WHAT'S NEW IN SOPHOS EDR 3.0

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

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

**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
Live Response – Respond Fast, Remotely

Live Response provides users cmd line 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
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.