

Anatomy of a cyberattack

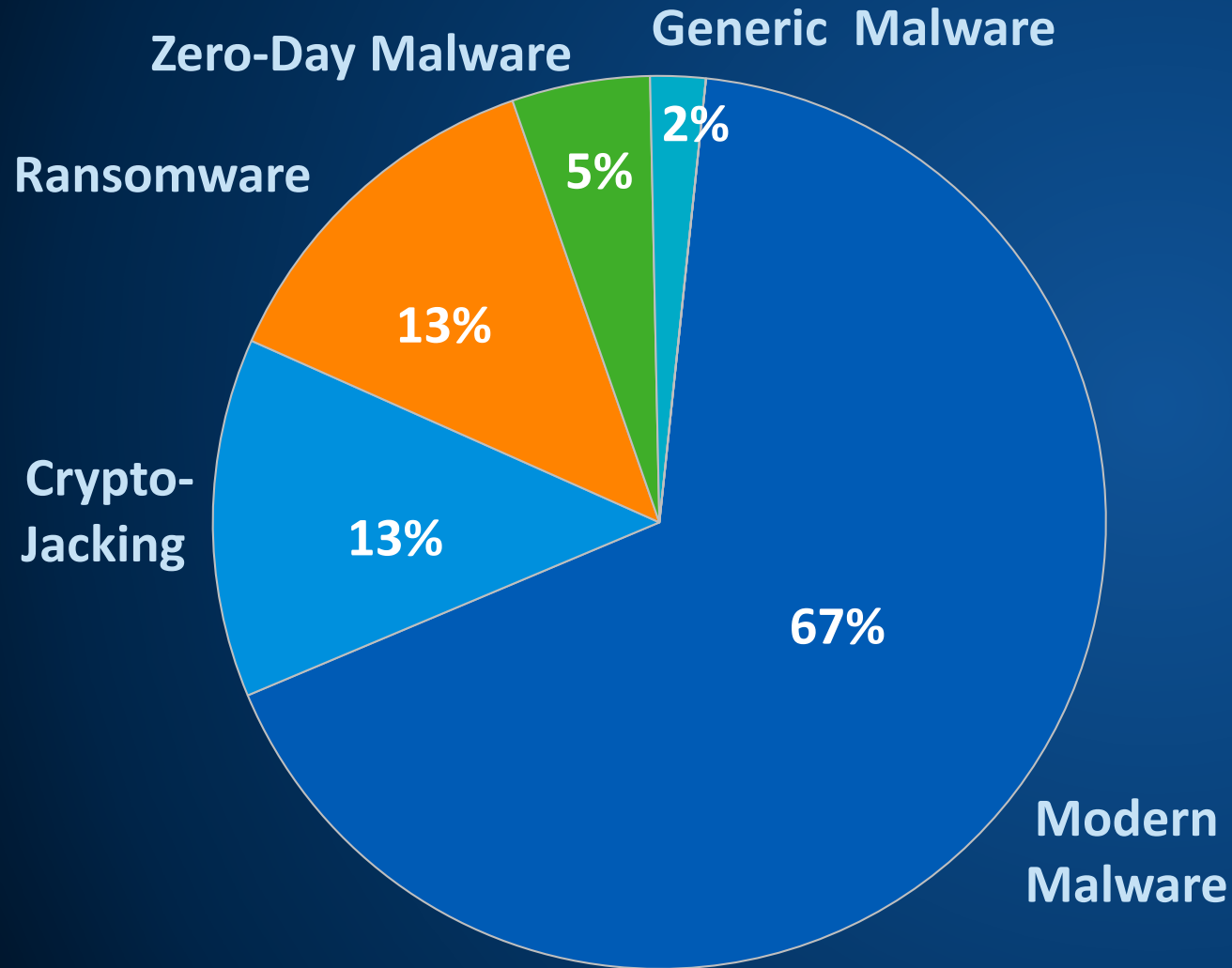
Forensics made simple with Artificial Intelligence

Peter Skondro
Senior Sales Engineer

SOPHOS

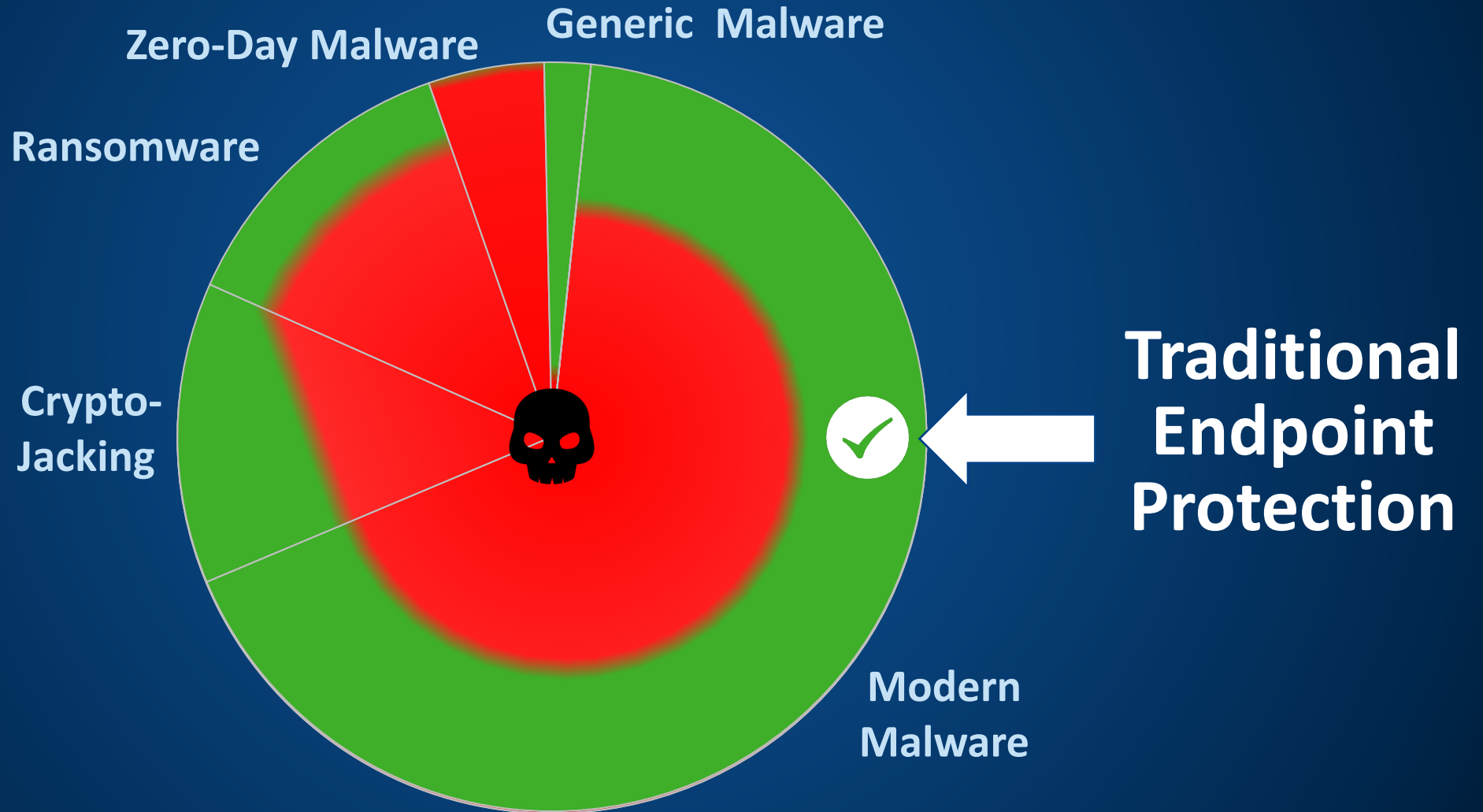
Threat Landscape

Which malware types are we dealing with today?

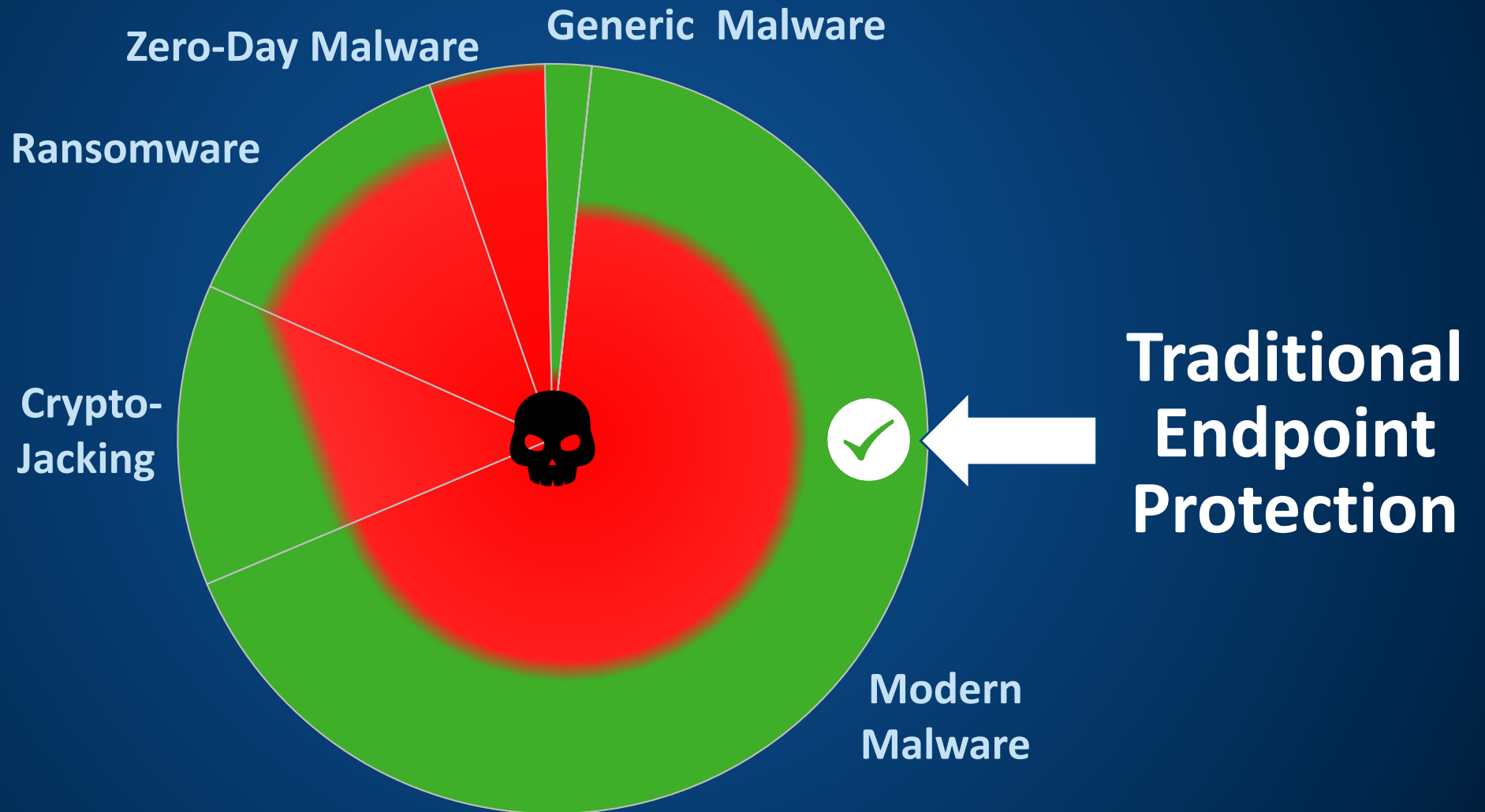


- **Generic Malware**
 - Variations of known Malware / Toolkits
- **Modern Malware**
 - (Known) Exploits, privilege escalation, password theft, persistence
 - Combination of several techniques
- **CryptoJacking**
 - Unauthorized use of CPU computing time for crypto currency mining
- **Ransomware**
 - Unauthorized encryption of files and hard disks
- **Zero-Day Malware**
 - Zero-Day attacks with several steps
 - Worms, Trojans, VB Script, PDF, file-less attacks

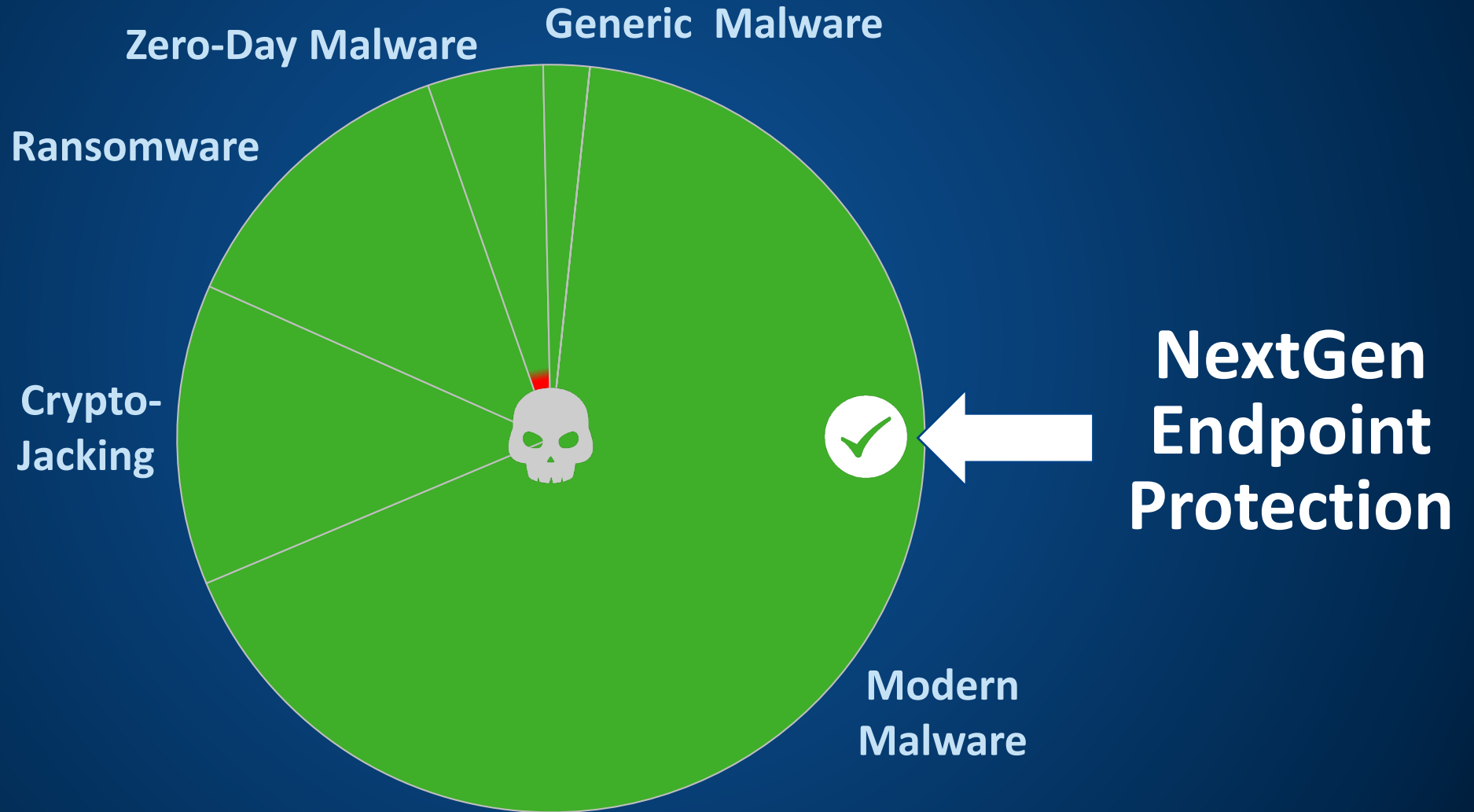
Protection with **traditional** Endpoint Protection



Protection with **NextGen** Endpoint Protection



Protection with **NextGen** Endpoint Protection



Evolution of Endpoint technologies

Past

Protection against known malware variants

Traditional Endpoint Protection

- Antivirus Signatures & Heuristics
- Control of infection paths

Yesterday

Protection against Ransomware and Exploits

NextGen Endpoint Protection

- Machine Learning
- Exploit Prevention
- Ransomware Detection

Today

Protection against Hacking & Advanced Persistent Threats

Endpoint Detection and Response

- Holistic integration of endpoint technologies
- Detection, containment and threat analysis



Endpoint Detection and Response

What is EDR (Endpoint Detection & Response)?

EDR is a holistic endpoint security approach focusing on

- **Detection of** security incidents
- **Reaction** to security incidents
- **Search** for threats
- **Forensic Investigation** after an incident



integrates all EDR components in a single solution

Why use EDR tools?

- On the **Endpoint**
 - most **Hacker activities** take place
 - we can find a lot of **valuable data**
- **Pure Endpoint Protection** solutions
 - Detect and log only clearly **malicious behavior**
 - Have only limited **reaction** capabilities
- Tightened **compliance requirements** for data protection
- EDR Tools enable the complete **management** of a security incident

EDR helps customers during a security incident

Am I under attack?

Is the threat over?

What is this file?

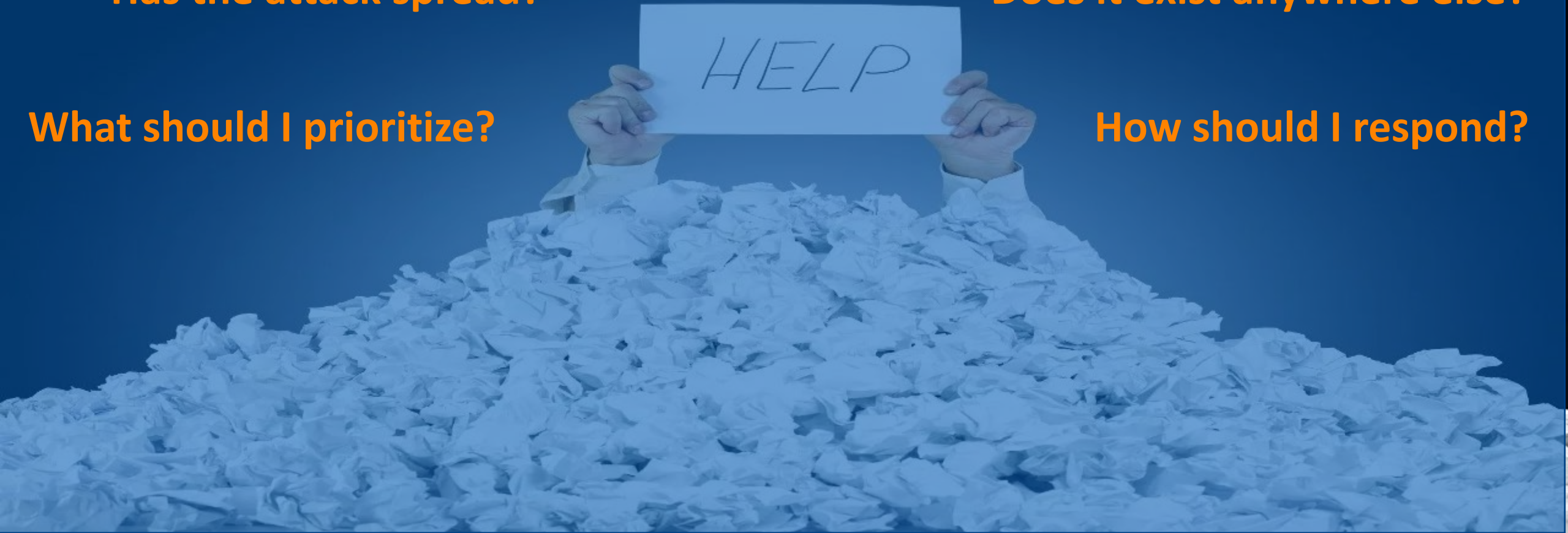
Are we out of compliance?

Has the attack spread?

Does it exist anywhere else?

What should I prioritize?

How should I respond?



Artificial Intelligence

Predictive Security

To foretell with precision of calculation, knowledge,
or shrewd inference from facts or experience



Better
Protection

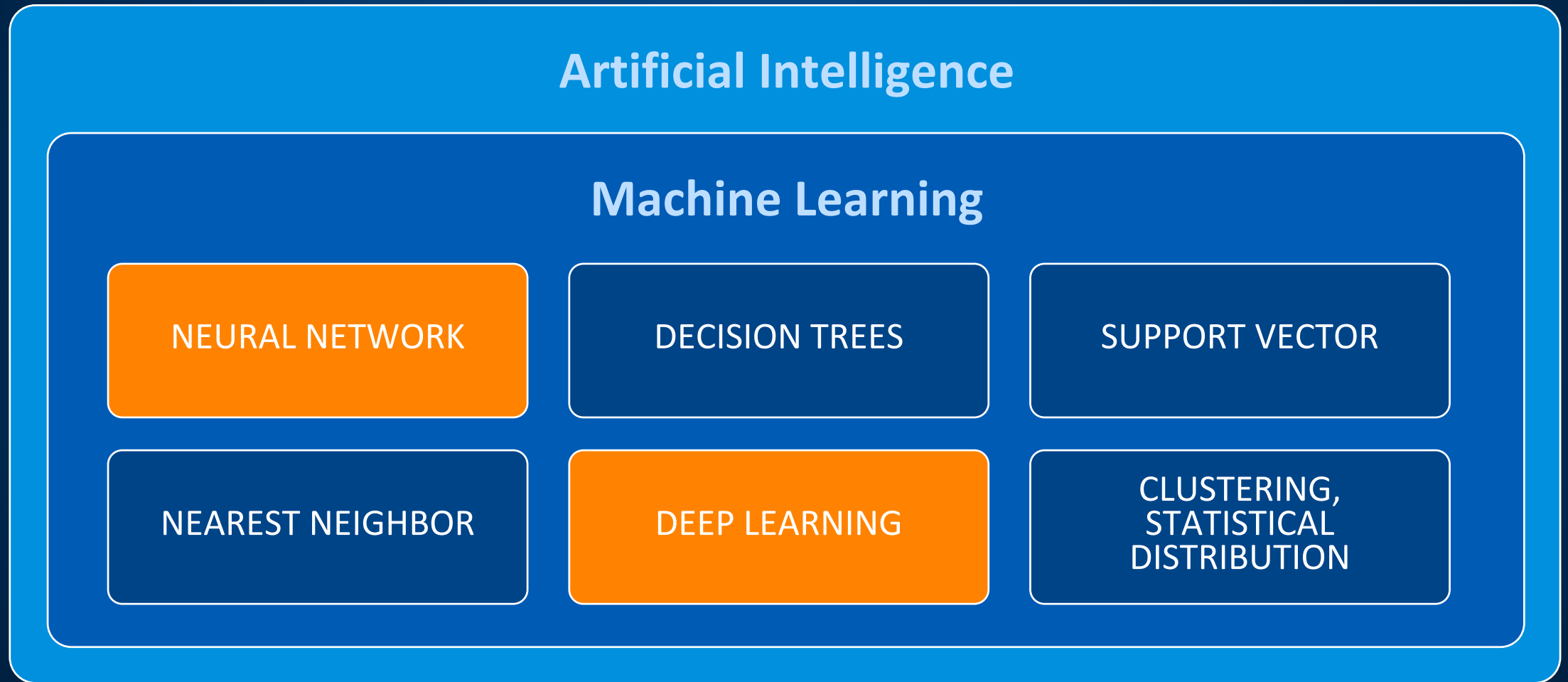


Better
Performance



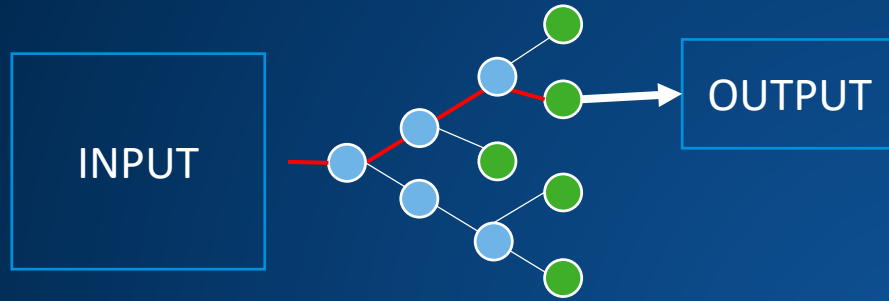
Better
Accuracy

The World of Artificial Intelligence (AI) in Cybersecurity



Machine Learning vs. Deep Learning

MACHINE LEARNING

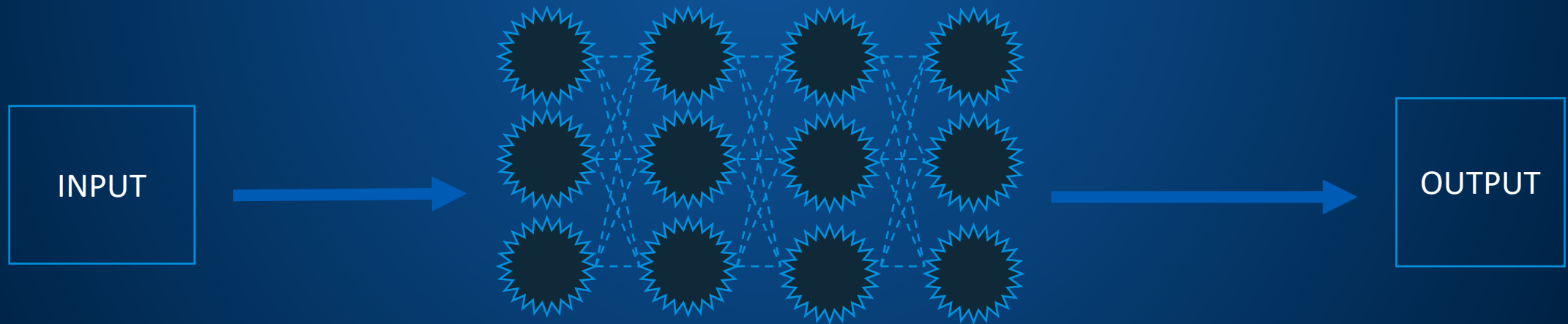


Decision Tree



Random Forest

DEEP LEARNING



Interconnected Layers of Neurons, Each Identifying More Complex Features

Deep Learning Neural Network



SMARTER

DEEP LEARNING

- High Detection Rates
- Gets Better with More Data



FASTER

20 – 100 ms
Detection



SMALLER

10 – 20 MB
Model Size

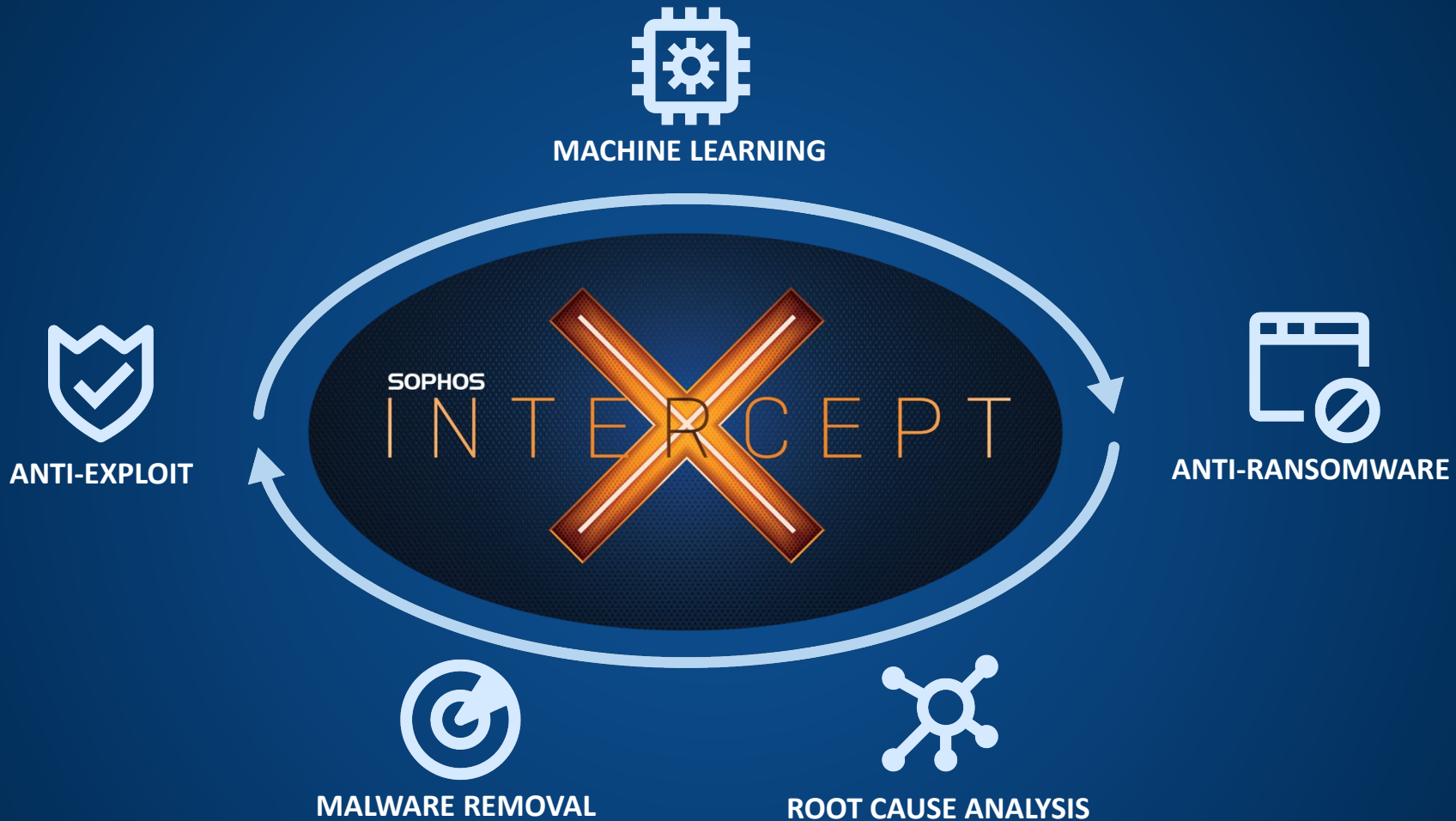
TRADITIONAL MACHINE LEARNING

- Low Detection Rates
- Diminishing Returns with More Data

100 – 500 ms
Detection

500 MB to 1 GB
Model Size

Intercept X for Endpoints and Servers

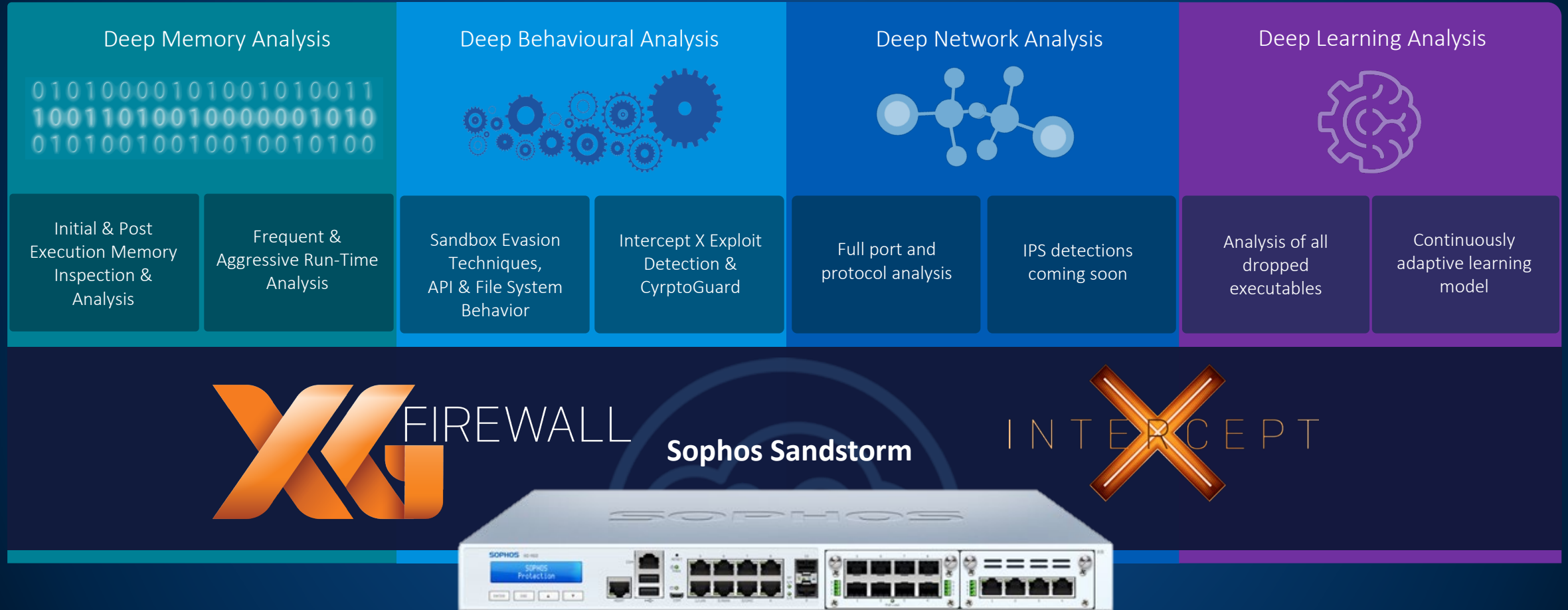


STOP UNKNOWN THREATS

PREVENT RANSOMWARE

DENY THE ATTACKER

Sandboxing - Sandstorm Deep Threat Prevention



Analysis with Machine Learning Assistance

SOPHOS

Root Cause Analysis

Threat Analysis Center - CryptoGuard

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Detected Threat Cases](#) / [CryptoGuard](#)

Help ▾ Peter Skondro ▾
Sophos Ltd · Super Admin



CentralW10
169.254.59.72



Root Cause
Outlook



Beacon
ransomware.exe



Detected
Jan 28, 2019 3:57 PM



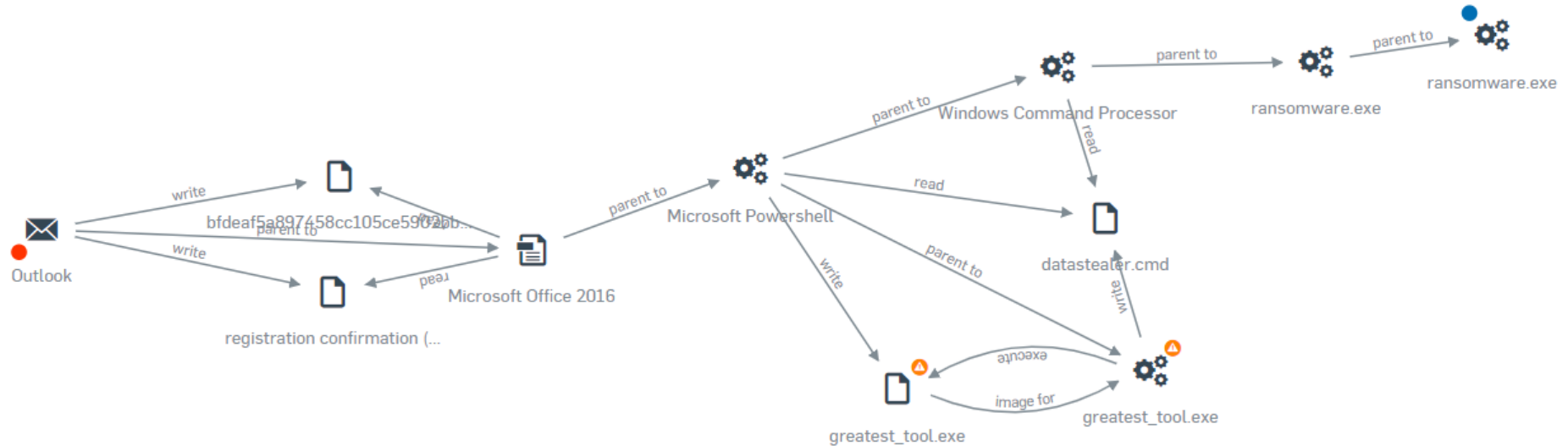
Cleaned

Analyze

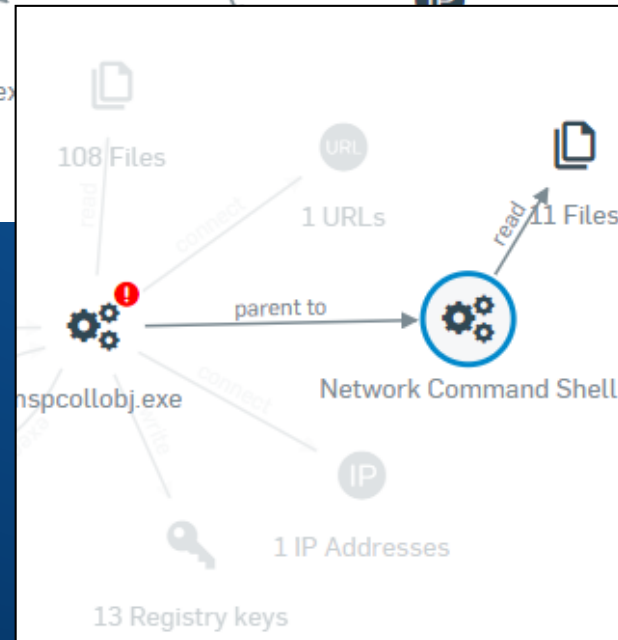
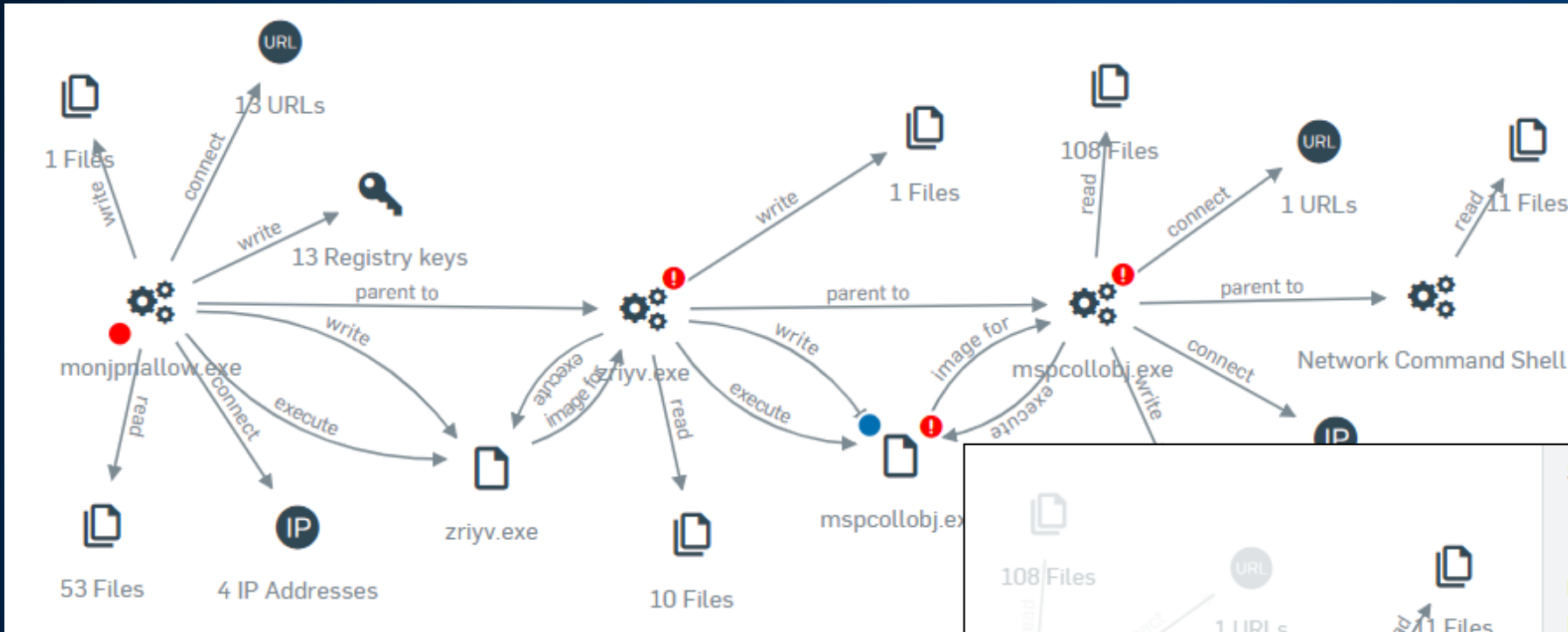
Case record

Filters: ☒ Processes ☒ Other files ☒ Business files ☒ Network connections ☒ Registry keys

Show direct path ▾



Example: EMOTET



SOPHOSLABS Threat Intelligence

Request latest intelligence

No current intelligence on this file.

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

Path: c:\windows\syswow64\netsh.exe

Name: netsh.exe

Command line:

netsh.exe advfirewall firewall delete rule name="Remote Assistance (50383)"

Process ID: 6252

Process executed by: NT AUTHORITY\SYSTEM

Machine Learning Analysis

[Download PDF](#) [Search for item](#) [Clean and block](#)
What does this do?

Other file : greatest_tool.exe

[Process details](#) [Report summary](#) [Machine learning analysis](#) [File properties](#) [File breakdown](#)

SOPHOSLABS Threat Intelligence

Current report created: Jan 28, 2019 2:30 PM

Global reputation

Known bad reputation

Known good reputation

Prevalence:

First seen: Not available

Last seen: Not available

AV detection: No Detection

Machine learning analysis:

- Attributes **51% Suspicious**
- Code similarity **80% Suspicious**
- File/path **80% Suspicious**

SOPHOSLABS Threat Intelligence

Current report created: Jan 28, 2019 2:30 PM

Attributes : 51% Suspicious
Analyzed over 29 million known good and over 15 million known bad items

Attribute	Seen in:	Known bad files	Known good files
Findcrypt: "Uses constants related to AES"		43.9k	67.3k
Compilation Date: "2018-Apr-30 12:00:00"		34	22
[!] The program may be hiding some of its imports: "Ge...		665.9k	1.2M
Stack Canary: "disabled"		672.7k	1.6M
[!] The program may be hiding some of its imports: "Lo...		217.3k	428.7k

Code similarity : 80% Suspicious
Analyzed over 30 million known good and over 29 million known bad items

File	Similarity
greatest_tool.exe	56%
recuva.exe	41%
xf-3dsmax_x64_7zshare.blogspot.com_.exe	38%
portable-virtualbox_v5.1.26-starter_v6.4.10-win...	31%
_just_cause_2.exe	31%
ultrasurf_12.04.exe	28%
p.exe	

File/path : 80% Suspicious
Analyzed over 1 million known good and over 23 million known bad items

Cross Estate Threat Search

Threat Analysis Center - Threat Searches

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Threat Searches](#)

Help ▾ Peter Skondro ▾
Sophos Ltd · Super Admin

New threat search [Threat search examples](#)

Search for potential threats on your devices. You can search for file names, SHA-256 file hashes, IP addresses, domains or command lines.

Searches find PE files (like applications) with uncertain or bad reputation and network connections.

Saved searches

When you go to a saved search, the search will re-run using the saved terms.

▾

	Name	Created on
--	------	------------

Threat Analysis Center - Threat Search Results

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Threat Searches](#) / [Threat Search Results](#)

Help ▾ Peter Skondro ▾
Sophos Ltd · Super Admin

[Save search](#)

Files **2** | Network connections **1**

Search for: 1 item [View item](#)
Found on 2 devices

[What does this do?](#)

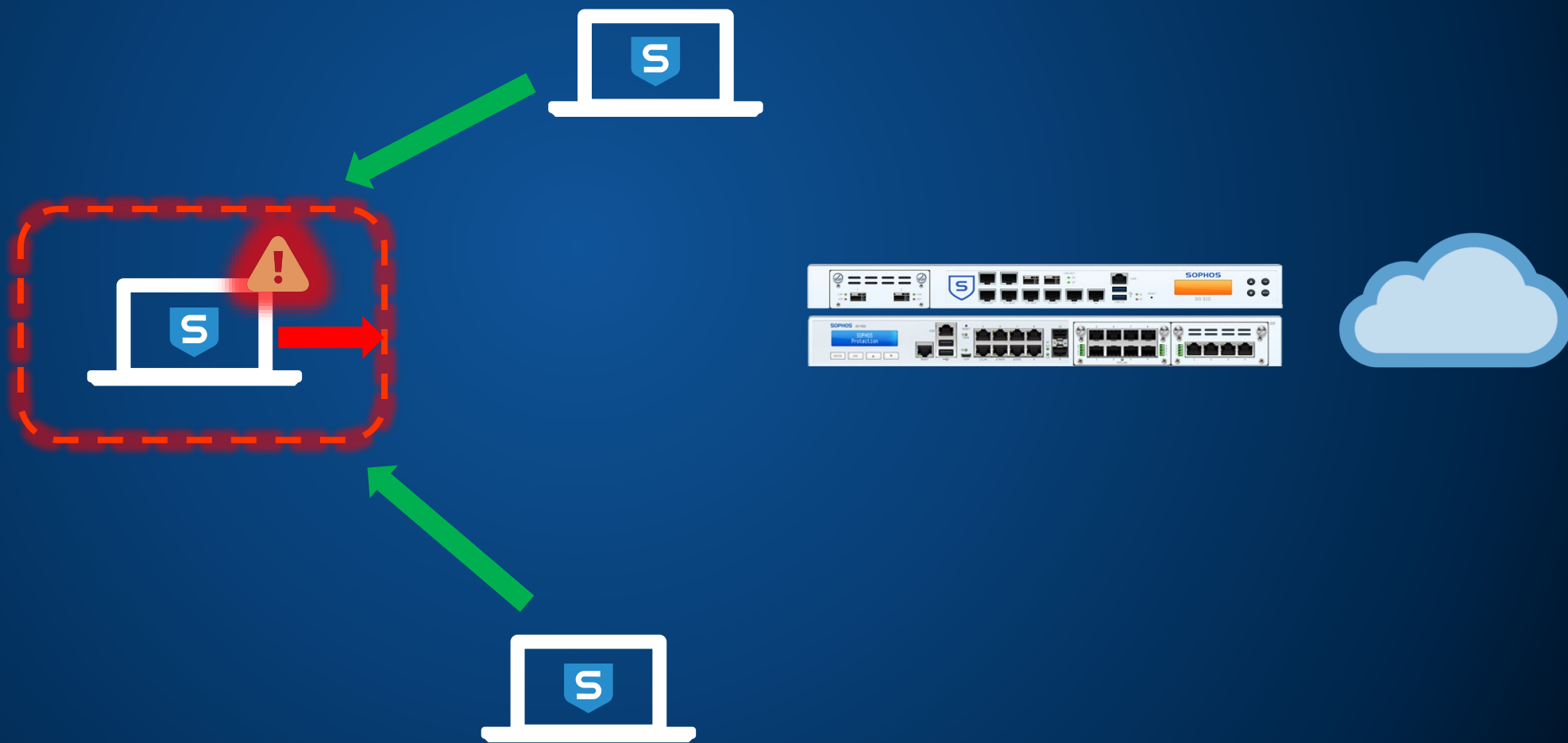
<input type="checkbox"/>	Device name	Device type	Isolated	Items found	File details
<input checked="" type="checkbox"/>	CentralW10	Computer	No	1	See details
<input checked="" type="checkbox"/>	CentralW7	Computer	No	1	See details

1 - 2 of 2 < >

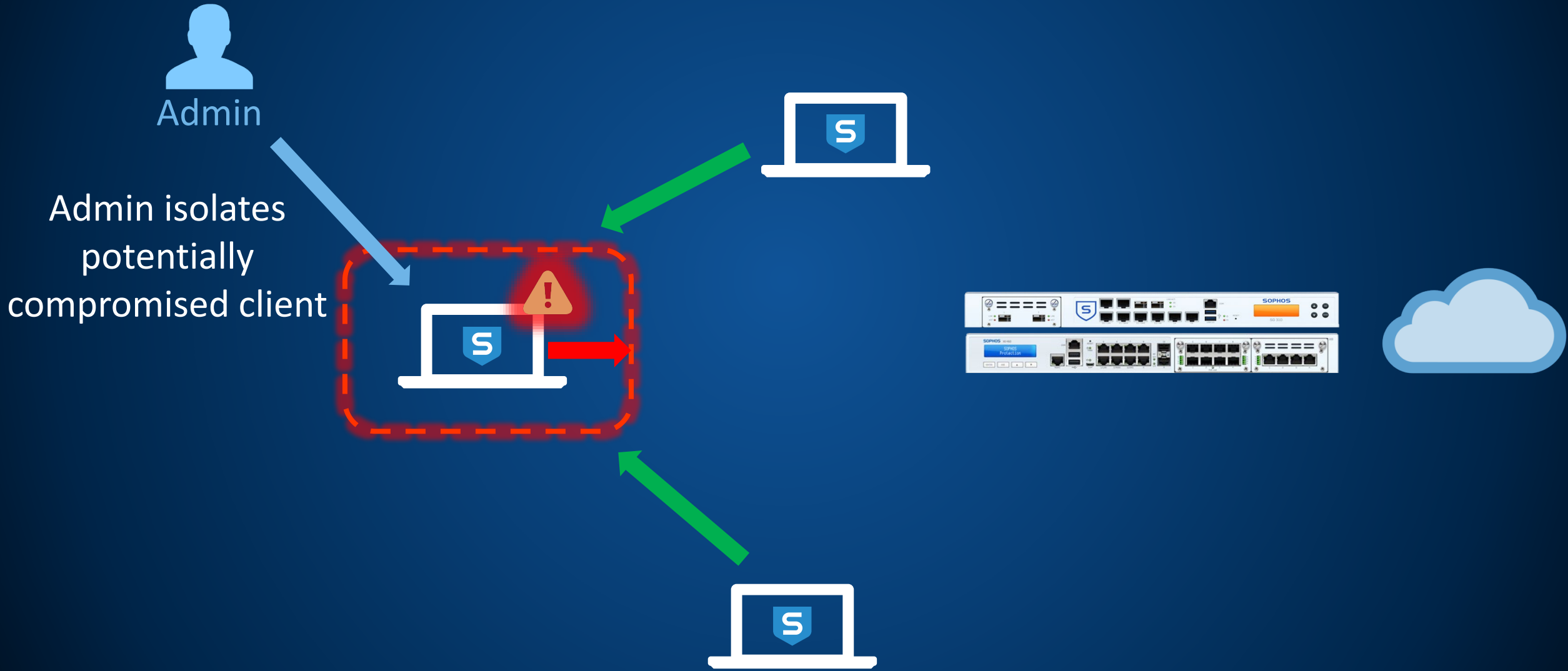
Containment of threats

Self Isolation

Infected client
Isolates himself



Admin Isolation



Traditional EDR



VISIBILITY & DETECTION

- *Incomplete protection*

- *Best Protection available on the market*



ANALYSIS & INVESTIGATION

- *Security experts required*

- *No expert knowledge required*



REACTION

- *Lengthy investigations*
- *Until manual reaction the damage might increase*

- *Automatic reaction*
- *Without delay*

Workshop:

EDR in Action

*Forensics and automatic containment of threats with
Sophos Synchronized Security*

EDR Live Demonstration
Automatic containment of threats
Lateral Movement Protection

SOPHOS

Cybersecurity made simple.