HYSOLATE

Hysolate Revolutionizes Privileged Access Workstations

Privileged Access Workstations (PAWs) are challenging to implement. Hysolate delivers a brand new approach to PAW implementation that is secure-by-design, boosts admin productivity, and enables IT flexibility.

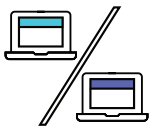
THE CHALLENGE

Cyber attackers most commonly seek out one person in an organization: IT administrators. Why? Because IT admins have privileged access to sensitive IT systems, critical business applications, and confidential data. As soon as attackers breach a machine with privileged access, they are undoubtedly at the last stage of their attack - finally able to steal PII, financial data and sensitive IP, or cause damage that brings your organization to a halt.

To thwart these attacks, IT administrators are encouraged to conduct all privileged activity on a separate machine that is isolated from normal user activity. These machines, which are locked down and highly restricted, are typically referred to as Privileged Access Workstations (PAWs). When used properly, they significantly reduce the risk of an attacker easily reaching privileged assets.

So, how can you implement Privileged Access Workstations?

Physical Air Gap



Although using separate physical machines ensures that the privileged workstation is completely locked-down, this is not a user-friendly approach. Users must lug around an extra machine and swivel between machines to accomplish their tasks, which impacts productivity. It's a burden also on administrators who are required to manage and support additional hardware.

Jump Box or VDI

Routing all privileged activity through a jump box or virtual desktop infrastructure (VDI) provides a certain level of security, but the operating system of the hardware used to access the jump box is still at risk of compromise - which means the privileged sessions are also at risk. In addition, this approach is 100% reliant on connectivity to another device, which introduces complexity, performance issues, latency and an additional potential point of failure.

> I didn't know where to start when it came to implementing PAW in the real world. It seemed great in theory but impossible in reality.
>
> **Hysolate made our PAW implementation not only possible but pleasurable. Our admins love it!**
>
> **— CISO of a Top 10 international financial institution**

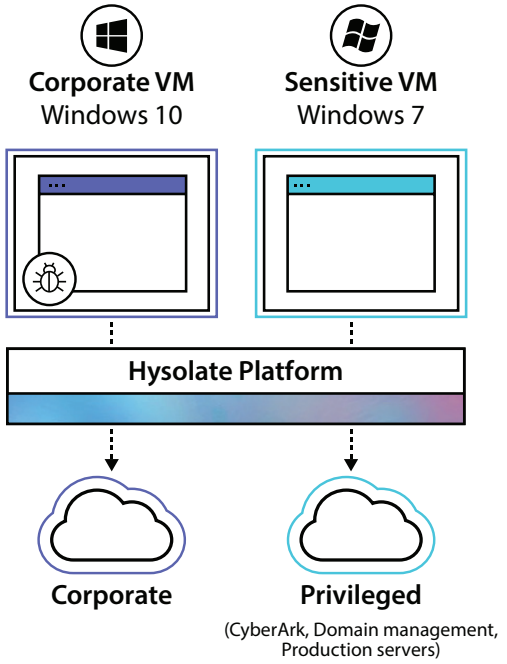
HYSOLATE

THE SOLUTION

Hysolate revolutionizes Privileged Access Workstations by seamlessly splitting a single physical device into multiple, completely isolated environments. By re-inventing the endpoint architecture from below the operating system (OS), Hysolate delivers a solution that is secure-by-design without compromising productivity.

This is all made possible by bringing virtualization into the endpoint. Hysolate places a hypervisor platform layer between the hardware and the OS. From this hypervisor layer, you can run multiple operating systems at the same time, side-by-side on your machine.

Hysolate enables your administrators to securely access privileged assets from the same device that they conduct their day-to-day corporate activities. The device will be equipped with two isolated VMs: A sensitive VM where all privileged activity takes place, and a corporate VM where all other corporate activities are conducted.



Key Features:

Virtual air gap

Each OS is entirely isolated as-is, not just a few selected applications.

Seamless user experience

All application windows are presented in a unified view, regardless of the VM the application is running in.

Network Security

Granular control over network traffic to each of the VMs.

Cross-VM transfers

Enable users to copy/paste between VMs by establishing fine-grained controls including size and content disarming.

URL redirection

Websites that are blocked due to policy on the sensitive VM can be automatically redirected to the corporate VM.

Hypervisor-based VPN module

VM traffic can be VPN-tunneled, eliminating the risk of rogue networks.

Benefits:

Reduce risk

Security administrators significantly reduce risk by isolating sensitive environments and removing access to the host. This ensures users cannot cause accidental or intentional risk (insider threat).

Improve manageability

IT administrators easily set policies, control transfer settings, and deploy and manage large environments from the user-friendly, centralized Hysolate management console.

Improve productivity

End users easily and securely work within each environment using Hysolate's "Seamless mode" that enables copy/paste and file transfer all from a single physical device. No more lugging multiple machines.

About Hysolate

Hysolate pioneered software-defined endpoints, the most innovative way to secure user devices and boost user productivity. The solution seamlessly splits devices into segregated environments by leveraging virtualization and provides protection below the operating system. Customers include leading financial, technology and services enterprises worldwide. Hysolate's team includes IT and cybersecurity experts who are veterans of VMware, Microsoft, CyberArk and Unit 8200 (Israel's NSA). The company was launched by Team8, a cybersecurity think tank, is privately held, and has headquarters in Tel Aviv and New York. Visit us at **www.hysolate.com** and follow us on **LinkedIn** and Twitter **@HysolateNow**.