Bitdefender GravityZone PHASR – FAQ

How can you purchase, and which base licenses are compatible with PHASR?

GravityZone PHASR is available as an add-on license to GravityZone Business Security Enterprise, XDR, and MDR solutions, and MSP Packages (Secure, Secure Plus, and Secure Extra). PHASR can be purchased only for the same number of devices as are available on the base license key. Even when there are several users leveraging the same devices or the same user leveraging multiple devices, PHASR is still licensed by number of devices, but it creates different behavioral profiles for different user-endpoint pairs.

What makes PHASR different from conventional security solutions?

Unlike conventional security solutions which are built to fit everyone and are static, PHASR leverages unique behavioral profiles and correlates them with active threat vectors to tailor hardening optimally for each user. It goes beyond allow/deny decisions and can restrict specific atypical actions within used tools and enable admins to dynamically apply attack surface reduction measures using the Autopilot Mode. This results in unprecedented attack surface reduction without impacting productivity or manageability.

How can you activate PHASR?

After purchasing the license and entering your license key within the GravityZone Control Center console, you will be able to activate PHASR from the policy for all, or a subset of users. After that, PHASR starts learning and building behavioral risk profiles and will provide attack surface reduction recommendations.

How does PHASR take advantage of Bitdefender Labs threat intelligence?

PHASR does not monitor all unused applications and playbooks or actions. Instead, it leverages Bitdefender threat intelligence and monitors tools and activities that have been involved in attacks and the monitored rules are constantly updated based on the latest attack vectors.

How many applications and behaviors does PHASR monitor?

PHASR monitors hundreds of applications and playbooks or actions and the number is updated constantly as new threat vectors emerge. These monitored rules are grouped in 5 categories: LOLBins, Tampering Tools, Remote Admin Tools, Miners, Hack Tools.

What are PHASR Autopilot Mode and Direct Control Mode?

PHASR learns the risky tools and applications that are not leveraged by each user and provides recommendations to reduce the unnecessary attack surface. Recommendations can be applied in Autopilot Mode, automatically adjusting attack surfaces to changing behaviors and reducing effort, or in Direct Control Mode, enabling admins to filter and decide which are the recommendations to be applied.

What are behavioral profiles?

Behavioral profiles are unique pairs of users and devices for which PHASR generates recommendations. A user may have multiple behavioral profiles if they have multiple devices.

What are the differences between monitored rules and recommendations?

The monitored rules are the foundation of the PHASR recommendations. Based on these rules PHASR will generate access management recommendations.

Can Autopilot and Direct control modes be configured for each category?

Yes, you can configure and choose between Autopilot and Direct control mode for each monitored category.

I've allowed access to an application, but the user is no longer using it. Will PHASR report it again?

Yes, PHASR continuously learns and if it detects the user is not leveraging the application, then it will generate again a recommendation to restrict access.

How can I add restrictions without recommendations?

You can add restrictions without recommendations from the PHASR monitored rules section.

How can I see who restricted or allowed access?

You can see who restricted or allowed access from the User activity section in GravityZone by using the Area filter which contains PHASR recommendations and PHASR monitored rules. This is available for actions taken within Direct Control mode.

I've activated PHASR, what happens next?

Once PHASR is activated it will start the learning phase in which it analyzes user behavior and once this phase is completed it will start generating recommendations. PHASR requires an initial learning phase and after the initial phase has been completed, it will provide recommendations while continuing to learn and adjust to changing user behavior and threats.