Extending “Zero Trust” to the Endpoint with Hysolate

The Problem

With Zero Trust architectures, enterprises no longer assume users within the network perimeter are trusted - instead they adopt a “Zero Trust” methodology in which all access to enterprise resources must be authenticated and verified before it is granted. However, these architectures often neglect to ensure that the endpoint’s security is at an adequate level.

Traditional endpoint security approaches keep failing, with attackers leveraging the endpoint as the weakest link in the Zero Trust model. As soon as an attacker breaches an endpoint, they can own the endpoint OS and operate on behalf of the user, once they are authenticated and granted access . Then, attackers can leverage this access to exfiltrate data, laterally move within the enterprise environment, and further deepen their incursion into the enterprise environment.

The Solution

Hysolate complements Zero Trust security architectures by comprehensively securing the endpoint, by design. With Hysolate, access to sensitive enterprise apps on the endpoint can only be done from an isolated trusted OS while access to risky/potentially malicious apps is done on a completely separate OS. This is done by leveraging the latest virtualization-based security technologies and enhancing them so that enterprises can instantly split the endpoint into these two isolated operating systems, in a way that is user-friendly and cloud-managed. Using Hysolate, you can increase the level of trust with a high level of assurance that access is being performed from a secure OS.

Benefits

/1
Full isolation of the two operating systems, including fine-grained security controls for clipboard data, networking, peripherals, keyboard, display, disk encryption, etc.

/2
It's impossible for the end-user to access sensitive applications from any other untrusted environment or device. This is done by leveraging "conditional access" features of the Zero Trust broker (e.g. Azure AD) that would only allow access from the trusted OS.

/3
Users can access any websites and applications that they need to do their jobs, from within the less restricted environment without risking corporate data and assets.

/4
The user experience is native and local and doesn't require any additional network hop for accessing the isolated OS, as it is running in a local VM.

/5
Spinning up the Hysolate VM can be done in minutes, and doesn't need costly infrastructure.

/6
The solution can be applied both to corporate-managed devices and to 3rd party devices.

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