Anatomy of a cyberattack

Forensics made simple with Artificial Intelligence

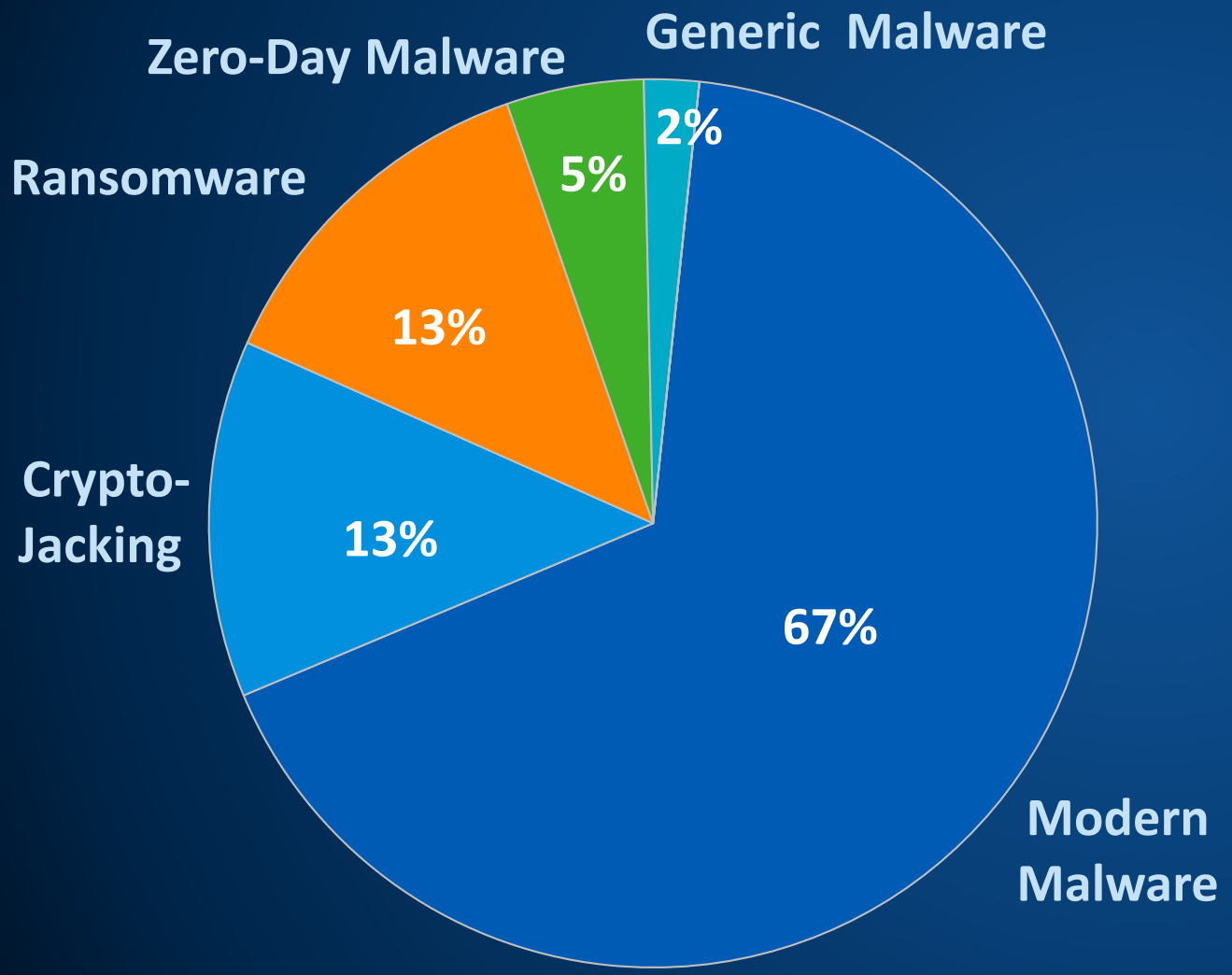
Peter Skondro
Senior Sales Engineer

SOPHOS

Threat Landscape

SOPHOS

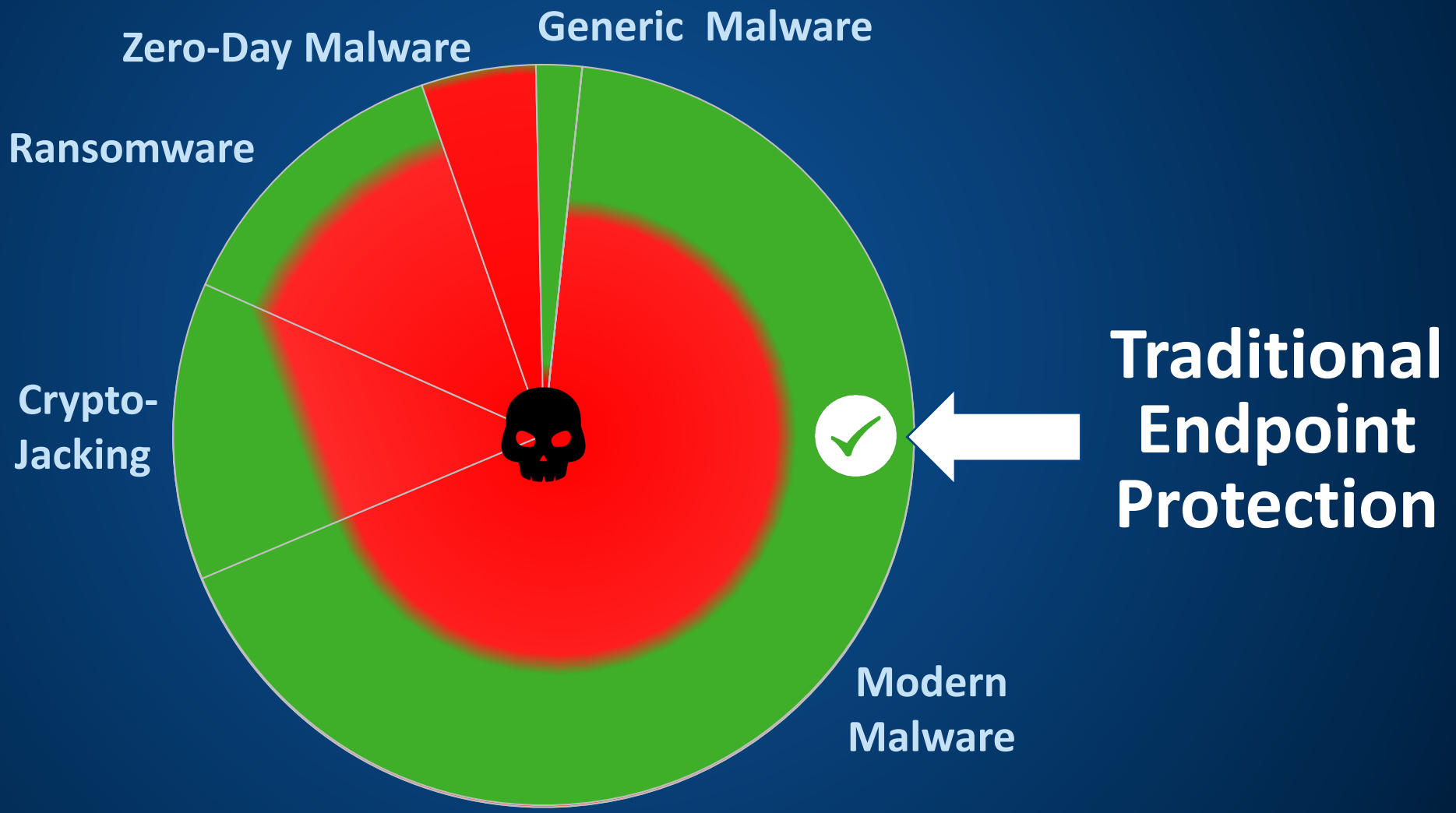
Which malware types are we dealing with today?



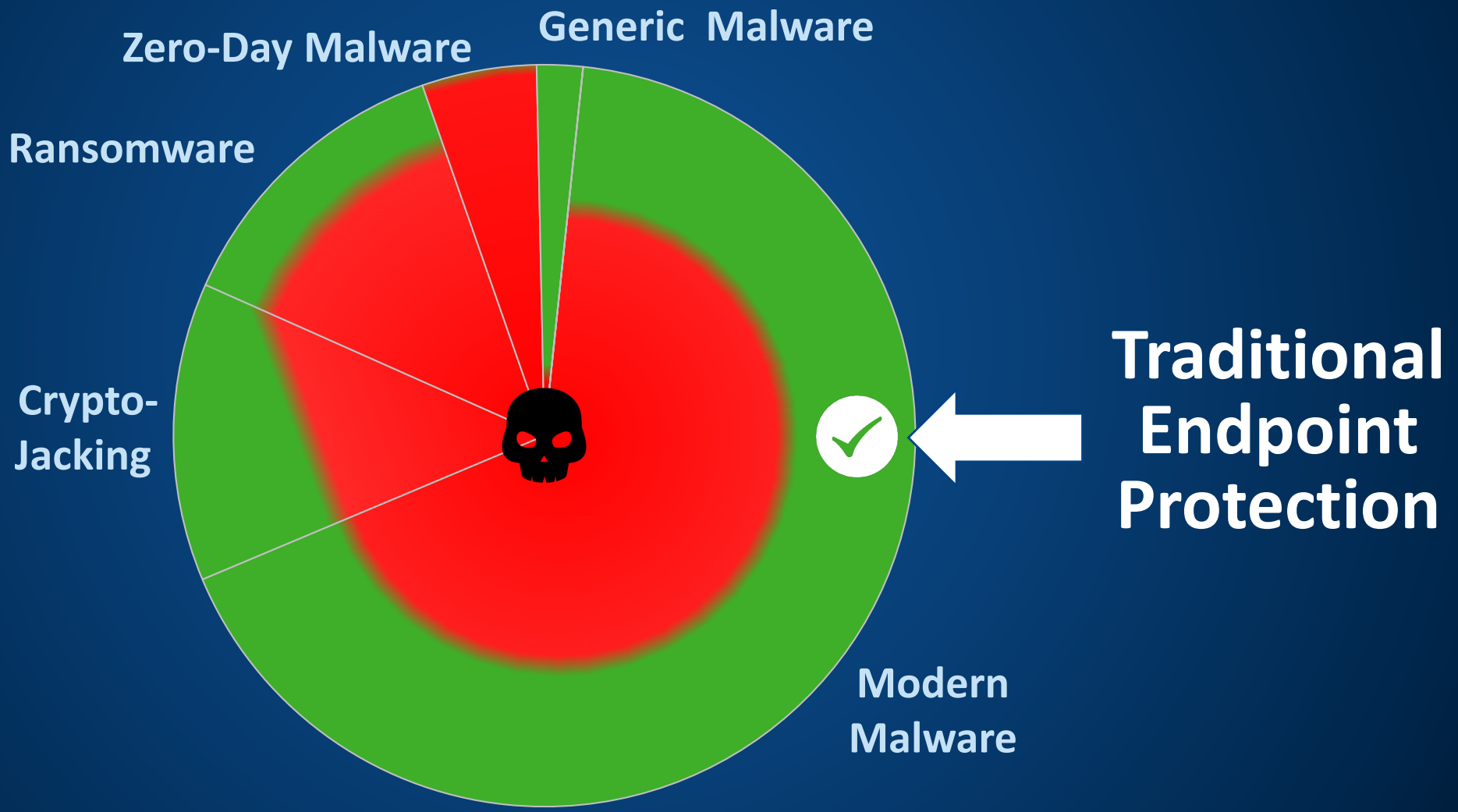
Source: SophosLabs, August 2018, Region: CEEMEA

- **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

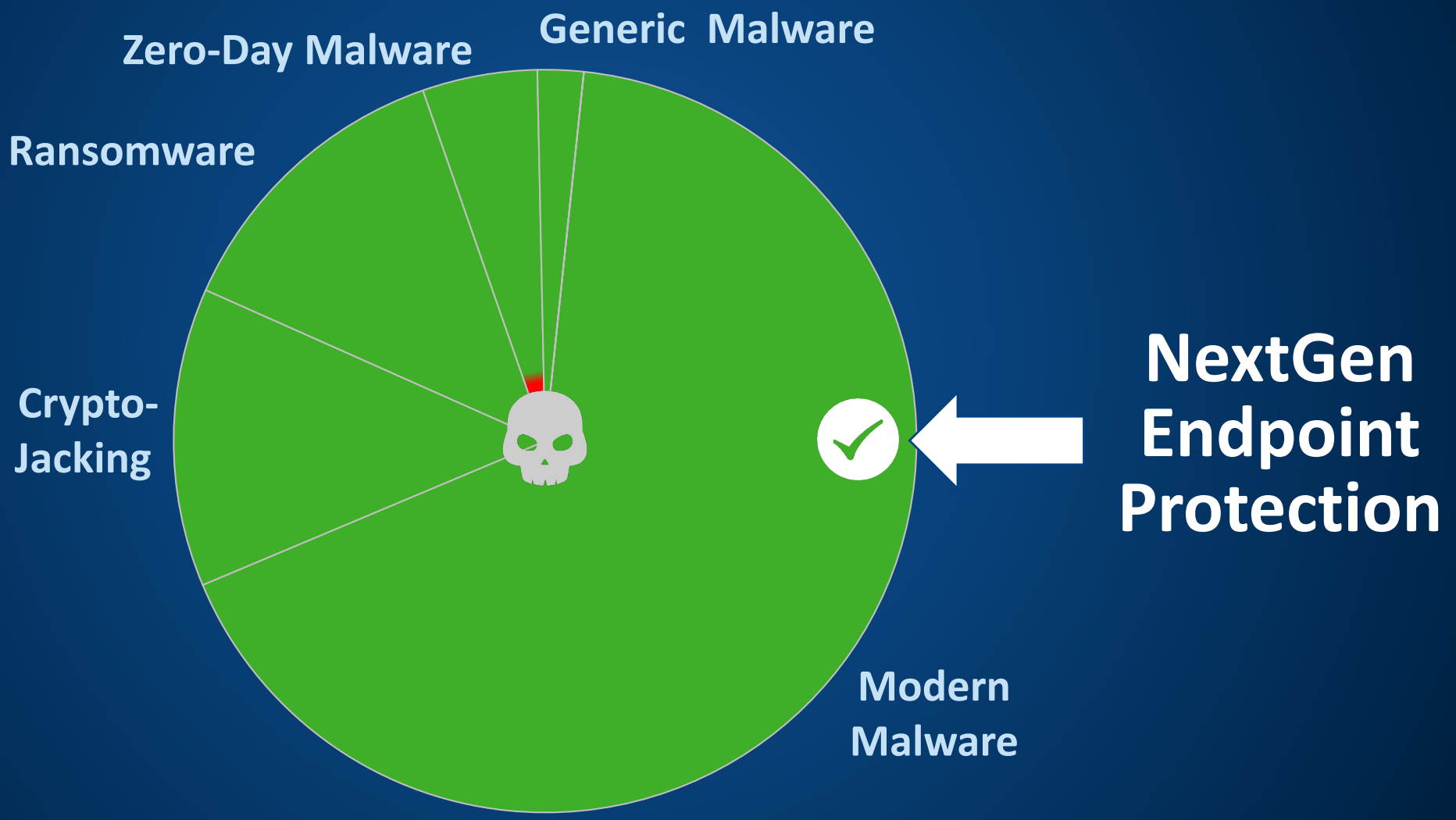
Protection with traditional Endpoint Protection



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

SOPHOS

Endpoint Detection and Response

SOPHOS

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?

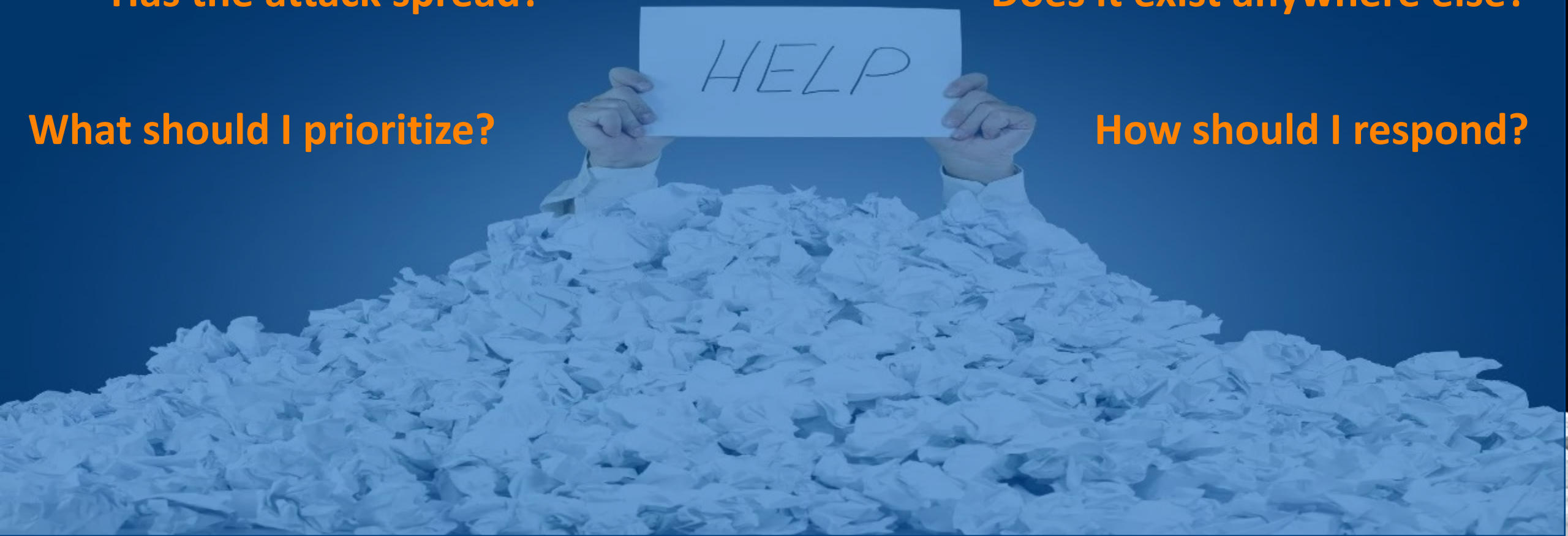
Are we out of compliance?

Has the attack spread?

Does it exist anywhere else?

What should I prioritize?

How should I respond?



Artificial Intelligence

SOPHOS

Predictive Security

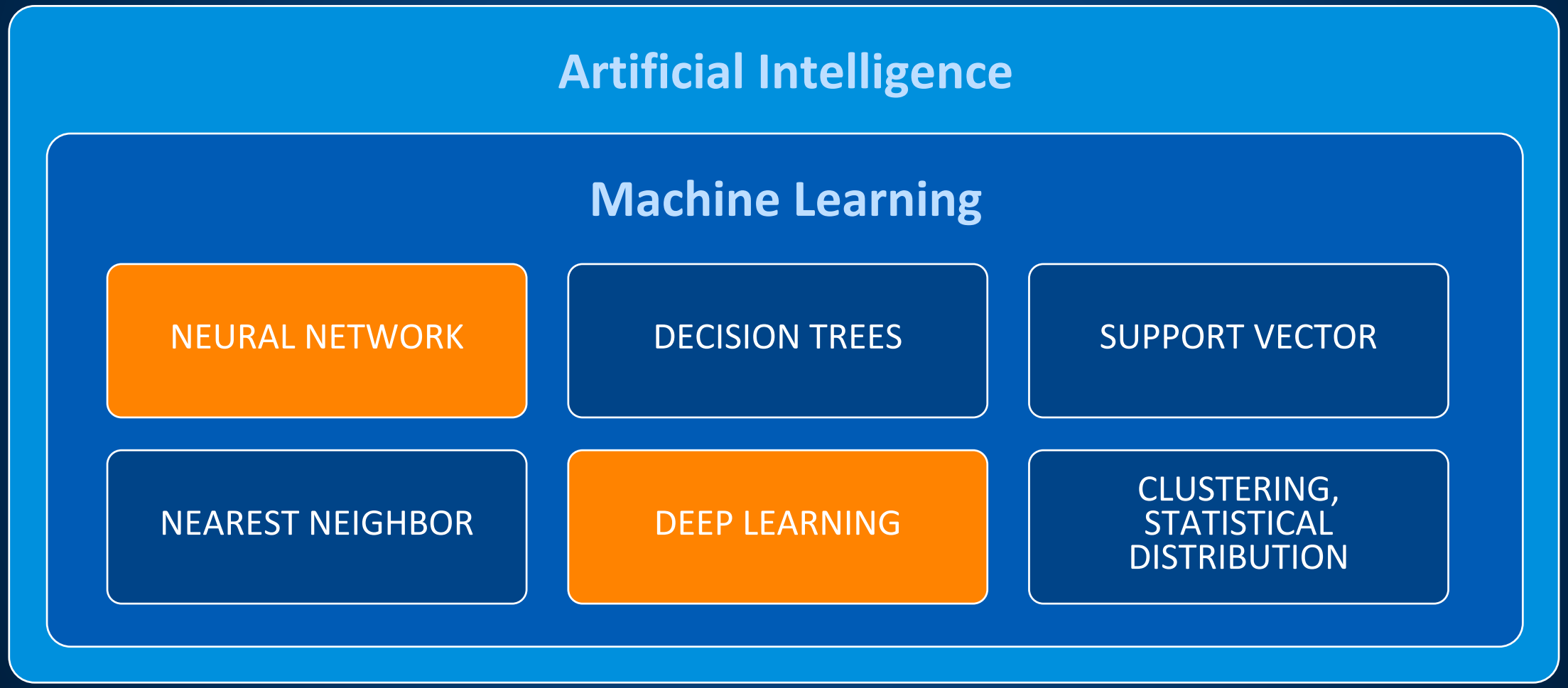
To foretell with precision of calculation, knowledge,
or shrewd inference from facts or experience

Better
Protection

Better
Performance

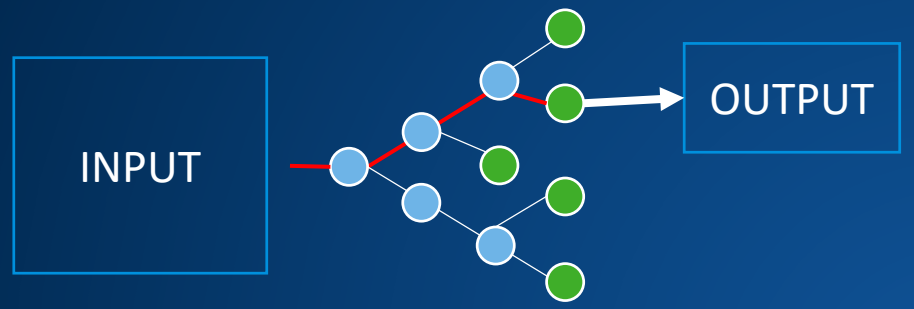
Better
Accuracy

The World of Artificial Intelligence (AI) in Cybersecurity



Machine Learning vs. Deep Learning

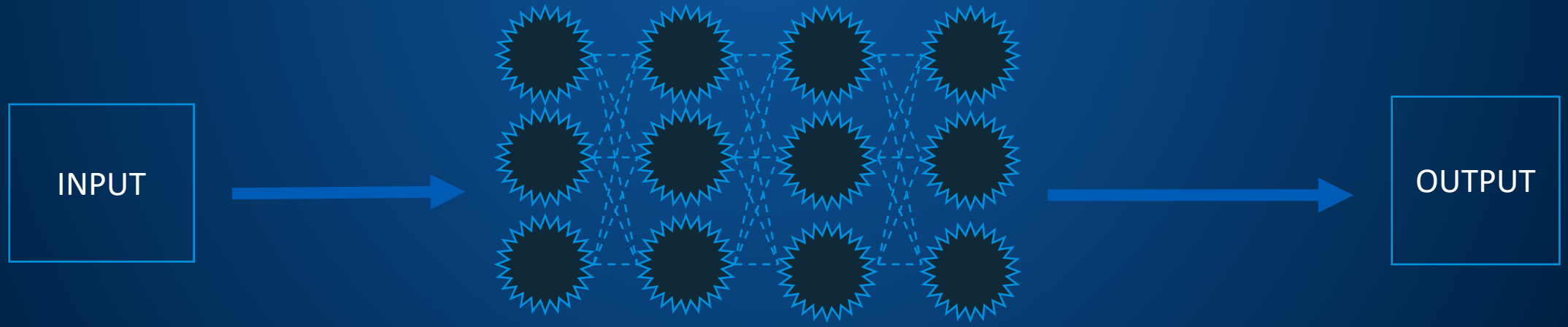
MACHINE LEARNING



Decision Tree

Random Forest

DEEP LEARNING



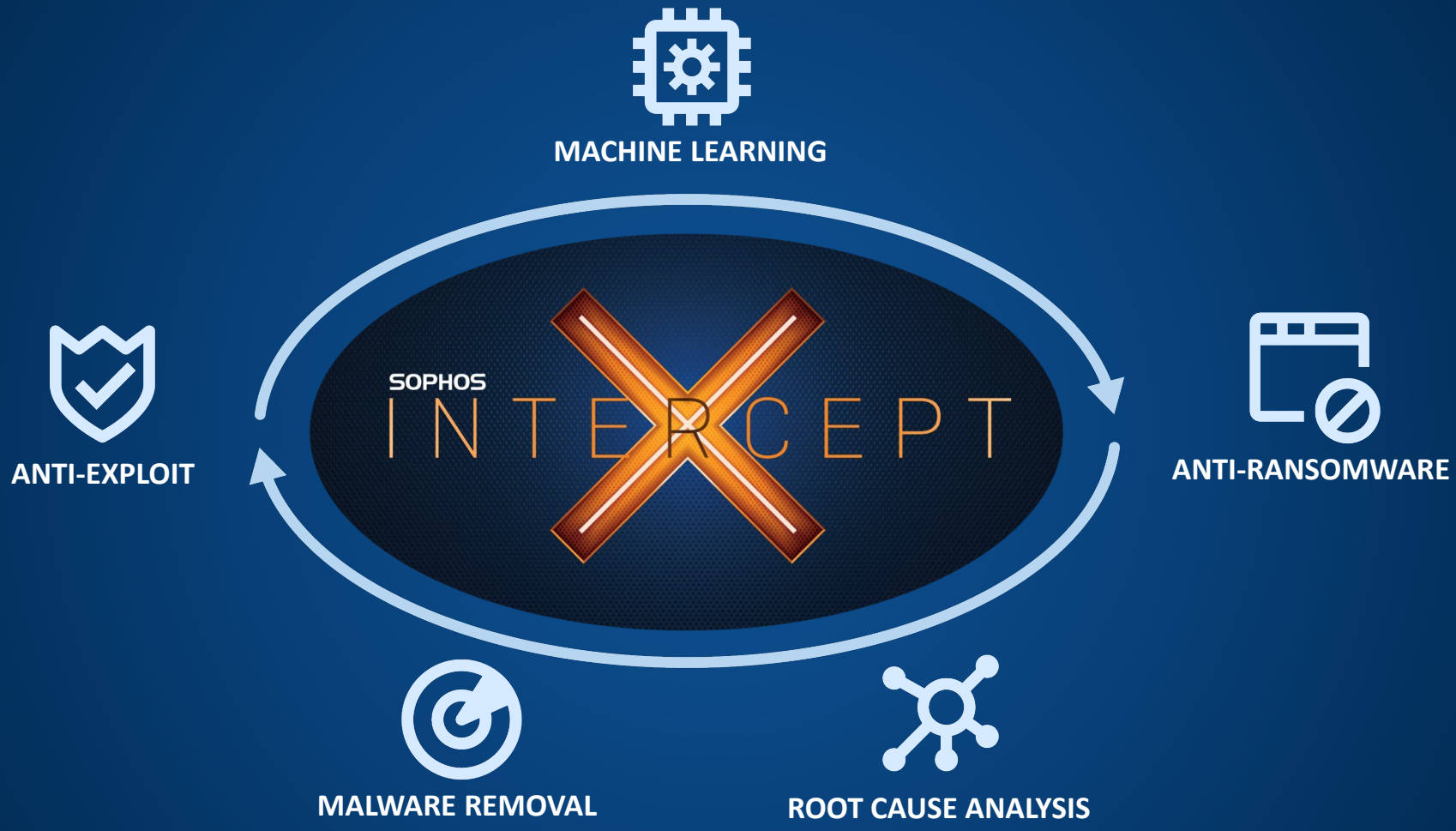
Interconnected Layers of Neurons, Each Identifying More Complex Features

SOPHOS

Deep Learning Neural Network

	SMARTER	FASTER	SMALLER
DEEP LEARNING	• High Detection Rates • Gets Better with More Data	20 – 100 ms Detection	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**

SOPHOS

Sandboxing - Sandstorm Deep Threat Prevention

Deep Memory Analysis		Deep Behavioural Analysis		Deep Network Analysis		Deep Learning Analysis	
Initial & Post Execution Memory Inspection & Analysis	Frequent & Aggressive Run-Time Analysis	Sandbox Evasion Techniques, API & File System Behavior	Intercept X Exploit Detection & CyrptoGuard	Full port and protocol analysis	IPS detections coming soon	Analysis of all dropped executables	Continuously adaptive learning model

XG FIREWALL

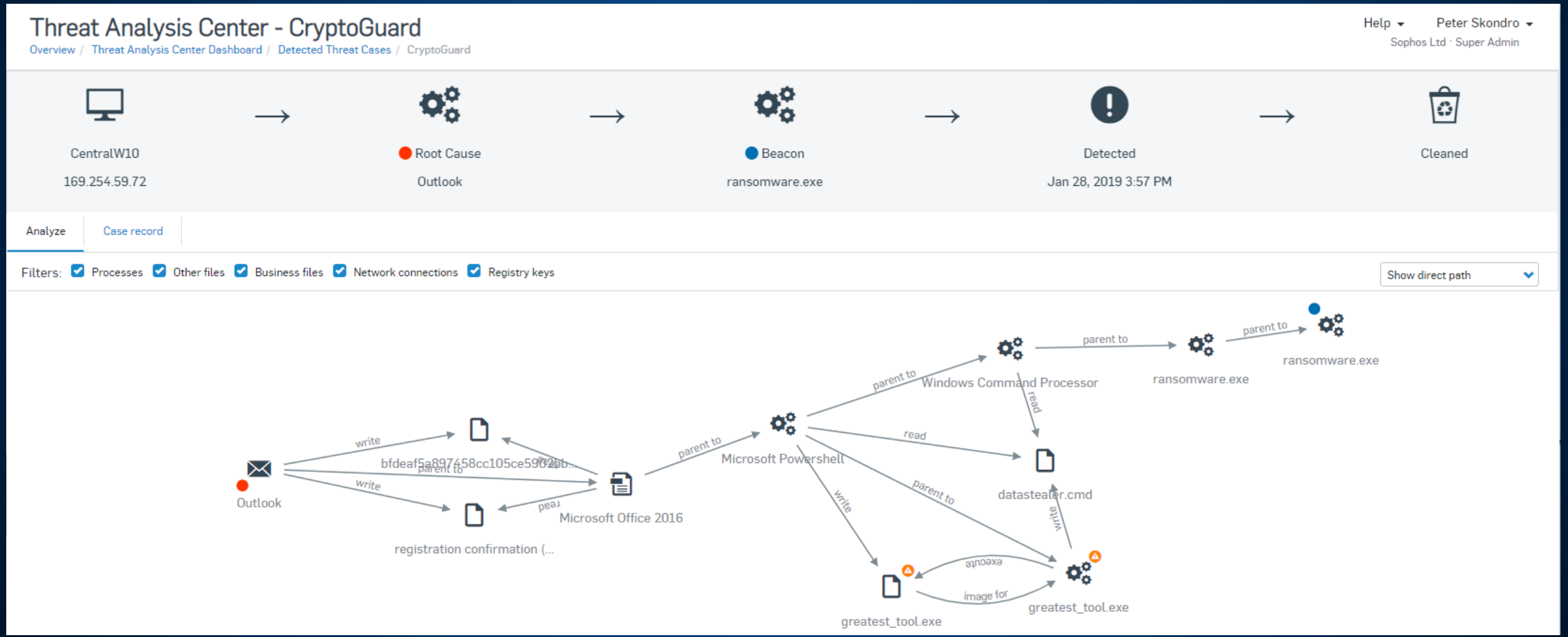
Sophos Sandstorm

INTERCEPT X

Analysis with Machine Learning Assistance

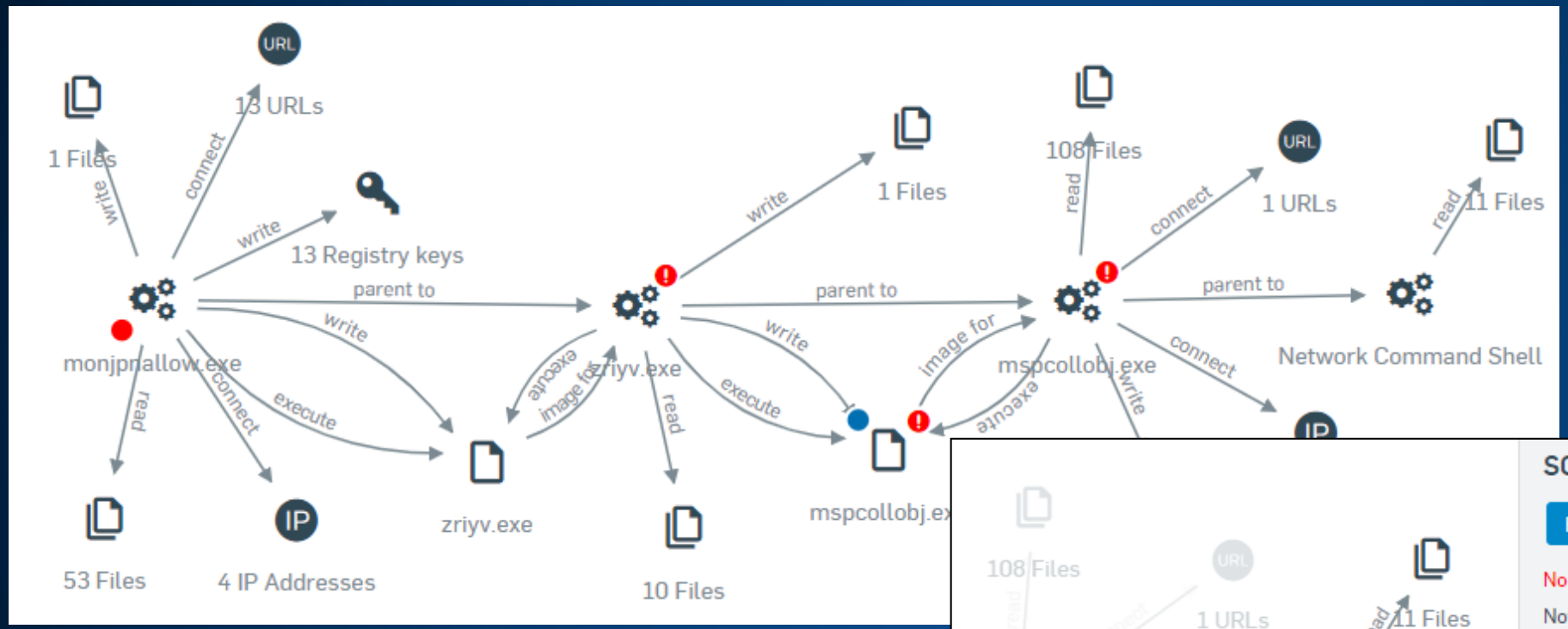
SOPHOS

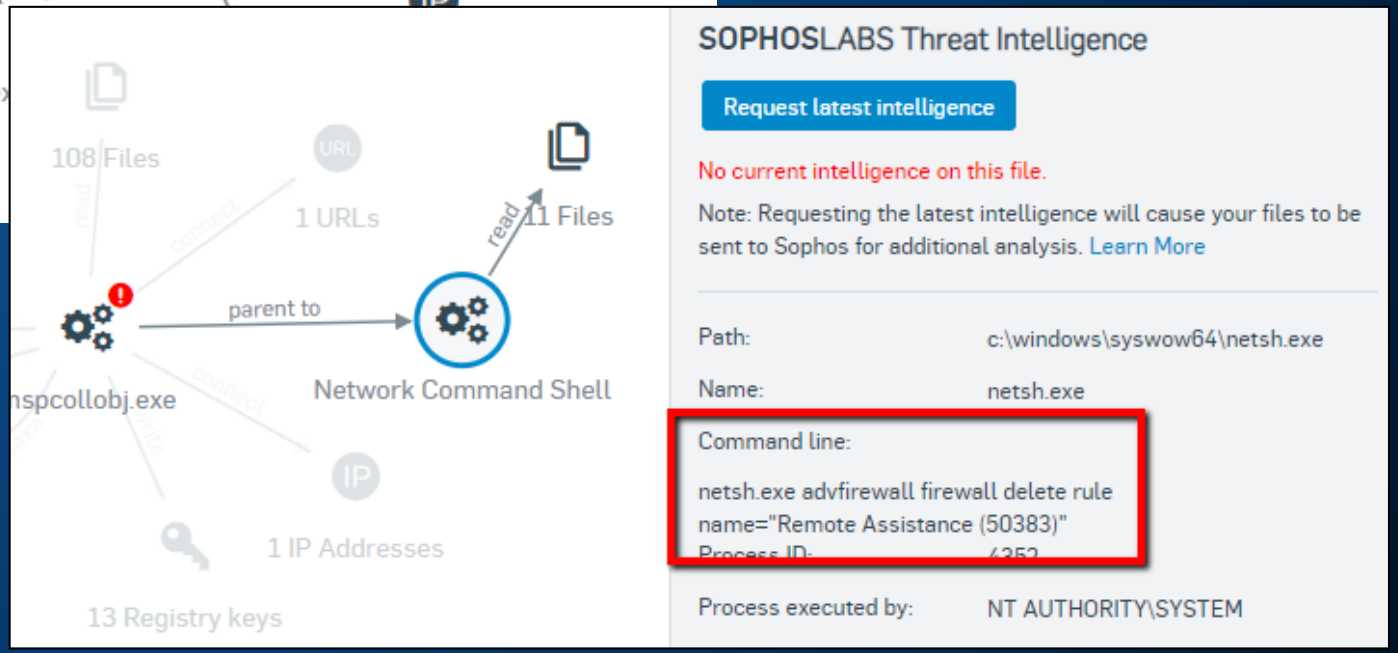
Root Cause Analysis



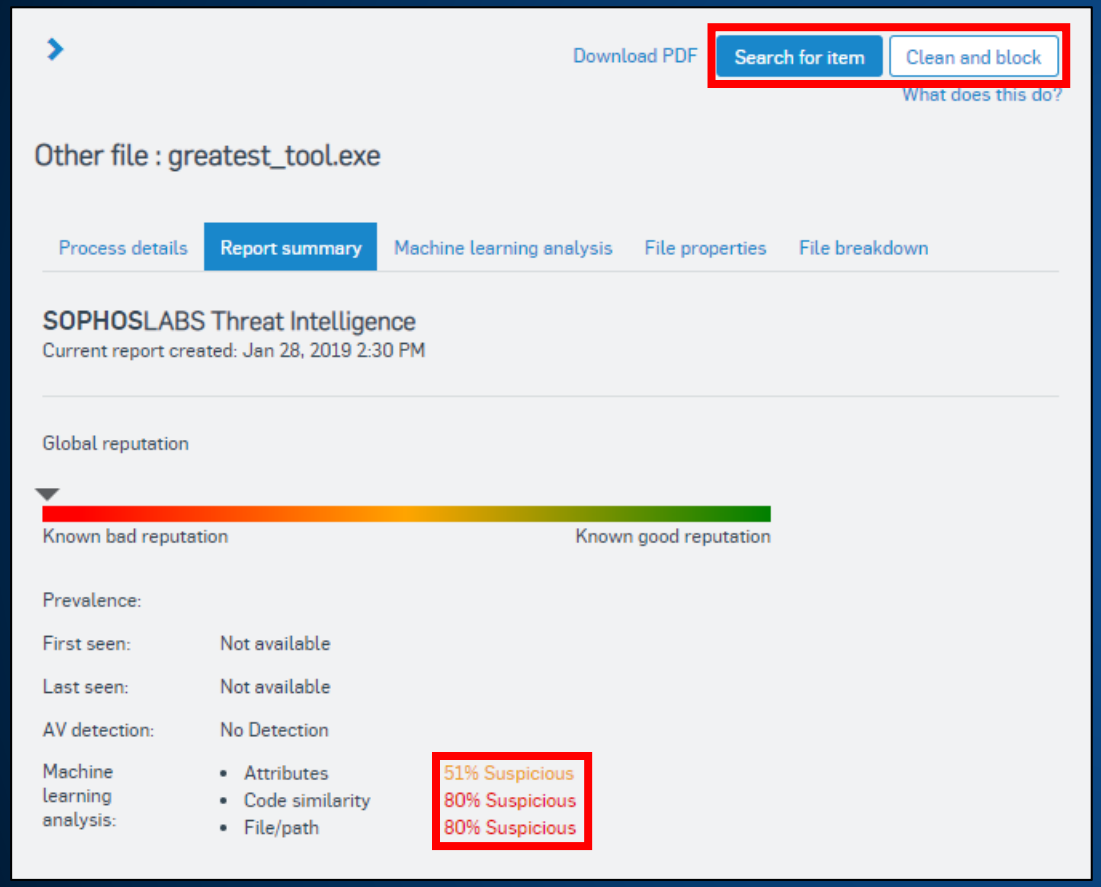
SOPHOS

Example: EMOTET

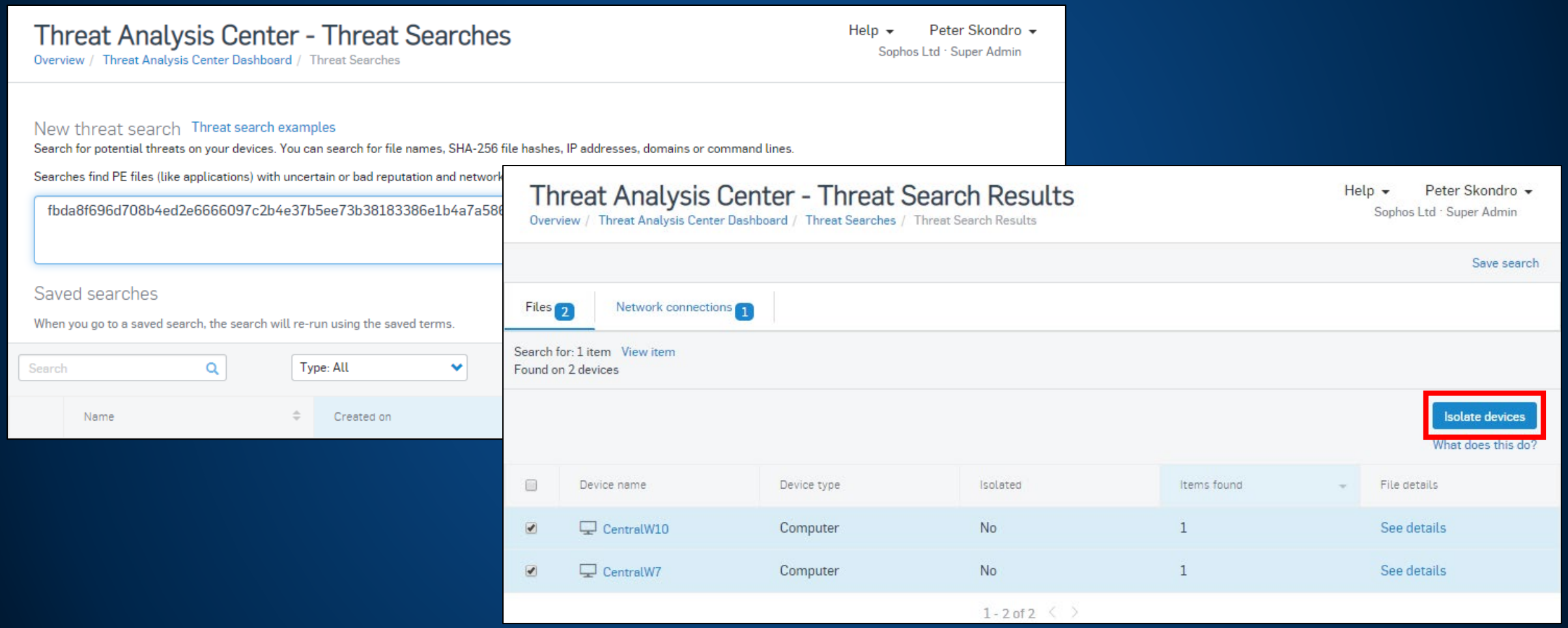




Machine Learning Analysis



Cross Estate Threat Search



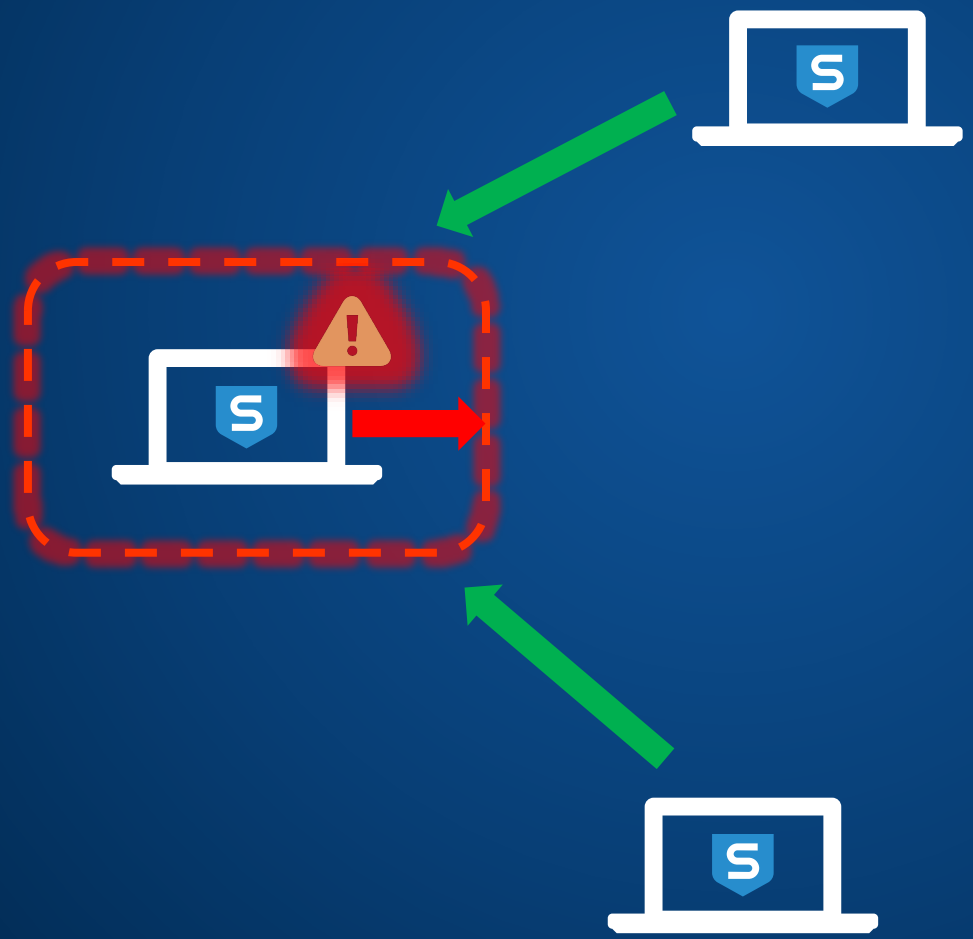
SOPHOS

Containment of threats

SOPHOS

Self Isolation

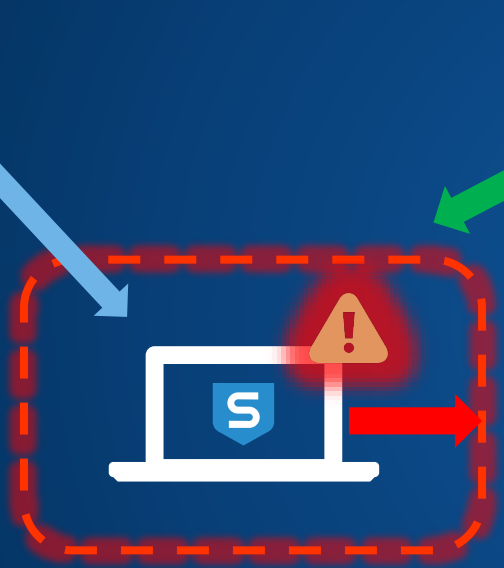
Infected client
Isolates himself



Admin Isolation

Admin

Admin isolates potentially compromised client



Traditional EDR

SOPHOS INTERCEPT X Advanced with 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

SOPHOS

Cybersecurity made simple.