HYSOLATE Solution Brief

Hysolate for Enhanced Data Leakage Protection

The Challenge

Securing corporate data is crucial for IT and Security teams. Sensitive data is constantly being accessed by both employees and contractors, often on unsecured end-user devices, outside of the corporate firewall. This data can be exfiltrated by different parties in several ways:

- Malware that captures the data (data file, screen shots, intercepted data streams)
- Careless employees and contractors, who may download data to a non corporate device, send data out of an organization via email, file sharing, or export to a USB device.
- Malicious insiders that try to exfiltrate data (via similar means as innocent employees/ contractors but with intent to damage the corporation.)

How can IT and Security secure corporate data and present data leakage from non corporate devices, while also giving employees and contractors the access they need to do their jobs?

The Solution

Hysolate's fully managed OS isolation solution sits on end user devices, but is managed via granular policies from the cloud. Admins can limit data transfer out of the isolated Hysolate Workspace via copy/paste, and can set anti keylogging and screen capture policies.

Employees can be provided with an isolated Workspace on their corporate device, so that they can access sensitive systems and data from a completely isolated and secure environment. Policies can be set to limit data exiting the Workspace, either accidentally or on purpose.

For contractors, Hysolate's isolated OS solution provides a secure Workspace to access the necessary data and applications they need to do their jobs. The Workspace can be pre-provisioned with all the required applications and policies that are required for the contractor to connect to and work in the corporate environment. At the end of the contractor's engagement, the Hysolate Workspace can be instantly deprovisioned remotely without leaving any data on the contractor's device.

Benefits

/1

An additional layer of data leakage protection for both corporate and non corporate devices

/2

Admins can set policies to limit data transfer in and out of the Hysolate Workspace, including files, documents and applications.

/3

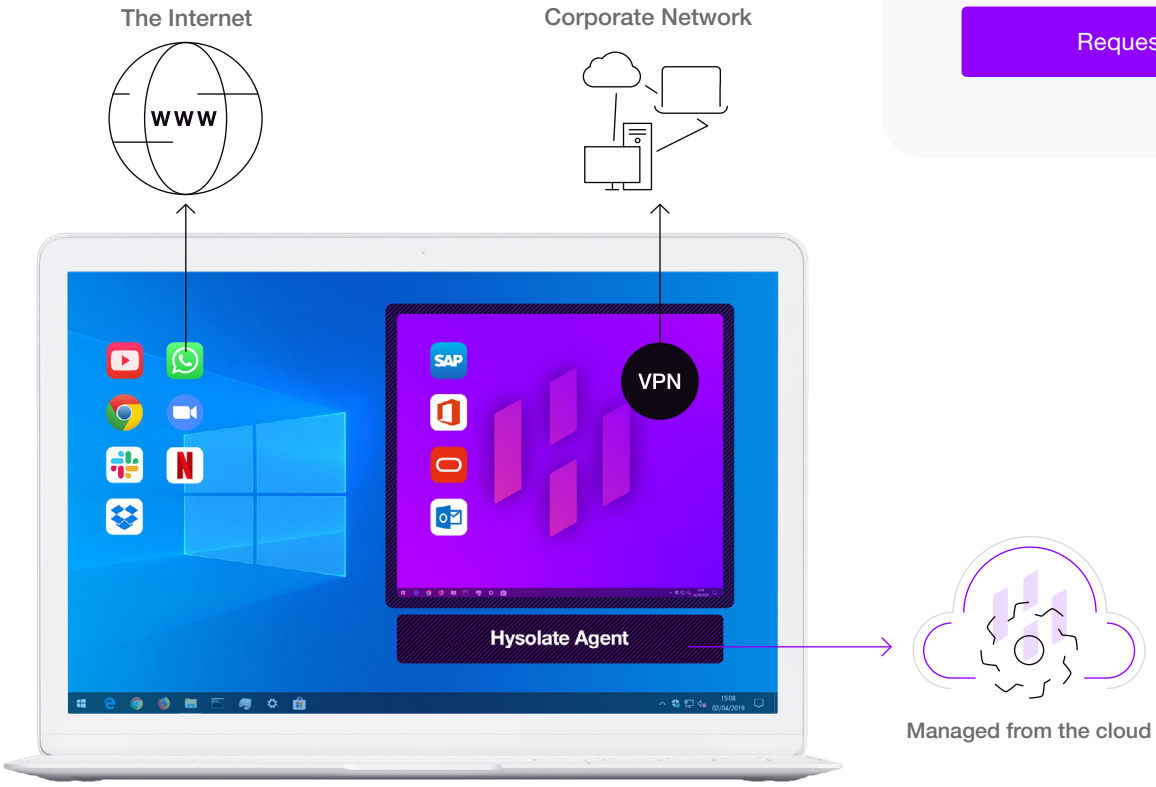
Policies can be set for anti keylogging and screen capture.

/4

Hysolate has security capabilities to lock the Workspace and enter only with a pin.

/5

Admins can wipe the Workspace OS remotely if a threat surfaces, or when it is no longer needed.



About Hysolate

Hysolate enables organizations to isolate risky or sensitive activities on users' endpoints with a local workspace that isolates applications and data. Hysolate has reinvented how an isolated virtual environment is instantly deployed on a user's device and remotely managed from the cloud. With Hysolate you can "split" the user's device into two isolated environments so users can work freely and be productive without compromising security.

Hysolate is backed by Bessemer Venture Partners, Innovation Endeavors, Team8 and Planven Capital.

For more information, visit:

www.hysolate.com

Request a Demo