WHAT'S NEW IN SOPHOS EDR 3.0

Available with Intercept X Advanced with EDR and Intercept X Advanced for Server with EDR

SOPHOS
Cybersecurity evolved.

Sophos EDR 3.0 – What's New

Available with Intercept X Advanced with EDR and Intercept X Advanced for Server with EDR

This release brings significant enhancements to Sophos Endpoint Detection and Response (EDR). Powerful, flexible and rapid querying across an organization's entire endpoint and server estates and the ability to quickly access a device to perform further investigation and take action even in remote situations.

Hunt down threats and perform IT security operations hygiene

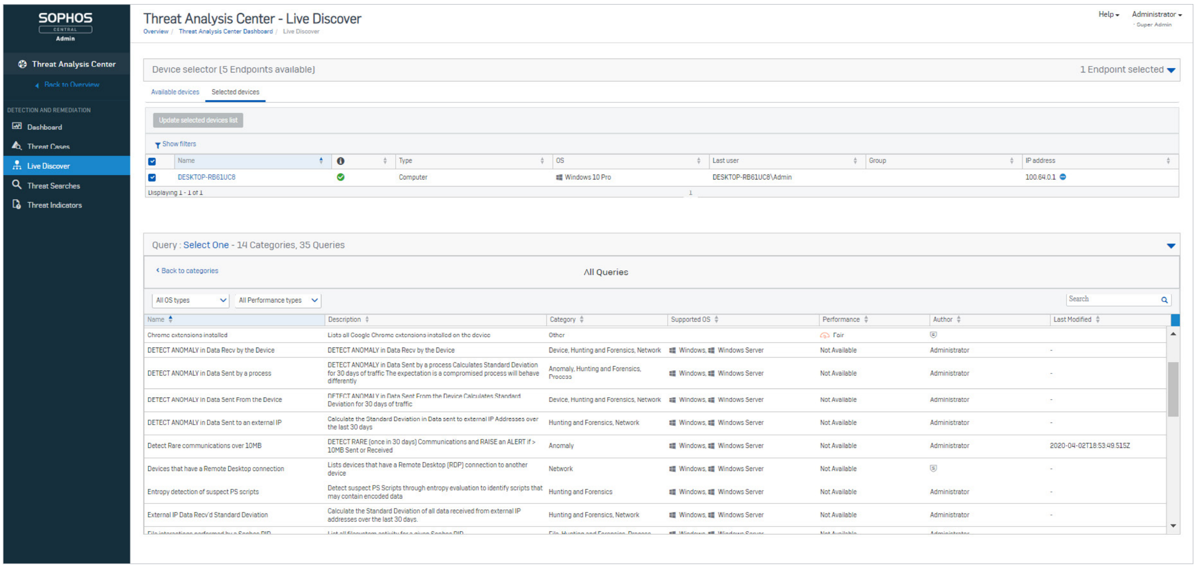
The ability to ask detailed questions makes it even easier and faster to hunt down and neutralize evasive and subtle threats. It is also incredibly effective at assisting IT admins with their daily IT security operations. Here are some example use cases:

Threat Hunting	IT Security Operations
What processes are trying to make a network connection on non standard ports?	Why is a machine running slowly? Is it pending a reboot?
List detected IoCs mapped to the MITRE ATT&CK framework	Which devices have known vulnerabilities, unknown services or unauthorized browser extensions?
Show processes that have recently modified files or registry keys	Are there programs running on the machine that should be removed?
Search details about PowerShell executions	Is remote sharing enabled? Are unencrypted SSH keys on the device? Are guest accounts enabled?
Identify processes disguised as services.exe	Does the device have a copy of a file I am looking for?

Live Discover – Answer Critical Questions

Live Discover gives security analysts and IT admins answers to critical threat hunting and IT security operations questions. It uses powerful SQL queries that can be selected from a library of pre-written options and fully customized to cater to all needs.

- Flexible and powerful SQL queries
- Choose from pre-written, fully customizable options
- Select only the endpoints and servers you need to query
- Up to 90 days on disk data retention for fast response



Threat Analysis Center - Live Discover

Device selector (5 Endpoints available) 1 Endpoint selected

☑	Name	ℹ	Type	OS	Last user	Group	IP address
☑	DESKTOP-RB61UC8	✓	Computer	Windows 10 Pro	DESKTOP-RB61UC8\Admin		100.64.0.1

Displaying 1 - 1 of 1

Query : Select One - 14 Categories, 35 Queries

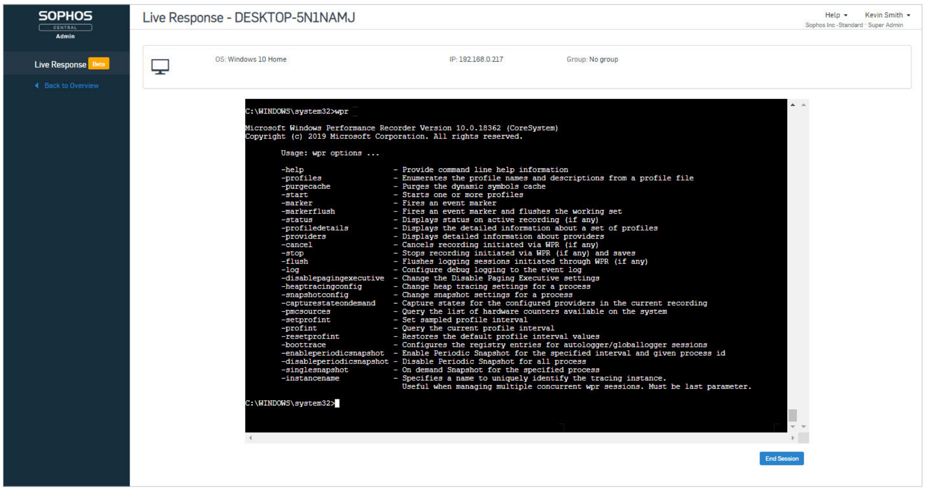
All Queries

Name	Description	Category	Supported OS	Performance	Author	Last Modified
Chrome extensions installed	Lists all Google Chrome extensions installed on the device	Other		Fair		
DETECT ANOMALY in Data Recv by the Device	DETECT ANOMALY in Data Recv by the Device	Device, Hunting and Forensics, Network	Windows, Windows Server	Not Available	Administrator	-
DETECT ANOMALY in Data Sent by a process	DETECT ANOMALY in Data Sent by a process Calculates Standard Deviation for 30 days of traffic The expectation is a compromised process will behave differently	Anomaly, Hunting and Forensics, Process	Windows, Windows Server	Not Available	Administrator	-
DETECT ANOMALY in Data Sent From the Device	DETECT ANOMALY in Data Sent From the Device Calculates Standard Deviation for 30 days of traffic	Device, Hunting and Forensics, Network	Windows, Windows Server	Not Available	Administrator	-
DETECT ANOMALY in Data Sent to an external IP	Calculate the Standard Deviation in Data sent to external IP Addresses over the last 30 days	Hunting and Forensics, Network	Windows, Windows Server	Not Available	Administrator	-
Detect Rare communications over 10MB	DETECT RARE (once in 30 days) Communications and RAISE an ALERT if > 10MB Sent or Received	Anomaly	Windows, Windows Server	Not Available	Administrator	2020-04-02T18:53:49.515Z
Devices that have a Remote Desktop connection	Lists devices that have a Remote Desktop (RDP) connection to another device	Network	Windows, Windows Server	Not Available		-
Entropy detection of suspect PS scripts	Detect suspect PS Scripts through entropy evaluation to identify scripts that may contain encoded data	Hunting and Forensics	Windows, Windows Server	Not Available	Administrator	-
External IP Data Recv'd Standard Deviation	Calculate the Standard Deviation of all data received from external IP addresses over the last 30 days.	Hunting and Forensics, Network	Windows, Windows Server	Not Available	Administrator	-
File interactions performed by a Sophos PID	List all filesystem activity for a given Sophos PID	File, Hunting and Forensics, Process	Windows, Windows Server	Not Available	Administrator	

Live Response – Respond Fast, Remotely

Live Response provides users cmdline access to endpoints and servers across their organization’s estate. They can remotely access devices in order to perform further investigation, install and uninstall software, or remediate any additional issues. Using the command line tool users can:

- Re-boot devices
- Terminate active processes
- Run scripts or programs
- Edit configuration files
- Install/uninstall software
- Run forensic tools



Live Response - DESKTOP-5N1NAMJ

OS: Windows 10 Home IP: 192.168.0.217 Group: No group

```
C:\WINDOWS\system32>wpr

Microsoft Windows Performance Recorder Version 10.0.18362 (CoreSystem)
Copyright (c) 2019 Microsoft Corporation. All rights reserved.

        Usage: wpr options ...

        -help                     - Provide command line help information
        -profiles                 - Enumerates the profile names and descriptions from a profile file
        -purgecache               - Purges the dynamic symbols cache
        -start                    - Starts one or more profiles
        -marker                   - Fires an event marker
        -markerflush              - Fires an event marker and flushes the working set
        -status                   - Displays status on active recording (if any)
        -profiledetails           - Displays the detailed information about a set of profiles
        -providers                - Displays detailed information about providers
        -cancel                   - Cancels recording initiated via WPR (if any)
        -stop                     - Stops recording initiated via WPR (if any) and saves
        -flush                    - Flushes logging sessions initiated through WPR (if any)
        -log                      - Configure debug logging to the event log
        -disablepagingexecutive   - Change the Disable Paging Executive settings
        -heaptracingconfig        - Change heap tracing settings for a process
        -snapshotconfig           - Change snapshot settings for a process
        -capturestateondemand     - Capture states for the configured providers in the current recording
        -pmcsources               - Query the list of hardware counters available on the system
        -setprofint               - Set sampled profile interval
        -profint                  - Query the current profile interval
        -resetprofint             - Restores the default profile interval values
        -boottrace                - Configures the registry entries for autologger/globallogger sessions
        -enableperiodicsnapshot   - Enable Periodic Snapshot for the specified interval and given process id
        -disableperiodicsnapshot  - Disable Periodic Snapshot for all process
        -singlesnapshot           - On demand Snapshot for the specified process
        -instancename             - Specifies a name to uniquely identify the tracing instance.
                                    Useful when managing multiple concurrent wpr sessions. Must be last parameter.

C:\WINDOWS\system32>
```

Multi-OS Support

Both Live Discover and Live Response will be available for Windows, MacOS and Linux, giving security analysts and IT admins powerful visibility and response options across their entire estates.

Initially Live Discover is available for Windows and Linux, with MacOS support following shortly. Live Response is initially available on Windows with MacOS and Linux support following shortly.

Included with all EDR licenses

These powerful features are available to all customers that have an Intercept X Advanced with EDR or Intercept X Advanced for Server with EDR license at no additional cost. There is also no install required, the new features will be added to the Sophos Central console.

Learn more

For more details on the power of EDR visit sophos.com/edr.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS