HYSOLATE Solution Brief

How Law Firms Can Protect Client Information with Hysolate

The Problem

Securing confidential client data is a serious concern for IT and Security managers at law firms. With 70% of security threats originating on the endpoint, they tend to deal with this by locking down endpoint devices and adding layers of security restrictions. This helps to protect client data, and the company's reputation, but makes it significantly harder for their team to do their jobs.
These restrictions may include:

- Browsing the web
- Connecting to public networks
- Exchanging digitally with their clients
- Installing unsanctioned applications
- Printing while not in the office
- Allowing secure data exchange from external sources

Legal teams face limitations on web browsing and installing applications, but these are needed for daily activities with their customers and vendors. The growth of remote collaboration and communications tools has compounded the situation. Lawyers need to be able to communicate safely with their clients without worrying about confidential information leakage or the infiltration of malware into the organization. How can your team get their jobs done without increasing security risks? How can you reduce overhead for legal IT and Security, while keeping corporate and client data secure?

The Solution

Hysolate provides an OS isolation solution that runs locally on the user's endpoint, essentially splitting it into two zones, a productivity Workspace, where you can install and access your third party applications and browse the web, and a corporate secure host Operating System, that is restricted. Untrusted websites can be opened only within Workspace, keeping all the risk away from your customer data in the host OS. Unlike traditional browser isolation solutions, you can also fully isolate risky applications, as well as peripherals like USBs and printers.

Hysolate is deployed within minutes, on your users' endpoints, and is managed from a cloud-based management console, with relevant policies for their department and needs. Your admins can control exactly which websites, applications and activities are limited to Hysolate, so your team can work productively and efficiently, and your client information remains secure.

Benefits

/1

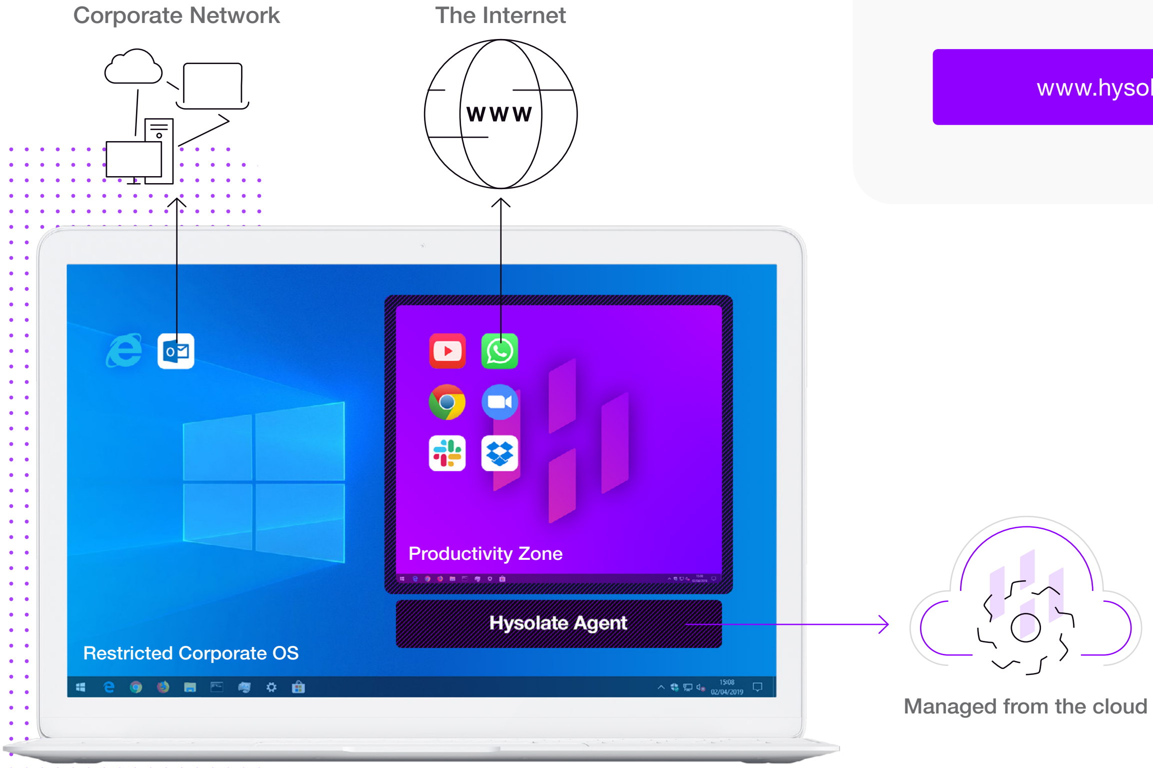
Stop your team from opening up risky websites or applications in the host OS, limiting them only to performing these activities within the Hysolate Workspace.

/2

Full admin management control, so you can easily deploy and scale Hysolate across all user endpoints, with customized policies per group or team.

/3

No more banning USBs or printer peripherals. Your team can access these devices for printing documentation and contracts safely within Hysolate, keeping your host OS clean.



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