



Sophos

Intercept X Advanced w/ EDR

Yannick Escudero

Snr. Sales Engineer

20.09.2018

SOPHOS

Organizations Struggle with Endpoint Detection & Response



VISIBILITY & DETECTION

Blind spots make it difficult to understand what is happening



ANALYSIS & INVESTIGATION

Teams suffer from a lack of data or are overwhelmed by data



INCIDENT RESPONSE

Need more talent and hours in the day to respond to incidents

Typical Endpoint Detection & Response Tools Also Struggle



DIFFICULT TO USE

EDR can be overwhelming, rely heavily on expert security analysts



PROVIDE LIMITED VALUE

Focused on manual workflows instead of proactive protection and automated response



RESOURCE INTENSIVE

Expensive, time consuming, require dedicated staff

Sophos Intercept X: EDR for All

Detect

Investigate

Respond

- **Intuitive to use, easy to understand**
Add visibility, analysis, and response capabilities without adding staff
- **More signals, less noise**
Automatic incident detection and prioritization, guided investigations, curated threat intelligence
- **Rapid Response**
Respond to incidents with the click of a button

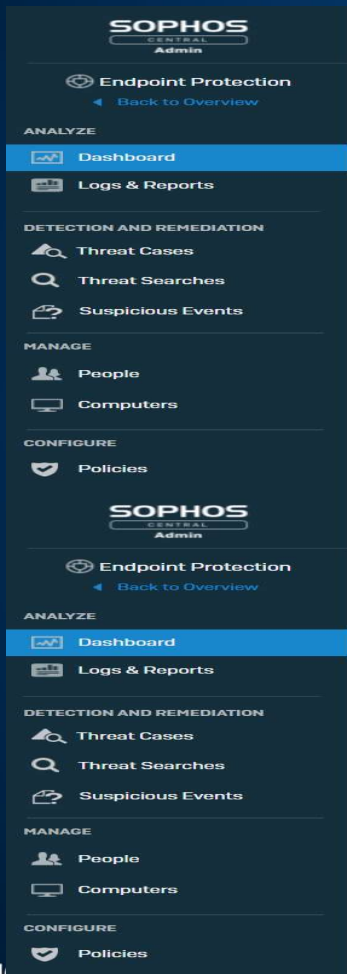
How Sophos EDR Can Make You More Secure

Answering those tough questions with Intercept X

- Am I under attack? Is there something we are missing? How can I be sure?
- How should I respond to this incident? What should I do next?
- What incidents should I be prioritizing?
- What is this file? Is it malicious? Is it a false positive?
- Does this threat exist anywhere in my network?
- Has the attack spread?



Intercept X w/ EDR: Detect



SOPHOS CENTRAL Admin

Endpoint Protection
Back to Overview

ANALYZE

- Dashboard
- Logs & Reports

DETECTION AND REMEDIATION

- Threat Cases
- Threat Searches
- Suspicious Events

MANAGE

- People
- Computers

CONFIGURE

- Policies

SOPHOS CENTRAL Admin

Endpoint Protection
Back to Overview

ANALYZE

- Dashboard
- Logs & Reports

DETECTION AND REMEDIATION

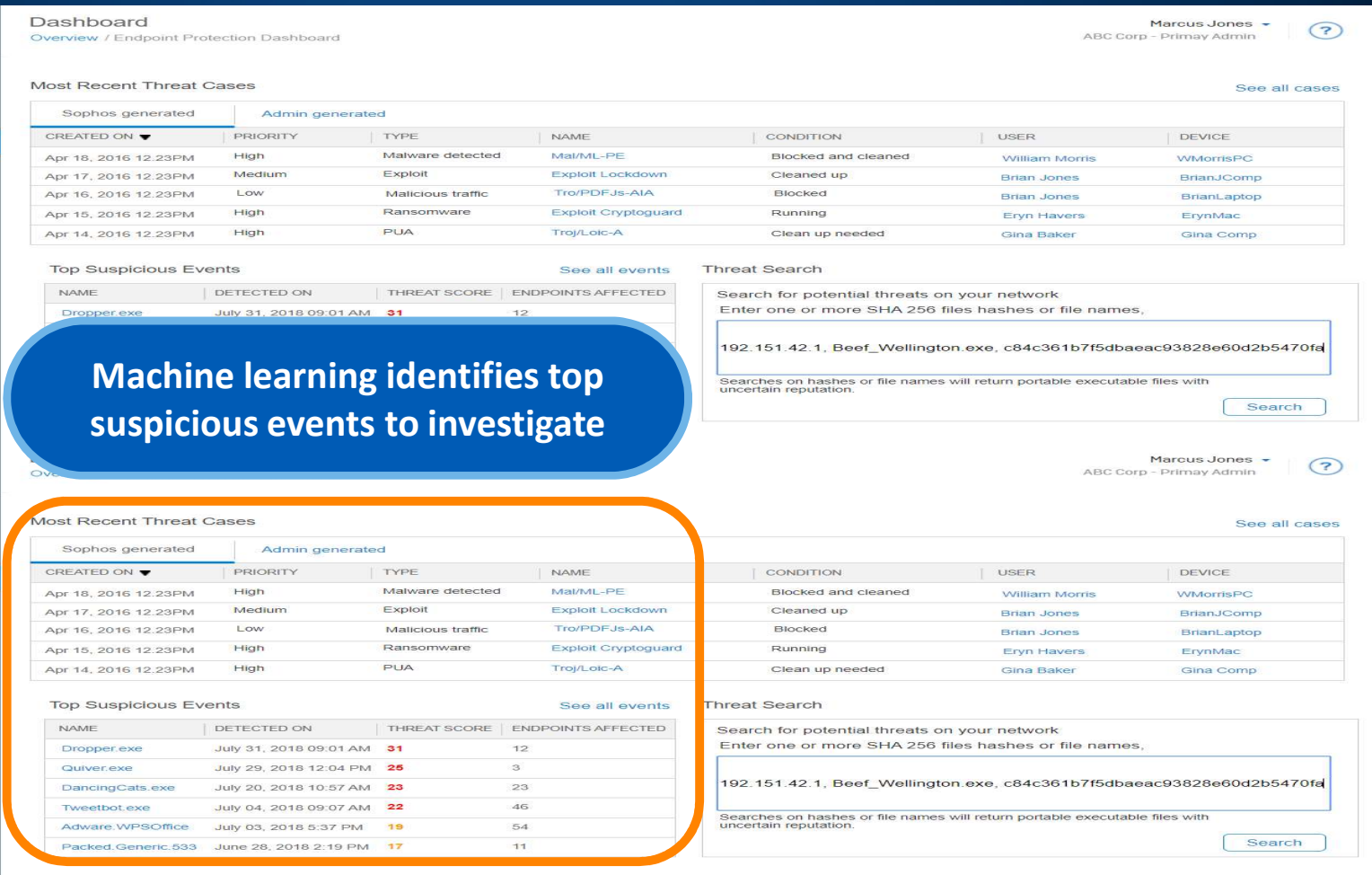
- Threat Cases
- Threat Searches
- Suspicious Events

MANAGE

- People
- Computers

CONFIGURE

- Policies



Dashboard
Overview / Endpoint Protection Dashboard

Marcus Jones
ABC Corp - Primay Admin

Most Recent Threat Cases

See all cases

Sophos generated		Admin generated				
CREATED ON	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12:23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
Apr 17, 2016 12:23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
Apr 16, 2016 12:23PM	Low	Malicious traffic	Troj/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
Apr 15, 2016 12:23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
Apr 14, 2016 12:23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Top Suspicious Events

See all events

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12

Threat Search

Search for potential threats on your network
Enter one or more SHA 256 files hashes or file names,

192.151.42.1, Beef_Wellington.exe, c84c361b7f5dbaeac93828e60d2b5470fd

Searches on hashes or file names will return portable executable files with uncertain reputation.

Search

Marcus Jones
ABC Corp - Primay Admin

Most Recent Threat Cases

See all cases

Sophos generated		Admin generated				
CREATED ON	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12:23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
Apr 17, 2016 12:23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
Apr 16, 2016 12:23PM	Low	Malicious traffic	Troj/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
Apr 15, 2016 12:23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
Apr 14, 2016 12:23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Top Suspicious Events

See all events

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	26	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Threat Search

Search for potential threats on your network
Enter one or more SHA 256 files hashes or file names,

192.151.42.1, Beef_Wellington.exe, c84c361b7f5dbaeac93828e60d2b5470fd

Searches on hashes or file names will return portable executable files with uncertain reputation.

Search

Machine learning identifies top suspicious events to investigate

Most Recent Threat Cases

Sophos generated		Admin generated				
CREATED ON	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12:23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
Apr 17, 2016 12:23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
Apr 16, 2016 12:23PM	Low	Malicious traffic	Troj/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
Apr 15, 2016 12:23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
Apr 14, 2016 12:23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Top Suspicious Events

See all events

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	26	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Intercept X w/ EDR: Detect



SOPHOS CENTRAL Admin

Endpoint Protection

Back to Overview

ANALYZE

- Dashboard
- Logs & Reports

DETECTION AND REMEDIATION

- Threat Cases
- Threat Searches
- Suspicious Events

MANAGE

- People
- Computers

CONFIGURE

- Policies

Dashboard
Overview / Endpoint Protection Dashboard

Marcus Jones
ABC Corp - Primay Admin

Most Recent Threat Cases [See all cases](#)

Sophos generated		Admin generated				
CREATED ON	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12:23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
Apr 17, 2016 12:23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
Apr 16, 2016 12:23PM	Low	Malicious traffic	Troj/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
Apr 15, 2016 12:23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
Apr 14, 2016 12:23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Top Suspicious Events [See all events](#)

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	25	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Easily search by IP address, file name, hash, etc.

Dashboard
Overview / Endpoint Protection Dashboard

Marcus Jones
ABC Corp - Primay Admin

Most Recent Threat Cases [See all cases](#)

Sophos generated		Admin generated				
CREATED ON	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12:23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
Apr 17, 2016 12:23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
Apr 16, 2016 12:23PM	Low	Malicious traffic	Troj/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
Apr 15, 2016 12:23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
Apr 14, 2016 12:23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Top Suspicious Events [See all events](#)

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	25	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Threat Search

Search for potential threats on your network
Enter one or more SHA 256 files hashes or file names,

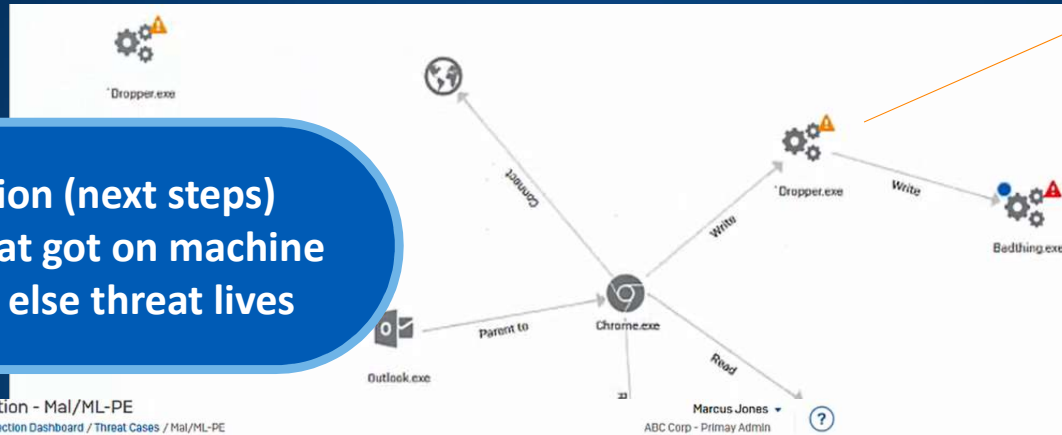
192.151.42.1, Beef_Wellington.exe, c84c361b7f5dbaeac93828e60d2b5470fd

Searches on hashes or file names will return portable executable files with uncertain reputation.

Search

Intercept X w/ EDR: Investigate

- Guided investigation (next steps)
- Analyze how threat got on machine
- Determine where else threat lives



Search for item Clean and block

Process details: dropper.exe

Reputation at time case was created: Uncertain

Known bad Known good

Detection status: Not detected at time case was created

You should investigate this item to determine whether it is harmful.

SOPHOS LABS Threat Intelligence

Request latest intelligence

Note: Requesting the latest intelligence will submit a copy of the file to SophosLabs for analysis

Path: c:\program files\temp\dropper.exe

Process ID: 9999

SHA256: 2cf24dba5fb0a30e26e83b2ac50e29e1b161e5c1fa7425e73043362930b9824

Start time: Apr 01, 2016 12:20PM

End time: Still running when threat case created on April 12, 2016 12:23PM

Duration: 11 days

Actions done to this artifact: None

Actions performed by this artifact: 1 executable file written, 1 program run

SOPHOS CENTRAL Admin

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events

MANAGE

People

Computers

Endpoint Protection - Mal/ML-PE

Overview / Endpoint Protection Dashboard / Threat Cases / Mal/ML-PE

WMorrisPC 11.222.33.45

Outlook.exe

Badthing.exe

Detected Apr 12 2017 5:46AM

Blocked and cleaned Apr 12 2017 5:46AM

Summary

Malware detected: Mal/ML-PE at C:\program files\WMorris\badthing.exe

On: WMorrisPC that belongs to William Morris

Condition: RAN CLEANED BUSINESS FILES INVOLVED

1

Detection summary: The root cause tried to access a URL known to be associated with malware

Suggested next steps

- Set status and priority for the case
- Investigate 1 process we've marked with an "uncertain" reputation. See graph below for details
- Isolate the computer while you investigate.
- Scan the computer

Details

Dropper.exe	Process	Uncertain	Mon dd yyyy tt:ttPM
-------------	---------	-----------	---------------------

Search for item Clean and block

Create forensic snapshot Export to CSV

Cleaned	Latest threat Intelligence
Yes	Mon dd yyyy tt:ttPM View
No	Mon dd yyyy tt:ttPM View

Intercept X w/ EDR: Investigate with SophosLabs Threat Intelligence

Process details: dropper.exe
Reputation at time case was created: Uncertain

Known bad | Known good

Detection status: Not detected at time case was created
You should investigate this item to determine whether it is harmful.

SOPHOS LABS Threat Intelligence

Request latest intelligence

Note: Requesting the latest intelligence will submit a copy of the file to SophosLabs for analysis

Path: c:\program files\temp\dropper.exe
Process ID: 9999
SHA256: 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362930b9824
Start time: Apr 01, 2016 12:20PM
End time: Still running when threat case created on April 12, 2016 12:23PM
Duration: 11 days
Actions done to this artifact: None
Actions performed by this artifact: 1 executable file written, 1 program run

Process details: dropper.exe
Current report created: Jun 06 2018 12:45pm

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

SOPHOS LABS Threat Intelligence

Threat Intelligence report summary

Global Reputation

Known bad | Known good

Prevalence: Low

First seen: mon dd, yyyy ttttPM
Last seen: mon dd, yyyy ttttPM

AV detection: Malware (high confidence) 15 anti-malware products detect this file. [Go to VirusTotal](#)

Machine learning analysis

Attributes: 87% suspicious
Genetic similarity: 82% suspicious
File path: 61% suspicious

Process details: dropper.exe
Current report created: Jun 06 2018 12:45pm

Process details | Report Summary | Machine learning analysis | File properties | File breakdown

SOPHOS LABS Threat Intelligence

Attributes: 87% suspicious | Over 52 million known good and 61 million know bad items analysed

Attribute of Dropper.exe | Seen in: Known bad files | Known good files

- Not signed: 4.3 Million (red) vs 1.0 Million (green)
- Unknown packs: 500 K (red) vs 205 K (green)
- Tiny code section: 1.0 Million (red) vs 1.0 Million (green)
- No icon: 2.1 Million (red) vs 980K (green)
- Uses encryption: 86K (red) vs 2 K (green)

Code similarity: 82% suspicious | Over 52 million known good and 61 million know bad items analysed

Dropper.exe

- x69.exe: 99%
- TradeStationForms.exe: 96%
- loquake3.x86_64.exe: 95%
- X3 ServiceHost.exe: 89%
- : 85%
- : 82%

- Access latest threat intelligence from SophosLabs
- AI threat researchers analyze suspicious files
- Explore machine learning analysis

Intercept X w/ EDR: Respond

Respond to incidents with a click of a button

- Full disclosure of potential threat activity
- Isolate machine(s)
- Clean file, blacklist or whitelist
- Investigate further, create forensic snapshots

The screenshot shows the Sophos EDR console interface. On the left is a navigation sidebar with sections: ANALYZE (Dashboard, Logs & Reports), DETECTION AND REMEDIATION (Threat Cases, Threat Searches, Suspicious Events), and MANAGE (People, Computers). The main area displays a table of suspicious files with columns: SHA256 Hash, Name, Reputation, Type, Cleaned, Path, and Actions. The first row shows an 'Installer.exe' file with an 'Uncertain' reputation. The 'Actions' column for this row is expanded, showing options: Actions, Clean and block, Generate threat case, and Request threat intelligence report. An orange arrow points from the 'Clean and block' option in this menu to a separate dialog box on the right.

SHA256 Hash	Name	Reputation	Type	Cleaned	Path	Actions
e92e02dff752778c13c1d788ac0781a535b86fcd04158b5be8f9810623a390c12	Installer.exe	Uncertain	Process	No	c:\program files\path name	Actions Clean and block Generate threat case Request threat intelligence report
2bf24dba5fb0a30e26e83b2ac5b9e25e1b161e5c1fa7425e73043362938b9824	Updater.exe	Uncertain	Process	No	c:\program files\path name c:\program files\second path name c:\program files\third path name c:\program files\fourth path name	Actions Actions Actions Actions
3cf24dba5fb0a30e26e83b2ac5b9e25e1b161e5c1fa7425e73043362938b9824	Keylogger.exe	Bad. Malware	Process	No	c:\program files\path name which is long and will wrap in the table row	Actions

The 'Clean and block' dialog box contains the following text: 'You're about to clean up this item on any computer where we've found it and block it on all your computers.' Below this is a text input field with the value 'Clean and remove this suspicious file and blacklist it'. A note at the bottom states: 'Note: You can see the items you've blocked or unblock them again in your Blocked Items list.' At the bottom right are 'Cancel' and 'Confirm' buttons.

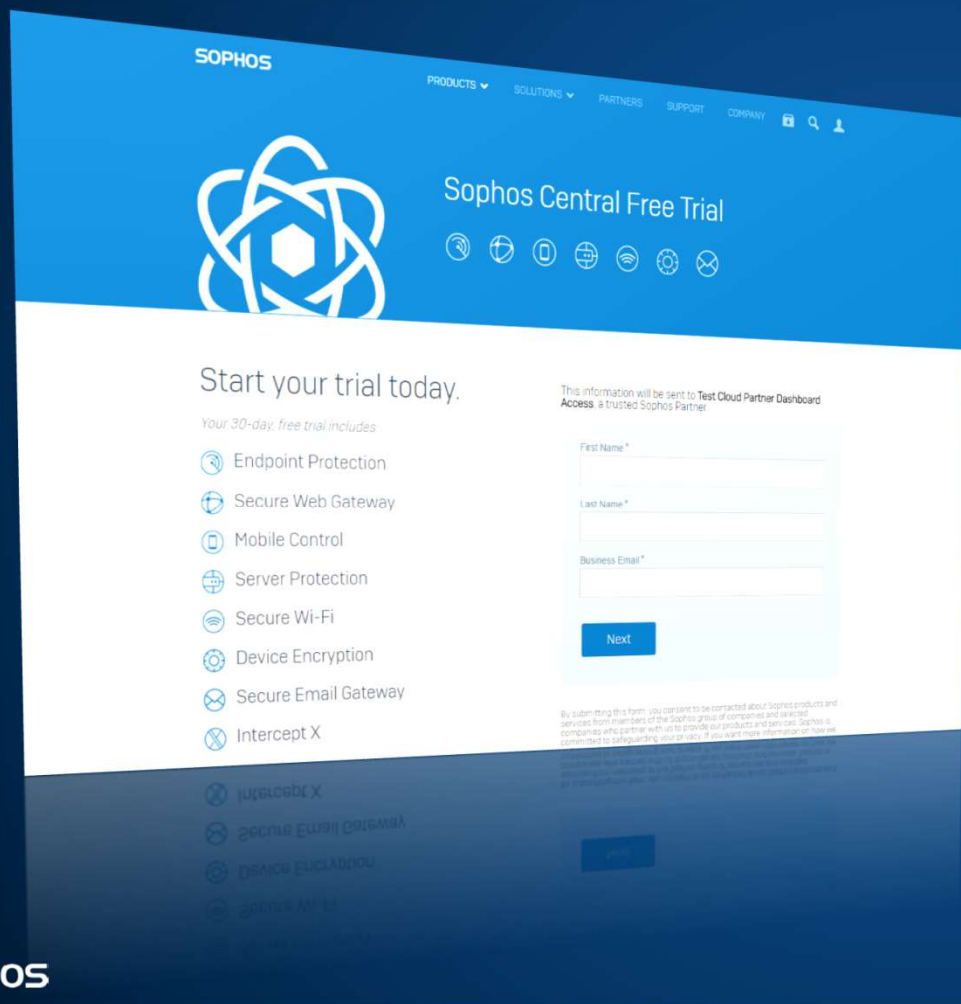
The 'Suggested next steps' panel lists the following actions:

- Set status and priority for the case (New, High)
- Investigate 1 process we've marked with an "uncertain" reputation. See graph below for details
- Isolate the computer while you investigate.
- Scan the computer

Demo

Benefits

- Get started quickly
 - Built on Intercept X – the industry’s #1 endpoint protection
 - Endpoint protection and EDR in a single solution
 - Part of Sophos Central
- Add visibility, context, and investigation capabilities without adding staff
 - Increase endpoint defenses, remove blind spots
 - Guided investigations
 - Machine learning prioritizes incidents, analyzes files, provides suggestions
 - SophosLabs threat intelligence on-demand
 - Make more informed decisions in less time
- Respond to incidents with a single click
- Prove compliance posture with increased ease



Coming Soon: Join the Early Access Program

Free to trial

Access via Central

Demo from Live Webcast

See here:

<https://vimeo.com/284228948/24498738a8>

SOPHOS
Security made simple.