3CiME TECHNOLOGY
ICT & INNOVATION

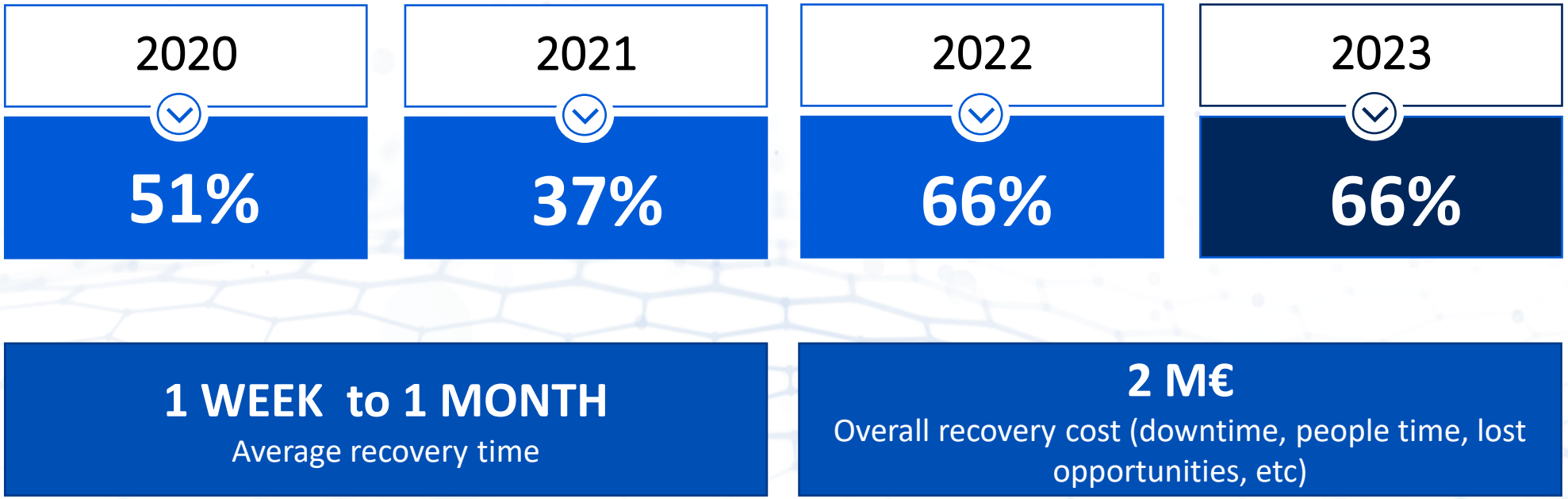
Managed Detection and Response

Massimiliano Catanzaro
Sales Engineer

SOPHOS

Ransomware: A Success Story

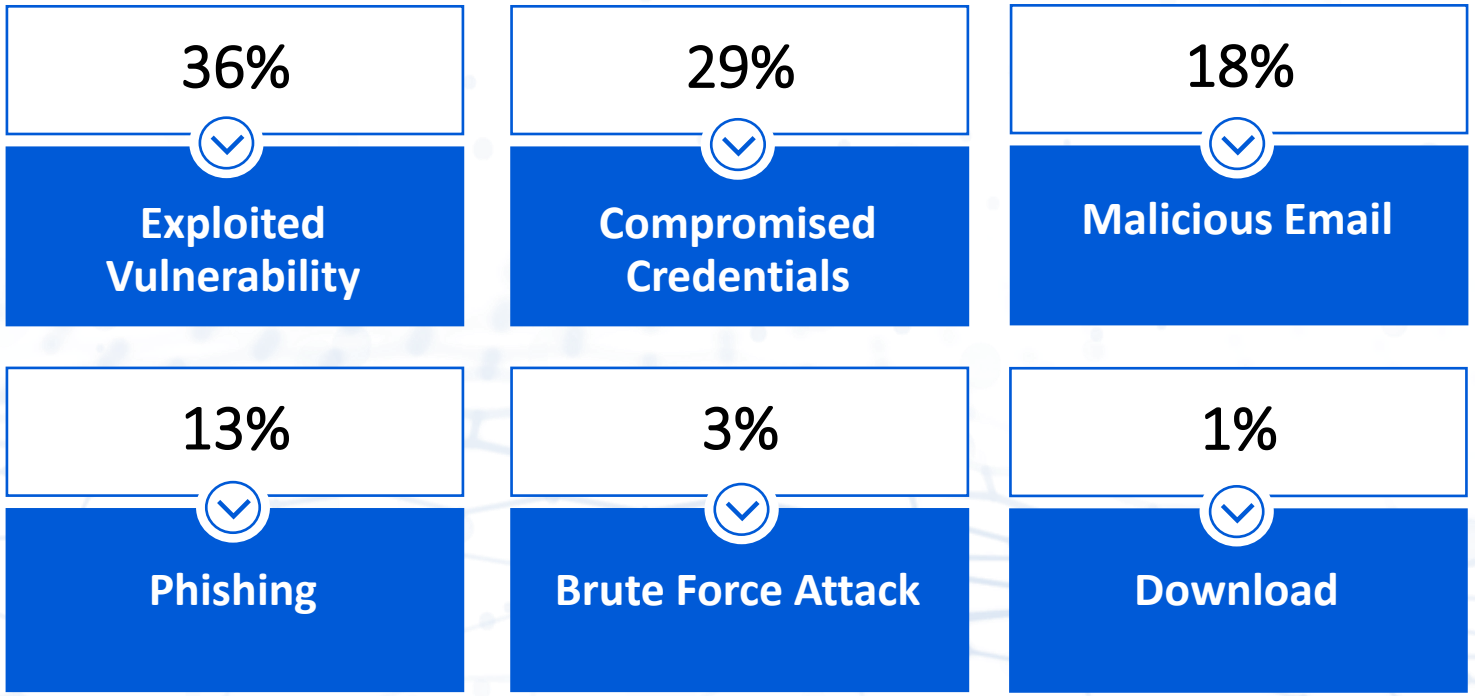
Percentage of organizations hit by ransomware in the last year has stayed level, indicating that adversaries are able to consistently execute attacks at scale.



Sophos The State of Ransomware 2023

Ransomware: A Success Story

Root Cause of Ransomware Attack



Sophos The State of Ransomware 2023

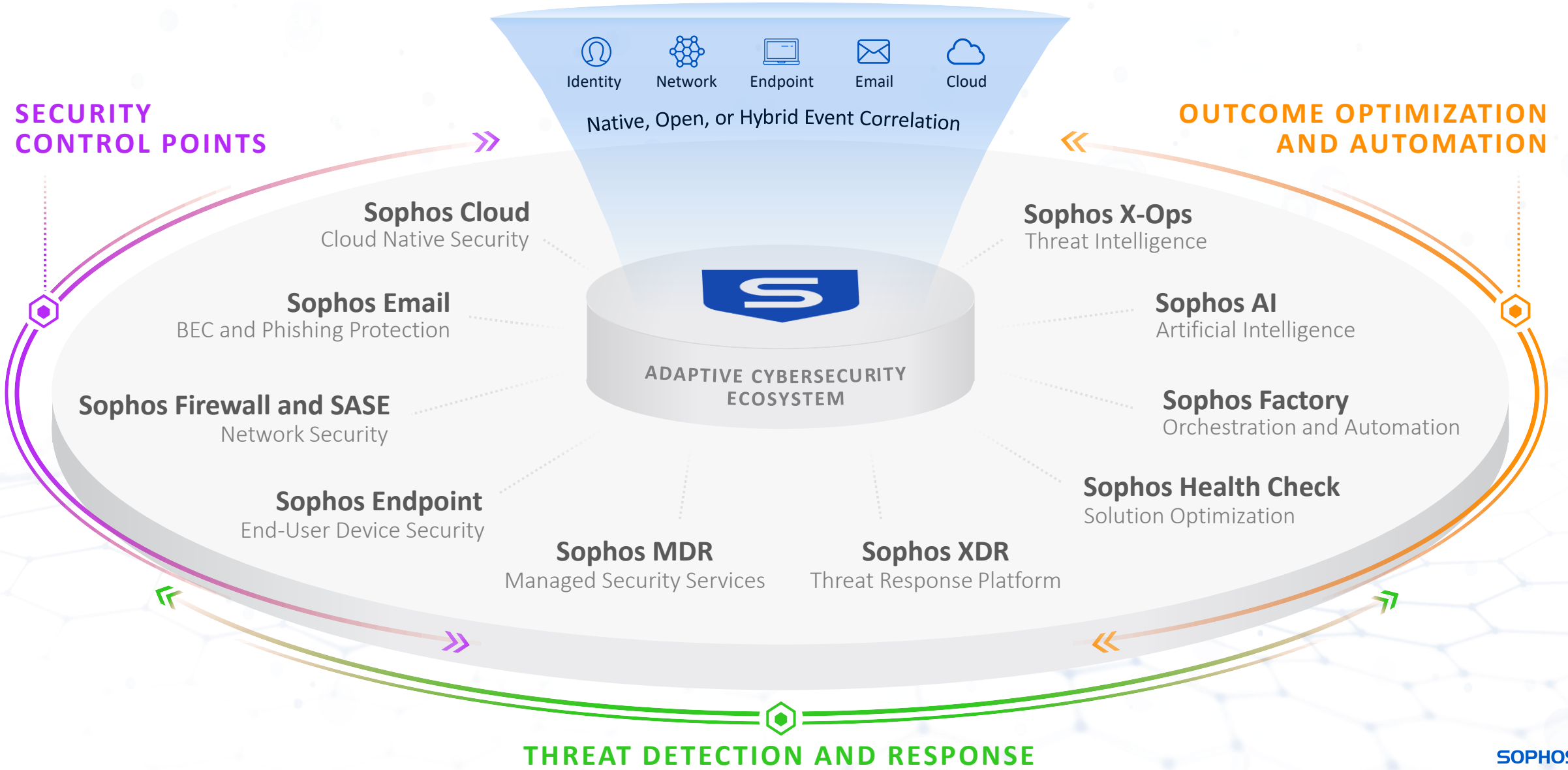
The Anatomy of Attacks

- 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

Sophos Active Adversary Playbook 2022

How Sophos can help



SOPHOS

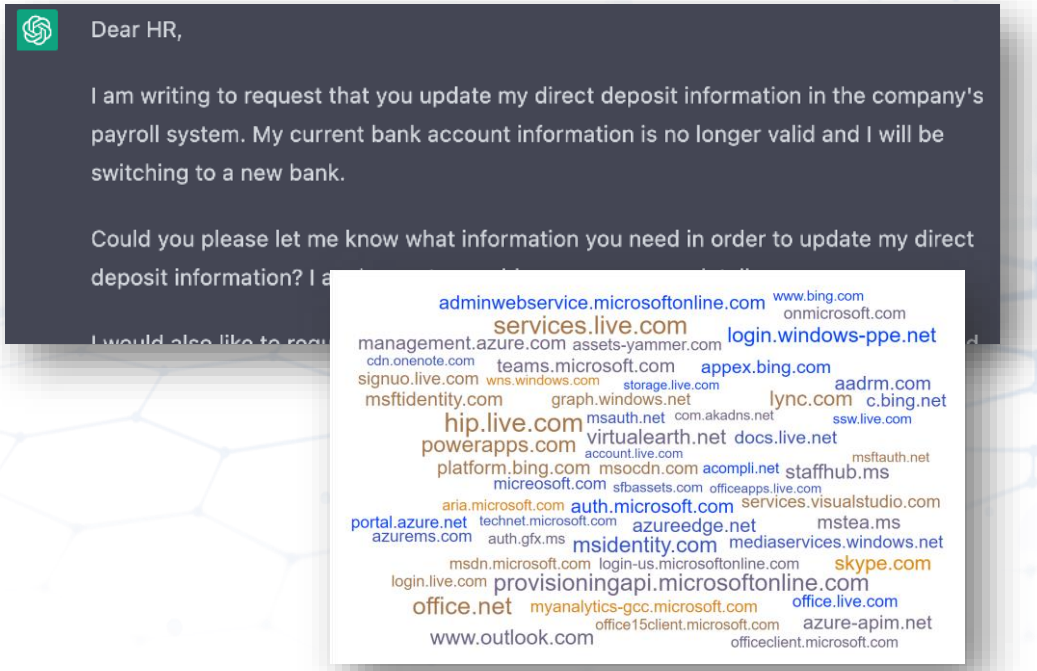
Protection with Intercept X

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

SOPHOS

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

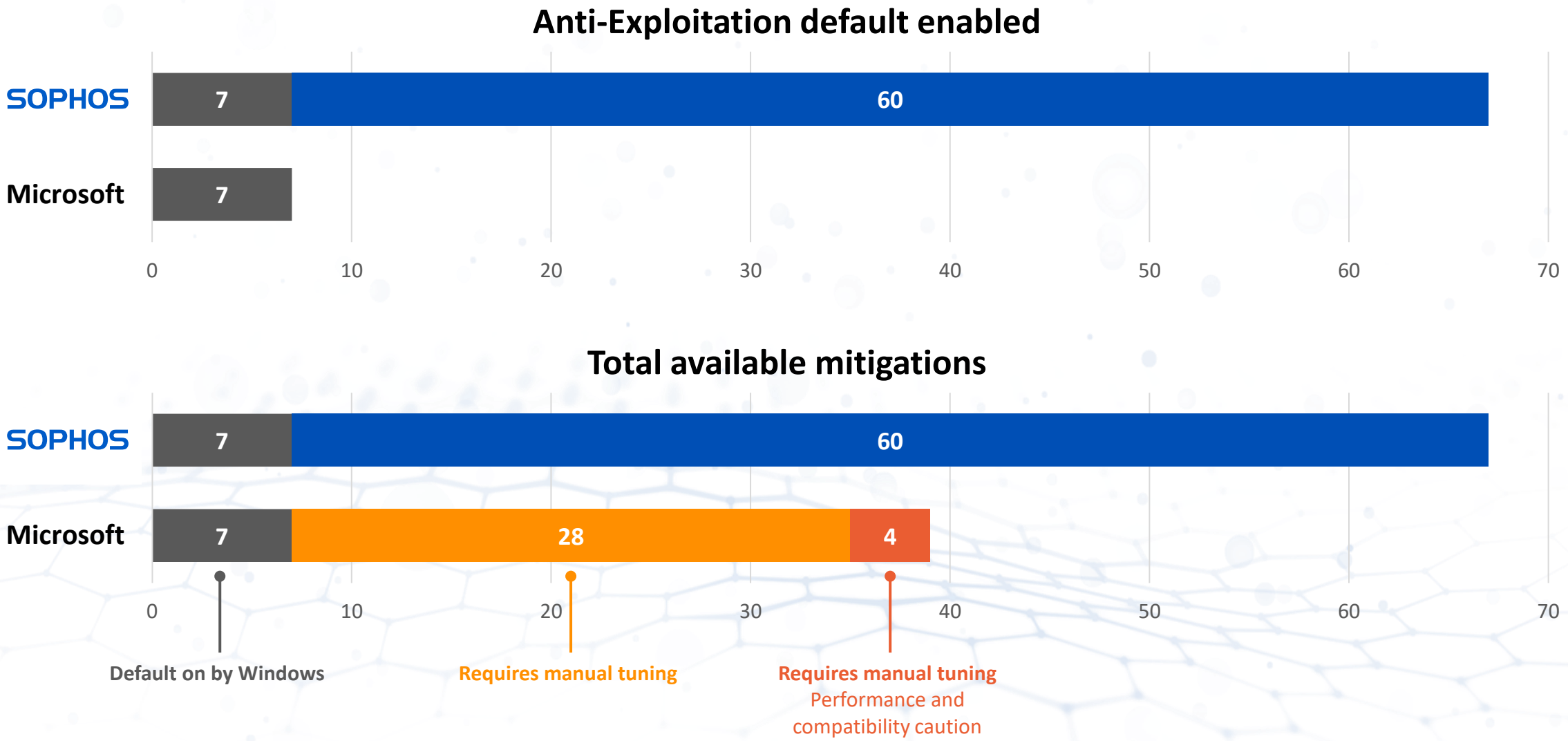
Detects encryption from files, scripts or trusted applications

Terminates process and rolls back encrypted file

Blocks ransomware delivered from other machines

SOPHOS

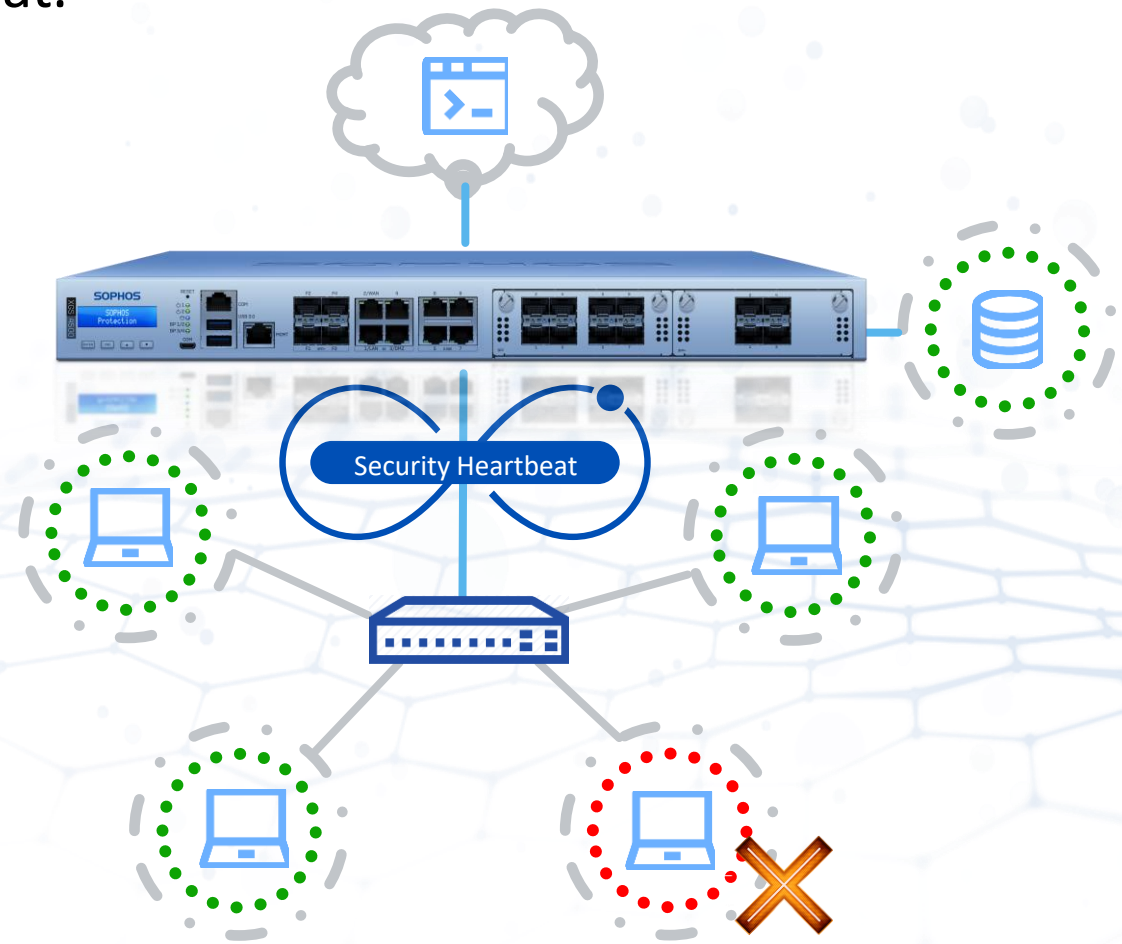
Anti-Exploitation: Supplementing Windows Defenses

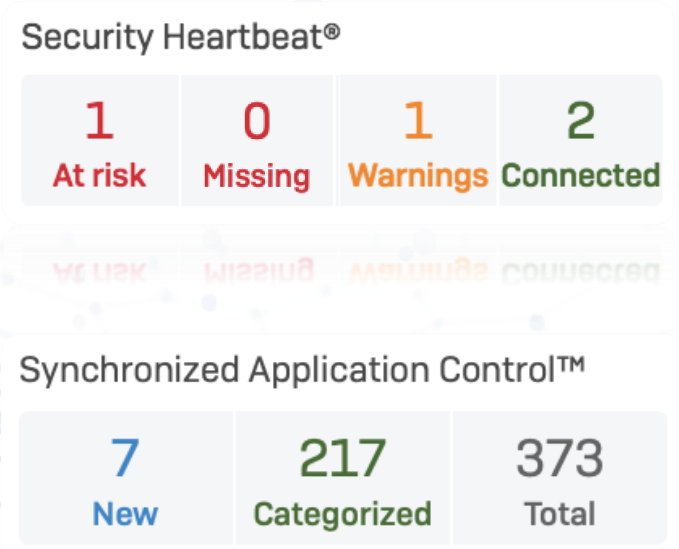


More: https://sophos.com/microsoft

Synchronized Security

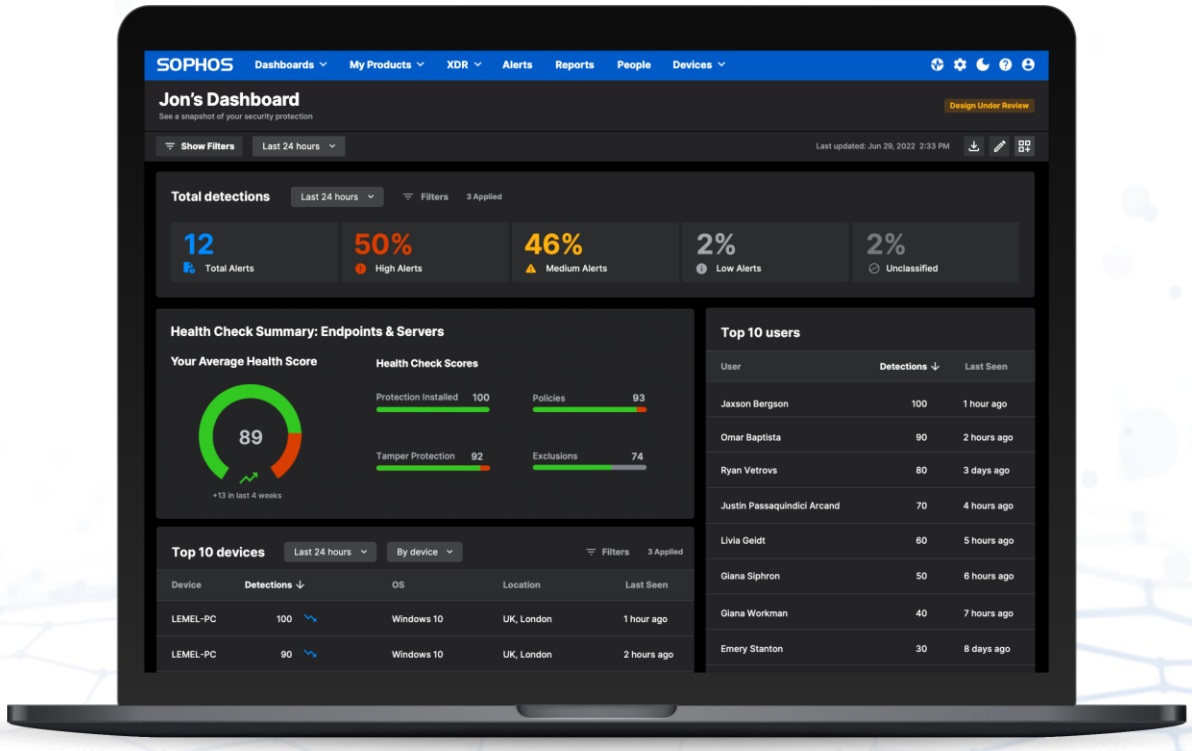
Synchronized Security is the technology used by Sophos Endpoints and Devices belonging to the same organization to communicate each other through a Security Heartbeat.





SOPHOS

Account Health Check with Score



Software assignment

Do devices have the right software assigned to them?

Threat policy

Are policies using recommended settings?

Exclusions

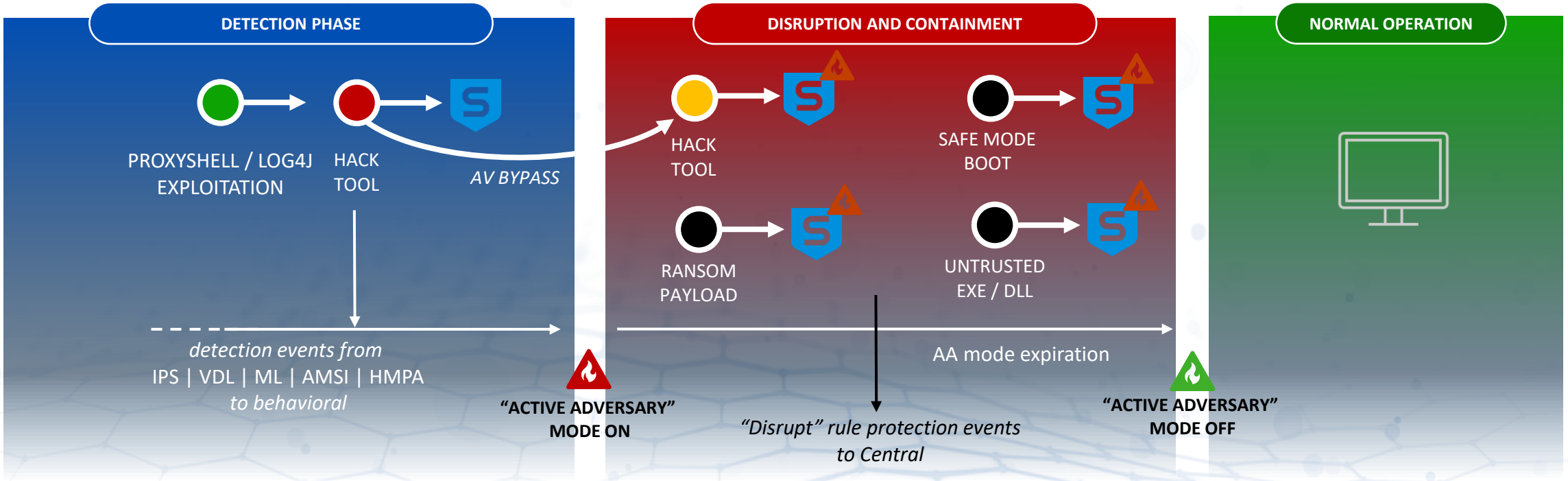
Are any exclusions creating significant exposure?

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



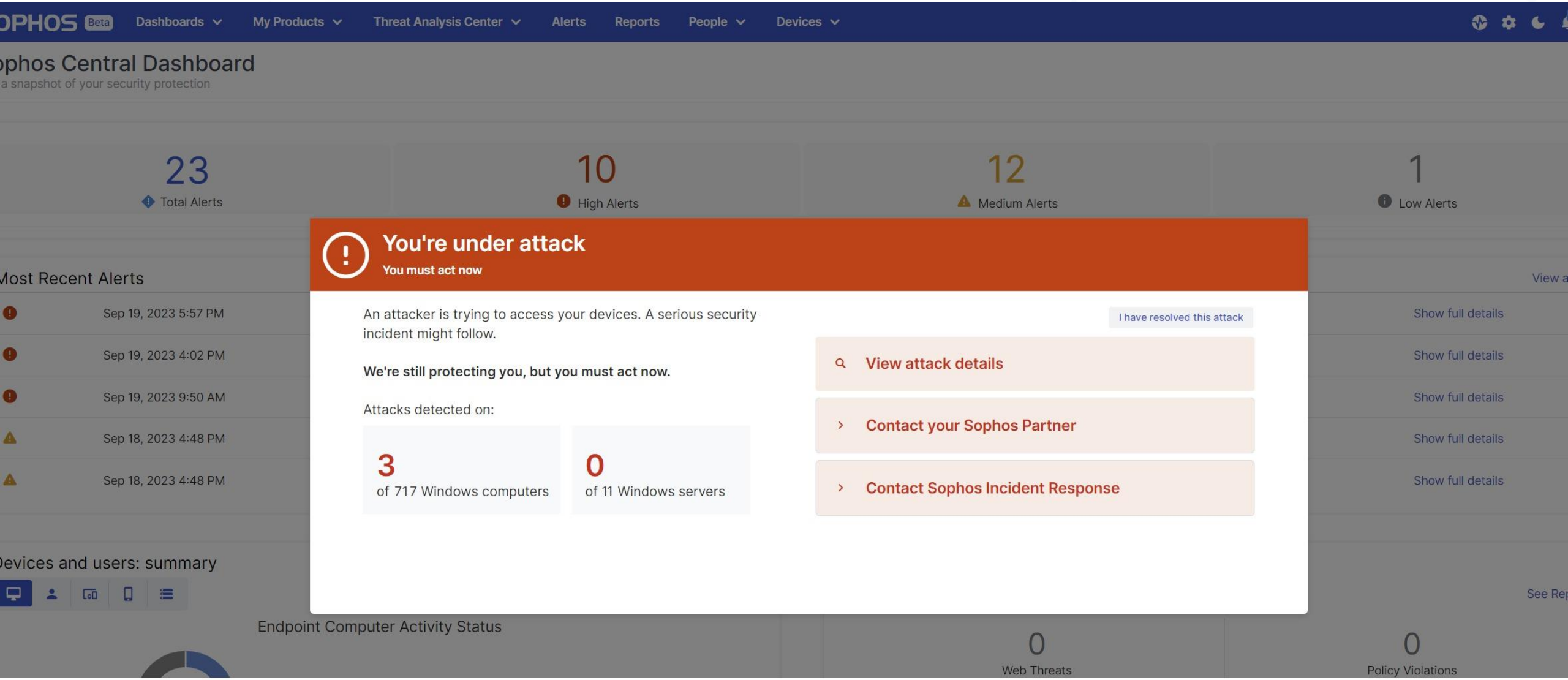
- Observe alerting detections from individual components
- A set of special Rules aggregate signals to detect "active adversary"

- 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

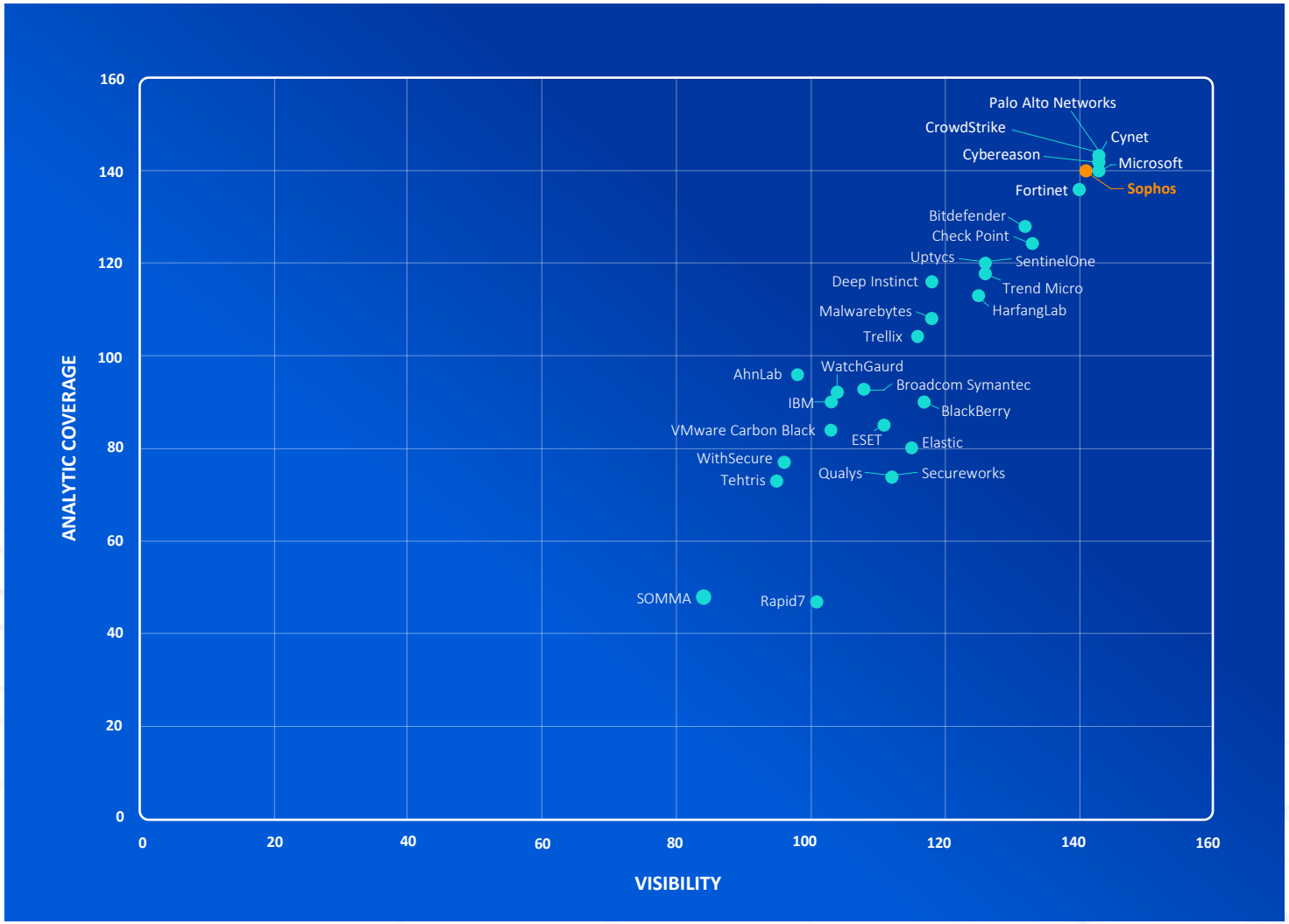
SOPHOS

Critical Attack Warning



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

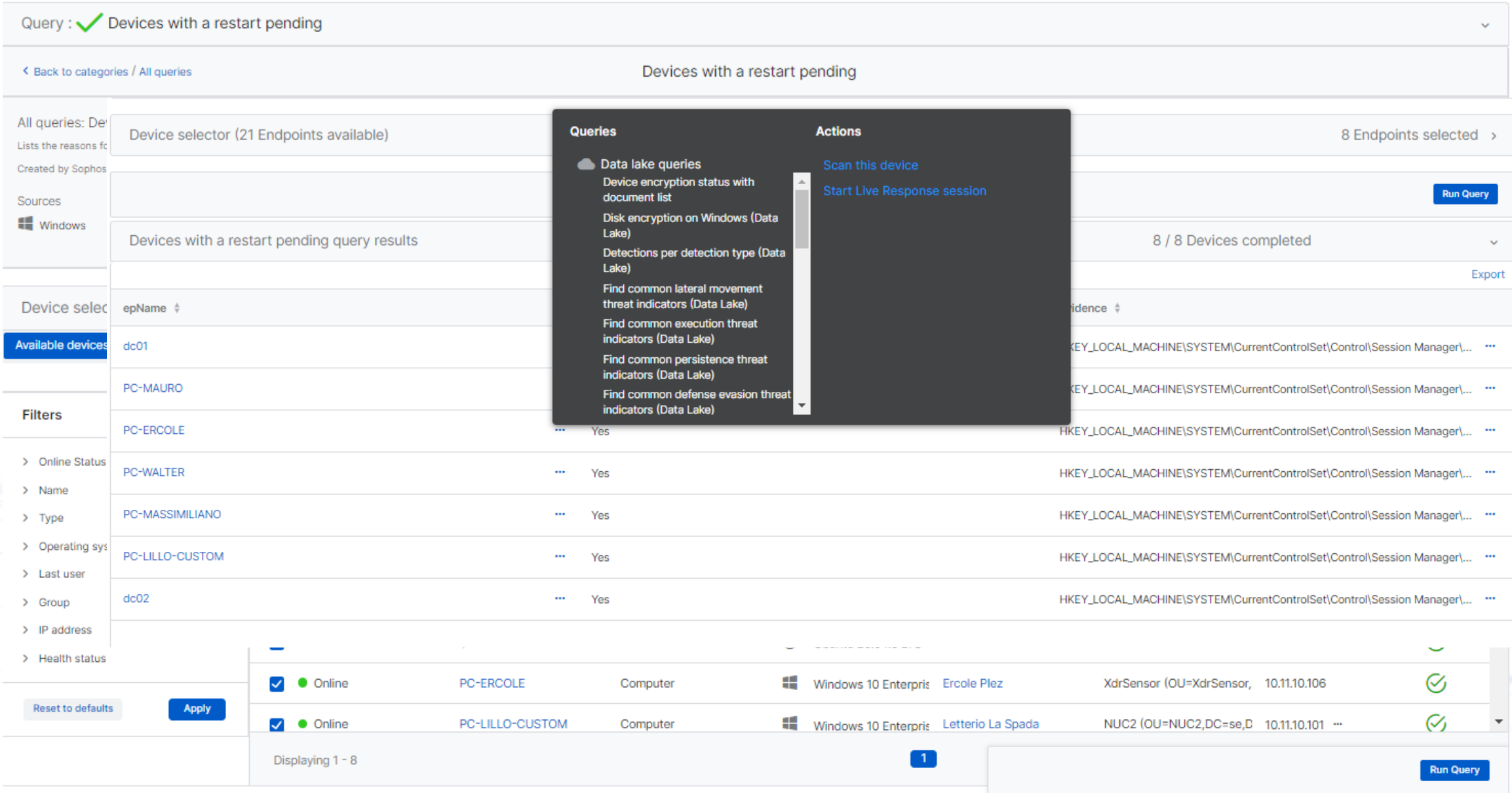
Forensic Investigation

Threat Hunting & IT Operations Hygiene

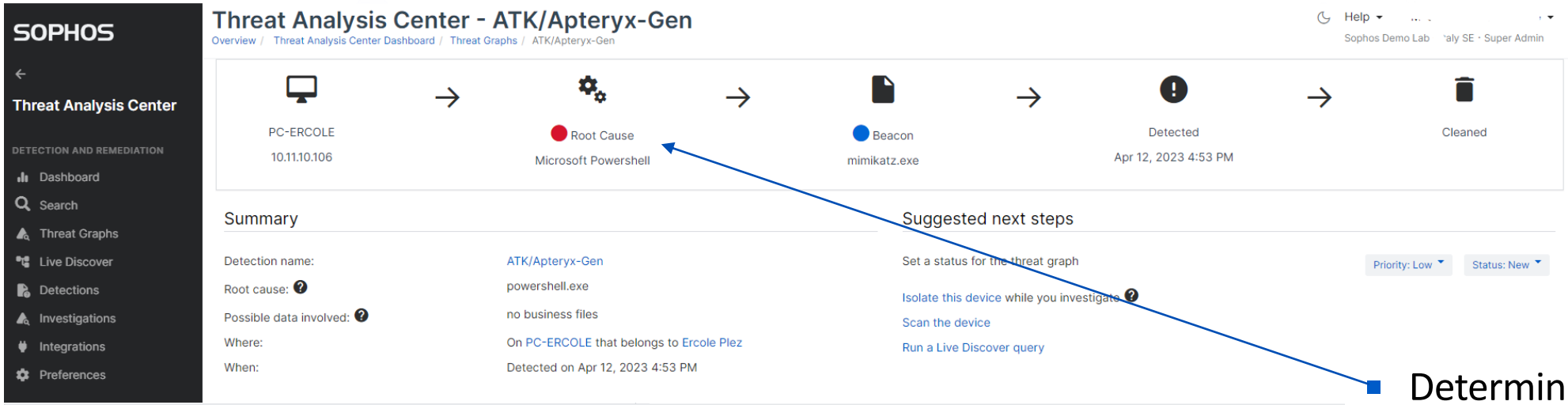
Provide Remote Support in Real Time

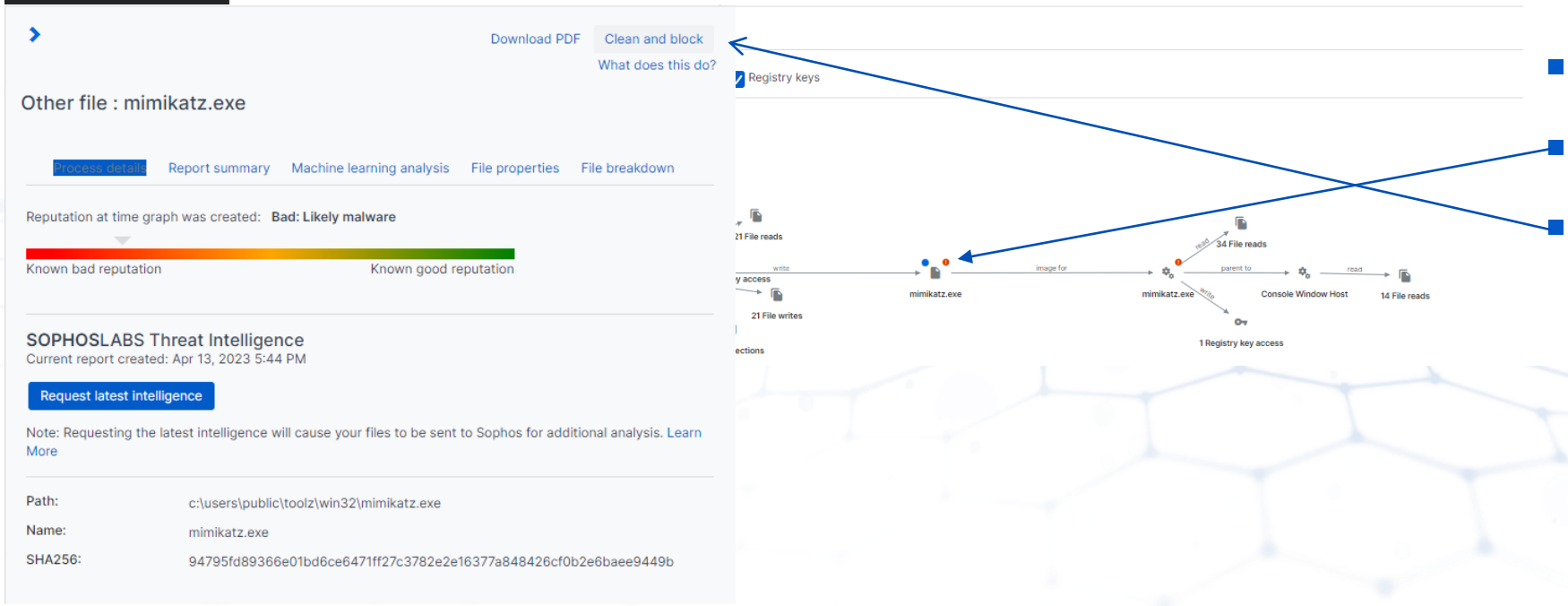
IDENTIFY HIDDEN THREATS BEFORE THE ATTACK BEGINS

Proactive Activity: Live Discovery Queries



Reactive Activity: Root Cause Analysis



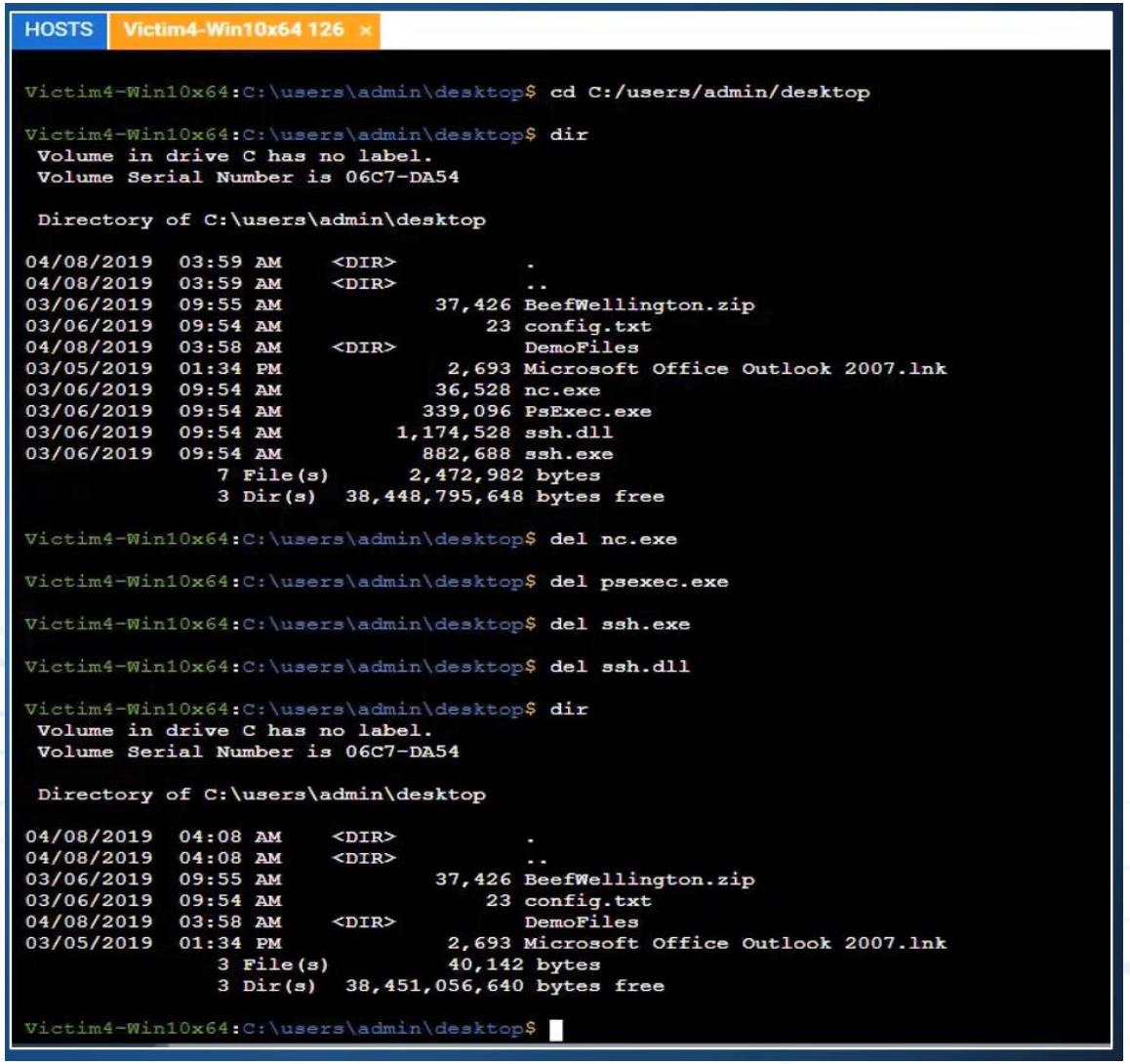


- Determine root cause
- Identify scope of threat
- See where it was neutralized
- Manually block an unwanted file

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



Cybersecurity As A Service

SOPHOS

Most Common Complains with Cybersecurity

71%

71%

CYBERSECURITY HAS BECOME TOO COMPLEX

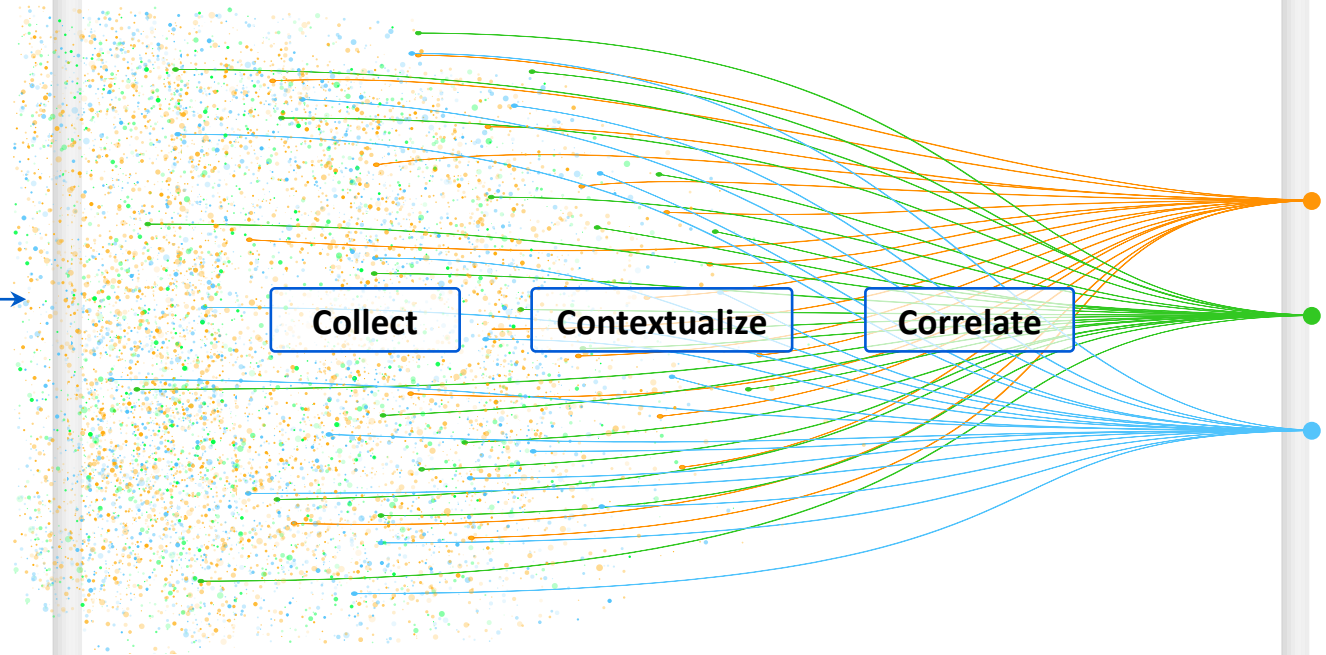
FOR MOST ORGANIZATIONS TO MANAGE EFFECTIVELY

Sophos MDR Complete

Event Sources

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identity
- Network

Threat Analysis and Correlation



Sophos MDR Complete

24/7 Managed Detection and Response Services

Full-Scale Incident Response

Root Cause Analysis and Remediation

$1M Breach Protection Warranty

Proactive Threat Hunting

Expert-Led Threat Investigation

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

Sophos Service Tiers

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

SOPHOS

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

Sophos MDR

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

- XDR Sophos XDR
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email
- Ep Sophos Endpoint

Endpoint - FREE

Microsoft, CROWDSTRIKE, SentinelOne, TREND MICRO, Symantec (A Division of Broadcom), Trellix, Malwarebytes, BlackBerry CYLANCE

Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO, SONICWALL, WatchGuard

Cloud SaaS

aws, Google Cloud, orca security

Email

mimecast, proofpoint

Identity

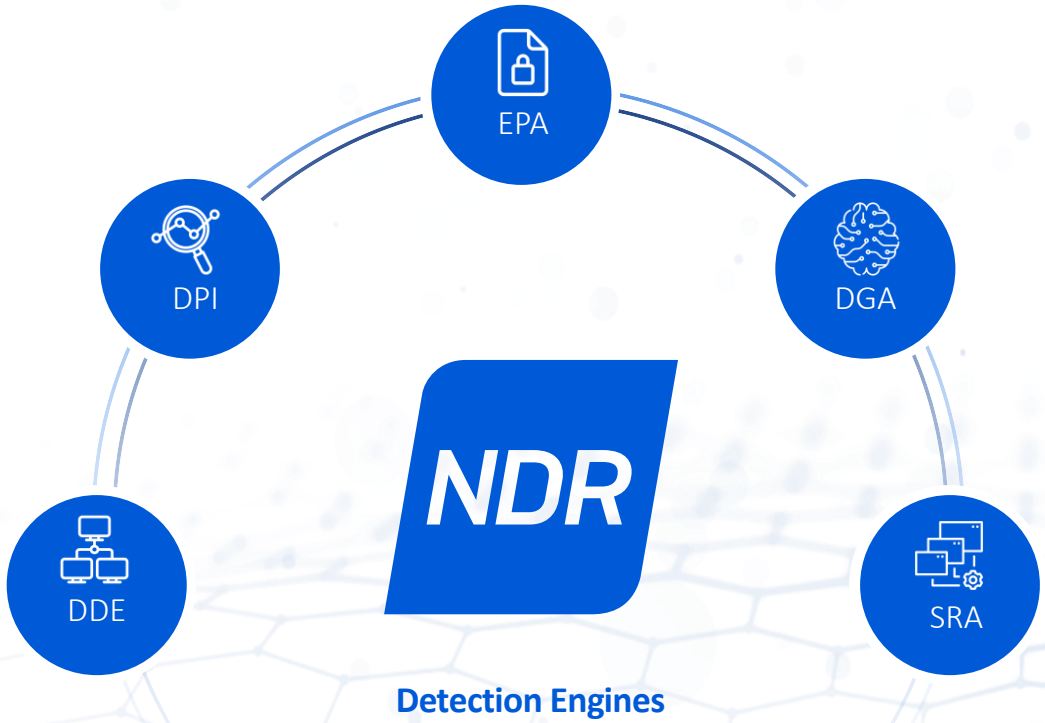
okta, DUO, ManageEngine

Network

DARKTRACE, THINKST CANARY, Skyhigh Security

SOPHOS

Sophos NDR

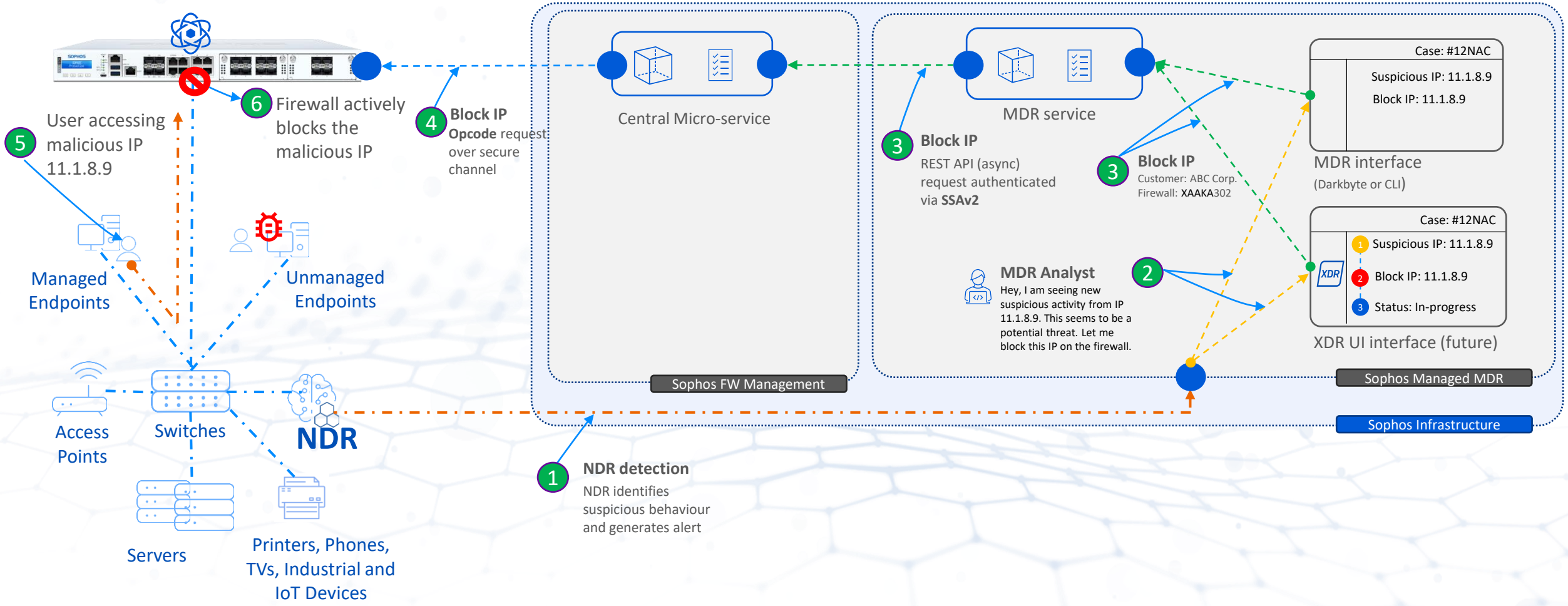


Overview

- 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



SOPHOS

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 3rd 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

For full terms and conditions of the warranty see www.sophos.com/legal.

SOPHOS

Want to Know more?

SOPHOS

SOPHOS State of Ransomware 2023 Report

Download the full report

www.sophos.com/ransomware2023

SOPHOS

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://attackevals.mitre-engenuity.org/results/enterprise?vendor=sophos&evaluation=turla&scenario=1

Questions & Answers

SOPHOS

Cybersecurity delivered.