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

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
Synchronized Security Platform and Strategy

Sophos Central

Cloud Intelligence

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

Sophos Labs | 24x7x365, multi-continent operation | URL Database | Malware Identities | File Look-up | Genotypes | Reputation | Behavioural Rules | APT Rules
Apps | Anti-Spam | Data Control | SophosID | Patches | Vulnerabilities | Sandboxing | API Everywhere

UTM/Next-Gen Firewall | Endpoint/Next-Gen Endpoint
Wireless | Mobile
Email | Server
Web | Encryption

In Cloud | On Prem
Sophos Synchronized Security

- Firewall
- Intrusion Prevention
- Gateway AV
- URL Protection
- App Control
- ATP
- Sandboxing
- Reporting

Automated Incident Response

Safeguard Encryption

- Full Disk
- File

Secures data even if system is hacked or compromised

Next-Gen Endpoint

- URL Protection
- Download Rep
- Anti-Malware
- Live Protection
- Behavior Monitor
- Exploit Protection
- CryptoGuard
- Root Cause
- Malicious Traffic
- Reporting
Security Heartbeat vs. Typical Security Alerts

Typical Security

- SIEM
- Endpoint Mgmt
- Network Mgmt
- Endpoint
- Network

Synchronized Security

- Unified Cloud Management
- End-users
- Networks

Security Heartbeat
Strength in Network and Endpoint

MAGIC QUADRANT for UNIFIED THREAT MANAGEMENT

MAGIC QUADRANT for ENDPOINT PROTECTION PLATFORMS

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

Gartner Analysts: Eric Ouellet, Ina McShane and Avivah Litan
The age of single-use disposable malware

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

1998
Melissa Virus
$1.2B

1999
Love Letter Worm
$15B

2003
FinFischer Spyware
$780M

2007
Zeus Trojan
$2.3B

2014
JSocket RATs
$800M

2015
Exploit as a Service
$500M

2016
Locky Ransomware
$1.1B

2009 - INTRODUCTION OF POLYPACK
“CRIMEWARE AS A SERVICE”

INTRODUCTION OF POLYPACK
“CRIMEWARE AS A SERVICE”

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
How Sophos protects on the endpoint
Signature based AV is no longer enough

EXPOSURE PREVENTION
80% malicious URL blocking, malicious web script detection
donload reputation

Pre-execution ANALYTICS AND HEURISTICS
10% Generic matching using heuristics and component level rules

SIGNATURES
5% Signature match of malware or malware components (1-1)

Run-time BEHAVIOUR ANALYTICS
3% Behavior matching and exploit prevention rules

2% Exploit detection

And Sophos Labs never stop innovating and assessing new techniques

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

- **Browser Exploit Prevention**
- **Exploit Technique Prevention**
- **Pre-Exec Behavior Analysis / HIPS Emulation Detection**
- **Malicious Traffic Detection**
- **Cryptoguard Anti-Ransomware**
- **Heartbeat Synchronized Security**
- **Root Cause Analysis**
- **Signatureless cleanup**

**Exploit**

- Before it reaches device

**Prevent**

- Before it runs on device

**Behavior**

- Anti-Malware
- Potentially Unwanted App Live Protection

**Detect**

- Runtime Behavior Analysis / HIPS

**Remediate**

- Quarantine Malware Removal

**Exposure**

- Web Security URL Category Blocking
- Download Reputation

- Application Control Device Control (USB) DLP

- File Scanning

- Anti-Malware
- Potentially Unwanted App

- Behavior

- Extortion

- Synchronize

- Investigate

- Clean

**Traditional Antivirus**

- Prevent
- Detect
- Remediate
Exploit Prevention and Next-Gen Endpoint Protection

- **Annual New Malware Samples**: 100,000,000s
- **Annual Known Exploits (CVE’s)**: 1,000s
- **Cumulative Known Exploit Techniques**: 24
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
Over $1B in transom payments projected for 2016 (source FBI)

Cryptowall
- Costs users $325M in 2015
- 2 out of 3 infections by phishing attack
- Delivered by drive by exploit kits
- 100's to thousands of victims worldwide

Now for MAC and Windows users

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

We have encrypted your files with CryptoLocker virus

Approximate destruction time of your private key

CRYPTOGUARD
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
# Core Features by Product

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

*Intercept X works with competitors AV products*
Server Protection Strategy

- Optimize performance
- Lightweight agent

Server Standard

Anti-malware

Server Advanced

Lockdown

MTD

Cryptoguard

Physical

- Optimize performance
- Lightweight agent

Virtual

- 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

- 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!