Next Generation Enduser Protection

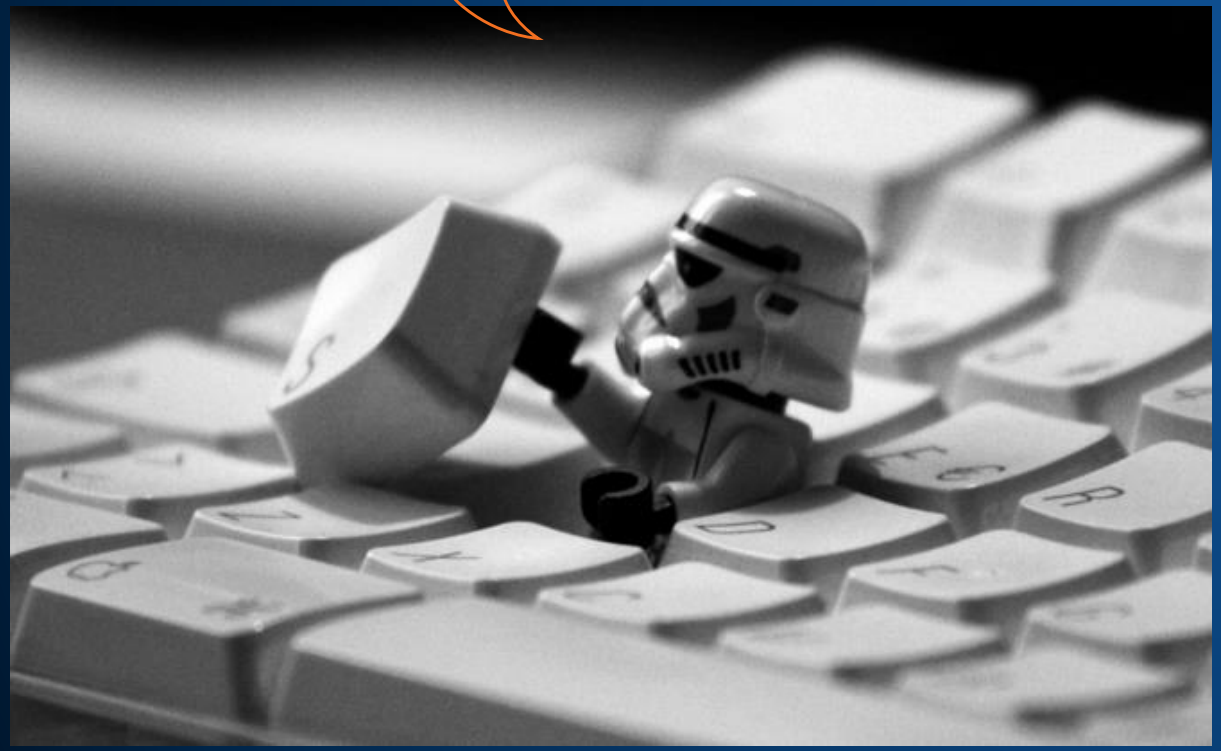
Janne Timisjärvi
Systems Engineer

10.5.2017

SOPHOS

What is the the real threat?

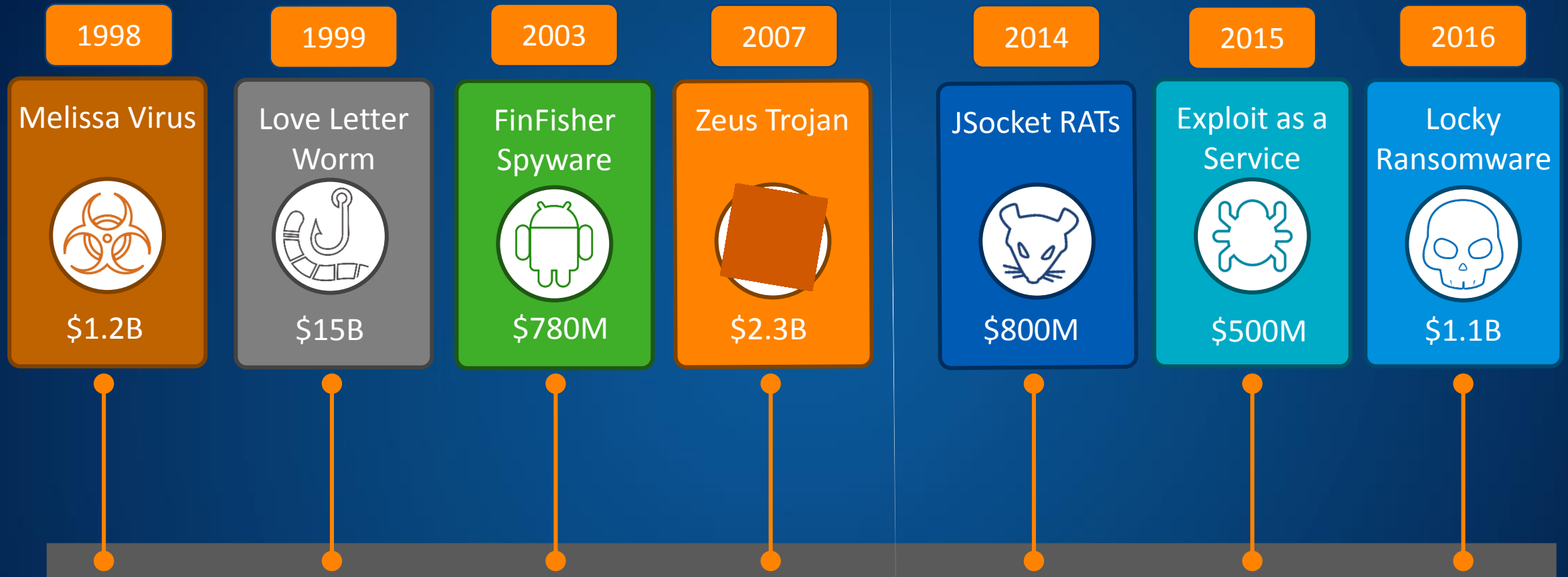
Encrypted!
Give me all
your Bitcoin$



Let‘s check if there
Is something of value

The Evolution of Endpoint Threats

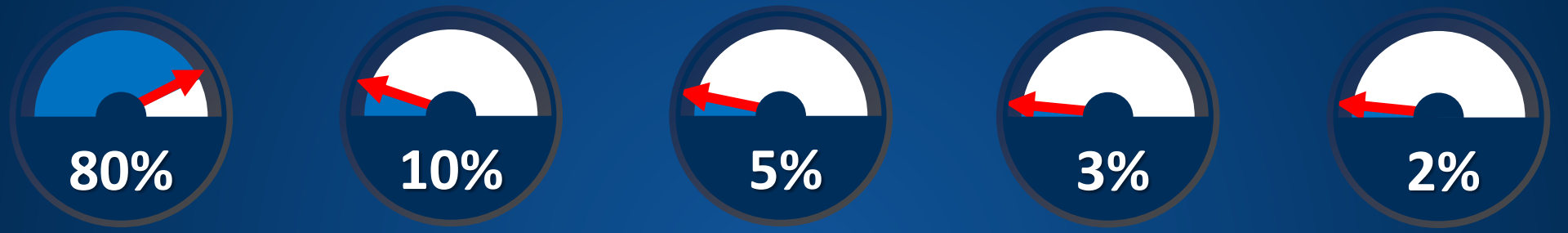
From Malware to Exploits



TRADITIONAL MALWARE

ADVANCED THREATS

Where Malware gets stopped



Exposure Prevention	Pre-Exec Analytics	Signatures	Run-Time	Exploit Detection
URL Blocking Web Scripts Download Rep	Generic Matching Heuristics Core Rules	Known Malware Malware Bits	Signatureless Behavior Analytics	Technique Identification

Traditional Malware

Advanced Threats

Sophos INTERCEPT X

Anti-Ransomware

Stops Ransomware

- Stops Malicious Encryption
- Behavior Based Conviction
- Automatically Reverts Affected Files
- Identifies source of Attack

Anti-Exploit

Stops unknown Malware

- Signatureless Exploit Prevention
- Blocks Memory-Resident Attacks
- Tiny Footprint & Low False Positives

Sophos Clean

Removes the threat

- Signatureless detection and remediation of unknown malware

Root Cause Analysis

Automated Analysis

- IT Friendly Incident Response
- Process Threat Chain Visualization
- Prescriptive Remediation Guidance

SOPHOS

Malicious URLs

Unauthorized Apps

Removable Media

Executable Files

MS Files & PDF

Ransomware Prevention

Exploit Prevention

Advanced Clean

Incident Response

90% of Data Breaches are From Exploits Kits

90% Of Exploit Kits Are Built From Known Vulnerabilities

And Yet...
More Than 60% of IT Staff Lack Incident Response Skills

Before it reaches device **Prevent** Before it runs on device

Detect

Respond

Complete Next-Gen Endpoint Protection

For server or locked-down endpoint environments, app control prevents unknown / unwanted apps from running.

Knowing the source/reputation of a file, URL, email, etc. can prevent an attack before it happens. Includes technologies such as MTD, download reputation, URL filtering, secure email gateway, etc.

.exe Malware

Non-.exe Malware

Script-based Malware

Phishing Attacks

The only effective way to set policy to ensure removable media cannot put an organization at risk.

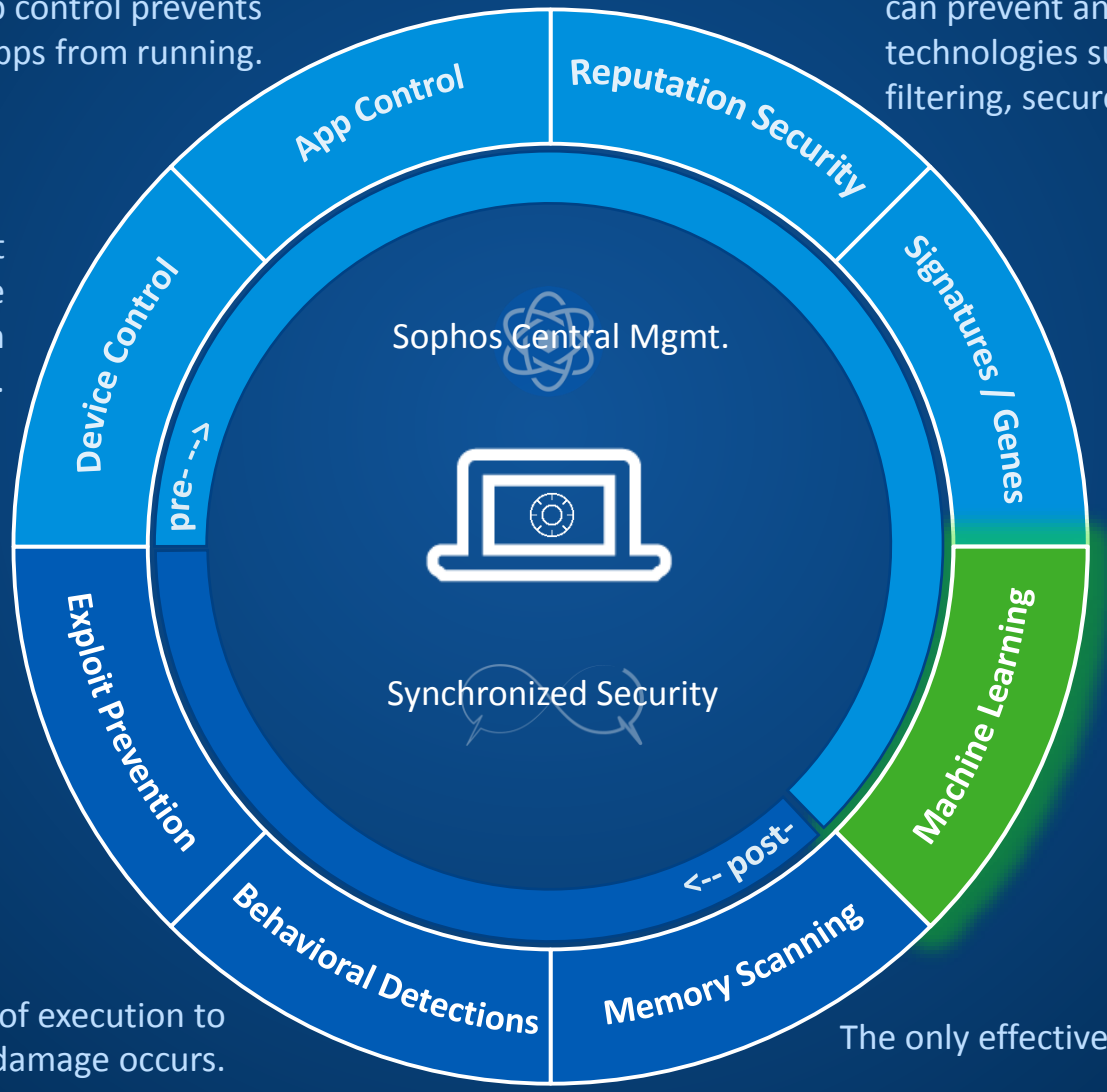
Provides reliable detection of script, document, and macro malware, and an efficient first line of defense against known executable variants.

Malicious URLs

Exploits

Removable Media

Unauthorized Apps



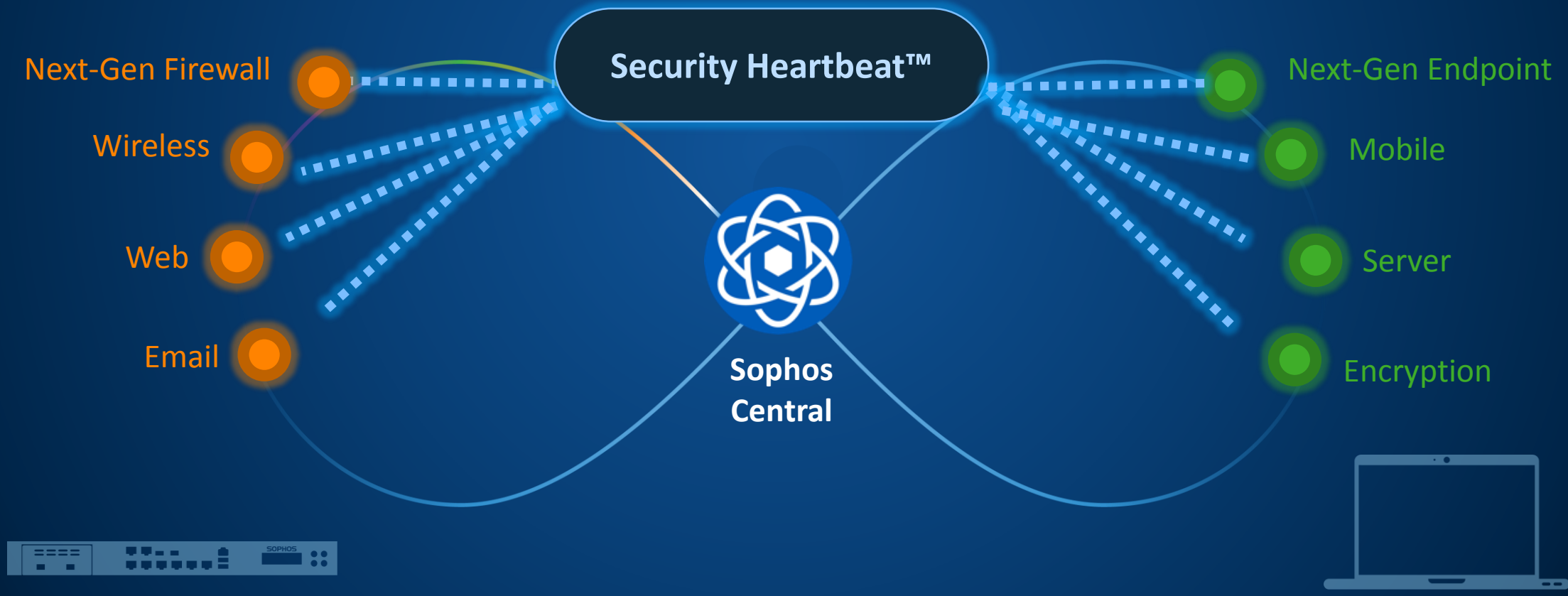
Effective for run-time prevention of exploit-based malware such as ransomware. **Sophos Intercept X** delivers highly-effective next-gen exploit prevention capabilities.

Via Invincea, pre-execution malware prevention that is highly scalable, fast, and effective, especially against zero-day threats. Invincea's pioneering ML technology delivers high detection rates and very low FP rates, which is unique.

Heuristic detections based on the behaviors of execution to stop evasive malware before damage occurs.

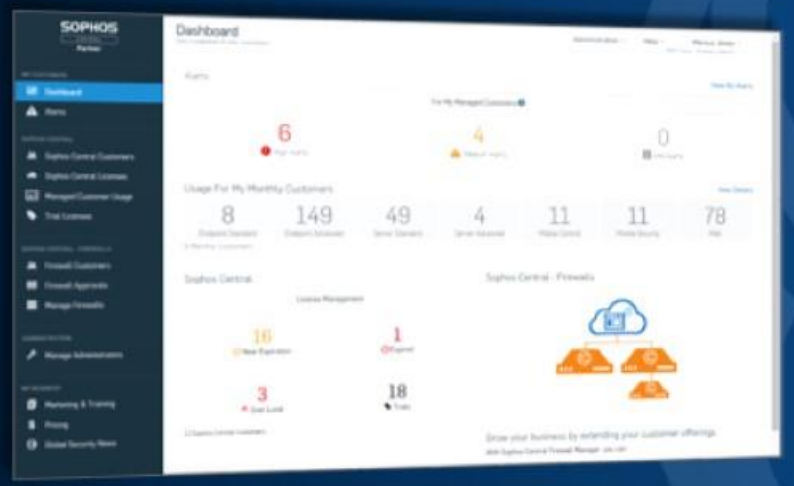
The only effective defense against in-memory malware.

Synchronized Security



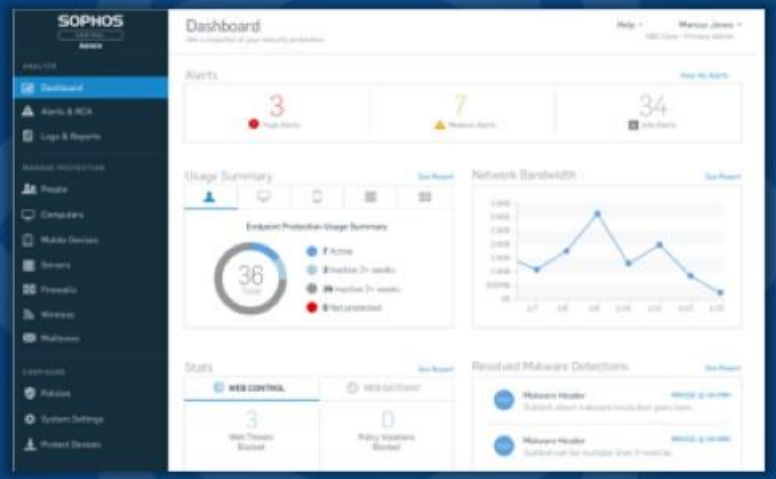
What is Sophos Central?

Partner Dashboard



Allows Partners to manage multiple customer installations

Admin



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

Self Service

Allows Users to customize security status and notifications

Sophos Central Phish Threat

Sophos Phish Threat is an advanced **security testing and training** platform designed to reduce your largest attack surface – your end-users – with effective security awareness testing and training.

#1

Pick a Phishing Attack Campaign

#2

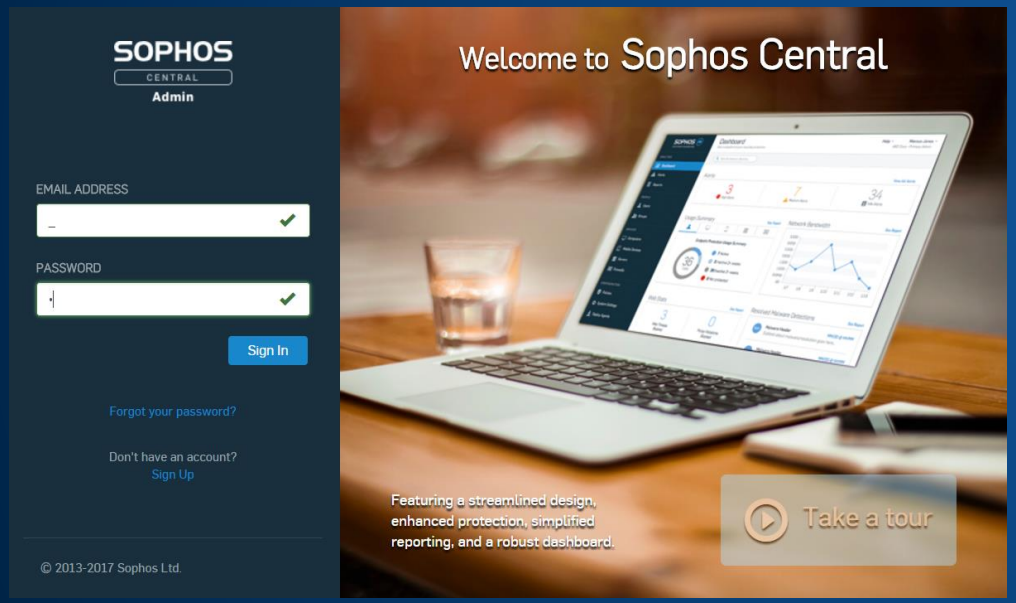
Pick a Security Training Module

#3

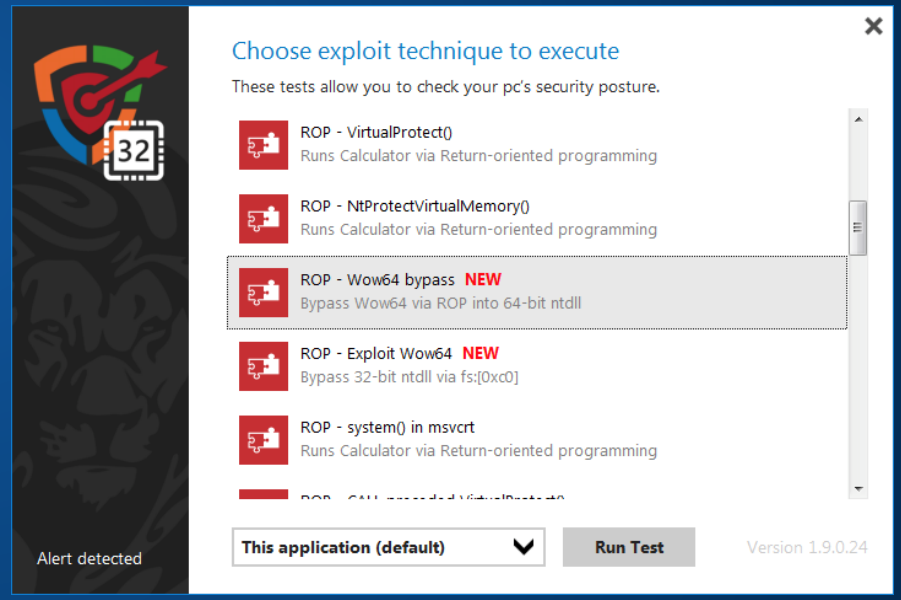
Manage End-User Response & Awareness

Don’t take my words – test it!

Central.Sophos.com



Hitmanpro – test tool



Summary

- Ransomware is not your enemy – Exploits are!
- Sophos Endpoint provides complete NG Endpoint protection, InterceptX can be run alongside with 3rd party AV
- We provide the platform; Sophos Central!
- Go and test

SOPHOS

Security made simple.