



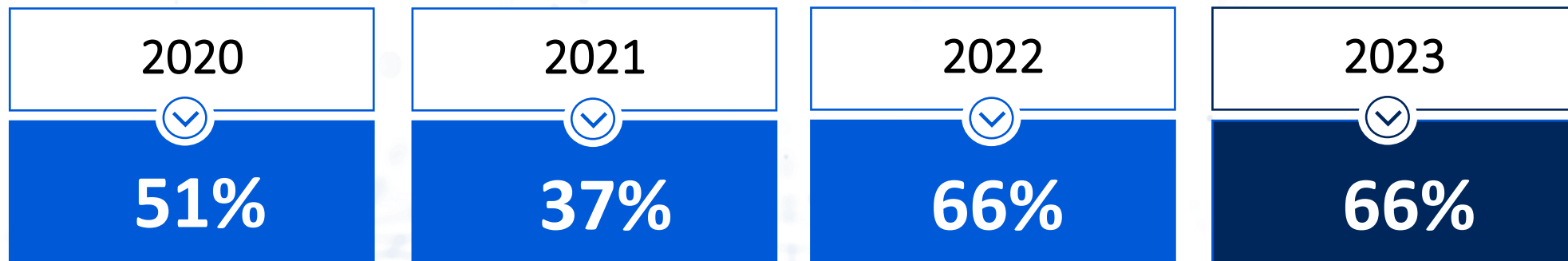
# Managed Detection and Response

**Massimiliano Catanzaro**  
Sales Engineer

**SOPHOS**

# Ransomware: A Success Story

Percentage of organizations hit by ransomware in the last year has stayed level, indicating that adversaries are able to consistently execute attacks at scale.



**1 WEEK to 1 MONTH**

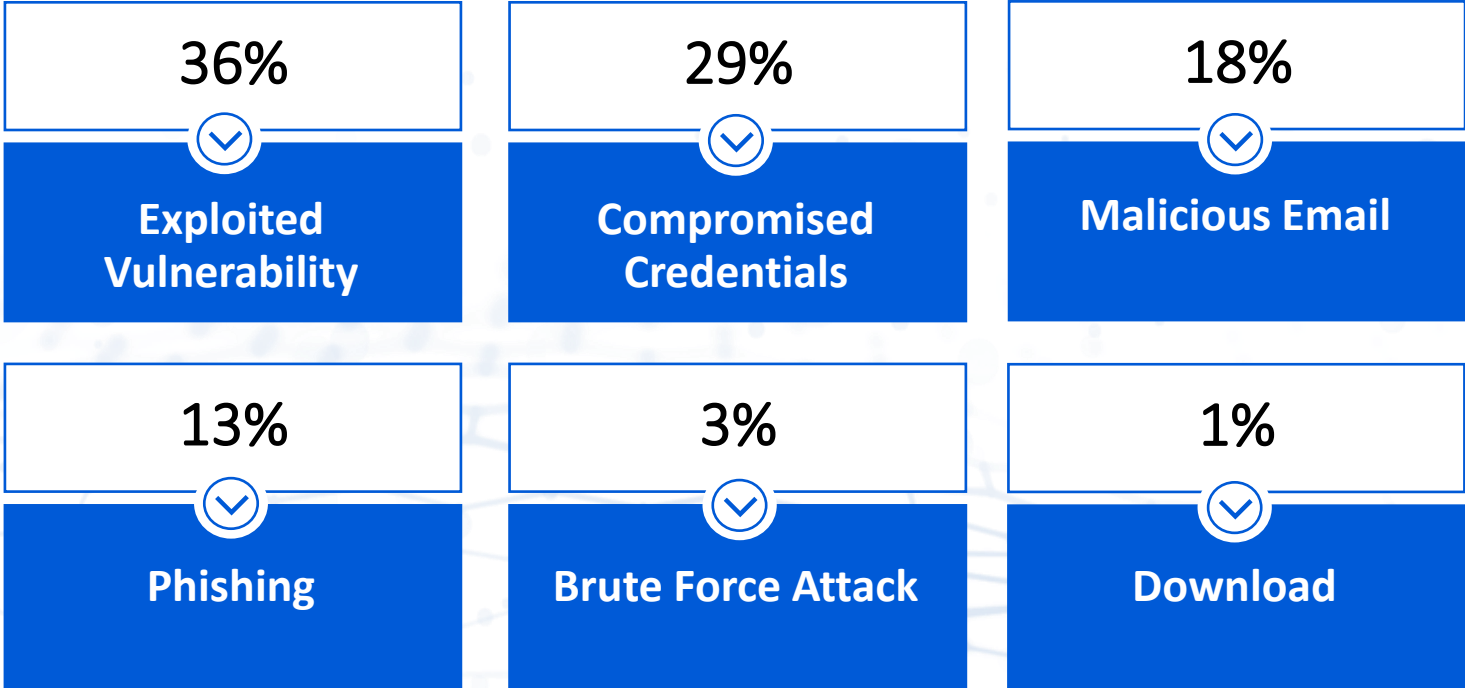
Average recovery time

**2 M€**

Overall recovery cost (downtime, people time, lost opportunities, etc)

# Ransomware: A Success Story

## Root Cause of Ransomware Attack



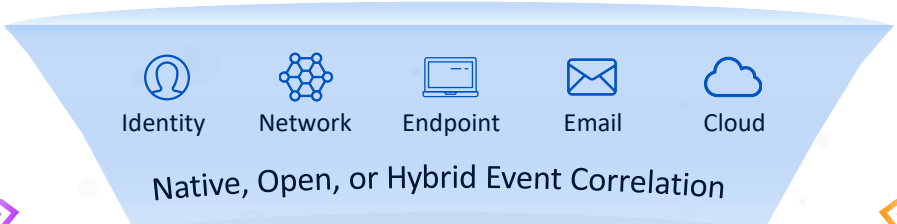
# The Anatomy of Attacks

- Specialists will offer different elements of an attack “as-a-service”
- Playbooks will enable different adversary groups to implement very similar attacks
- Initial Access Brokers (IABs) and malware delivery platforms will find and target victims
- Commercial attack simulation tools (i.e. Cobalt Strike) are designed to test defenses, alerts relating to these tools may indicate the presence of an intruder



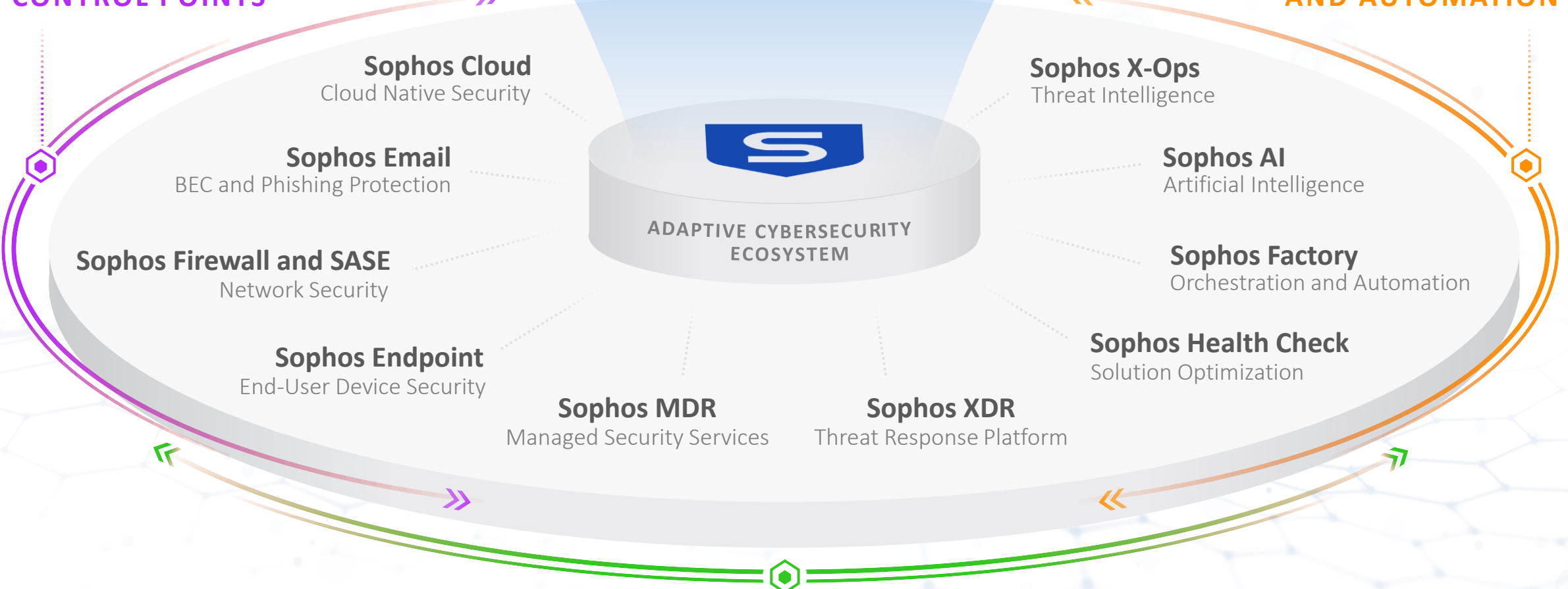
**VICTIMS AND ATTACKERS BOTH USE THE SAME TOOLBOX**

# How Sophos can help



**SECURITY CONTROL POINTS**

**OUTCOME OPTIMIZATION AND AUTOMATION**



**THREAT DETECTION AND RESPONSE**

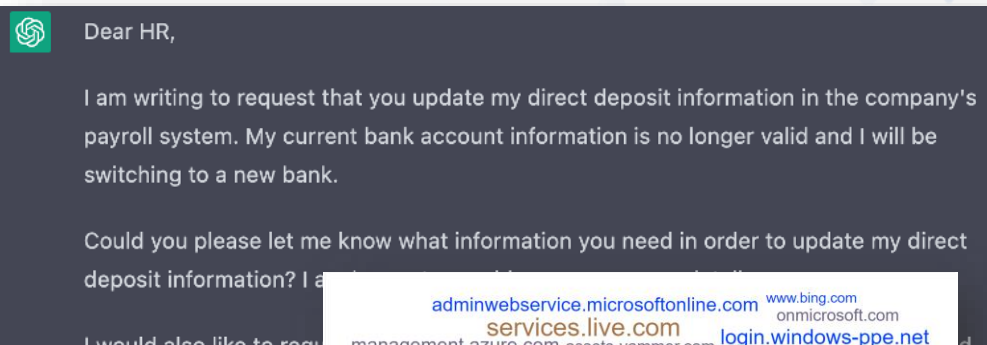
# Protection with Intercept X

# Blocking Web Threats

Stop threats before they arrive, both in and out of the office

## Security Training Under Pressure

It's increasingly difficult for end users to spot a malicious link or website.



## Web Protection

Blocks access to phishing and other malicious sites

Analyses files, web pages, and IP addresses

Continuously updated for freshness and accuracy



## Powered By Leading Threat Intelligence

SophosLabs global team of threat experts

Real-time intelligence from the Sophos Managed Detection & Response threat hunting specialists

# Stop Ransomware in its Tracks

Behaviour based ransomware prevention

## Ransomware Techniques

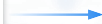
Ransomware comes in many forms



File overwrite encryption



Intermittent encryption



Remote encryption



Boot level encryption



## Sophos Intercept X

**Blocks ransomware irrespective of source**

Identifies file changes indicative of ransomware

Detects encryption from files, scripts or trusted applications

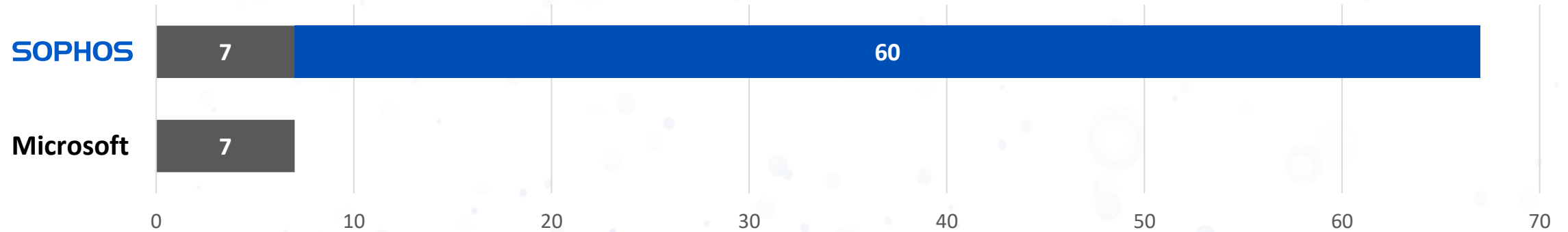
Terminates process and rolls back encrypted file

Blocks ransomware delivered from other machines

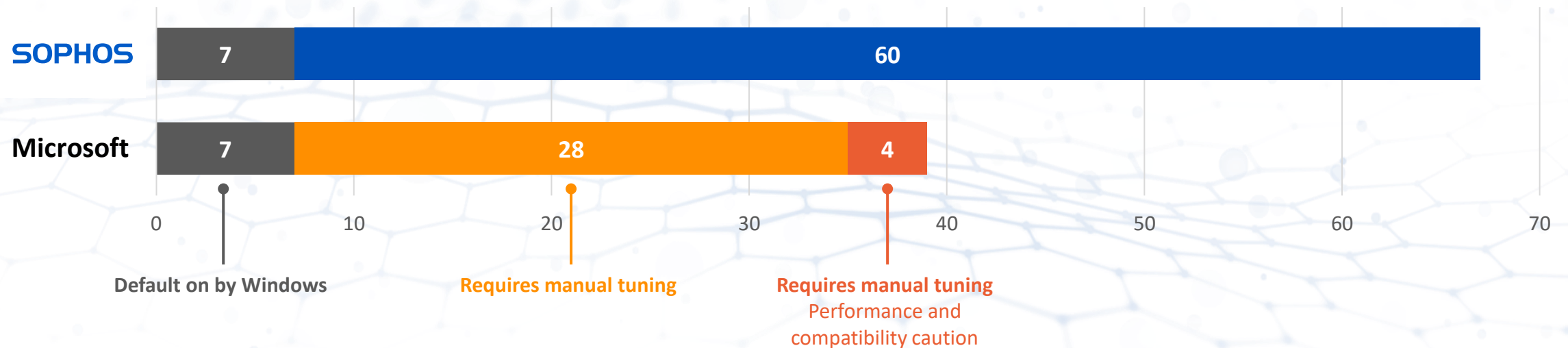


# Anti-Exploitation: Supplementing Windows Defenses

## Anti-Exploitation default enabled



## Total available mitigations



More: <https://sophos.com/microsoft>

# Synchronized Security

Synchronized Security is the technology used by Sophos Endpoints and Devices belonging to the same organization to communicate each other through a Security Heartbeat.



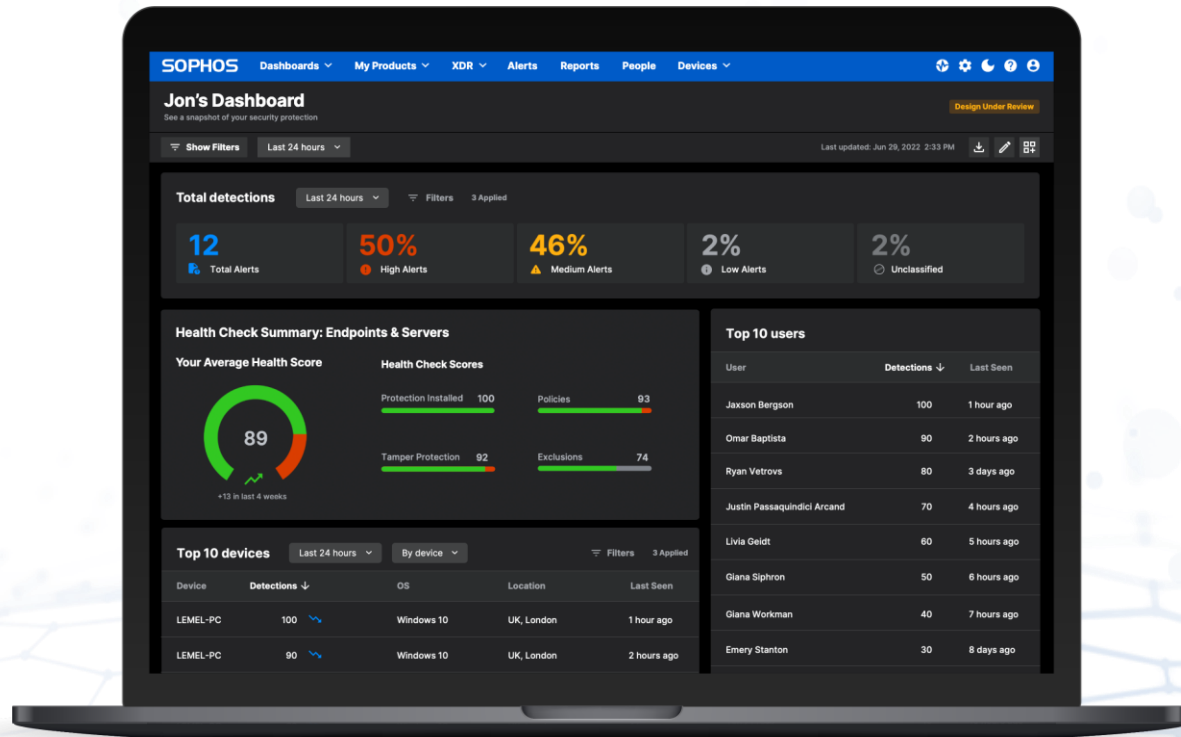
### Security Heartbeat®

1	0	1	2
At risk	Missing	Warnings	Connected

### Synchronized Application Control™

7	217	373
New	Categorized	Total

# Account Health Check with Score



## Software assignment

Do devices have the right software assigned to them?



## Threat policy

Are policies using recommended settings?



## Exclusions

Are any exclusions creating significant exposure?

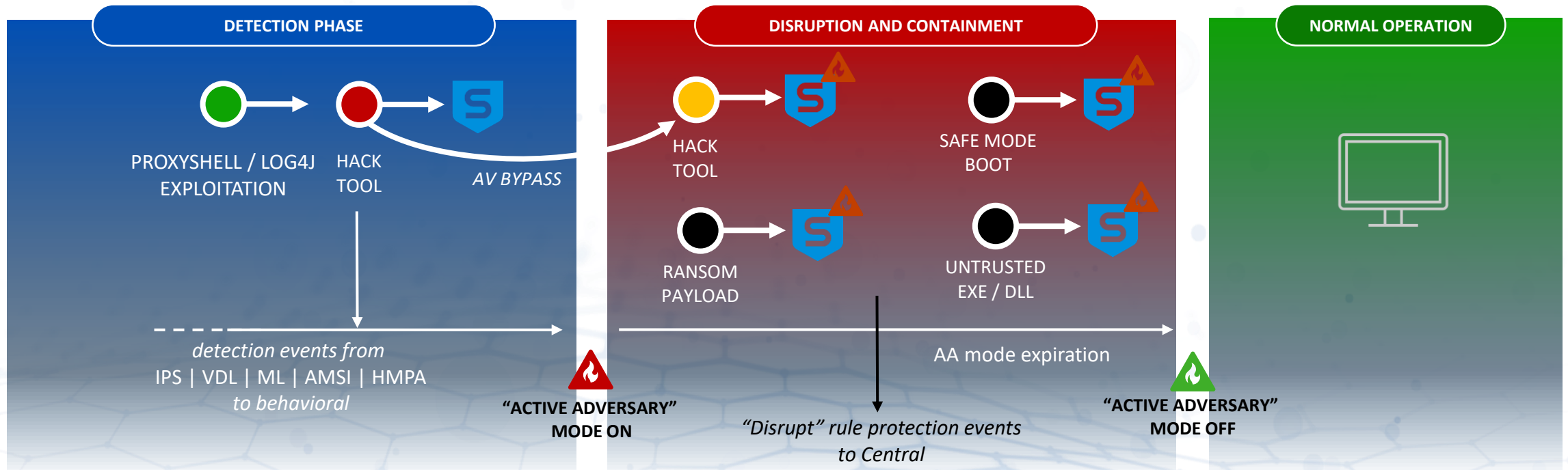


## Tamper protection

Has tamper protection been disabled?

# Active Adversary Behavior Protection

Disrupt and delay attackers. Buy time for Security Teams to respond to an advanced threat



- Observe alerting detections from individual components
- A set of special Rules aggregate signals to detect “active adversary”

- Cripple, slowdown & frustrate attacker with aggressive host-level “lockdown” actions
- Granular lockdown logic updatable with data
- Alerts to MDR/XDR for hand-to-hand combat

- Ideally “someone” took action..
- Attacker is off the network
- Remediation complete

# Critical Attack Warning

Sophos Central Dashboard  
a snapshot of your security protection

23  
Total Alerts

10  
High Alerts

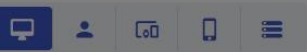
12  
Medium Alerts

1  
Low Alerts

### Most Recent Alerts

- Sep 19, 2023 5:57 PM
- Sep 19, 2023 4:02 PM
- Sep 19, 2023 9:50 AM
- Sep 18, 2023 4:48 PM
- Sep 18, 2023 4:48 PM

### Devices and users: summary



Endpoint Computer Activity Status

0  
Web Threats

0  
Policy Violations

## You're under attack

You must act now

An attacker is trying to access your devices. A serious security incident might follow. [I have resolved this attack](#)

We're still protecting you, but you must act now.

Attacks detected on:

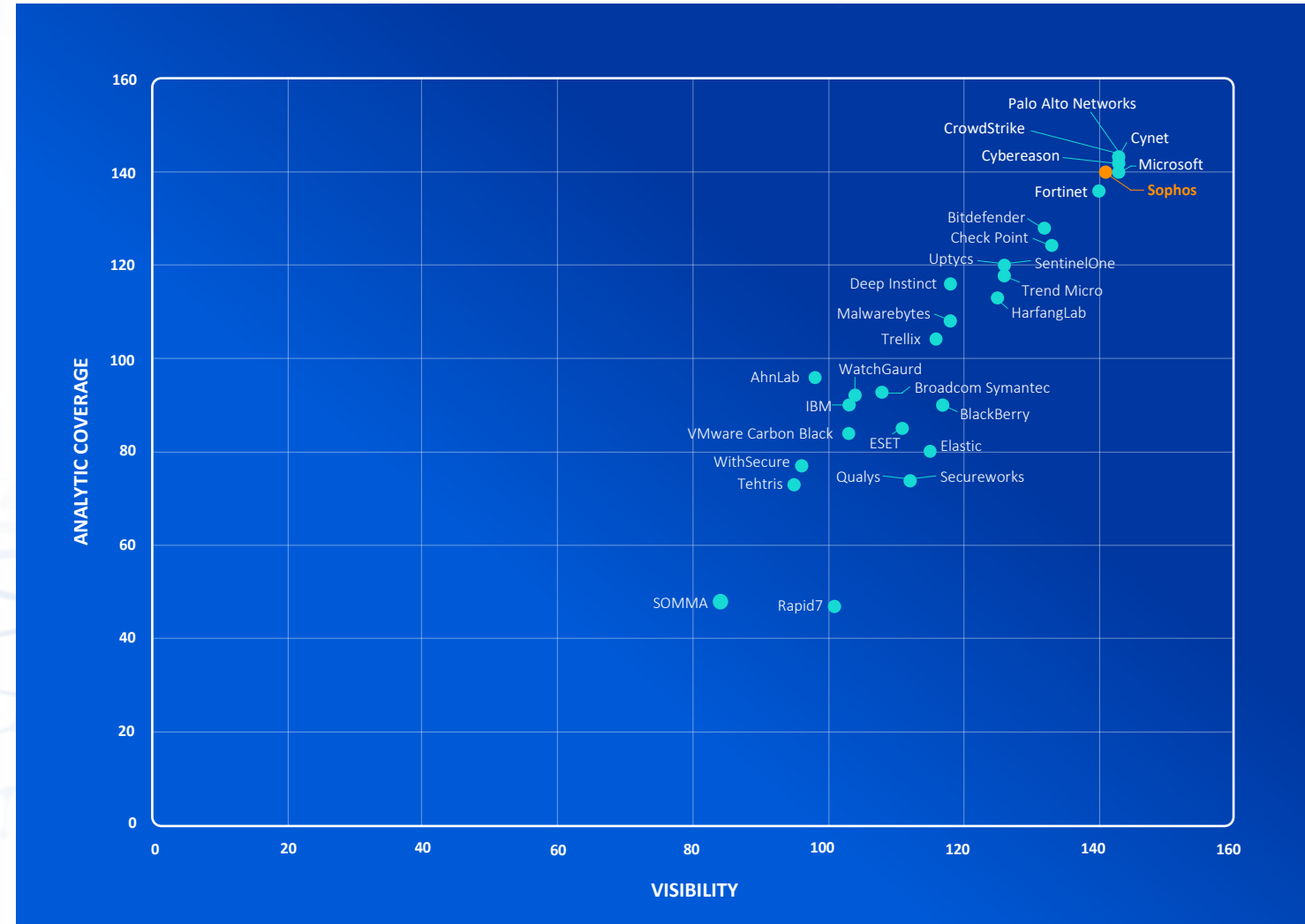
3 of 717 Windows computers	0 of 11 Windows servers
-------------------------------	----------------------------

- View attack details
- Contact your Sophos Partner
- Contact Sophos Incident Response

# Good News: MITRE Engenuity Attack Evaluations 2023



- Sophos had 141 of 143 detection coverage for adversary behavior (Visibility)
- 140 of 143 Sophos detections included rich context on the “What”, “Why”, or “How” of adversary activity (Analytic Coverage)



# Detection & Response

# Why Detection & Response

Event/Incident Detection  
and Response

Forensic Investigation

Threat Hunting & IT  
Operations Hygiene

Provide Remote Support in  
Real Time

**IDENTIFY HIDDEN THREATS BEFORE THE ATTACK BEGINS**



# Proactive Activity: Live Discovery Queries

Query : Devices with a restart pending

[Back to categories / All queries](#)

Devices with a restart pending

All queries: Devices with a restart pending

Created by Sophos

Sources

Windows

Device selector (21 Endpoints available)

8 Endpoints selected

Devices with a restart pending query results

8 / 8 Devices completed

Run Query

Export

Device selector

epName

Available devices

dc01

PC-MAURO

PC-ERCOLE

PC-WALTER

PC-MASSIMILIANO

PC-LILLO-CUSTOM

dc02

Filters

Online Status

Name

Type

Operating system

Last user

Group

IP address

Health status

Reset to defaults

Apply

Online

PC-ERCOLE

Computer

Windows 10 Enterpris Ercole Plez

XdrSensor (OU=XdrSensor, 10.11.10.106

Online

PC-LILLO-CUSTOM

Computer

Windows 10 Enterpris Letterio La Spada

NUC2 (OU=NUC2,DC=se,D 10.11.10.101 ...

Displaying 1 - 8

1

Run Query

Queries	Actions
<ul style="list-style-type: none"> <li> Data lake queries</li> <li>Device encryption status with document list</li> <li>Disk encryption on Windows (Data Lake)</li> <li>Detections per detection type (Data Lake)</li> <li>Find common lateral movement threat indicators (Data Lake)</li> <li>Find common execution threat indicators (Data Lake)</li> <li>Find common persistence threat indicators (Data Lake)</li> <li>Find common defense evasion threat indicators (Data Lake)</li> </ul>	<ul style="list-style-type: none"> <li>Scan this device</li> <li>Start Live Response session</li> </ul>

# Reactive Activity: Root Cause Analysis

**SOPHOS**

## Threat Analysis Center - ATK/Apteryx-Gen

Overview / Threat Analysis Center Dashboard / Threat Graphs / ATK/Apteryx-Gen

Help | Sophos Demo Lab | User: SE - Super Admin

PC-ERCOLE 10.11.10.106 → **Root Cause** Microsoft Powershell → **Beacon** mimikatz.exe → **Detected** Apr 12, 2023 4:53 PM → **Cleaned**

### Summary

Detection name: ATK/Apteryx-Gen  
Root cause: powershell.exe  
Possible data involved: no business files  
Where: On PC-ERCOLE that belongs to Ercole Plez  
When: Detected on Apr 12, 2023 4:53 PM

### Suggested next steps

Set a status for the threat graph (Priority: Low, Status: New)  
Isolate this device while you investigate  
Scan the device  
Run a Live Discover query

Download PDF | **Clean and block** (What does this do?) | Registry keys

Other file : mimikatz.exe

Process detail | Report summary | Machine learning analysis | File properties | File breakdown

Reputation at time graph was created: **Bad: Likely malware**

SOPHOSLABS Threat Intelligence  
Current report created: Apr 13, 2023 5:44 PM

Request latest intelligence

Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. Learn More

Path: c:\users\public\toolz\win32\mimikatz.exe  
Name: mimikatz.exe  
SHA256: 94795fd89366e01bd6ce6471ff27c3782e2e16377a848426cf0b2e6baee9449b

21 File reads  
21 File writes  
1 Registry key access  
34 File reads  
14 File reads

actions

- Determine root cause
- Identify scope of threat
- See where it was neutralized
- Manually block an unwanted file

**SOPHOS**

# Reactive Activity: Live Response

- Direct system access
- All actions are logged
- Enable/Disable by policy
- Cannot see user's desktop
- Transparent for device users

```
HOSTS Victim4-Win10x64 126 x
Victim4-Win10x64:C:\users\admin\desktop$ cd C:/users/admin/desktop
Victim4-Win10x64:C:\users\admin\desktop$ dir
Volume in drive C has no label.
Volume Serial Number is 06C7-DA54

Directory of C:\users\admin\desktop
04/08/2019 03:59 AM <DIR> .
04/08/2019 03:59 AM <DIR> ..
03/06/2019 09:55 AM 37,426 BeefWellington.zip
03/06/2019 09:54 AM 23 config.txt
04/08/2019 03:58 AM <DIR> DemoFiles
03/05/2019 01:34 PM 2,693 Microsoft Office Outlook 2007.lnk
03/06/2019 09:54 AM 36,528 nc.exe
03/06/2019 09:54 AM 339,096 PsExec.exe
03/06/2019 09:54 AM 1,174,528 ssh.dll
03/06/2019 09:54 AM 882,688 ssh.exe
7 File(s) 2,472,982 bytes
3 Dir(s) 38,448,795,648 bytes free

Victim4-Win10x64:C:\users\admin\desktop$ del nc.exe
Victim4-Win10x64:C:\users\admin\desktop$ del psexec.exe
Victim4-Win10x64:C:\users\admin\desktop$ del ssh.exe
Victim4-Win10x64:C:\users\admin\desktop$ del ssh.dll
Victim4-Win10x64:C:\users\admin\desktop$ dir
Volume in drive C has no label.
Volume Serial Number is 06C7-DA54

Directory of C:\users\admin\desktop
04/08/2019 04:08 AM <DIR> .
04/08/2019 04:08 AM <DIR> ..
03/06/2019 09:55 AM 37,426 BeefWellington.zip
03/06/2019 09:54 AM 23 config.txt
04/08/2019 03:58 AM <DIR> DemoFiles
03/05/2019 01:34 PM 2,693 Microsoft Office Outlook 2007.lnk
3 File(s) 40,142 bytes
3 Dir(s) 38,451,056,640 bytes free

Victim4-Win10x64:C:\users\admin\desktop$
```

# Cybersecurity As A Service

# Most Common Complains with Cybersecurity



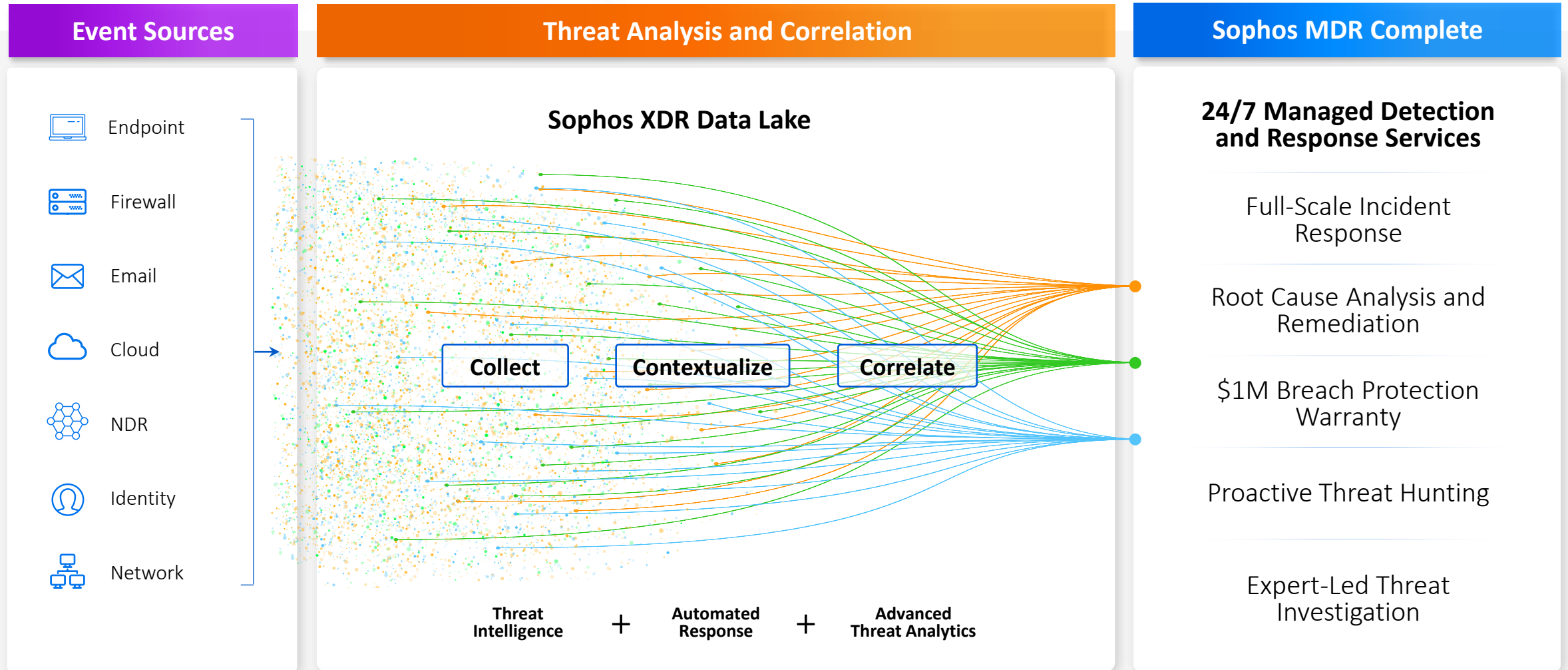
71%

71%

**CYBERSECURITY HAS BECOME TOO COMPLEX  
FOR MOST ORGANIZATIONS TO MANAGE EFFECTIVELY**



# Sophos MDR Complete



# MDR Activities

## Threat Hunting

Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own

## Threat Detection

Enabled by extended detection and response (XDR) capabilities that detect known threats and potentially malicious behaviours wherever your data reside

## Incident Response

Our analysts respond to threats in minutes whether you need full-scale incident response or assistance making more accurate decisions

## Reporting

Monthly and Weekly Reports about detections, closed and on-going cases, escalations and threats, most investigated devices



Time to Detect

Less than 1 Minute

Time to Investigate

Less than 25 Minutes

Time to Respond

Less than 12 Minutes

**FIXED AND TRANSPARENT COSTS  
WHATEVER THE NUMBER OF INCIDENTS**

# Sophos Service Tiers

Sophos MDR for  
Microsoft Defender



Sophos MDR  
Essentials

Sophos MDR  
Complete

<b>24/7 expert-led threat monitoring and response</b>	✓	✓
<b>Compatible with non-Sophos security products</b>	✓	✓
<b>Weekly and monthly reporting</b>	✓	✓
<b>Monthly intelligence briefing: “Sophos MDR ThreatCast”</b>	✓	✓
<b>Sophos Account Health Check</b>	✓	✓
<b>Expert-led threat hunting</b>	✓	✓
<b>Threat Response: active attacks are stopped and contained</b> <small>Uses full Sophos XDR Agent (protection, detection, and response) or Sophos XDR Sensor (detection and response)</small>	✓	✓
<b>Direct call-in support during active incidents</b>	✓	✓
<b>Root Cause Analysis: performed to prevent future recurrence</b>		✓
<b>Full-scale Incident Response: threats are fully eliminated</b> <small>Requires full Sophos XDR agent (protection, detection, and response)</small>		✓
<b>Dedicated Incident Response Lead</b>		✓
<b>Sophos Breach Protection Warranty</b>		✓



# Attack Scenario: Spearphishing

## Attack Scenario

User opens a spearphishing email and clicks a link that downloads a malicious file

## MITRE | ATT&CK®

TACTIC	Initial Access	Execution	Defense Evasion	Persistence
TECHNIQUE	Spearphishing Link	Malicious File	Process Injection	Schedule Task

▲  
INITIAL DETECTION

### Sophos MDR and Sophos MDR Complete

#### Threat Containment Actions

- Isolate the affected user's device
- Remove the malicious file
- Remove the scheduled task
- Notify the customer of actions taken and provide remediation guidance

### Sophos MDR Complete

#### Incident Response and Root Cause Analysis

- Locate the spearphishing email/URL that delivered the malicious link/file used to execute the attack
- Investigate if other users received the spearphishing email associated with this attack
- Notify the customer and provide remediation guidance

### Performed by Customer

#### Remediation Guidance

- Block the sending domain from the email client and/or email security product
- Reset the credentials of any users impacted by the attack

# Sophos MDR: Industry-Leading Openness and Flexibility



## Compatible with your environment

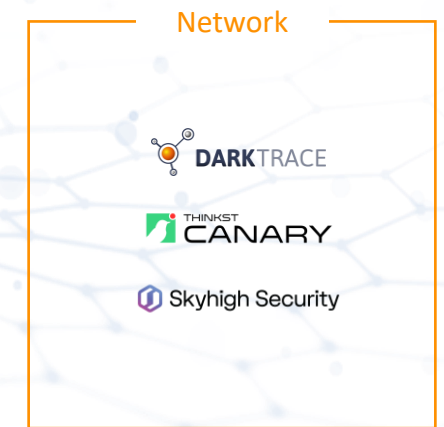
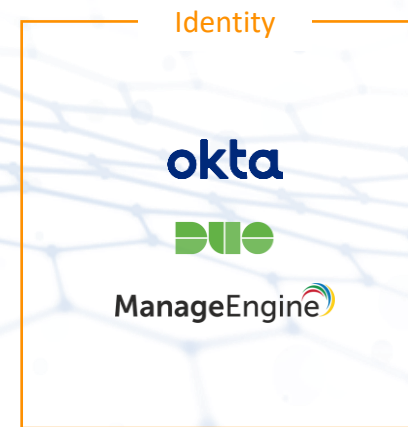
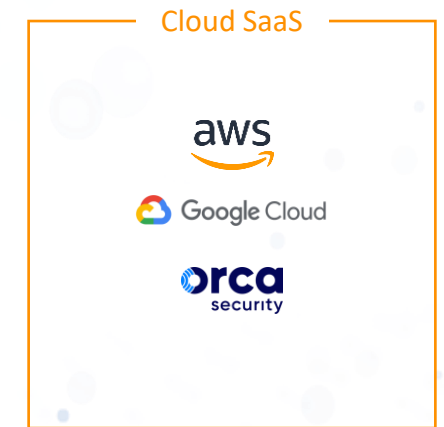
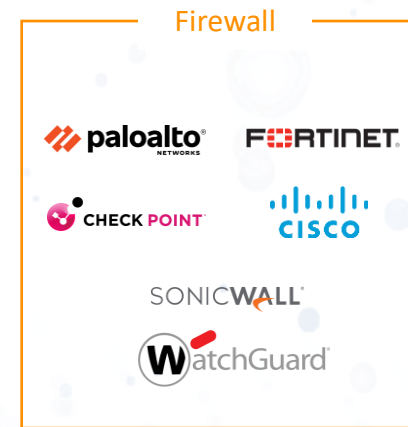
We can use our tools, another vendor's tools or any combination of the two

## Compatible with your needs

Whether you need full-scale incident response or assistance making more accurate decisions

## Compatible with your business

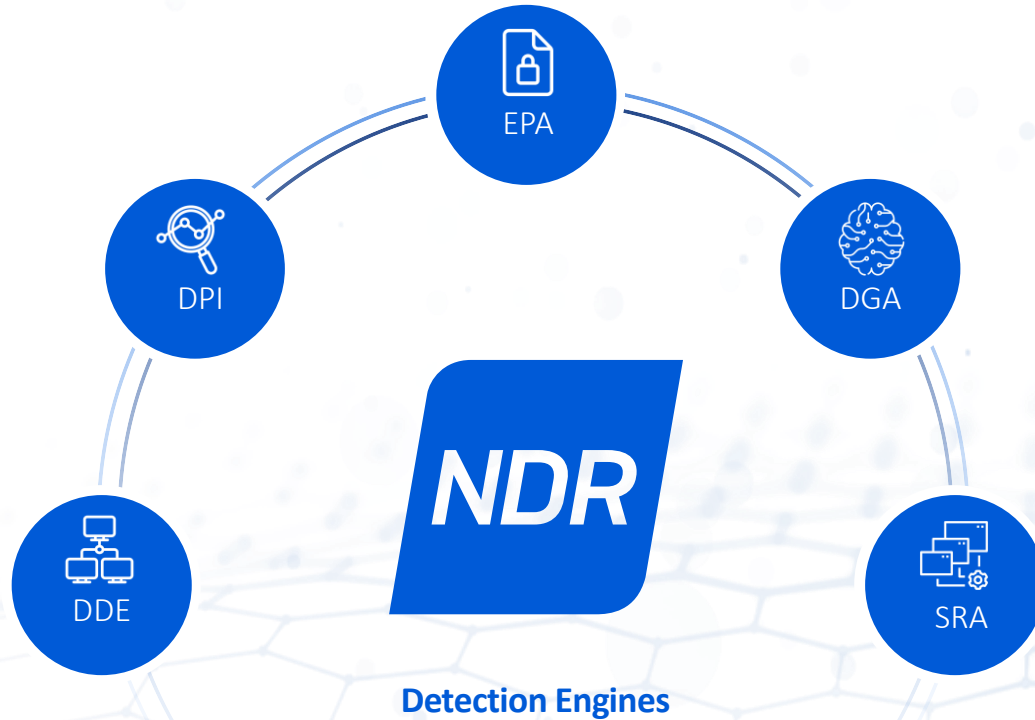
Our team has deep experience hunting threats targeting organizations in every industry



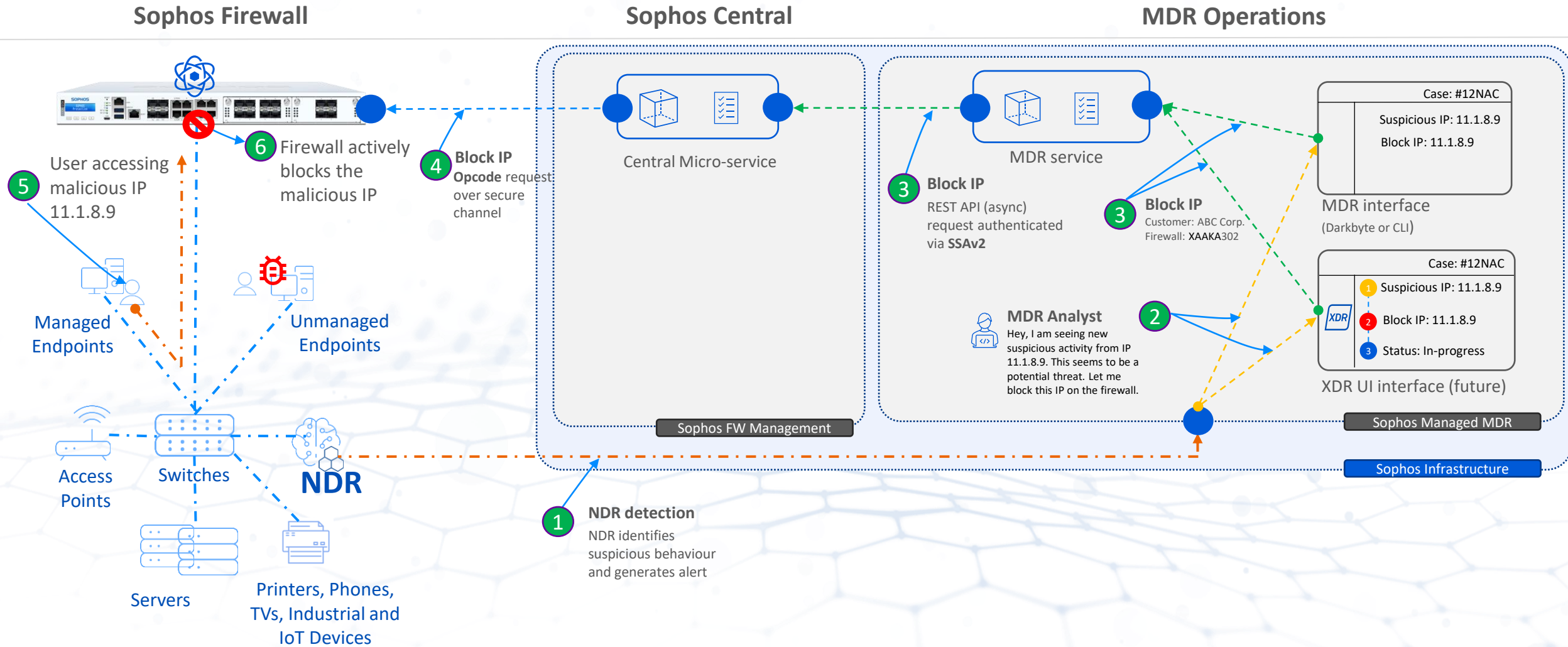
# Sophos NDR

## Overview

- Based on the July 2021 Braintrace acquisition
- Virtual appliance that connects to TAP/SPAN capture and analyzes network flows.
- Utilizes 5 independent detection engines in real-time.
- Detects known IOCs amongst encrypted and plain text traffic to rapidly identify threat actors and TTPs
- Detects zero-day C2 servers and new variants of malware families based on patterns found in the session packets size, direction, and interarrival times
- Risk analytics to detect abnormal activity and identify patterns that may warrant investigation
- Generate alerts that can be correlated and prioritized as part as of Sophos MDR
- Available for MDR Customers only



# Remediation with Sophos Firewall SFOS v20 **NEW**



# Why You should choose Sophos MDR

**Top-rated products help to build a good CSaaS**

**Over 550000 customers and More than 18000 MDR customers help to discover new threats BEFORE CSaaS help to improve products capabilities**

**Fixed Costs**

**Customer can change MDR preferences WHENEVER he needs  
Costs do not change, WHATEVER the number of incidents**

**Sophos Products and Integrations all in a Single Management Console**

**Sophos and 3<sup>rd</sup> Parties Products telemetries ingested and correlated in a SINGLE CONSOLE to speed-up Detections of potential threats**

# Breach Protection Warranty

The Sophos Breach Protection Warranty covers up to **\$1 million** in response expenses



Included with new **Sophos MDR Complete** annual (term) subscriptions – at no additional cost



Built-in automatically with **1-, 2- and 3-year licenses**, both new customers and renewals



**Comprehensive coverage:** endpoints, servers, Windows, macOS, no geographic limits



**Underwritten by Sophos**, demonstrating our confidence in our protection

**Want to Know more?**

# SOPHOS State of Ransomware 2023 Report



**Download the full report**  
[www.sophos.com/ransomware2023](http://www.sophos.com/ransomware2023)



# MITRE Engenuity ATT&CK Evaluations 2023 Results



## Sophos News Post

<https://news.sophos.com/en-us/2023/09/20/results-from-the-2023-mitre-engenuity-attck-evaluations-round-5-turla/>

## MITRE Engenuity ATT&CK Result Pages

<https://attachevals.mitre-engenuity.org/results/enterprise?vendor=sophos&evaluation=turla&scenario=1>

# Questions & Answers

**SOPHOS**  
Cybersecurity delivered.