An Extra Line of Defense Against Phishing and Malware

How can government agencies let employees do their jobs without worrying that clicking on an infected file or link will trigger a ransomware attack? One tactic is to deploy software to create tiny virtual machines that isolate malware so it can't infect users' PCs. **James Dobra**, *director of security solutions with HP Wolf Security, gives a concise overview of the benefits of this approach.*

How do virtualization and isolation reduce cyber risk?

With the right software, you can create a super small, super fast, super secure virtual machine that isolates the contents of a risky file or website so it cannot infect a user's PC. We call this interactive isolation. It means the user can still interact with that file or website and do their job, but in a safe way that protects against potential malware or credential theft. It literally doesn't matter to the user if the file or website is malicious.

What's the impact on the PC user experience when agencies deploy this kind of virtualization?

IT pros tend to think of a full-sized virtual machine (VM) as slow to build, slow to start and slow to run. But it's possible to create micro-VMs so small that there's no impact on the user experience. With interactive isolation, users can still view, edit, print and even save the file to their hard drive without risk of malware infecting the PC or the internal network.

What are important features of a cybersecurity solution that uses micro-VMs?

A few questions government IT people should ask: Where does the isolation occur? Is it happening on a PC you already own, or are you paying for cloud resources around the globe you may not need? Is the user experience seamless, or is it so slow that it feels like connecting to the web via dial-up? Does it protect the users across multiple browsers to prevent credential theft?

How does this technology fit into a comprehensive cyber defense strategy?

We look at this at from the defense-in-depth point of view.

Your PC is like an office building and anti-virus defenses are like the security guard. Somebody is bound to sneak past the front desk somehow, so you have security cameras to catch them in the act. Endpoint Detection & Response (EDR) software is like the cameras, collating data from your endpoints to catch unauthorized people walking out the back door with lots of data or changing things on your PC that shouldn't be changed.

Interactive isolation gives you a third line of defense. It's similar to meeting visitors in a conference room (micro-VM) outside the front desk. Your front desk (anti-virus) and security cameras (EDR) have less work to do and fewer false positives to resolve because your office (PC) has fewer visitors (risky files or clicks). And it won't matter if the visitor in the room tries to steal something: There isn't anything for them to steal.

4AA8-2631ENUS, Feb 2023