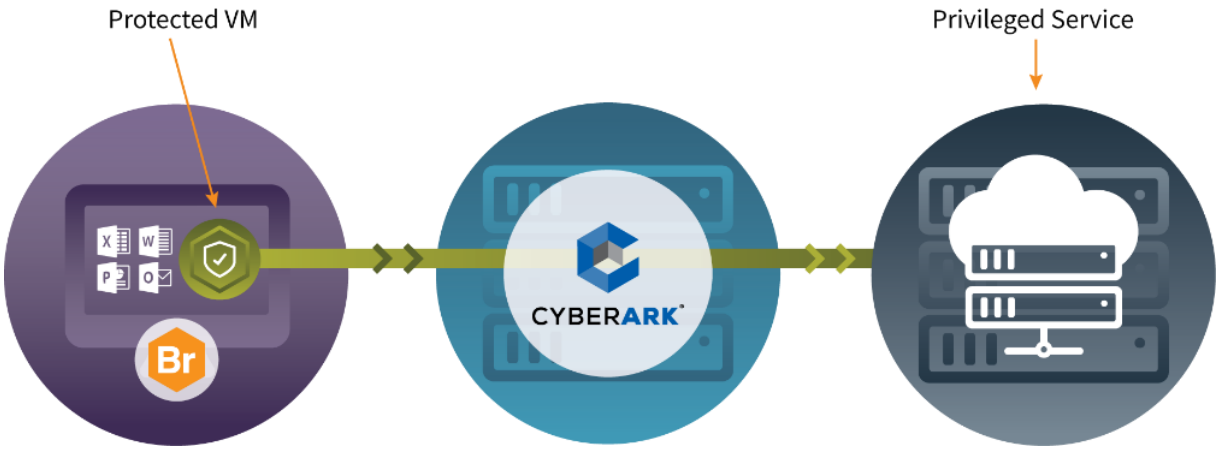
When an administrator's workstation is compromised an attacker could log key strokes of the legitimate user, capture the contents of the screen and issue commands to the privileged device installing a 'back door' to provide future access. In order to eliminate that risk, CyberArk Core Privileged Access Security can be integrated with Bromium Protected App to achieve end-to-end protected privileged access. This integration preserves all the PSM functionality (session isolation and recording) while providing the additional benefit of securing the first mile, between the user's device and the Privileged Session Manager.

The Integration requires the deployment of the Bromium Protected App product on your administrators' workstations, by manual installation or via software distribution tools (.msi).

A web-based controller – in the cloud or on premise – facilitates the central management platform to define connections that shall be opened within Protected VMs. Bromium, CyberArk and their partners' Professional Services teams will provide directions and guidance how to apply such Protected VM configuration.

Bromium Protected App can be configured to either run Protected VMs for connecting to the CyberArk Portal only or starting privileged connections with CyberArk Privileged Session Manager straight away.



Bromium Protected App with CyberArk allows for end-to-end protected privileged access, from the administrator's workstation to the most critical assets within an organization, such as the Windows domain controller. Not only does it add significant security to the 1st mile from the administrator's device to the CyberArk Portal and Core Privileged Access Security Solution, it also eliminates the need for dedicated Privileged Access Workstations (PAW) and improves a seamless user experience when connecting to target devices via CyberArk.