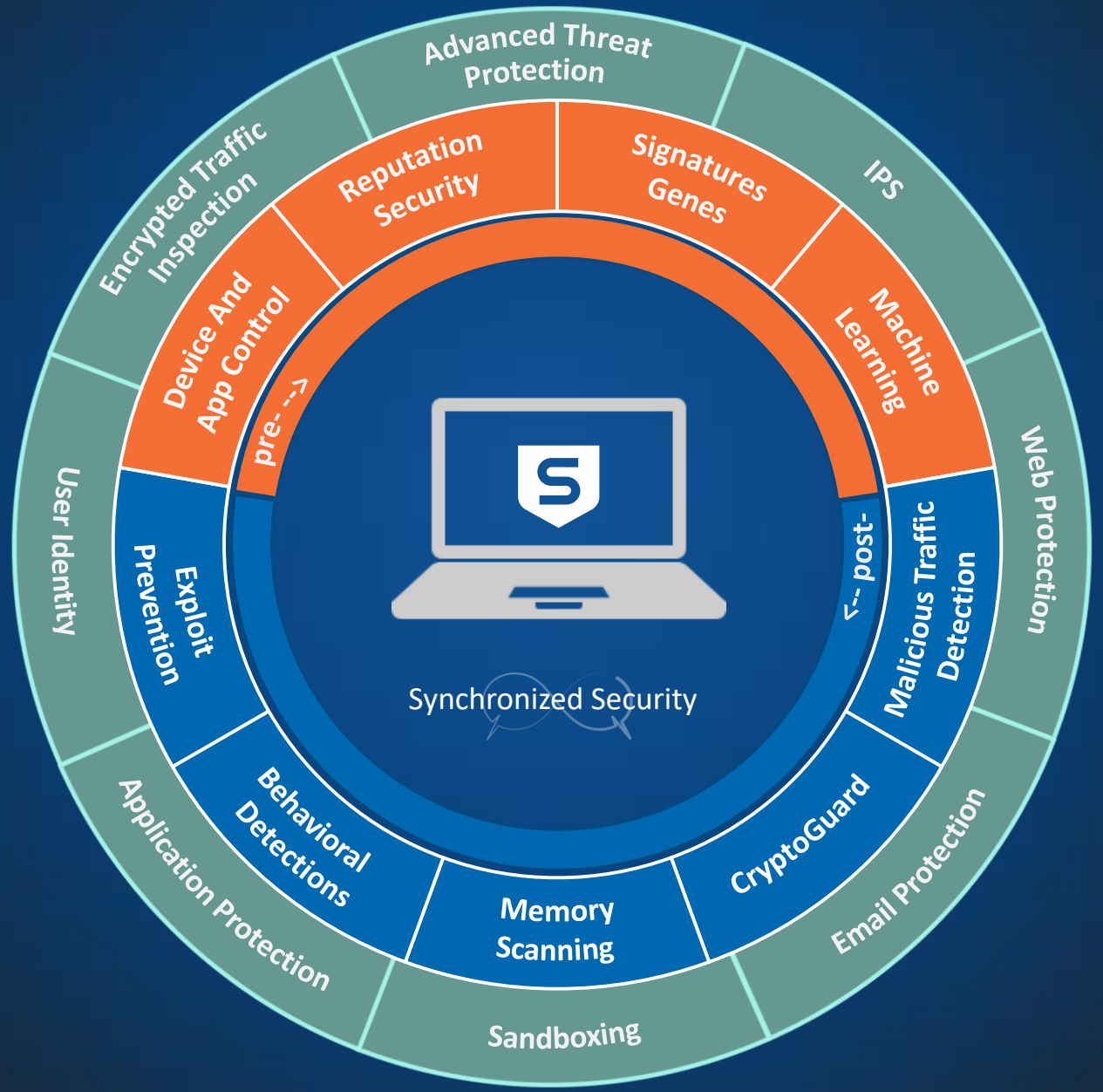
Cita

"Seguridad Sincronizada fue la razón por la que adquirimos Sophos con XG Firewalls."

Next-Gen Endpoint Protection



Next-Gen Endpoint and Network Protection



CREDENTIAL HARVESTING

UNKNOWN THREATS

STEALTH MALWARE

CRYPTO MALWARE

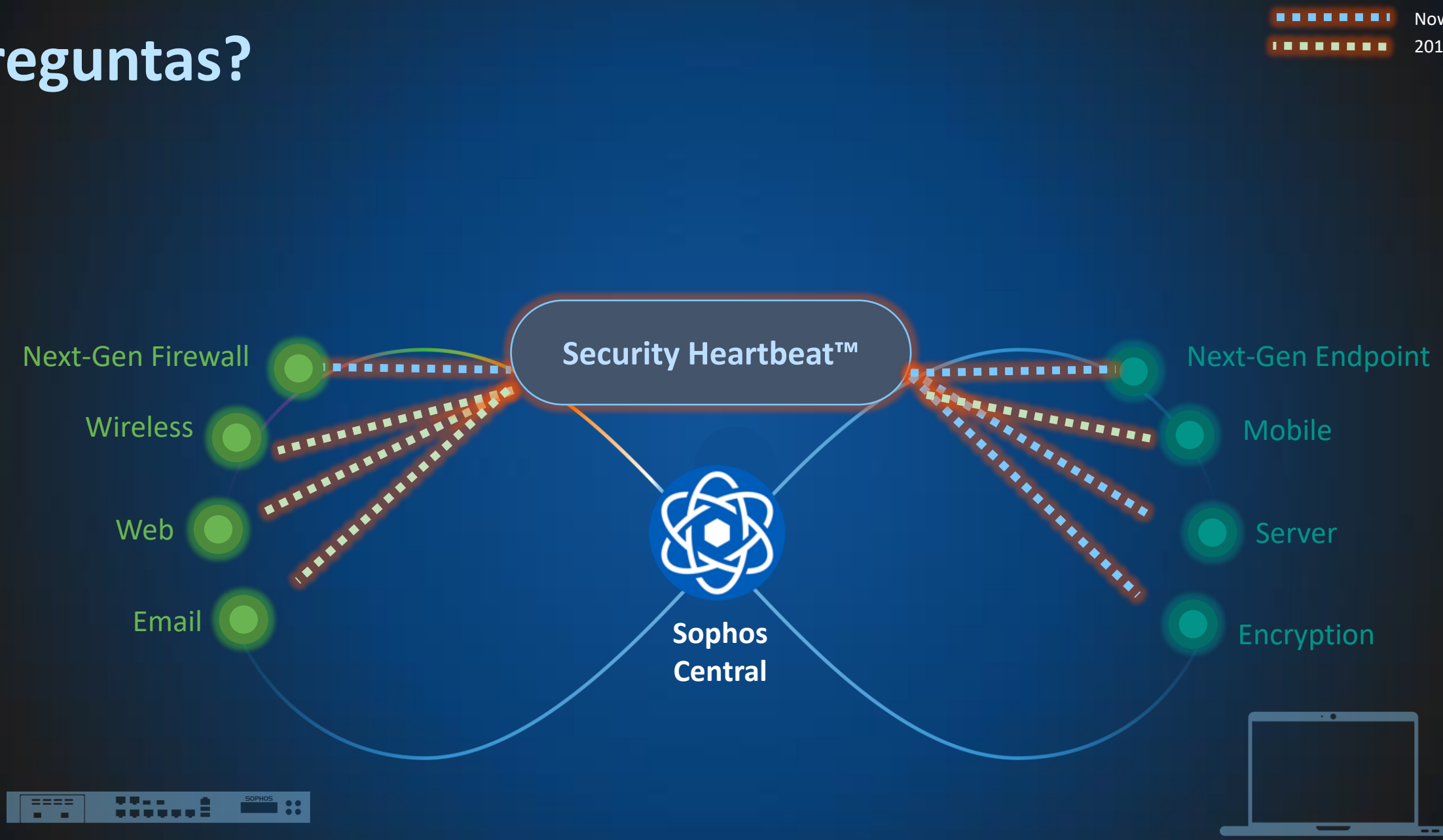
MALICIOUS URLS

SOFTWARE EXPLOITS

PROCESS ATTACKS

UNAUTHORIZED APPS

Preguntas?


Now
2017
Security Heartbeat™
Next-Gen Firewall
Wireless
Web
Email
Next-Gen Endpoint
Mobile
Server
Encryption
Sophos
Central

SOPHOS

Security made simple.