

# END-TO-END SECURITY

## HOW TO SECURE YOUR HYBRID WORLD?

**Lars Putteneers**

Sales Engineer

October 2017

**SOPHOS**

# Sophos snapshot

 **1985**  
FOUNDED  
OXFORD, UK

 **\$450M**  
IN FY15 BILLING  
(APPX.)

 **3,500**  
EMPLOYEES  
(APPX.)

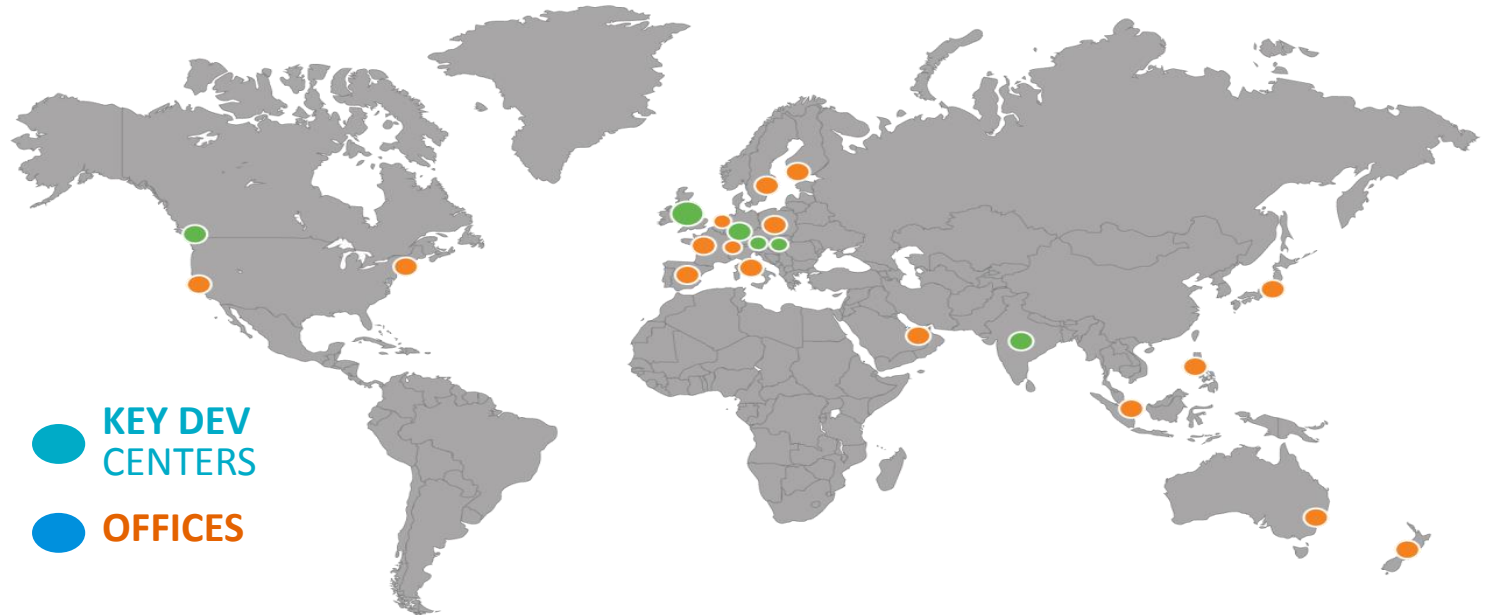
 **HQ**  
OXFORD, UK

**200,000+**  
CUSTOMERS  **100M+**  
USERS

 **90+%**  
BEST IN CLASS  
RENEWAL RATES

 **15,000+**  
CHANNEL  
PARTNERS

## OEM PARTNERS:



**WHY**

**SOPHOS**

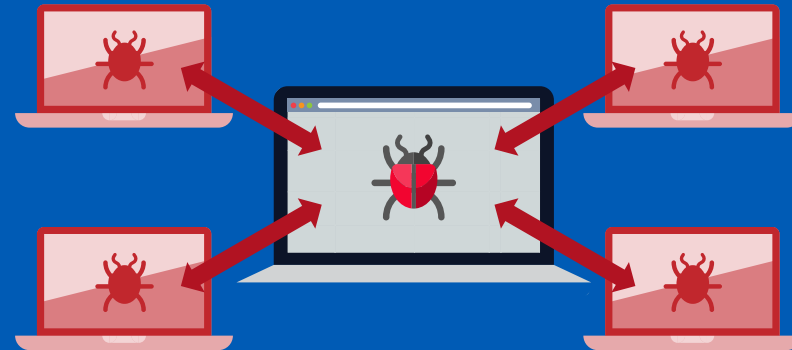
# Increasing attacks, increasing sophistication

**Attack surface exponentially larger**



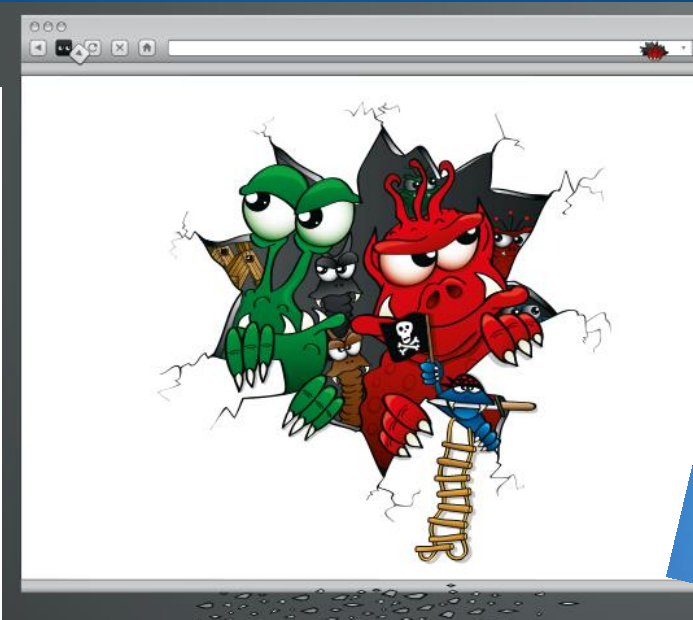
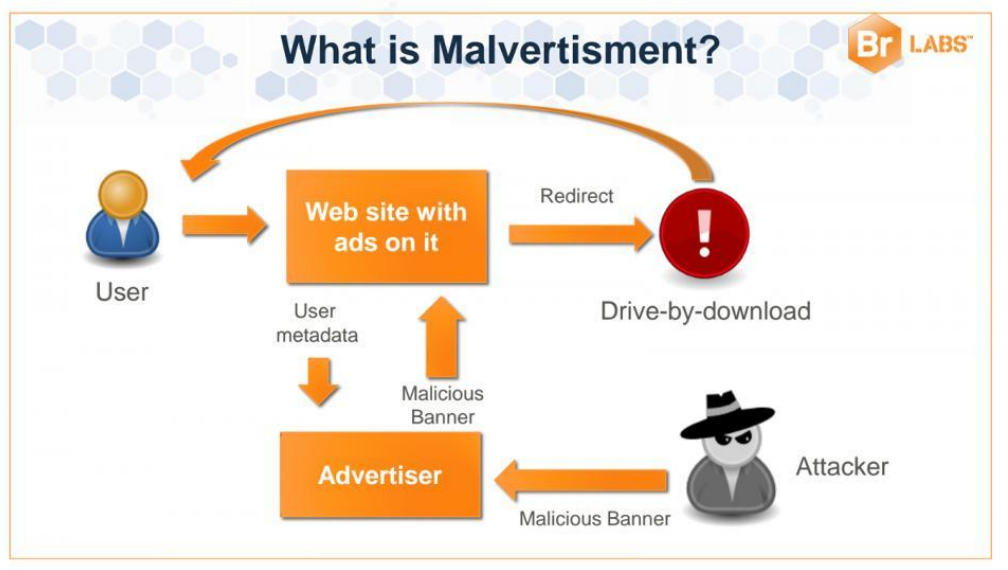
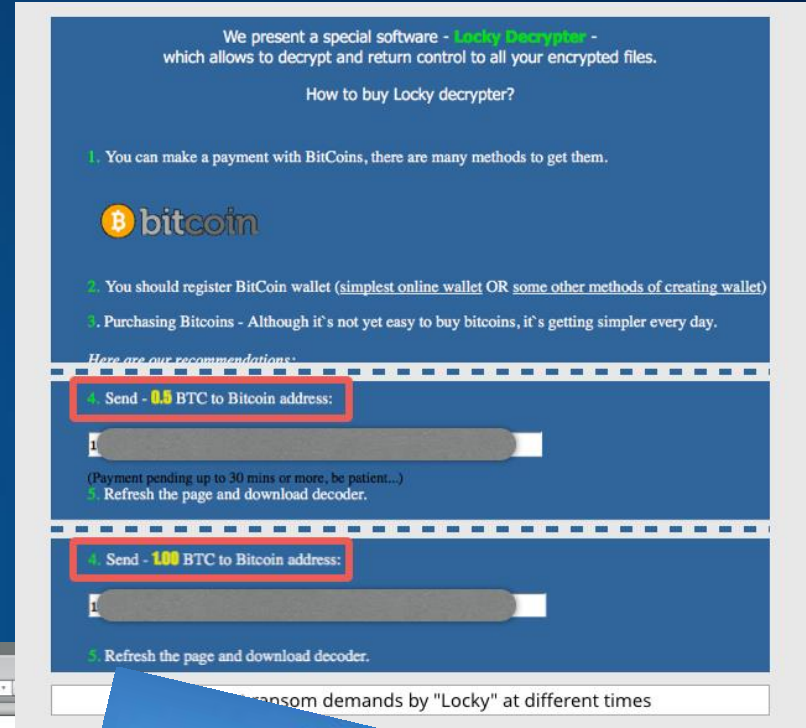
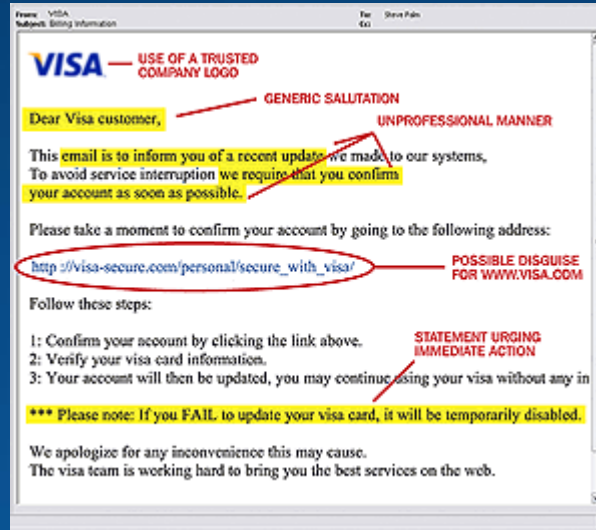
*Laptops/Desktops  
Phones/Tablets  
Virtual servers/desktops  
Cloud servers/storage  
IoT*

**Attacks are more sophisticated than defenses**



*Syndicated crime tools  
Zero day exploits  
Memory resident  
Polymorphic/metamorphic  
Multilevel botnets*

# Attacks are evolving



# We believe

- Security must be:
  - Simple
  - Comprehensive
  - Easy to use
  - Single console
  
- You need to have MORE SECURITY with LESS EFFORT

**HOW**

**SOPHOS**

# Synchronized Security



**Admin** | Manage All Sophos Products



**Self Service** | User Customizable Alerts



**Partner** | Management of Customer Installations

## Sophos Central

In Cloud  On Prem 



UTM/Next-Gen Firewall



Wireless



Email



Web



Next-Gen Endpoint



Mobile



Server



Encryption



## Cloud Intelligence



**Analytics** | Analyze data across all of Sophos' products to create simple, actionable insights and automatic resolutions



**Sophos Labs** | 24x7x365, multi-continent operation |

Malware Identities | URL Database | Machine Learning | Threat Intelligence | Genotypes | Reputation | Behavioral Rules | APT Rules | App Identities | Anti-Spam | DLP | SophosID | Sandboxing | API Everywhere



**WHAT**

**SOPHOS**

# An Endpoint is an Endpoint is an Endpoint



# Mobile in Sophos Central

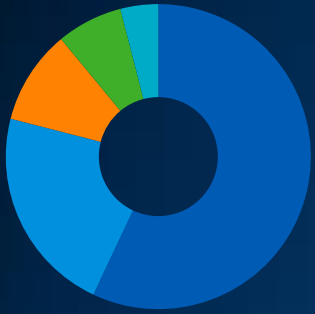
The screenshot shows the Sophos Central Admin interface for Mobile management. The left sidebar contains navigation menus for INFORM, MANAGE, CONFIGURE, and SETTINGS. The main dashboard area displays several widgets:

- Getting started videos:** A list of five video links: Quick tour, Initial setup, Configuration, Device enrollment, and Day-to-day tasks.
- Compliance status - All:** A pie chart showing 4 managed devices (dark blue) and 1 not managed device (light blue).
- Compliance violation severity:** A bar chart showing 1 low severity violation, 0 medium, and 0 high.
- Device enrollment wizard:** A large button labeled "Add device" with a smartphone icon.
- Managed status - All:** A summary showing 4 Managed devices and 1 Not managed device.
- SSP registration status:** A bar chart showing 0 unenrolled, 2 in progress, and 0 failed.
- Split by platform:** A pie chart showing the distribution of devices by platform: WM (Windows Mobile), iOS, WD (Windows Desktop), and AND (Android).
- Versions - iOS:** A large blue circle representing 1 iOS device.
- Versions - Android:** A large blue circle representing 1 Android device.

At the top right of the dashboard, there is a "Help" link and the user's email "thomas.lippert@sophos.com" with the role "Administrator".

# Data is the new gold. Encrypt it.





# How far do **you** want to go to manage the risk from GDPR?

DATA SECURITY SCALE



Sophos Central

Sophos SafeGuard

# Future?

**SOPHOS**



# Machine Learning:

## Pre-execution Malware Prevention & Detection



# 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.

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

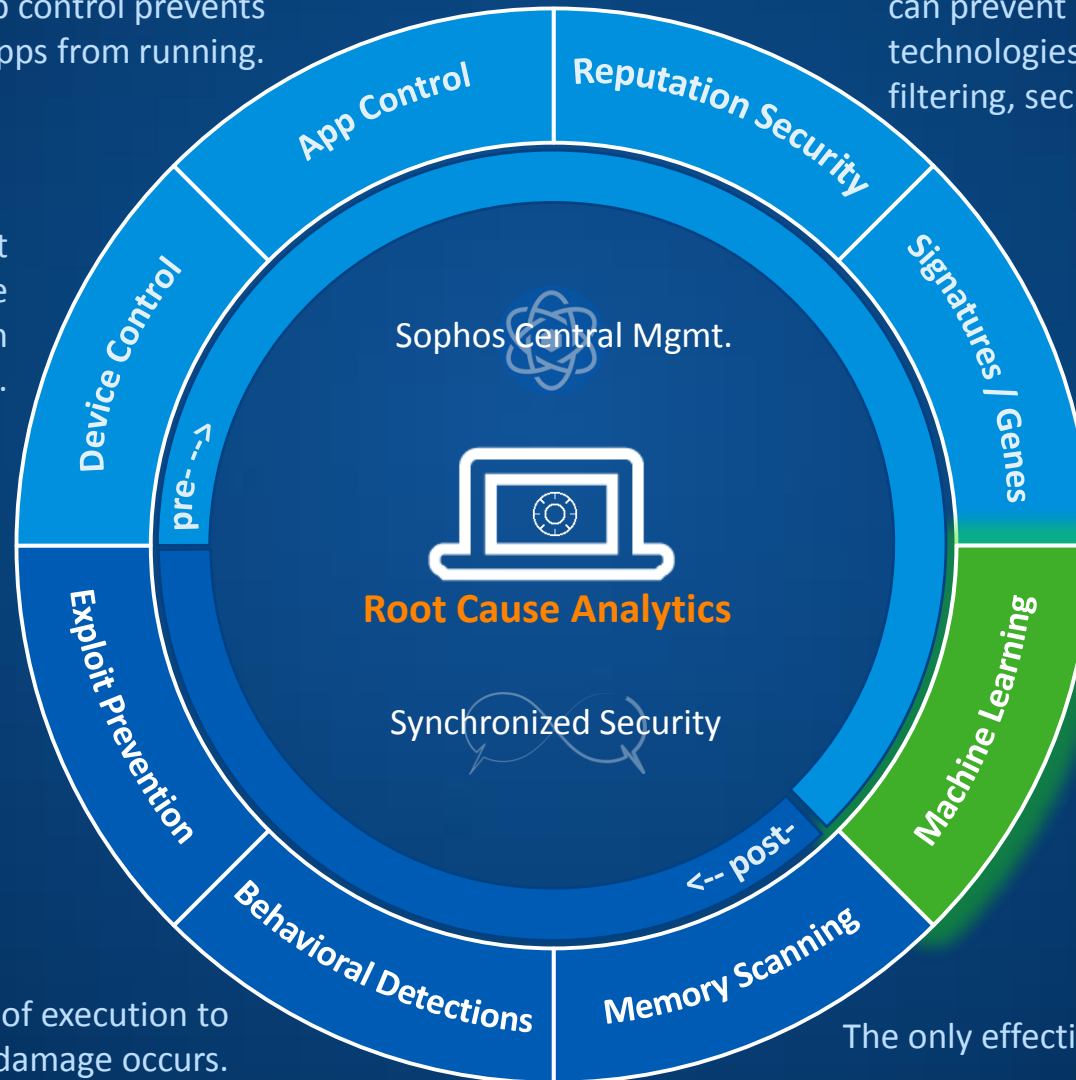
Provides reliable detection of script, document, and macro malware, and an efficient first line of defense against known executable variants.




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




**Invincea** pre-execution malware prevention 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.



-  .exe Malware
-  Non-.exe Malware
-  Script-based Malware
-  Phishing Attacks

-  Malicious URLs
-  Exploits
-  Removable Media
-  Unauthorized Apps



# Questions?

**SOPHOS**

**SOPHOS**  
Security made simple.