



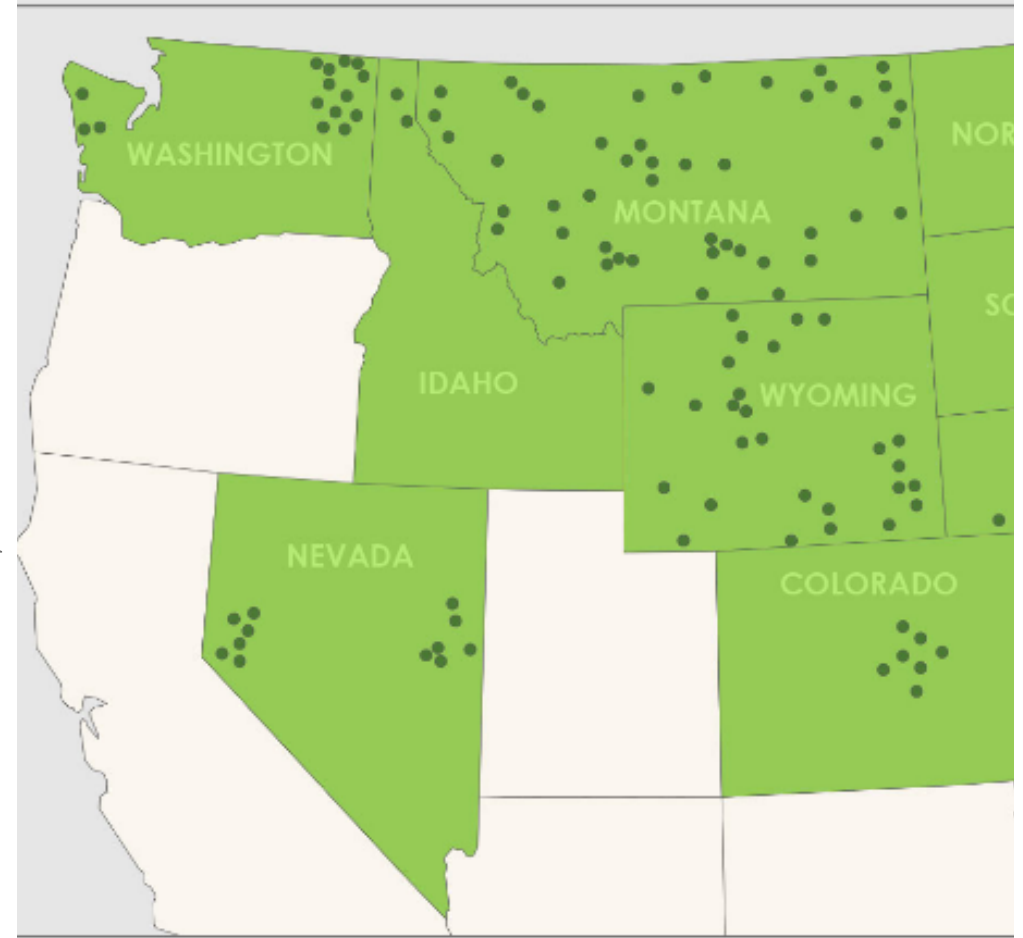
SYNCHRONIZED SECURITY YOUR DISTRICT

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 ★ ★



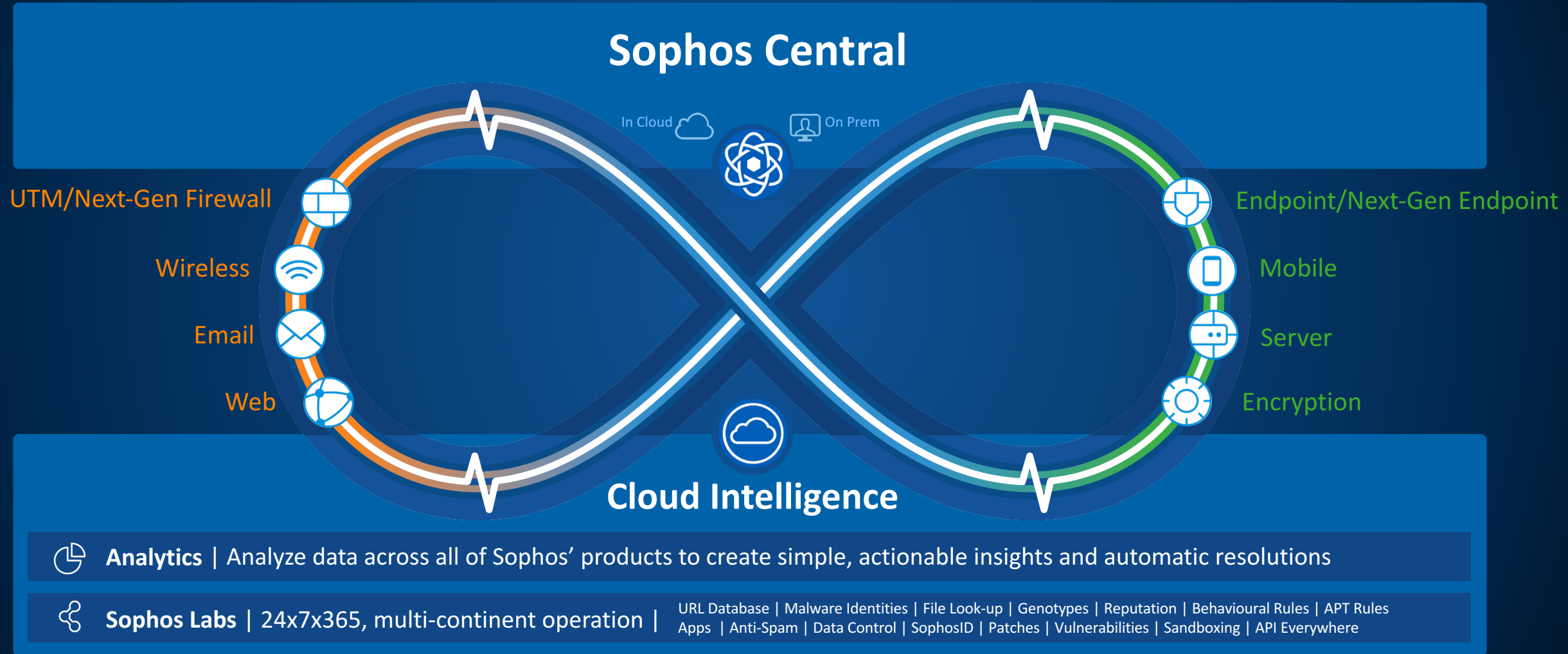
Sophos Snapshot

- 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



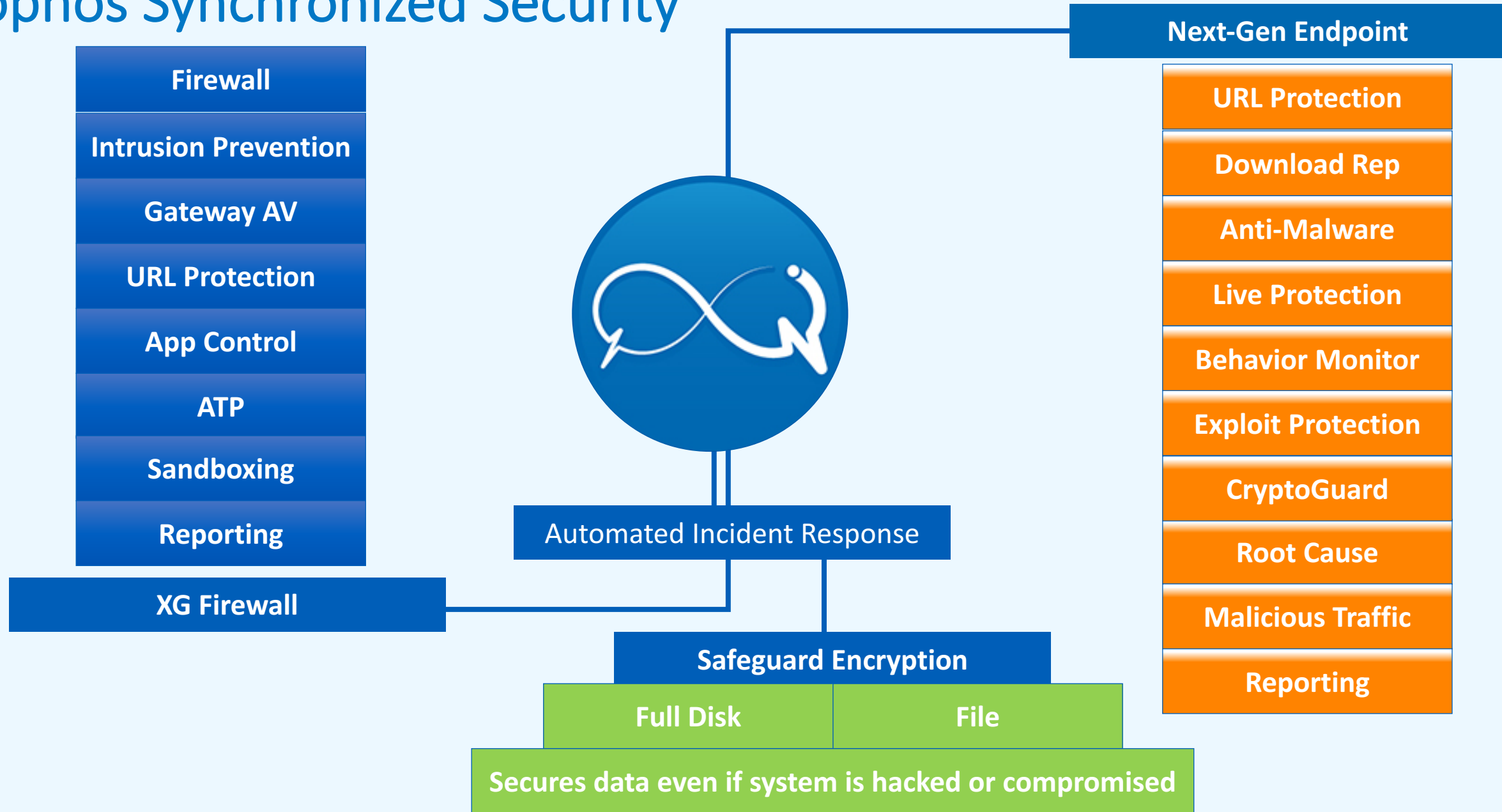


Endpoint

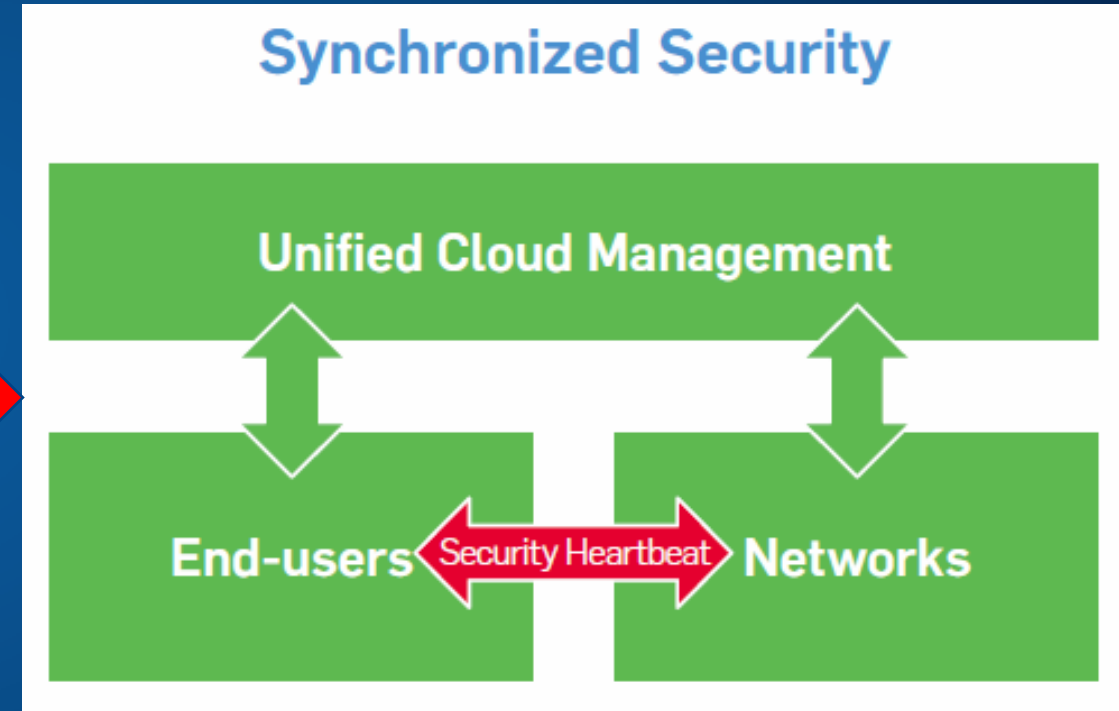
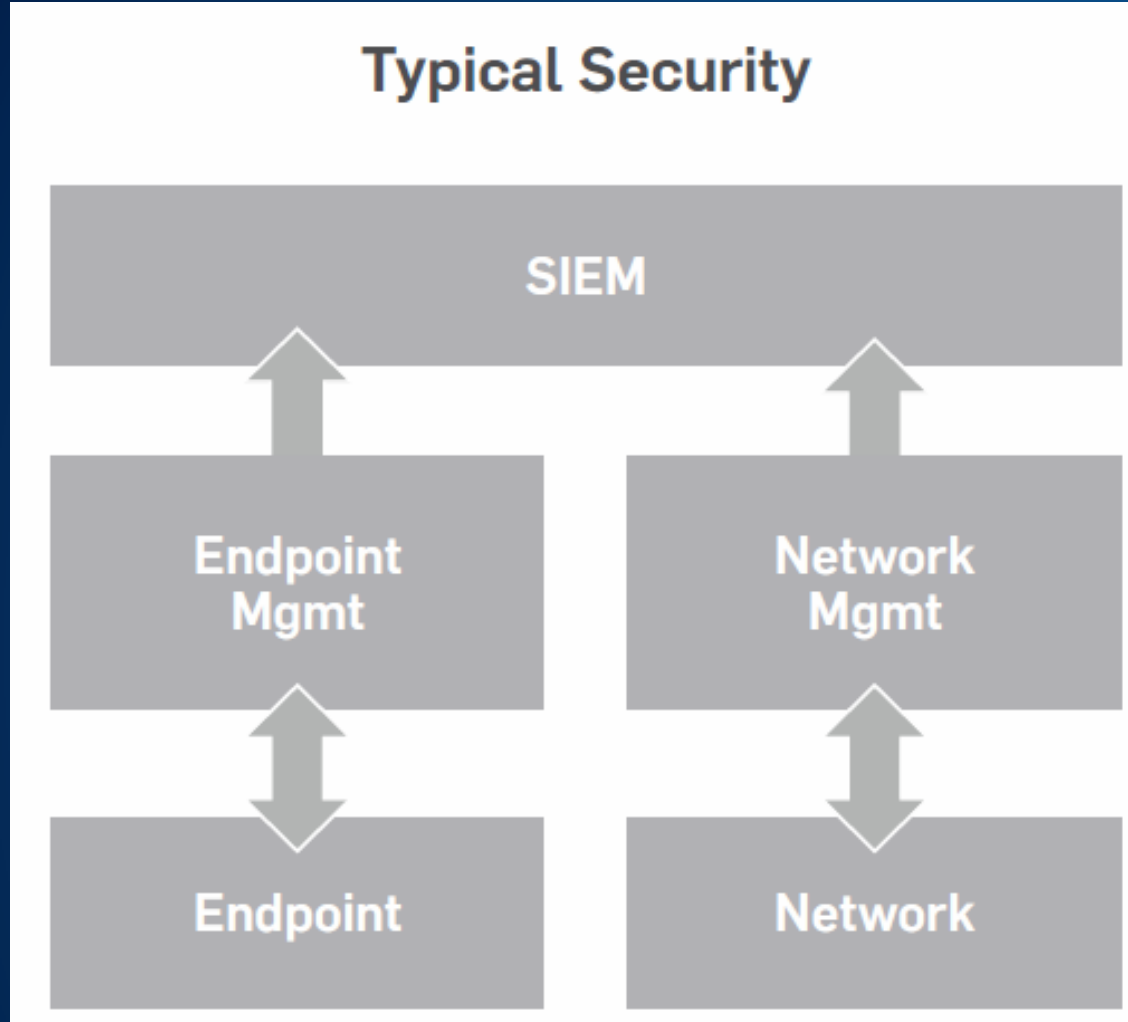
Firewall



Sophos Synchronized Security



Security Heartbeat vs. Typical Security Alerts



Strength in Network and Endpoint

MAGIC QUADRANT for UNIFIED THREAT MANAGEMENT



MAGIC QUADRANT for ENDPOINT PROTECTION PLATFORMS



The age of single-use disposable malware



400,000

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

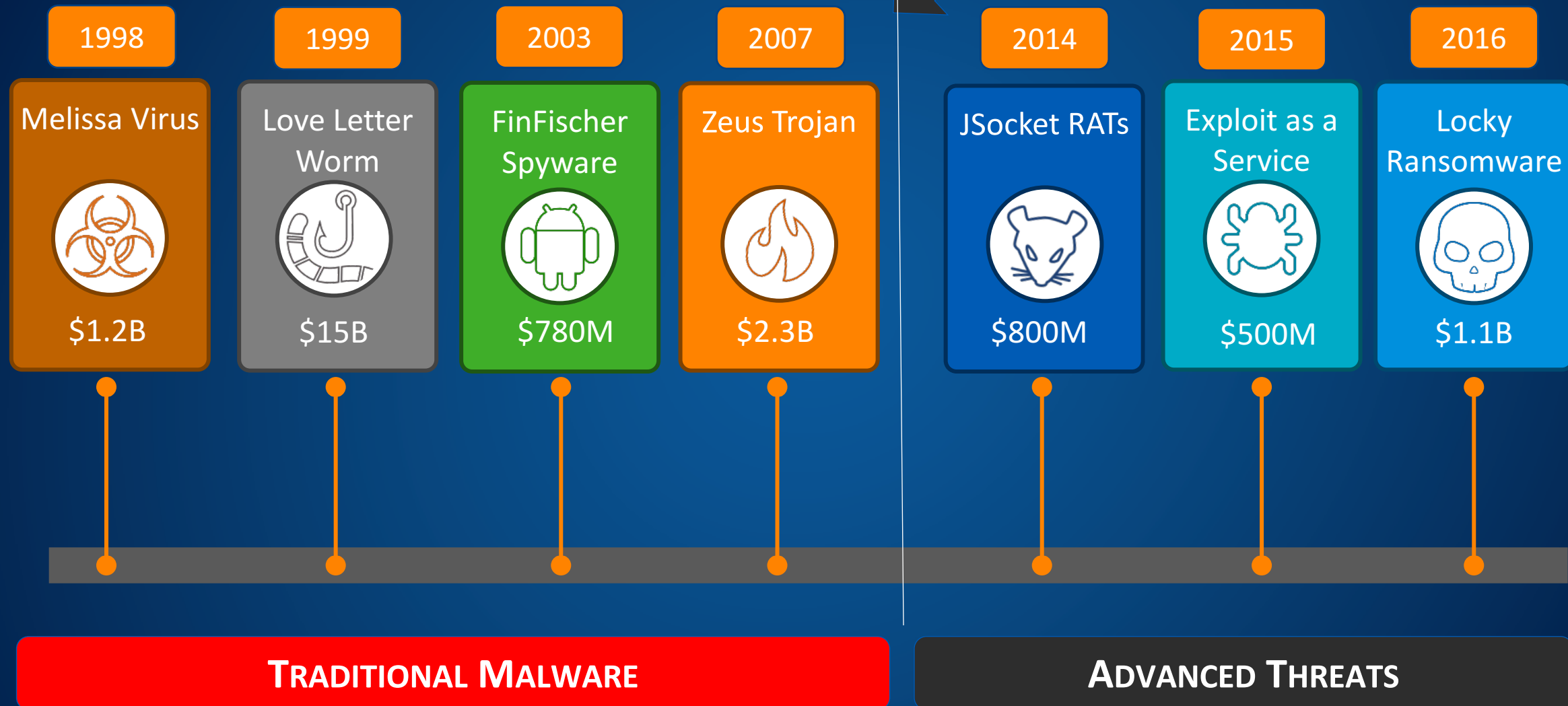


75% of the malicious files SophosLabs detects are found only within a single organization.

The Evolution of Endpoint Threats

From Malware to Exploits

2009 - INTRODUCTION OF POLYPACK
"CRIMEWARE AS A SERVICE"



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

Traditional Malware



Run-Time

Behavior Analytics
Runtime Behavior

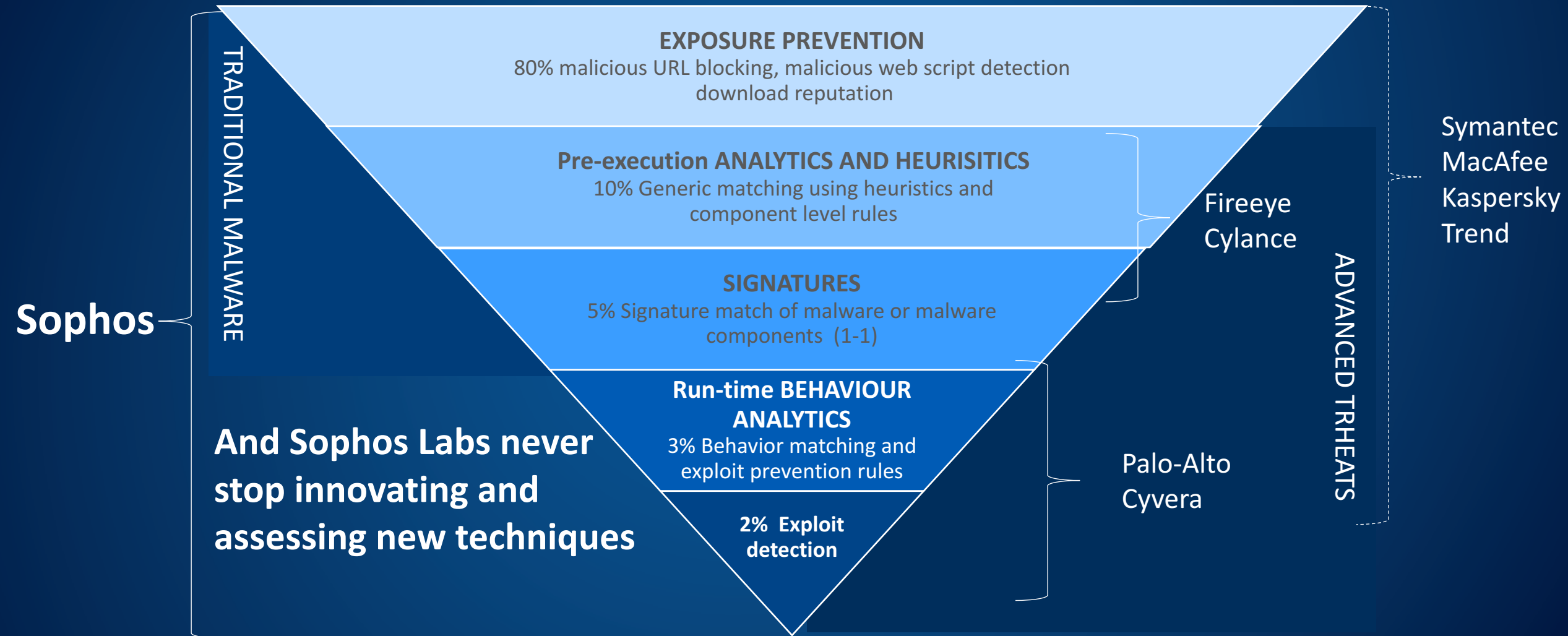
Exploit
Detection

Technique
Identification

Advanced Threats

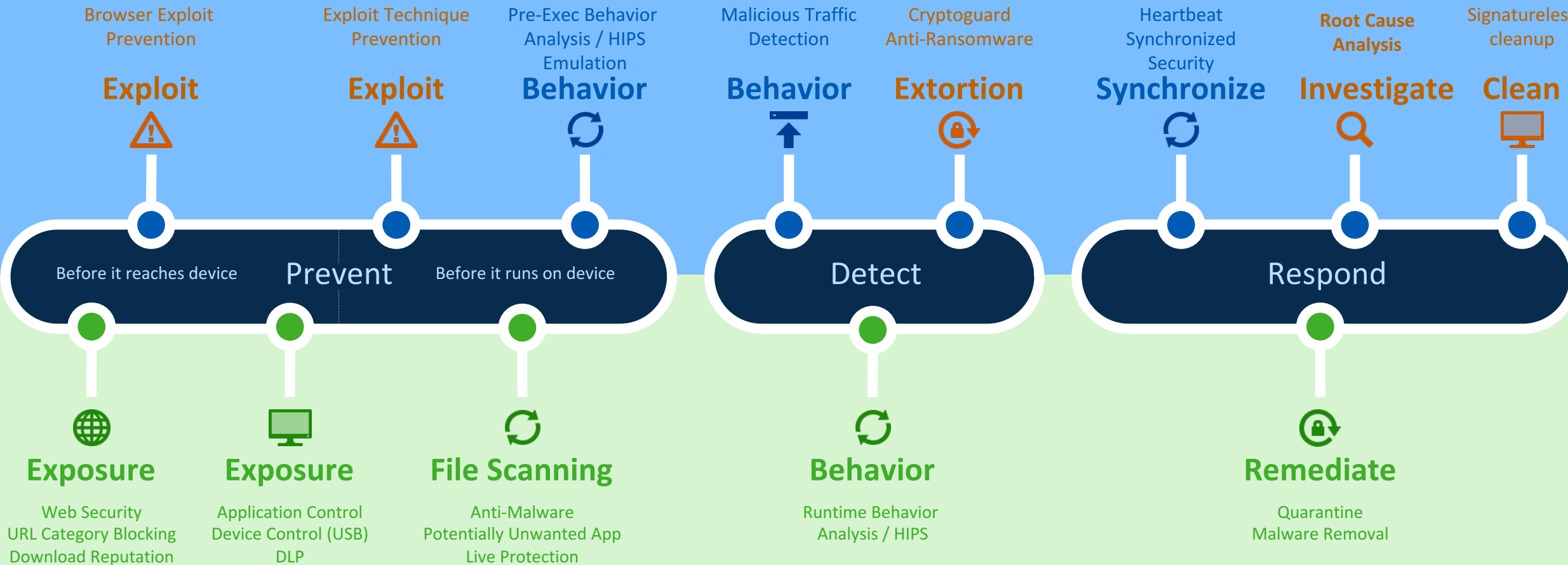
How Sophos protects on the endpoint

Signature based AV is no longer enough



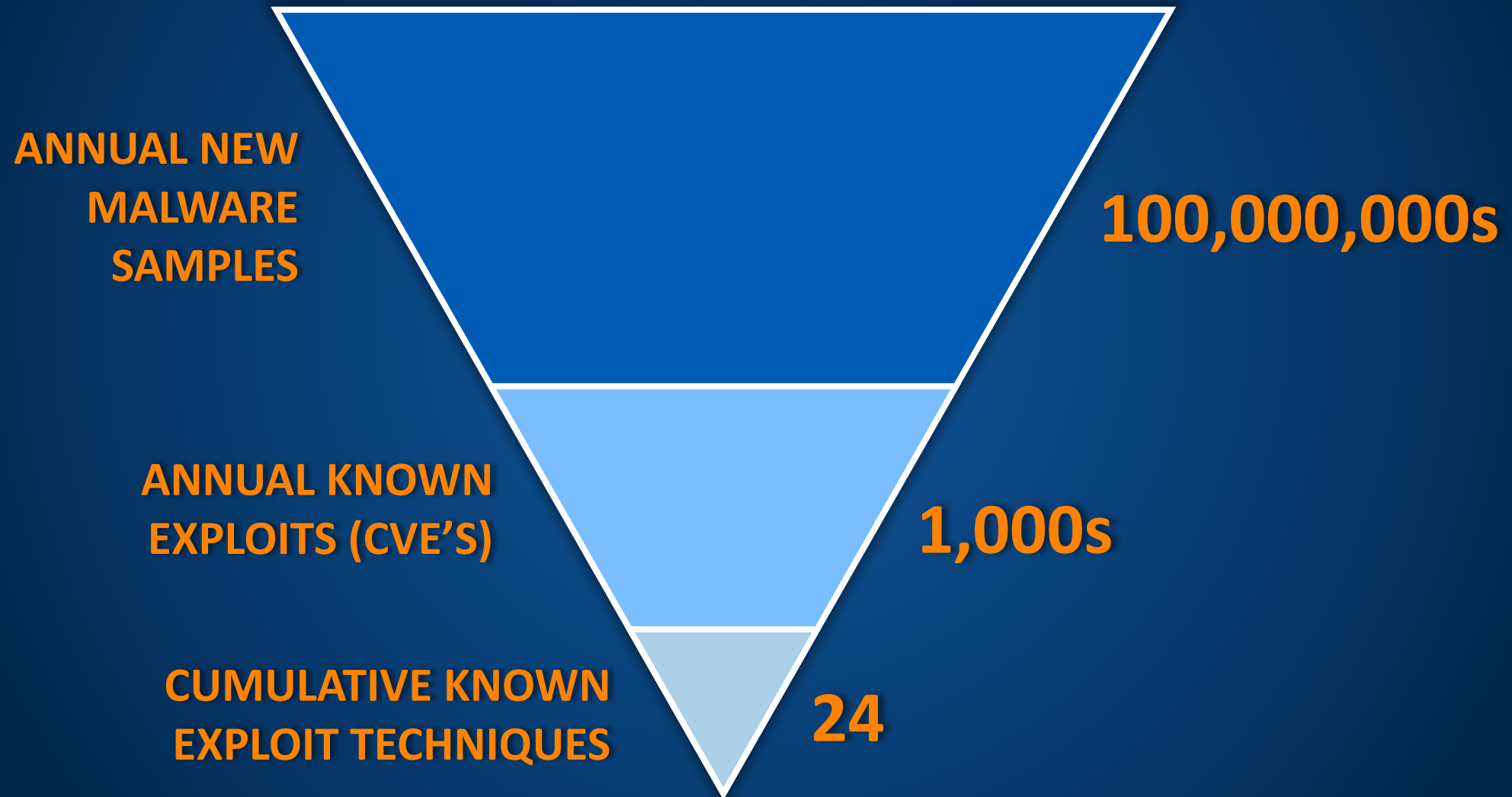
Endpoint Advanced + Intercept X

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

TECHNIQUE DESCRIPTION



Stack Pivot

Points stack pointer to heap allocated memory: XCHG ESP, EAX



Stack Exec

Marks the stack executable: PAGE_EXECUTE_READWRITE



SEHOP

Runs Calculator by overwriting Structured Exception Handler



Heap Spray 1

Runs Calculator via single-byte NOP sled



Heap Spray 2

Runs Calculator via polymorphic NOP sled

Heap Spray 3

Runs Calculator with prepared Flash-Vector objects

Heap Spray 4

Runs Calculator with prepared JavaScript ArrayBuffer objects

Process Injection

Injects another exe in a trusted process

Library Injection

Loads library from an UNC path

URLMon 1

Downloads a file via urlmon.dll, called from anonymous memory

URLMon 2

Downloads a file via urlmon.dll, called via ROP chain



URLMon 3

Downloads a file via urlmon.dll, called via ROP chain



Lockdown 1

Create calc.exe and execute



Lockdown 2

Create calc.tmp, rename to calc.exe and execute



IAT Filtering

Get address of VirtualProtect() from IAT



Null Page

Runs Calculator via NULL pointer dereference

CryptoGuard

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

Cryptov
2015

- 2 o
- att
- Del
- 100
- wid

CryptoGuard

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

Now for MAC and Windows users
Targeting everyone



Root Cause Analysis

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

The image displays the Sophos Central Root Cause Analysis (RCA) interface, showing a detailed view of a security incident. The interface is divided into several sections:

- Summary:** Provides a high-level overview of the incident.
 - What:** Exploit CryptoGuard, 13 business files were involved
 - Where:** On WIN-SLODIK002FN that belongs to WIN-SLODIK002FN\Mark
 - When:** Detected on Sep 14, 2016 9:19 AM
 - How:** outlook.exe
- Next Steps:** Offers guidance on how to proceed.
 - See if your business files have been impacted by checking the list on the **Artifacts** tab.
 - Use **Visualize** to see a recording of the threat as it happened. Use this information to help with improve your security posture
- Activity Record:** A detailed timeline of the incident, visualized as a graph showing the flow of data and actions between various entities (Processes, Files, Registry Keys, Network Connections).

The **Activity Record** visualization shows a complex network of interactions. The graph includes nodes representing different entities (Processes, Files, Registry Keys, Network Connections) and edges representing the actions taken (e.g., write, read, execute, parent to). The graph is color-coded to show different types of entities and actions.

The interface also includes a sidebar with navigation options for various Sophos Central features, such as Dashboard, Alerts, Logs & Reports, Root Cause Analysis, People, Computers, Mobile Devices, Servers, Firewalls, Wireless, Mailboxes, Policies, System Settings, and Protect Devices.

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

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			✓	✓
	Supplies Clean Malware Removal			✓	✓

Server Protection Strategy

Server Standard



Anti-malware

Server Advanced



Lockdown



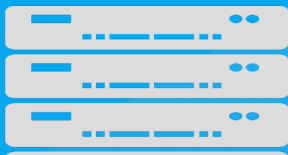
MTD



Cryptoguard

Optimized for performance

PHYSICAL



- Optimize performance
- Lightweight agent

VIRTUAL

vmware®



- Performance is key
- Agentless/Light agent

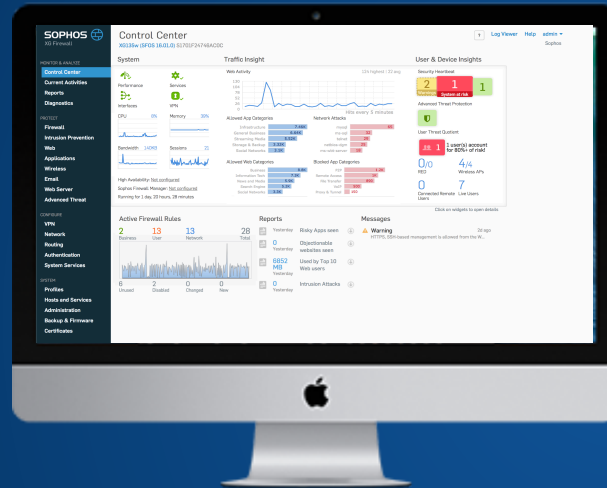
IaaS



- 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

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

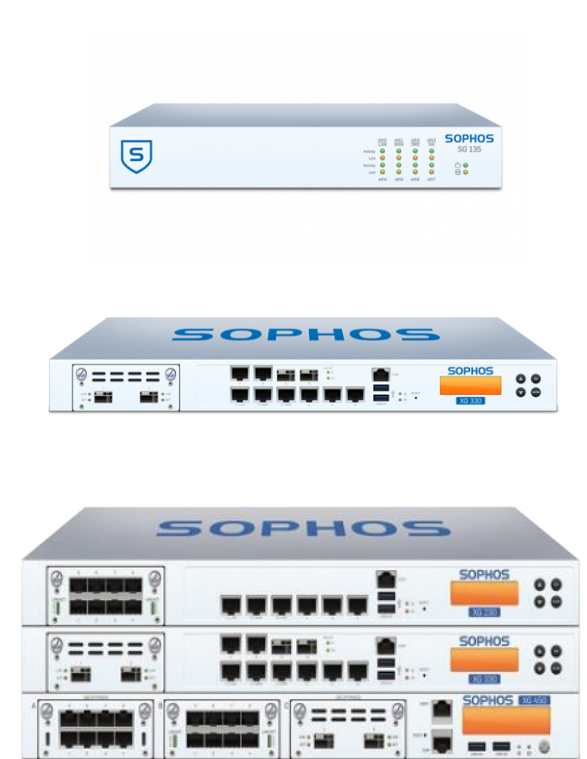
Base License
incl. network firewall and VPN

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



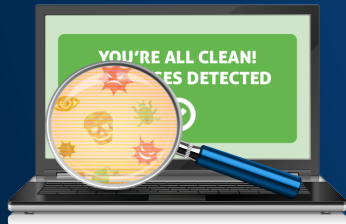
Mobile Security
for iOS



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!