Secure Developer Access to Sensitive Production Environments

Developers have unique characteristics that make them and their endpoints a high priority security risk:

1

Developers are typically granted local administrator rights to install dev-related applications, packages, extensions, drivers, etc.

This means that malware that reached their machine will be usually running with local administrator rights and would be able to modify settings, harvest additional user credentials and have full network access.

2

Developers require full access to the Internet to download code samples, 3rd party source code packages and libraries or new tools. The development tool stack is rapidly changing and these internet resources cannot be easily whitelisted and often do not work well in conjunction with web proxies.

This full Internet access increases the chances of downloading malware that would probably be able to access its C&C server. It also means that developers (by mistake or intent) can upload sensitive data to any Internet server.

3

By definition, developers are building and running software on their machines and that software can have bugs that in some cases lead to catastrophic consequences on corporate resources that are accessible from the developer's machine, for example: deleting all the files on a network share, or doing mass wrong modifications to a database.

Some companies actually segregate developer machines to a separate network and separate devices to try to reduce the impact of this risk.

4

Developers have access to the crown jewels of the organization, including:

- Access to proprietary source code, including the ability to leak out the source code or introduce back doors.
- Access to sensitive customer information that is sometimes provided to developers for testing purposes.

To get their work done, developers either use two separate devices (one for development and one for corporate), or they are frustrated and non-productive because of lacking one of the following: Internet access, admin. rights, or access to customer data for testing.

Stop Frustrating Your Developers

Hysolate Isolated Workspace-as-a-Service (IWaaS) is a local hyper-isolated virtual environment that provides users with a superior user experience. It is built to spin up instantly on any Windows 10 OS and managed, at scale, from the cloud. This as a result, reduces the risks associated with developers by providing them with isolated operating systems that run locally on their endpoint:

One for the internet, with local admin rights, so they can install whatever dev-related apps, extensions, and drivers that they need.

And one for an operating system that is locked down, providing access to customer environments, proprietary source code, mission critical production servers, etc.

The results

- No local admin rights on corporate/ sensitive environments
- No need to open the entire corporate network to the internet
- Limit the scope of software bugs/ experimentation
- Limited access to sensitive systems/data, including insider threat protection

Benefits

IWaaS provides the following benefits for developers:

- Full Internet access
- A safe playground for experimentation with full local admin rights
- Replace a 2-device solution with a single productive device
- Ensure developers access production /customer data only from a trusted environment

About Hysolate

Hysolate is the isolated workspace innovator, bridging the gap between enterprise endpoint security and user productivity. Hysolate is the first solution that lets you easily create Isolated workspaces on corporate and non-corporate devices, in minutes, and manage them from the cloud.

Companies use Hysolate to: (1) protect their corporate devices with an isolated workspace for high risk activities, and (2) secure corporate access from unmanaged devices with a strong, VM-based, isolated workspace. Hysolate is backed by Bessemer Venture Partners, Innovation Endeavors, Team8 and Planven Capital.

Start your 14-day free trial. GET STARTED