Stop the Exploit.
Stop the Attack.

Justin Walker &
Chris Chaves

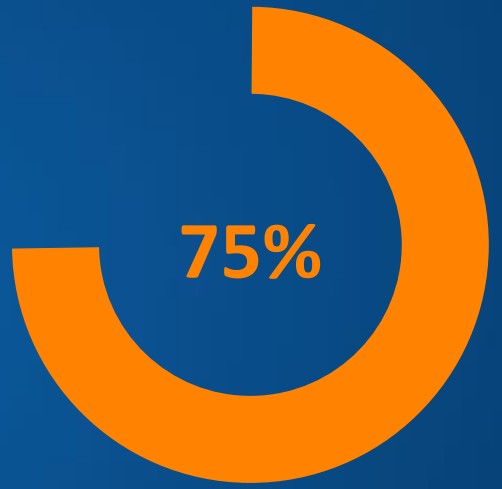
February 2018

SOPHOS

The age of single-use disposable malware

400,000

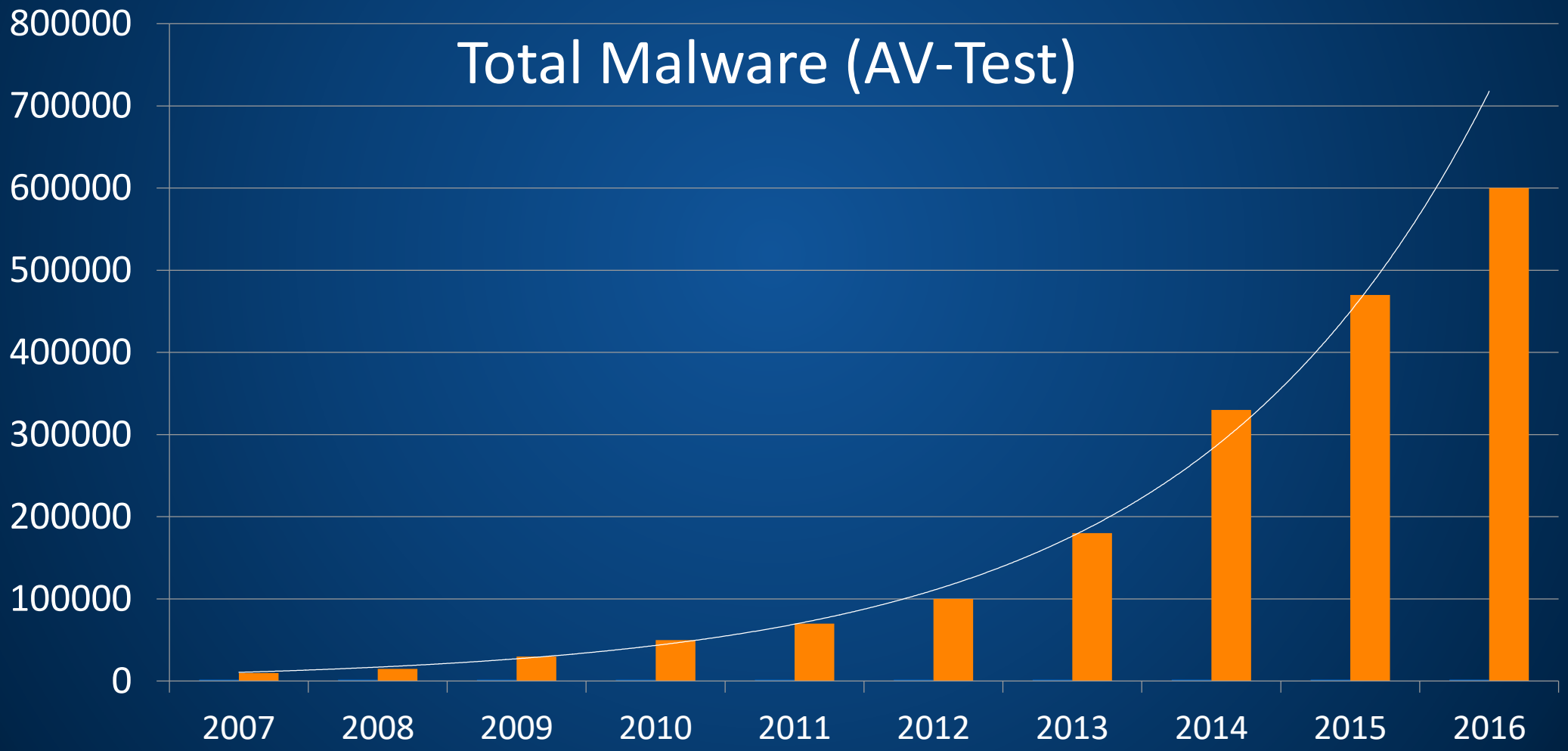
SophosLabs receives and processes **400,000** previously unseen malware samples each day.



75% of the malicious files SophosLabs detects are found only within a single organization.

Exponential growth in new malware

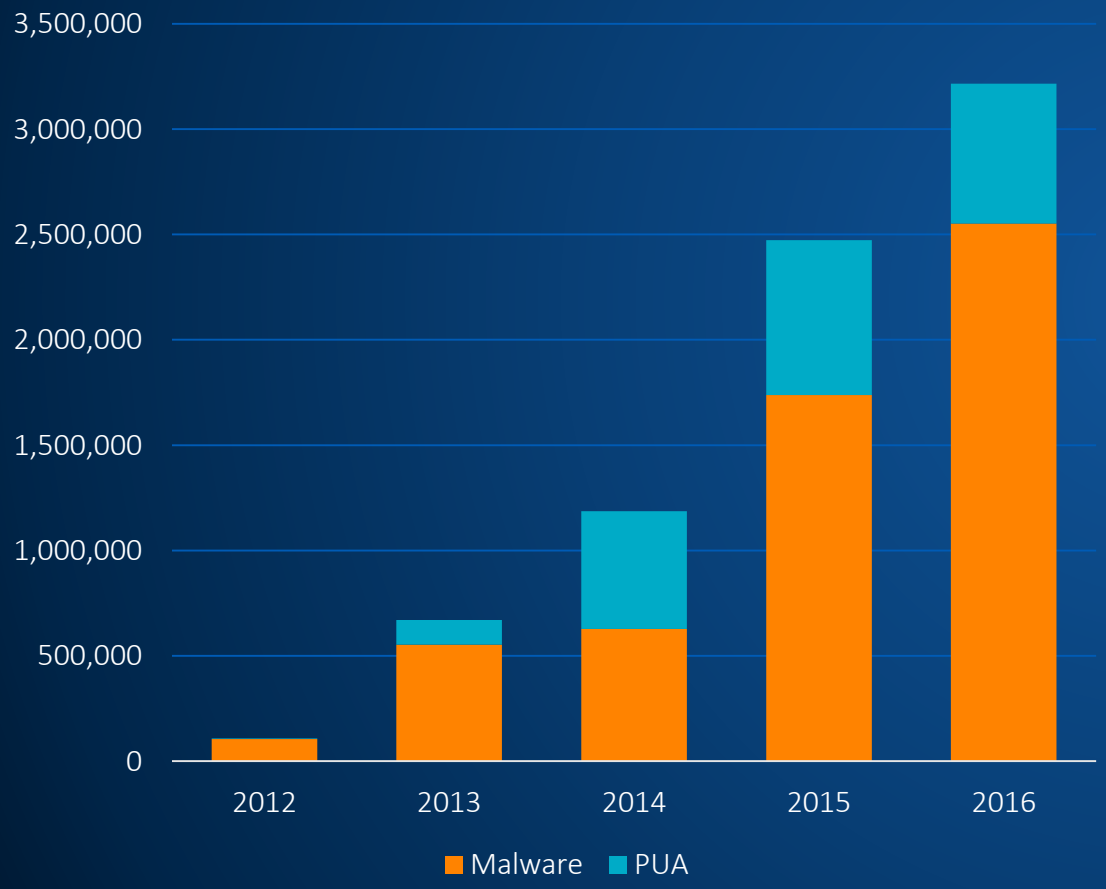
27% of all malware variants in history were created in the last 12 months



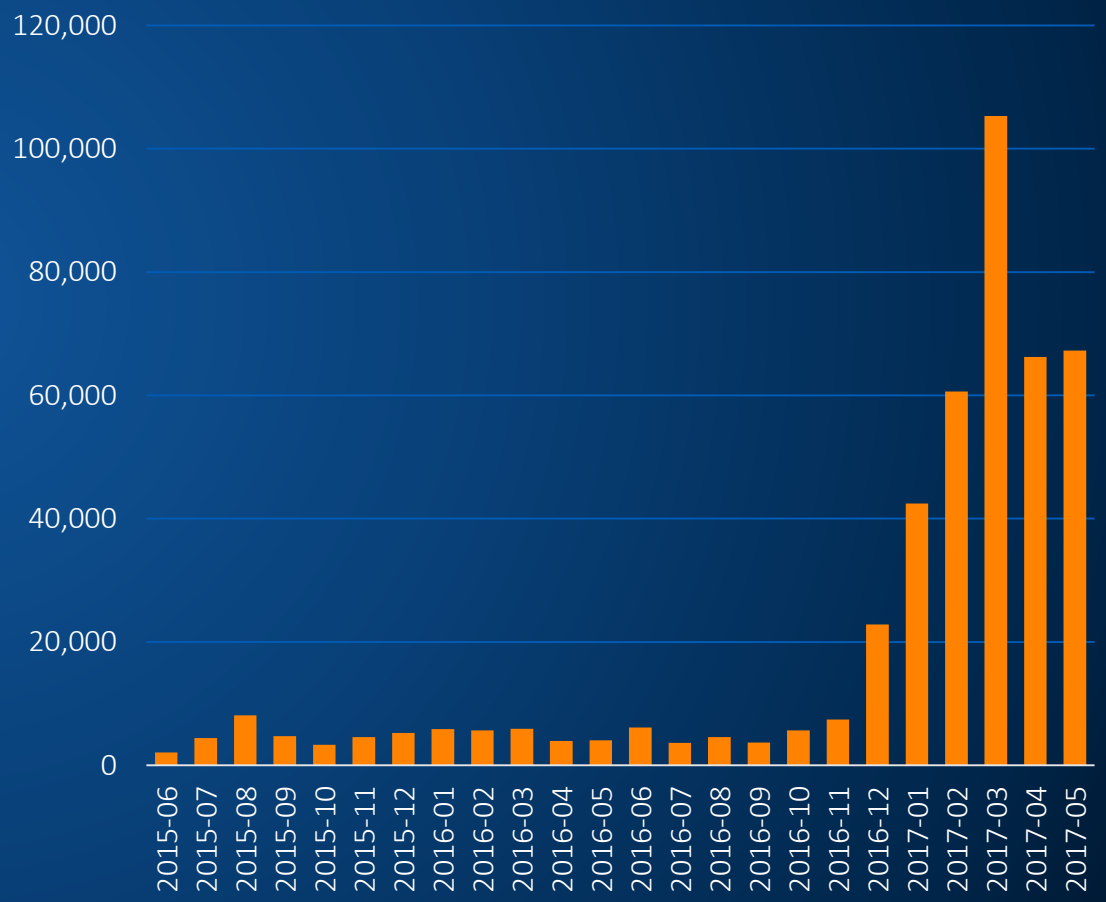
SOPHOS

Mobile Threats Are Real…

Android malware keeps growing



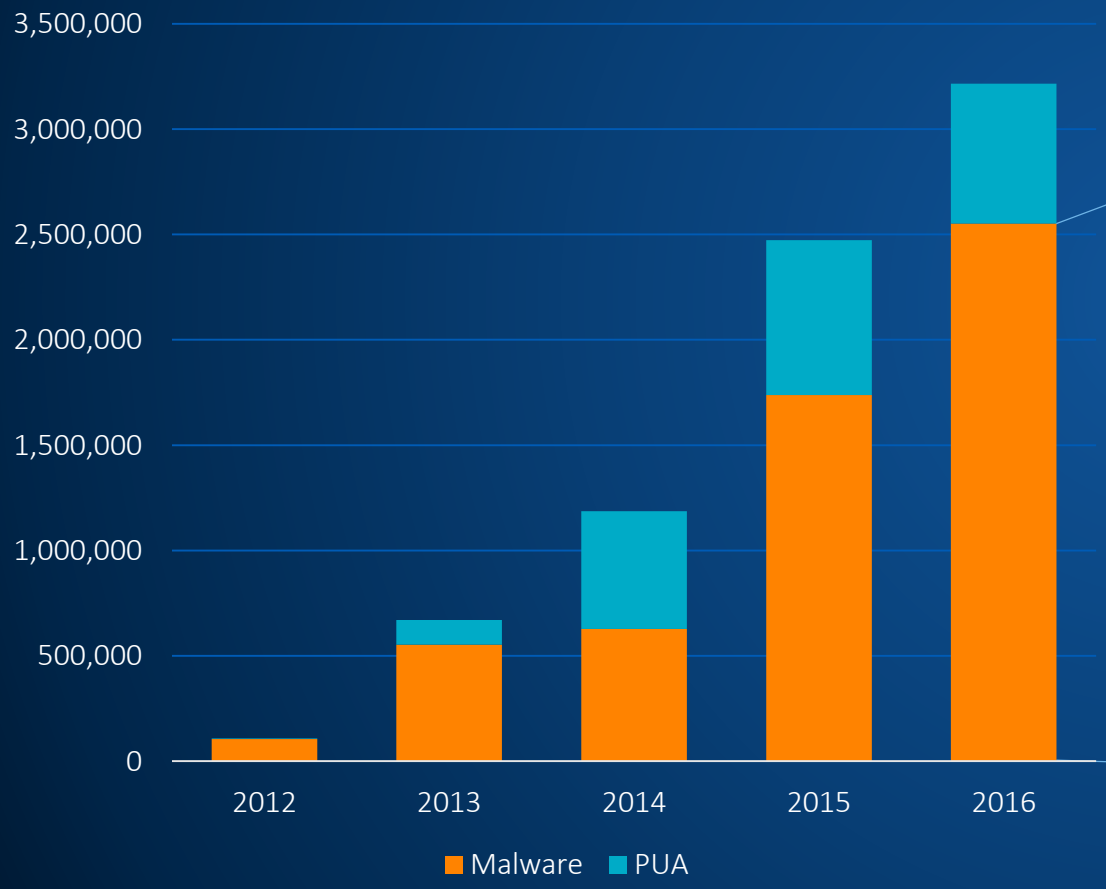
Android ransomware



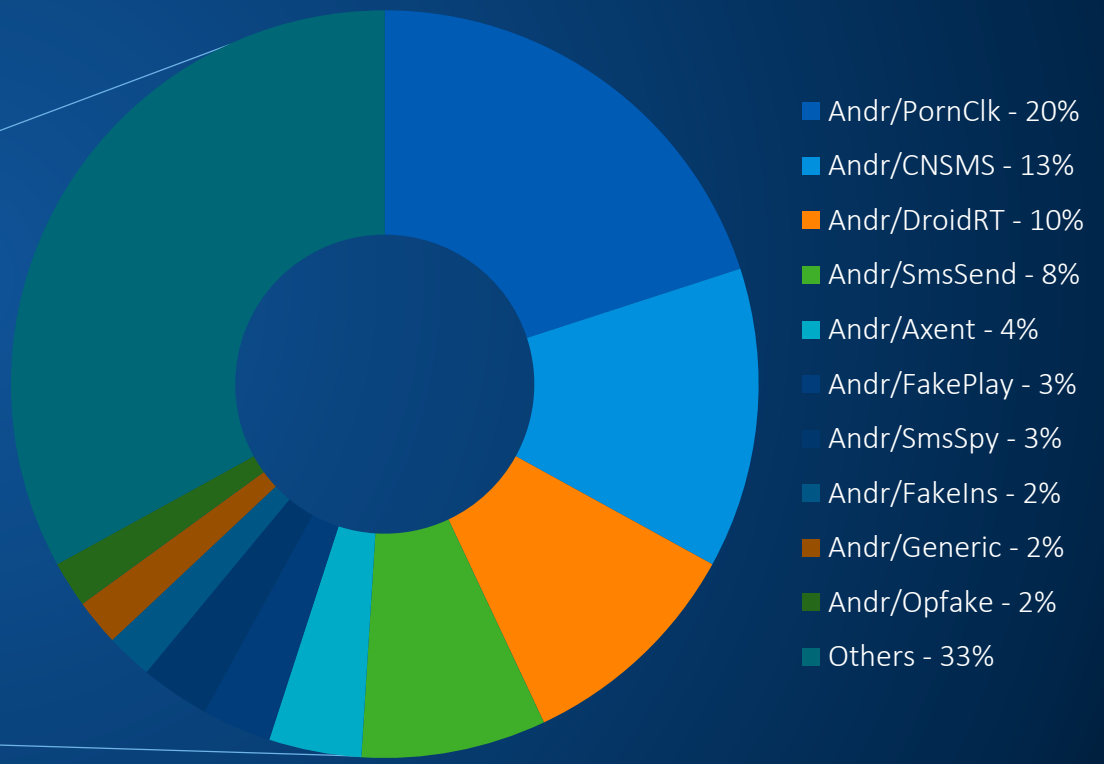
Source: SophosLabs, 2017

Mobile Threats Are Real…

Android malware keeps growing



Top ten Android malware 2016



Source: SophosLabs, 2017

Business Ramifications of a Cyber Attack

- *Attacks are from within the perimeter, focused on Software Exploits*
- *Ransomware alone reached over $1.2B in damages last year*
- *Lack of Threat Intelligence after a Breach (What? Where? When? & HOW?)*

The Evolution of Endpoint Threats

From Malware to Exploits

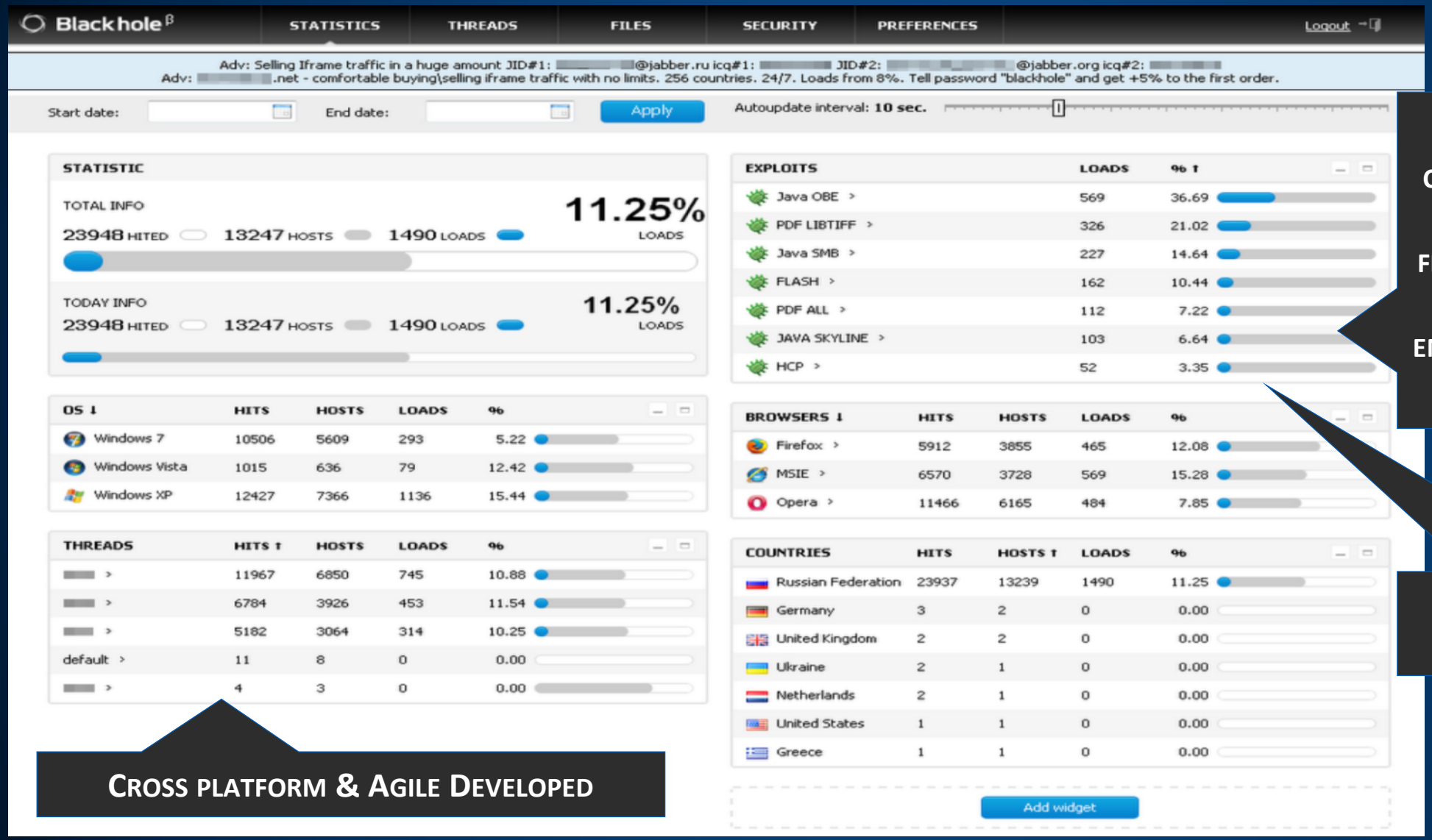
2009 - Introduction of Polypack "Crimeware as a Service"

1998	1999	2003	2007	2014	2015	2016
Melissa Virus	Love Letter Worm	FinFischer Spyware	Zeus Trojan	JSocket RATs	Exploit as a Service	Locky Ransomware
						
$1.2B	$15B	$780M	$2.3B	$800M	$500M	$1.1B

Traditional Malware

Advanced Threats

From cottage industry for full industrialization



Fully integrated SaaS console including network and endpoint techniques from infecting a website, all the way to delivering an endpoint payload and selling the results

Zero day exploits automatically included

Cross platform & Agile Developed

SOPHOS

We insist on being vulnerable

“Patch Tuesday”

In the Perfect World

- Patch Fast, Patch Often
- Defect-Free Software

“Exploit Wednesday”

In the Real World

- Slow to Patch
- Zero-Day Exploits Continue

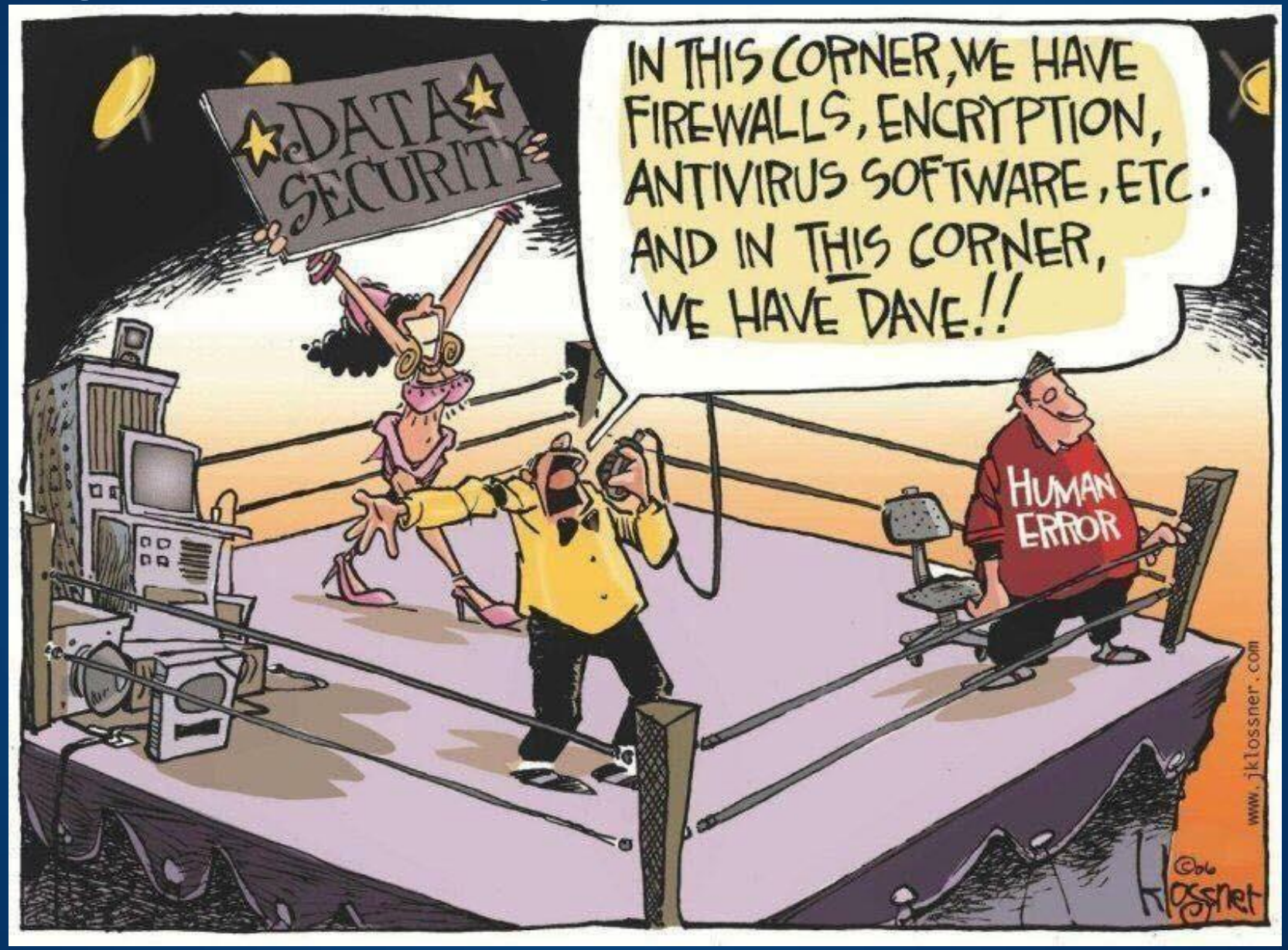
Threats evolve and security must adapt or die

ADVANCED MALWARE

ACTIVE ADVERSARY

LIMITED VISIBILITY

You’re only as secure as your users



Sophos Intercept X

Core Capabilities

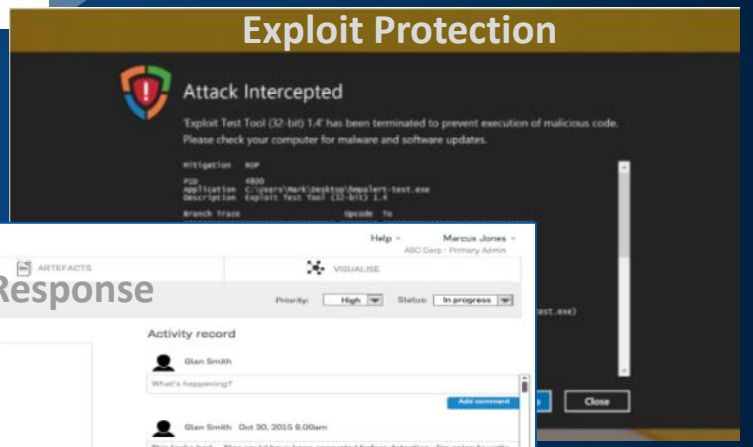
- Signatureless detection
  - CryptoGuard – Detect and recover from ransomware
  - Comprehensive Exploit Prevention
  - Malicious Traffic Detection
  - Synchronized Security
- Incident Response Report
  - Automatic Identification of root cause
  - IOC artifact list
  - Visualization of the attack events
- Forensic Malware Removal
  - Sophos Clean a 2nd opinion scanner

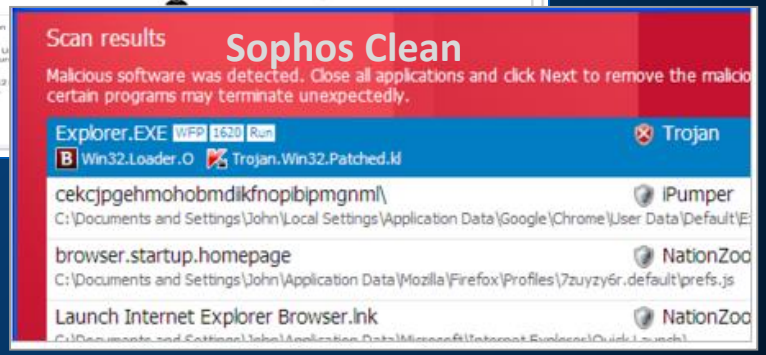
Packaging

- Intercept Runs alongside competitive AV
- Ultimate is the most complete Sophos EP

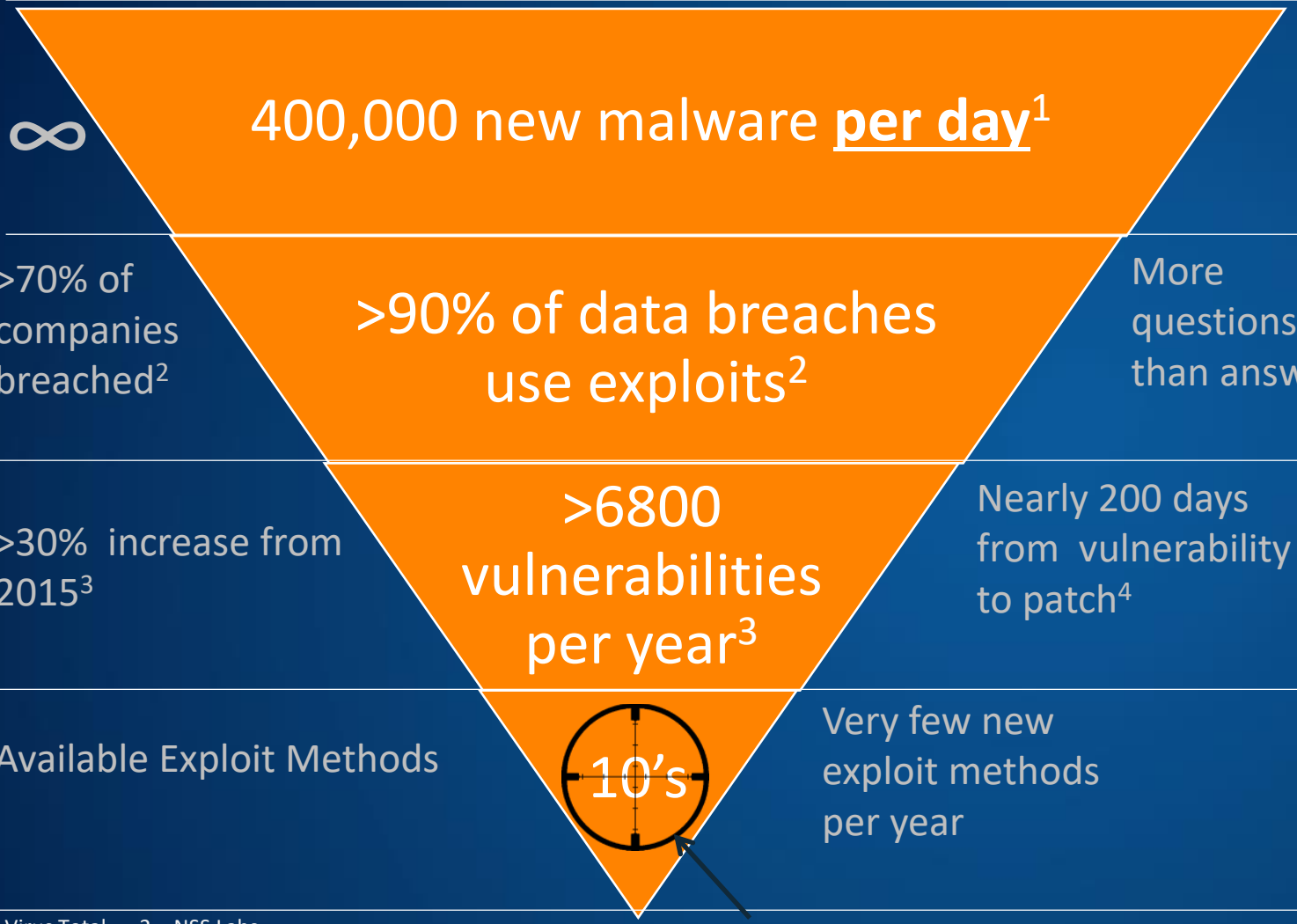
CryptoGuard

- Simple and Comprehensive
- Universally prevents spontaneous encryption of data
- Notifies end user on rapid encryption events
- Rollback to pre-encrypted state





Data Breaches - The root of the problem



Traditional Anti-Virus

- File Analytics
- Heuristics
- URL Blocking

SIEM, EDR, UEBA

- Anomaly Detection
- Security Operations Center
- Forensic breach assessment teams

Patch Management

- Vulnerability Scanning
- Device Management
- Patch testing and deployment

Sophos - Intercept

- Exploit and Ransomware prevention
- Incident Response Report
- Automatic Root Cause Attribution

Anti-Exploit – Targets the root of the problem

1 – Virus Total 2 – NSS Labs
3 – Gartner 4 – White Hat Security

SOPHOS

Exploit Mitigation Techniques by Vendor

Comprehensive Exploit Mitigation

- 20+ mitigation techniques
- Successful attacks often leverage 2-4 techniques in series
- Only 1-2 major new techniques are developed per year
- 100% signatureless

Exploit Mitigation Tecniques	Sophos Intercept X	ESET Smart Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Office Scan	Webroot	Cylance PROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	Crowdstrike Falcon
Enforce Data Execution Prevention (DEP) Prevents abuse of buffer overflows	●			●					●	●	●	●
Mandatory Address Space Layout Randomization (ASLR) Prevents predictable code locations	●								●[1]		●	●[1]
Bottom Up ASLR Improved code location randomization	●								●	●		
Null Page (Null Dereference Protection) Stops exploits that jump via page 0	●								●			
Heap Spray Allocation Pre-allocated common memory areas to block attacks	●				●				●	●	●	●
Dynamic Heap Spray Stops attacks that spray suspicious sequences on the heap	●										●[2]	
Stack Pivot Stops abuse of the stack pointer	●			●		●		●	●	●	●	
Stack Exec (MemProt) Stops attacker' code on the stack	●					●		●	●			
Stack-based ROP Mitigations (Caller) Stops standard Return-Oriented Programming attacks	●		●	●		●			●	●	●	
Branch-based ROP Mitigations (Hardware Augmented) Stops advanced Return-Oriented Programming attacks	●											
Structured Exception Handler Overwrite Protection Stops abuse of the exception handler	●				●				●			

[1] Based on ASLR functionality offered by Windows, available only in Windows Vista and newer versions of Windows

[2] NOP sled and Polymorphic NOP sled only; no Flash Vector heap spray detection

SOPHOS

Exploit Mitigation Techniques by Vendor (cont.)

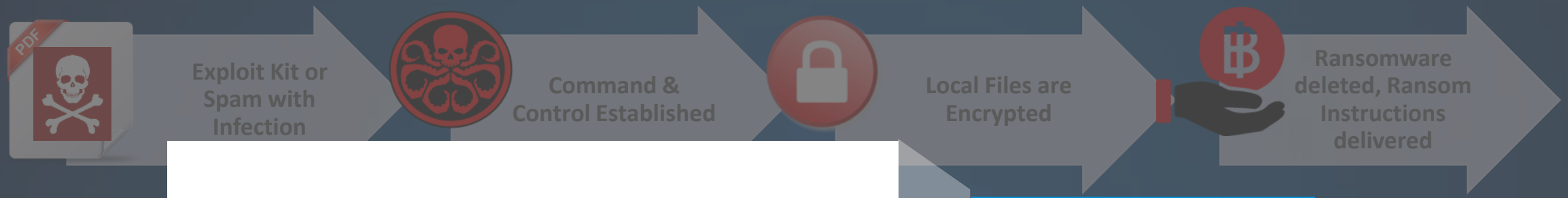
Comprehensive Exploit Mitigation

- Detection of exploit techniques requires no prior knowledge of the vulnerability being exploited
- Exploit behavior is a clear indicator of malicious intent

Exploit Mitigation Tecniques	Sophos Intercept X	ESET Smart Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Office Scan	Webroot	Cylance PROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	Crowdstrike Falcon
Import Address Table Access Filtering (IAF) Stops attackers that lookup API addresses in the IAT	●								EAF[3]			
Load Library Prevents loading of libraries from UNC paths	●								●	●	●	
Reflective DLL Injection Prevents loading of a library from memory into a host process	●										●	
Shellcode Stops code execution in the presence of exploit shellcode	●											
VBScript God Mode Prevents abuse of VBScript in IE to execute malicious code	●								●	●		
WoW64 Stops attacks that address 64-bit function from WoW64 process	●											
Syscall Stops attackers that attempt to bypass security hooks	●											
Hollow Process Stops attacks that use legitimate processes to hide hostile code	●										●	
DLL Hijacking Gives priority to system libraries for downloaded applications	●										●	
Application Lockdown Stops logic-flaw attacks that bypass mitigations	●									●	●	
Java Lockdown Prevents attacks that abuse Java to launch Windows executables	●				●					●	●	
Squiblydoo AppLocker Bypass Prevents regsvr32 from running remote scripts and code	●											

[3] EAF - Export Address Filtering

Anatomy of a Ransomware Attack



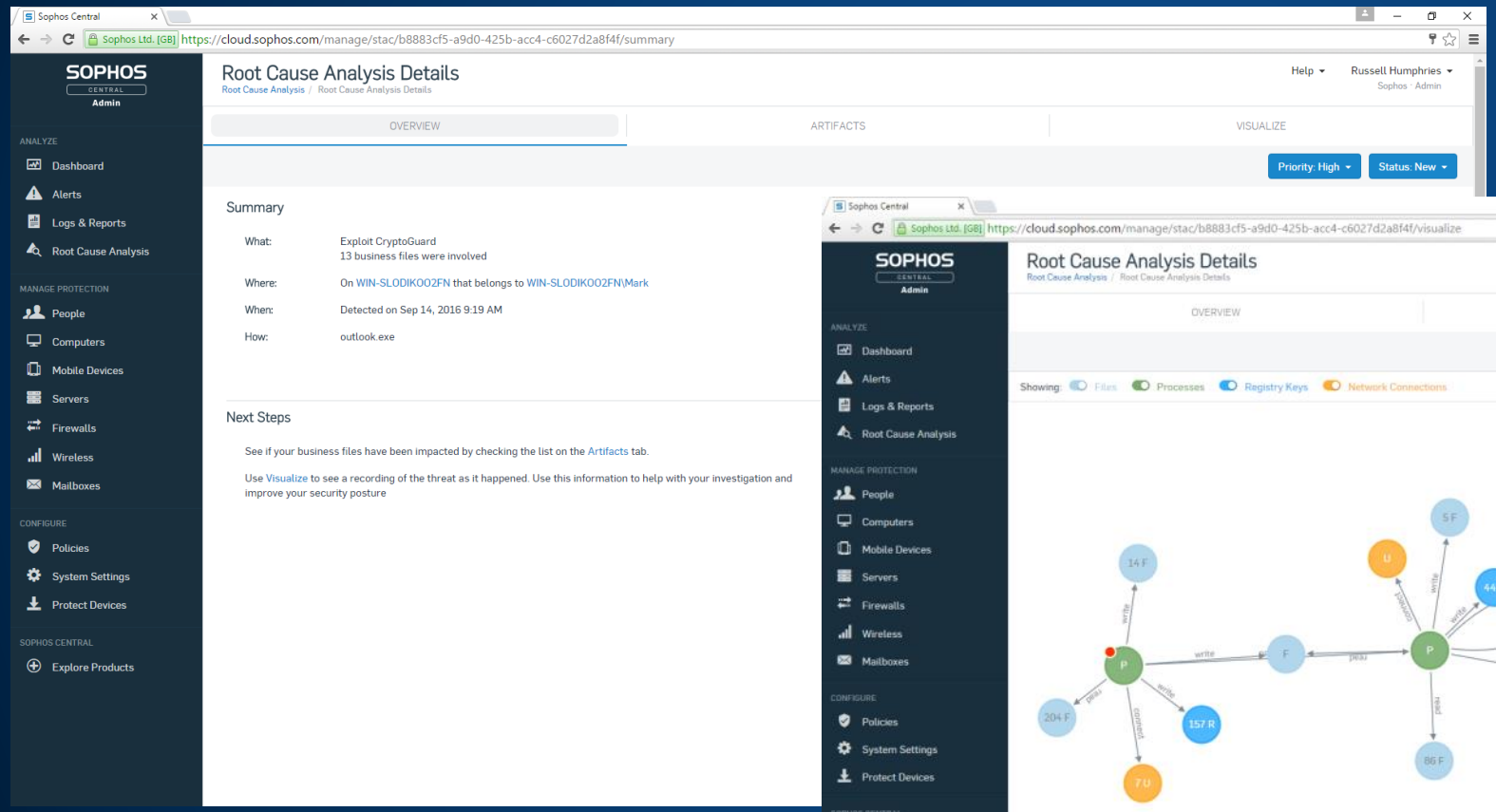
CryptoGuard – Behavior Monitor

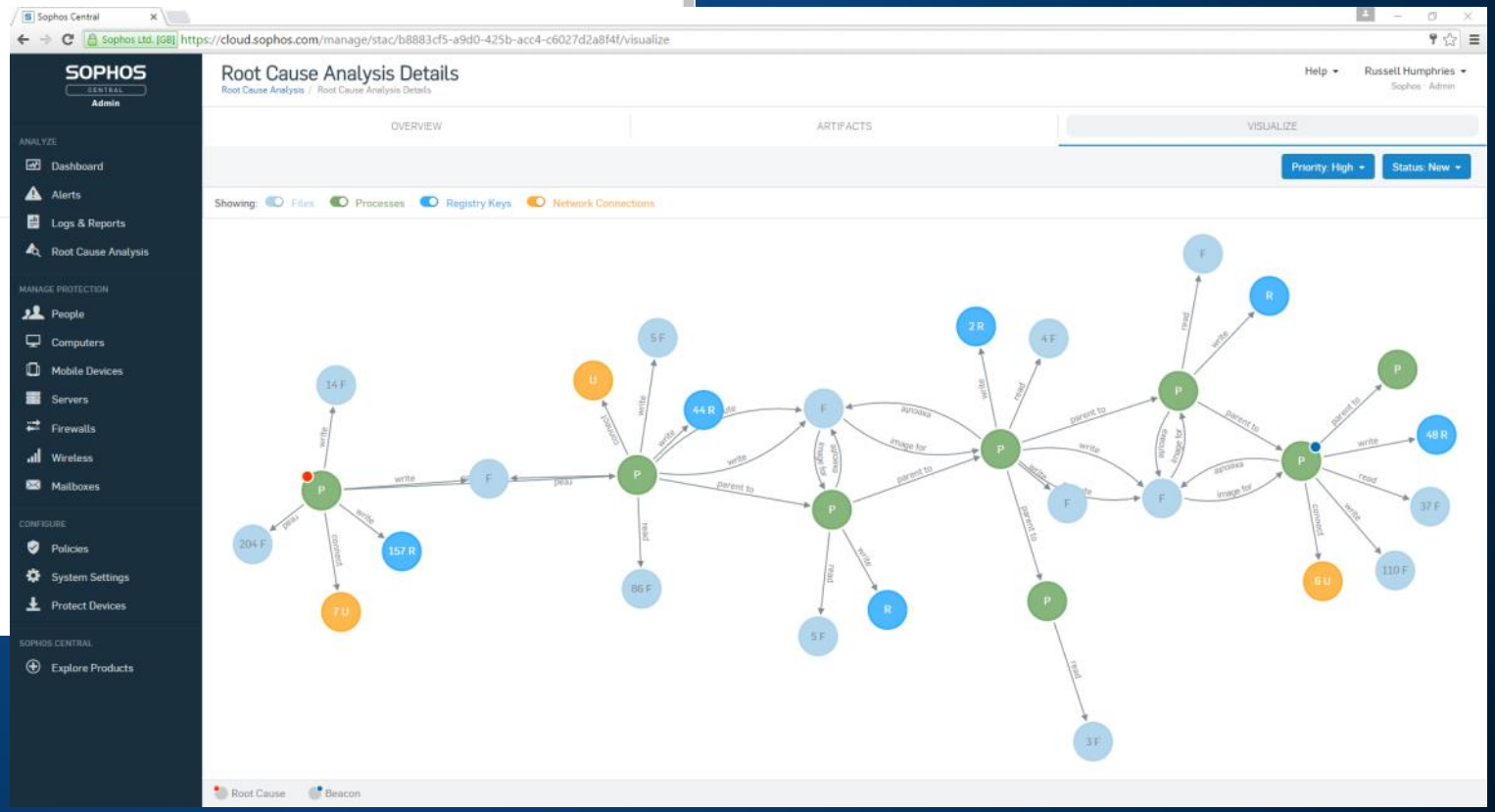
- Simple and Comprehensive
- Universally Prevents Spontaneous Encryption of Data
- Restores Files to Known State
- Simple Activation in Sophos Central

CRYPTOGUARD

Root Cause Analysis

Understanding the Who, What, When, Where, Why and How





SOPHOS

Security made simple.