HYSOLATE Solution Brief

Reduce the Risks of Ransomware with Hysolate

The Challenge

In a global business environment up to 70 percent of security breaches are still originating at the endpoint. Despite this, employees need to opendocuments, install applications, access websites and use peripherals, to perform routine day to day tasks. This can introduce risks of ransomware and other malicious software via your employees' endpoint devices.

One solution is to severely lock down endpoints to reduce malware and ransomware risks. This leads to increased resources spent on deciding which software and applications can or can't be trusted, and users who are frustrated and less productive.

The Solution

Hysolate offers a fully isolated OS environment that's installed on the user's endpoint, splitting it into a more risky zone and a secure zone. Corporate applications can be run in the secure zone, on the host device, while untrusted websites and applications are opened and used in the Hysolate Workspace, the "more risky" zone, which is totally separate from corporate data and applications.

The Hysolate Workspace creates full network, browser, and application isolation. Untrusted websites that users attempt to open on their host devices are automatically redirected into Workspace, reducing the risk of ransomware and other threats. Risky documents, files, and even peripherals like USBs and printers can be limited to only be accessed from within Workspace, reducing the risk of ransomware on the corporate device.

> **Hysolate's URL redirection feature gives us peace of mind that those links are now being opened in a totally isolated environment.**
>
> Jon Booth
> Information Security Administrator
>
> MIB
> Midwest Independent BankersBank

Benefits

/1

Reduce the time and money spent on security auditing, certifying and whitelisting applications.

/2

Reduce risks from USBs and printer applications by automatically redirecting their usage to the Hysolate Workspace.

/3

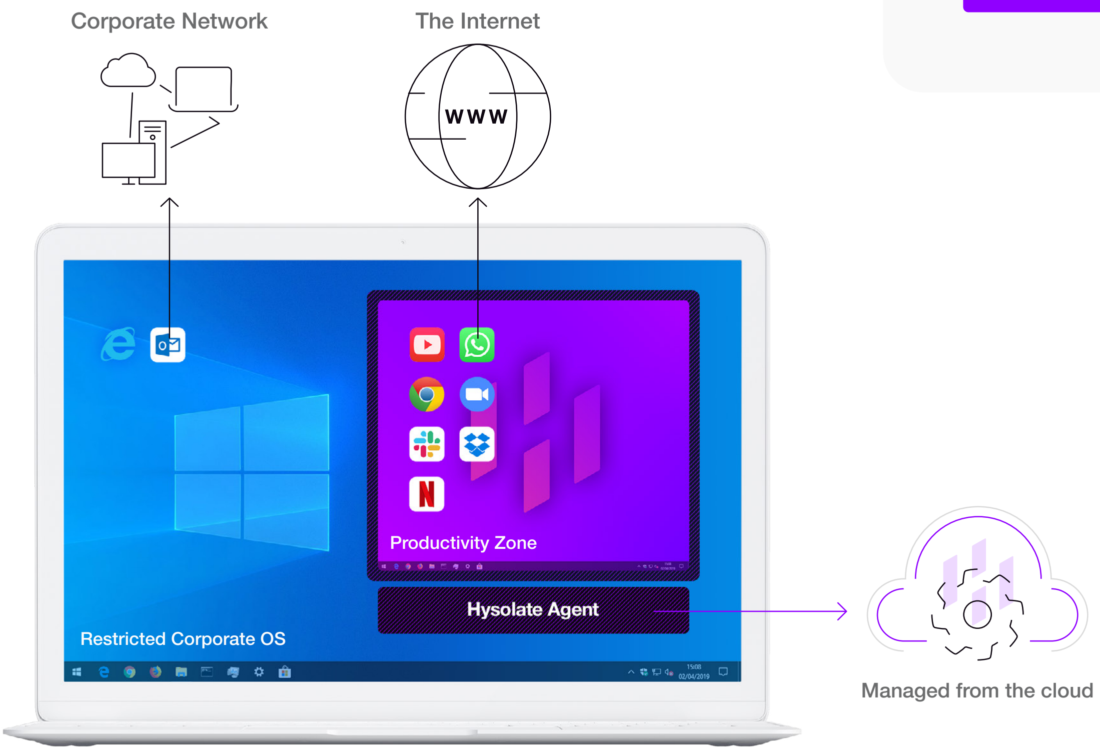
Your employees can access untrusted websites, without security concerns inside the Hysolate Workspace. Risky websites opened on the corporate host device will be automatically transferred into Workspace.

/4

Untrusted files and documents can also be opened in Workspace, reducing the risks from malware and other downloadable threats.

/5

Productivity and connectivity applications like Adobe Reader, Zoom, and Slack can be used in your risky workspace, isolating incoming files and data, so you can work without concern about introducing malware, viruses and other issues.



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