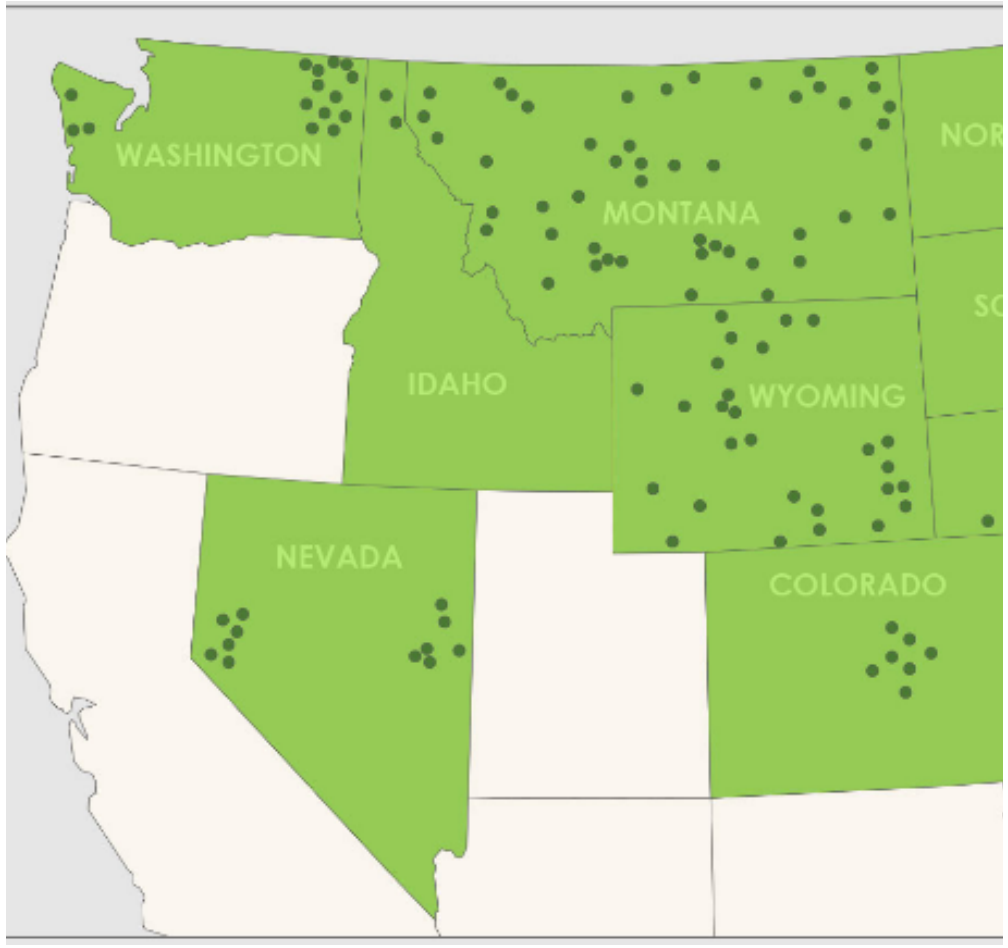
SYNCHRONIZED SECURITY YOUR DISTRICT

Protecting, detecting and responding to the inevitable cyber breach

Who are we?

Pine Cove Consulting:

- Headquartered in Bozeman
- 24 Years in the Industry
- K12 Focus
- Cyber-Security Focus
- Serve on META Network Security Council
- Support 20k+ Users Daily



How Can We Help?

- Consultation/Assessment
- Create a Protection, Detection, and Response Plan
- Synchronized Security Services
- Cyber Security Assessment:
  - Penetration Testing
  - Network Vulnerability Assessments
  - Spoof Email Campaign
  - Dark Web Visibility Testing
- Faculty Professional Development

Sophos & Pine Cove

- Sophos partner since 2002
- North American Complete Security Partner of the Year (2016)
- Only Platinum partner in Montana
- Only Synchronized Security partner in Montana
- Currently hold 33 Sophos technical certifications
- Work closely with Sophos product development teams

Sophos National Partner of the Year

Pine Cove Consulting

SOPHOS

Complete Security Partner of the Year Americas

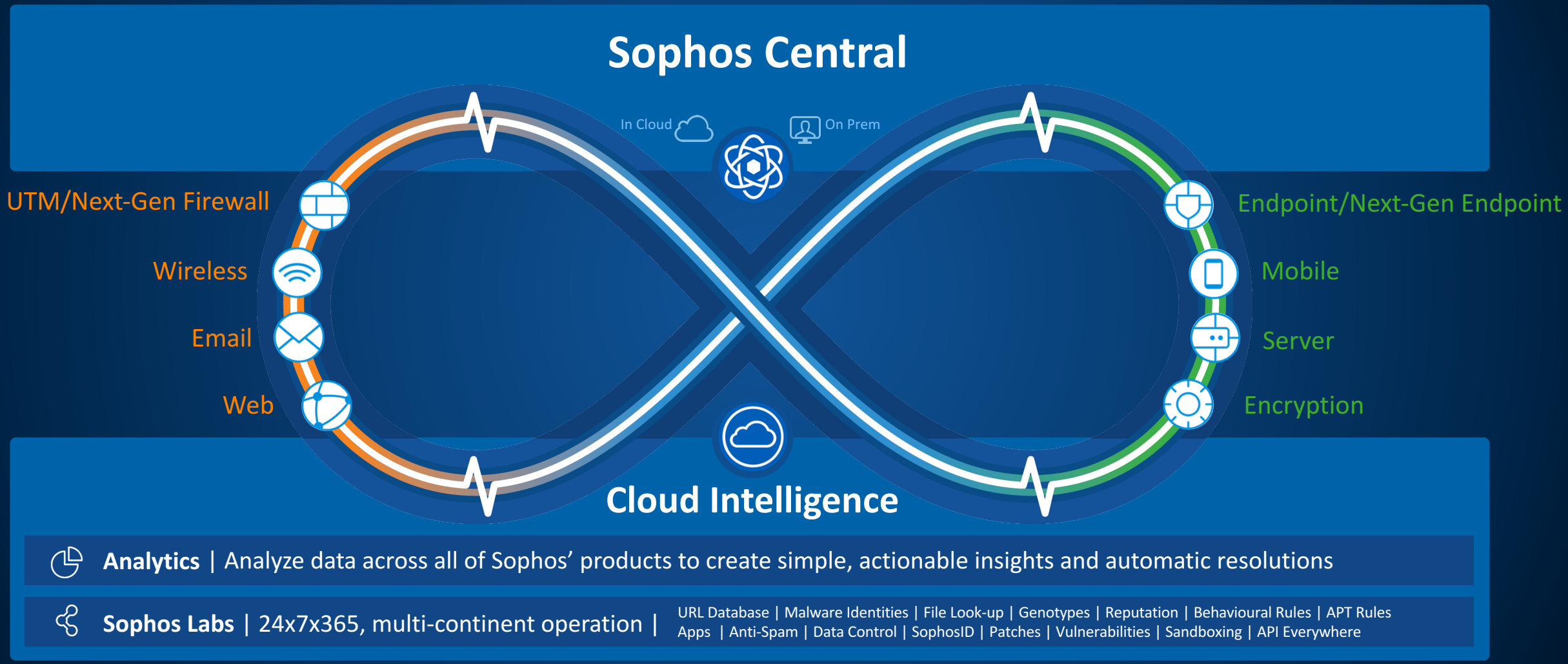
2016

Sophos Snapshot

- Founded 1985 in Oxford, UK
- $600+ million in FY17 billings
- Leader in endpoint and network security
- 3,000 employees
- 250,000+ customers
- 100+ million users
- 90%+ best in class renewal rates
- 26,000+ channel partners
- SophosLabs threat research facility
- “Channel first” go to market model
- History of organic and acquired growth

Sophos HQ, Abingdon, UK

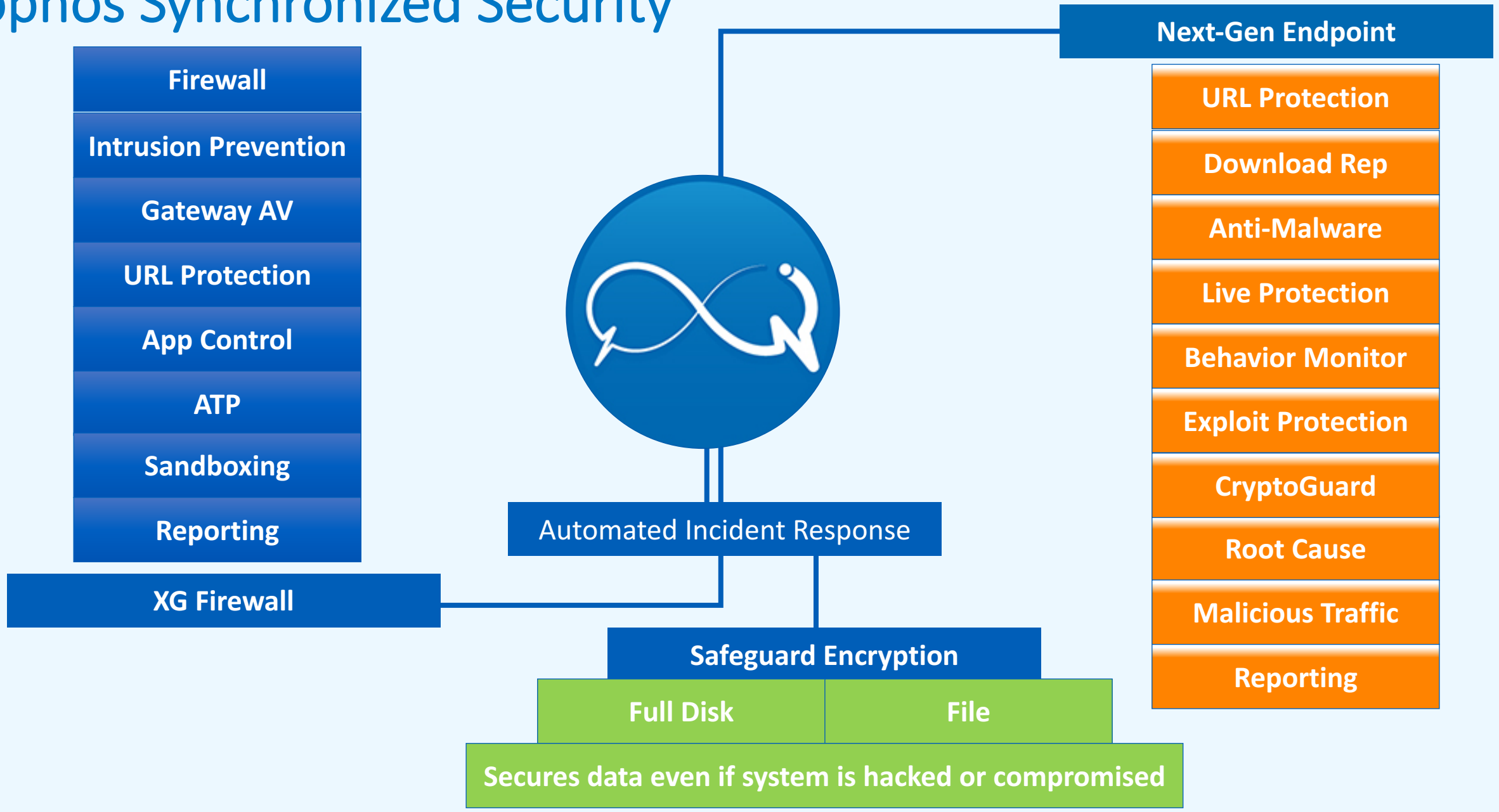
Synchronized Security Platform and Strategy



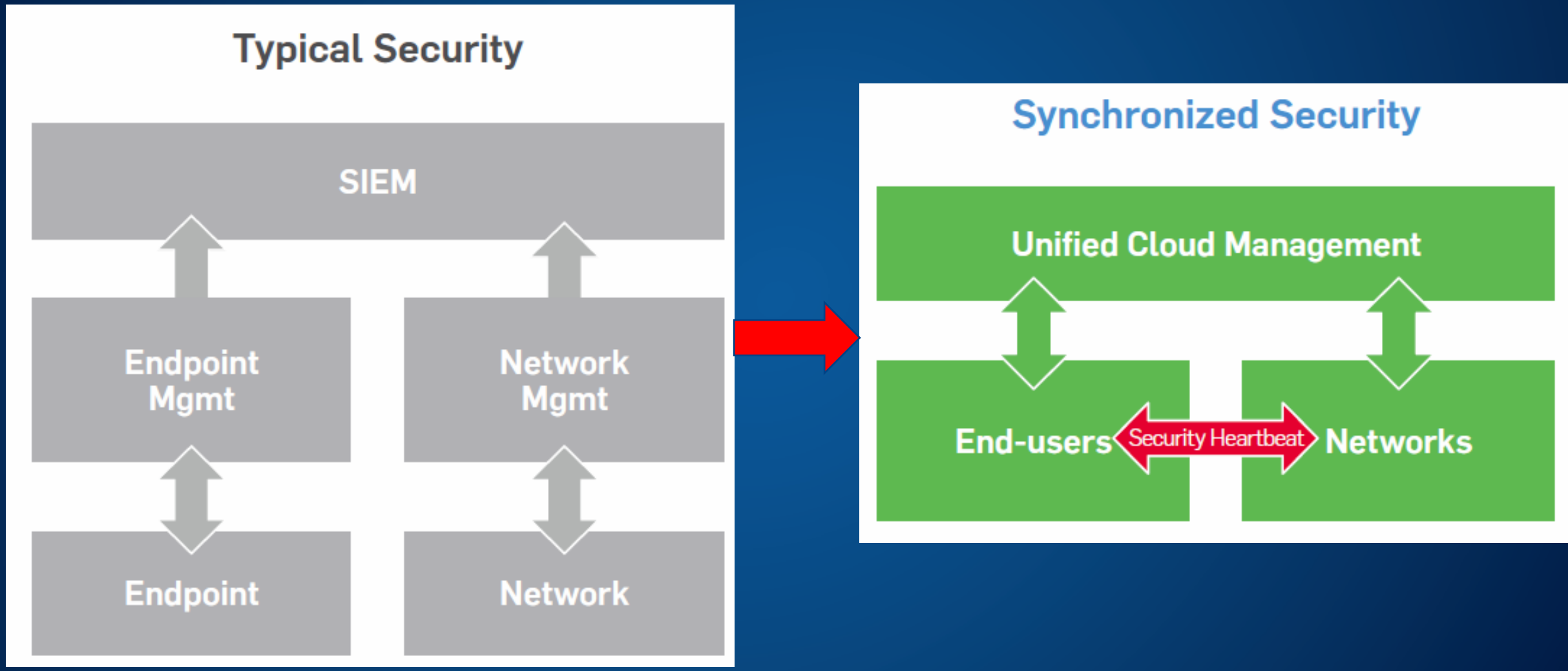
Endpoint

Firewall

Sophos Synchronized Security



Security Heartbeat vs. Typical Security Alerts



Strength in Network and Endpoint

MAGIC QUADRANT for UNIFIED THREAT MANAGEMENT

Gartner Analysts: Jeremy D'Hoinne, Adam Hils and Rajpreet Kaur

MAGIC QUADRANT for ENDPOINT PROTECTION PLATFORMS

Gartner Analysts: Eric Ouellet, Ina McShane and Avivah Litan

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.

The Evolution of Endpoint Threats

From Malware to Exploits

2009 - Introduction of Polypack "Crimeware as a Service"

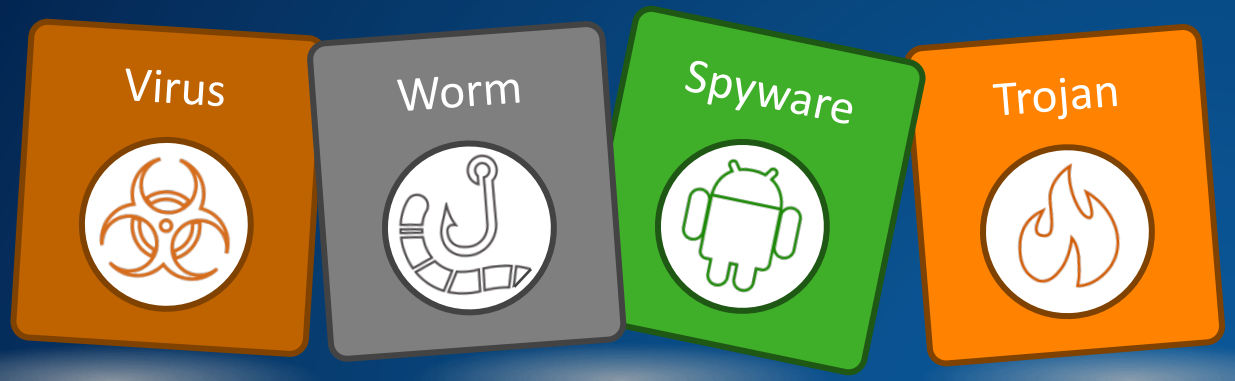
1998	1999	2003	2007	2014	2015	2016
Melissa Virus	Love Letter Worm	FinFischer Spyware	Zeus Trojan	JSocket RATs	Exploit as a Service	Locky Ransomware
$1.2B	$15B	$780M	$2.3B	$800M	$500M	$1.1B

Traditional Malware

Advanced Threats

The Evolution of Endpoint Security

From Anti-Malware to Anti-Exploit



Exposure Prevention

URL Blocking
Web/App/Dev Ctrl
Download Rep

Pre-Exec Analytics

Generic Matching
Heuristics
Core Rules

File Scanning

Known Malware
Malware Bits

Run-Time

Behavior Analytics
Runtime Behavior

Exploit Detection

Technique Identification

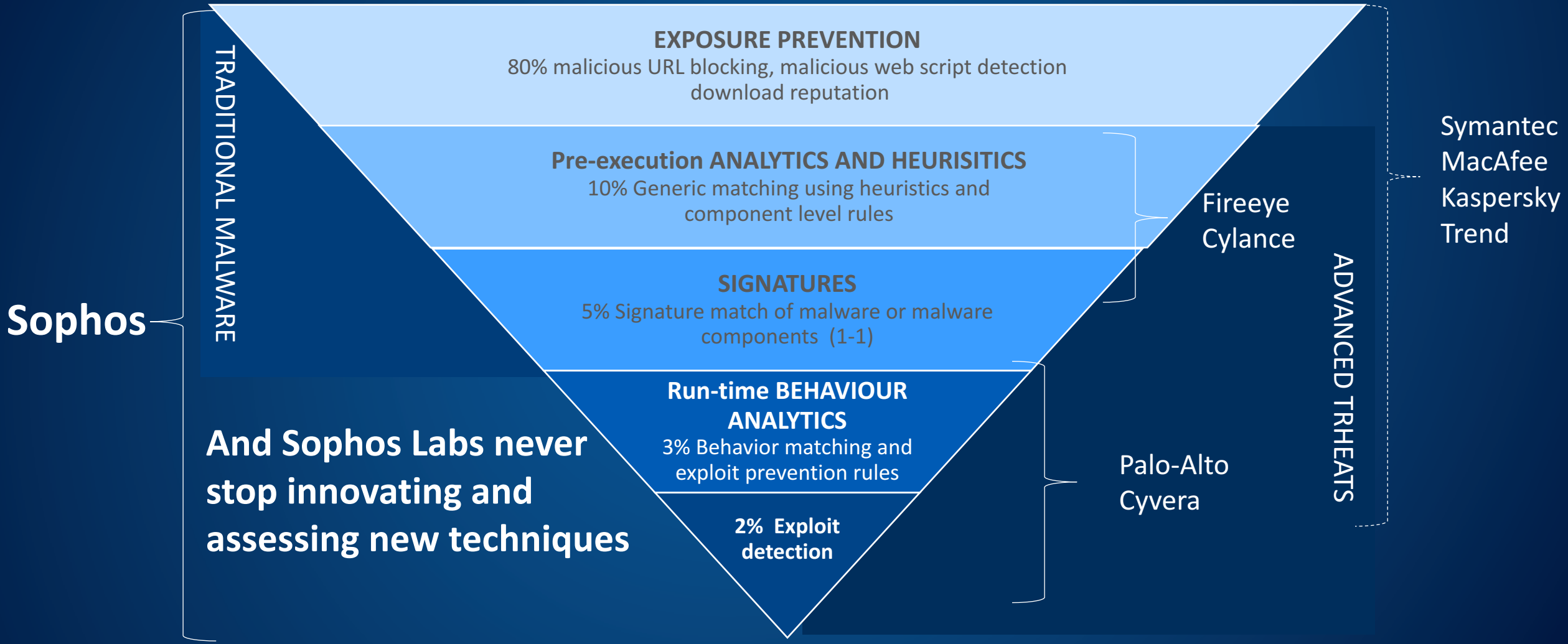
Traditional Malware

Advanced Threats

SOPHOS

How Sophos protects on the endpoint

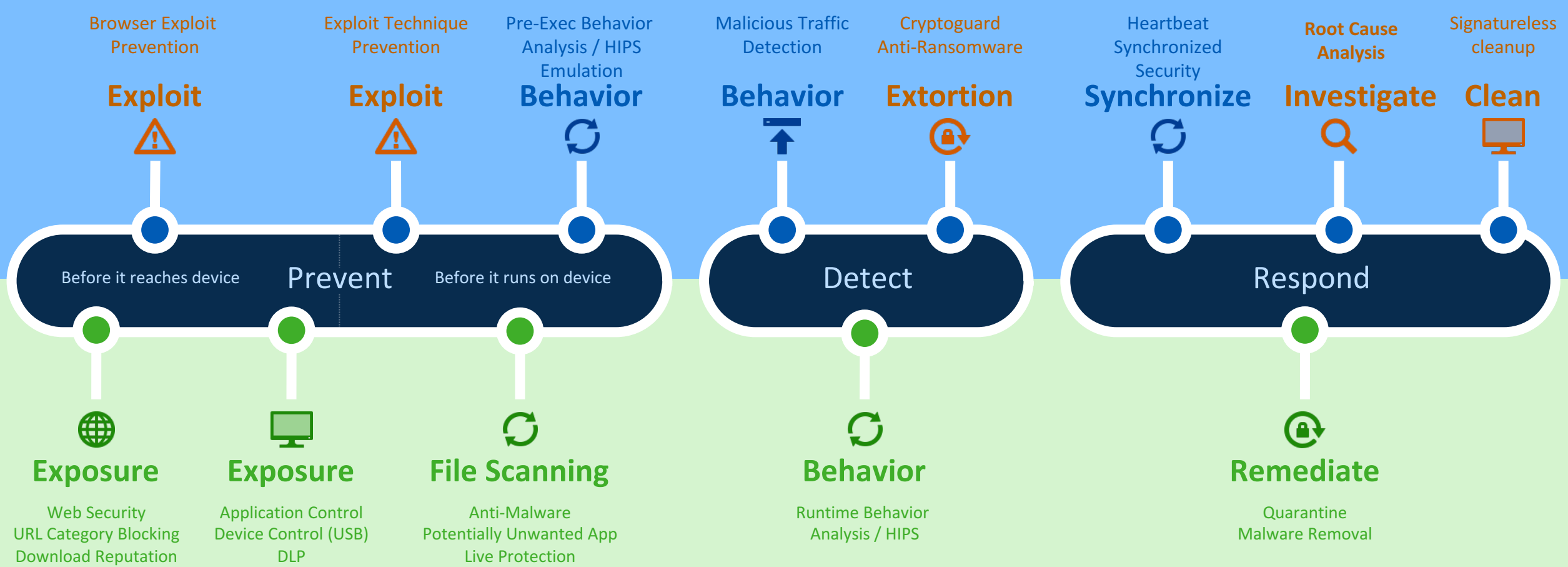
Signature based AV is no longer enough



Methods and techniques vary depending on device type and operating system (Windows, Mac, Linux/Unix variants, Android, iOS)

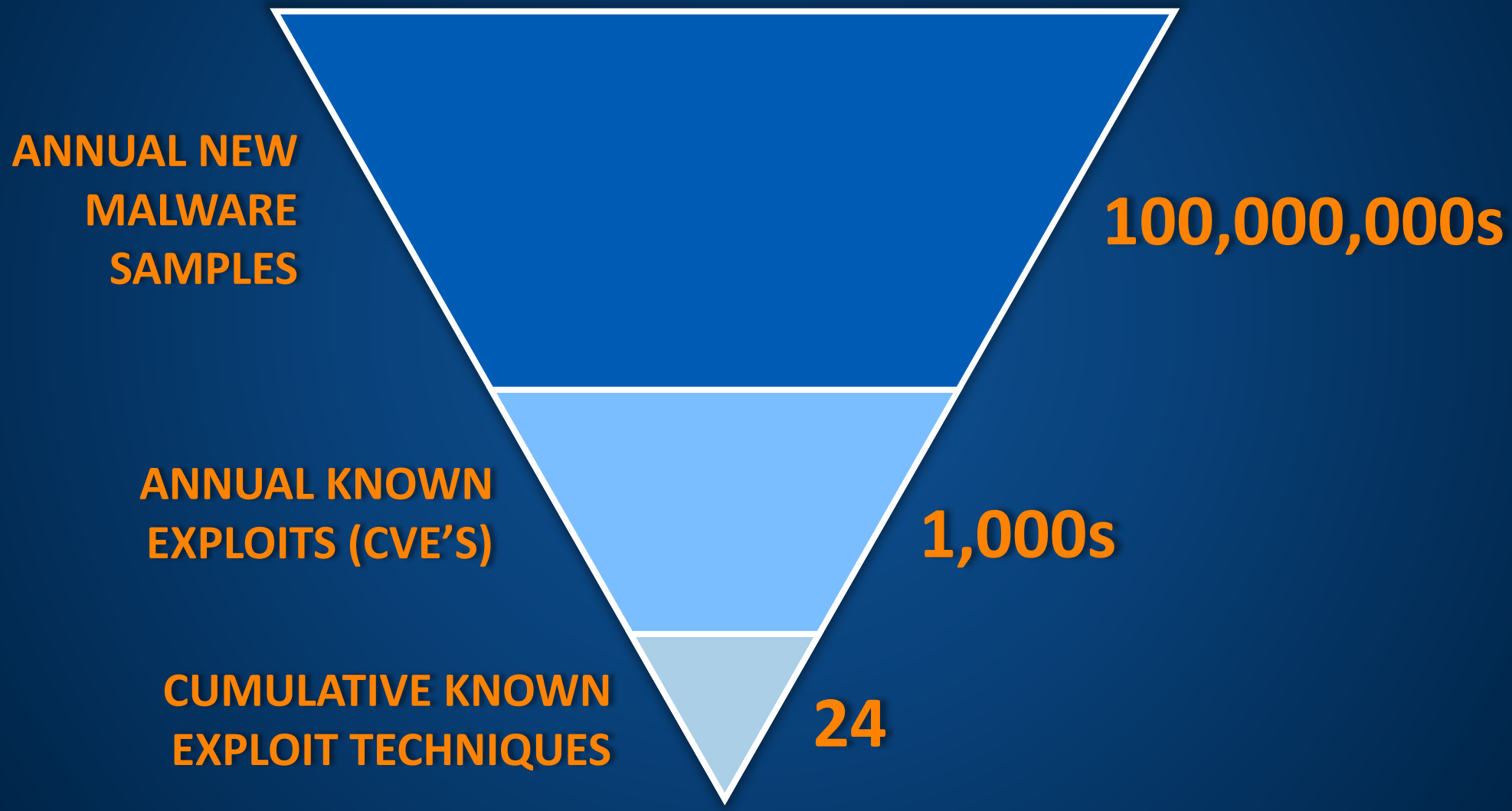
Endpoint Advanced + Intercept X

Next-Generation Endpoint

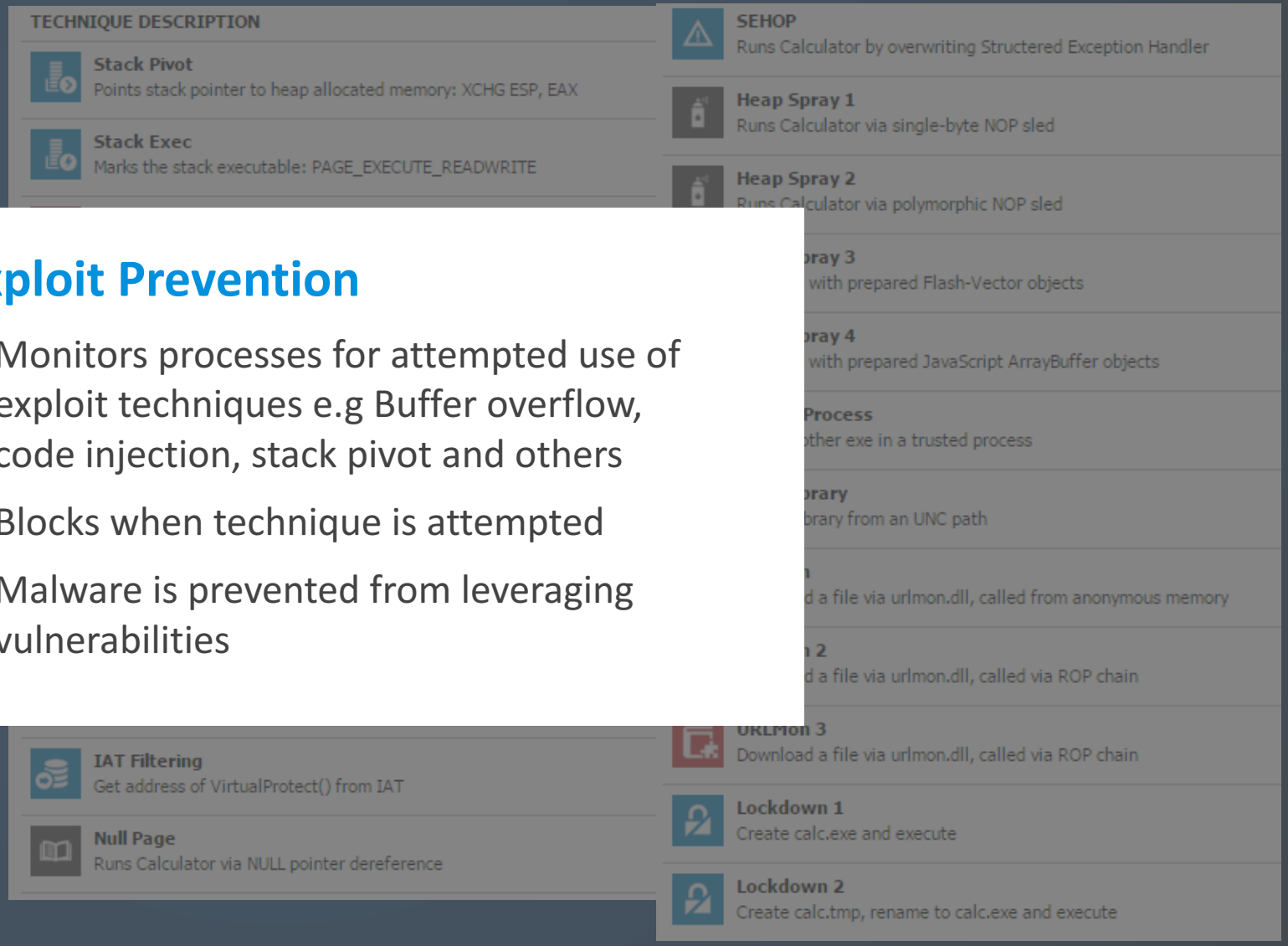


Traditional Antivirus

Exploit Prevention and Next-Gen Endpoint Protection



Intercepting Exploits



Exploit Prevention

- Monitors processes for attempted use of exploit techniques e.g Buffer overflow, code injection, stack pivot and others
- Blocks when technique is attempted
- Malware is prevented from leveraging vulnerabilities

CryptoGuard

Over $1B in ransom payments
projected for 2016 (source FBI)

Cryptov
2015

- 2 o
  atta
- Del
- 100
  wic

Now for MAC and Windows users

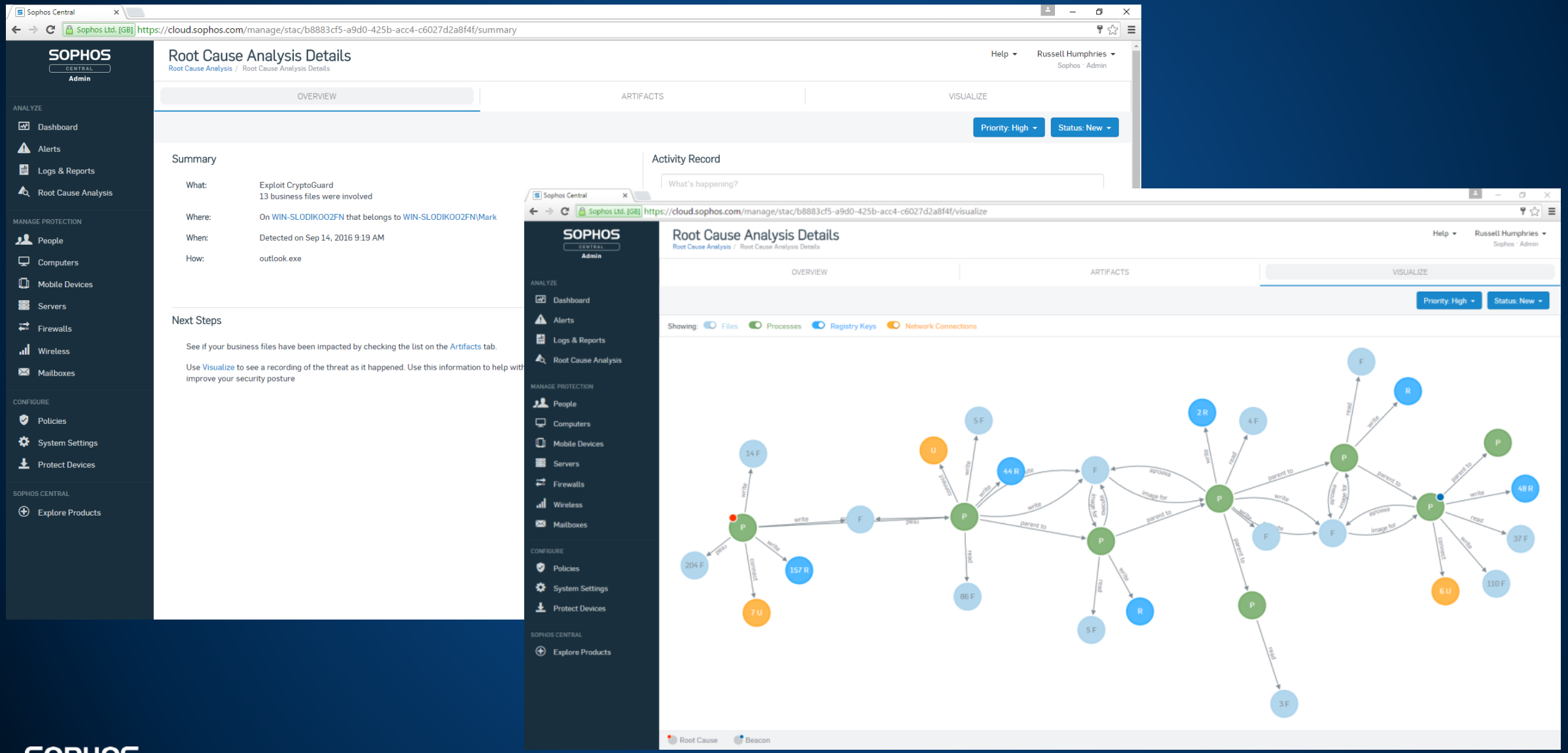
Targeting everyone

CryptoGuard

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

Root Cause Analysis

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



Sophos Clean

Malware Removal. Forensic-Level Cleanup.

Removes Threats

- **Deep System Inspection**
- **Removes Malware Remnants**
- **Full Quarantine / Removal**
- **Effective Breach Remediation**

On-Demand Assessment

- **Identifies Risky Files / Processes**
- **Constantly Refreshed Database**
- **Provides Additional Confidence**
- **Command-Line Capable**

- 100% Automated with Intercept X
- Also available as a standalone Forensic Clean Utility

SOPHOS

Core Features by Product

Intercept X works with competitors AV products

	Product Name	ENDPOINT PROTECTION			INTERCEPT
	SKU	CENTRAL ENDPOINT STANDARD	CENTRAL ENDPOINT ADVANCED	CENTRAL ENDPOINT Adv + Intercept	CENTRAL ENDPOINT INTERCEPT
	Pricing	Per User	Per User	Per User	Per User
PREVENT	Web Security	✔	✔	✔	
	Download Reputation	✔	✔	✔	
	Web Control / URL Category Blocking		✔	✔	
	Device Control (e.g. USB)		✔	✔	
	Application Control		✔	✔	
	Browser Exploit Prevention			✔	✔
DETECT & STOP	Anti-malware / Anti-virus	✔	✔	✔	
	Live Protection	✔	✔	✔	
	Pre-execution & Runtime Behavior Analysis / HIPS	✔	✔	✔	
	Potentially Unwanted Application (PUA) Detection	✔	✔	✔	
	Malicious Traffic Detection (MTD)		✔	✔	✔
	Synchronized Security Heartbeat		✔	✔	✔
	Cryptoguard Ransomware Protection			✔	✔
	Exploit Technique Prevention			✔	✔
RESPOND	Root Cause Analysis / Threat Analysis			✔	✔
	Sophos Clean Malware Removal			✔	✔

Server Protection Strategy

Server Standard

Server Advanced

Optimized for performance

PHYSICAL

- Optimize performance
- Lightweight agent

VIRTUAL

vmware

Microsoft Hyper-V

- Performance is key
- Agentless/Light agent

IaaS

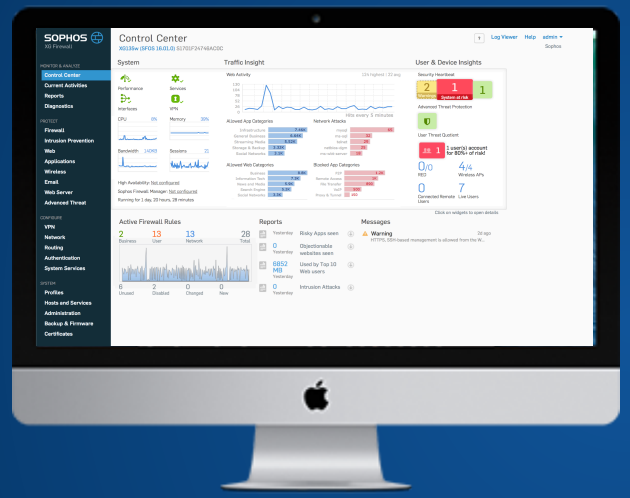
amazon web services™

Microsoft Azure

- On-demand resources
- Usage based licensing

Sophos XG Firewall

Solving today's top problems with existing Firewalls



Simpler to manage

- ✓ Streamlined workflows
- ✓ Unified policies
- ✓ Policy templates

Instant visibility

- ✓ New control center
- ✓ User & App Risk
- ✓ On-box reporting

Complete protection

- ✓ Firewall & Wireless
- ✓ Web, APT, Apps
- ✓ Email and WAF

Synchronized security

- ✓ Linking firewall & EP
- ✓ Security Heartbeat™
- ✓ Dynamic app ID

Top performance

- ✓ Industry-leading HW
- ✓ FastPath optimization
- ✓ High-performance proxy

Central Management

- ✓ Full-featured & consistent
- ✓ Cloud or on-premise
- ✓ Free for partners

SOPHOS

XG Firewall Bundles

TotalProtect Plus
Hardware + FullGuard Plus

XG Series or Virtual Appliance
- Base License
  incl. network firewall and VPN
  - Wireless Protection

FullGuard Plus
incl. Enhanced Support
- Network Protection
- Web Protection
- Email Protection
- Web Server Protection
- Sandstorm Protection

TotalProtect
Hardware + FullGuard

XG Series or Virtual Appliance
- Base License
  incl. network firewall and VPN
  - Wireless Protection

FullGuard
incl. Enhanced Support
- Network Protection
- Web Protection
- Email Protection
- Web Server Protection

EnterpriseProtect
Hardware + EnterpriseGuard

XG Series or Virtual Appliance
- Base License
  incl. network firewall and VPN
  - Wireless Protection

EnterpriseGuard
incl. Enhanced Support
- Network Protection
- Web Protection

- **Bundles: 1,2 and 3 year options**
- **Enhanced Support (24/7)**

Free Tools

Sophos gives out free tools that check for security risk, remove viruses and protect home networks

Sophos Home

Mobile Security for iOS

XG Firewall Home Edition

Antivirus for Linux

Free 30-day trial of HitmanPro and HitmanPro.Alert

Mobile Security for Android

UTM Home Edition

275,000+ average monthly visitors!