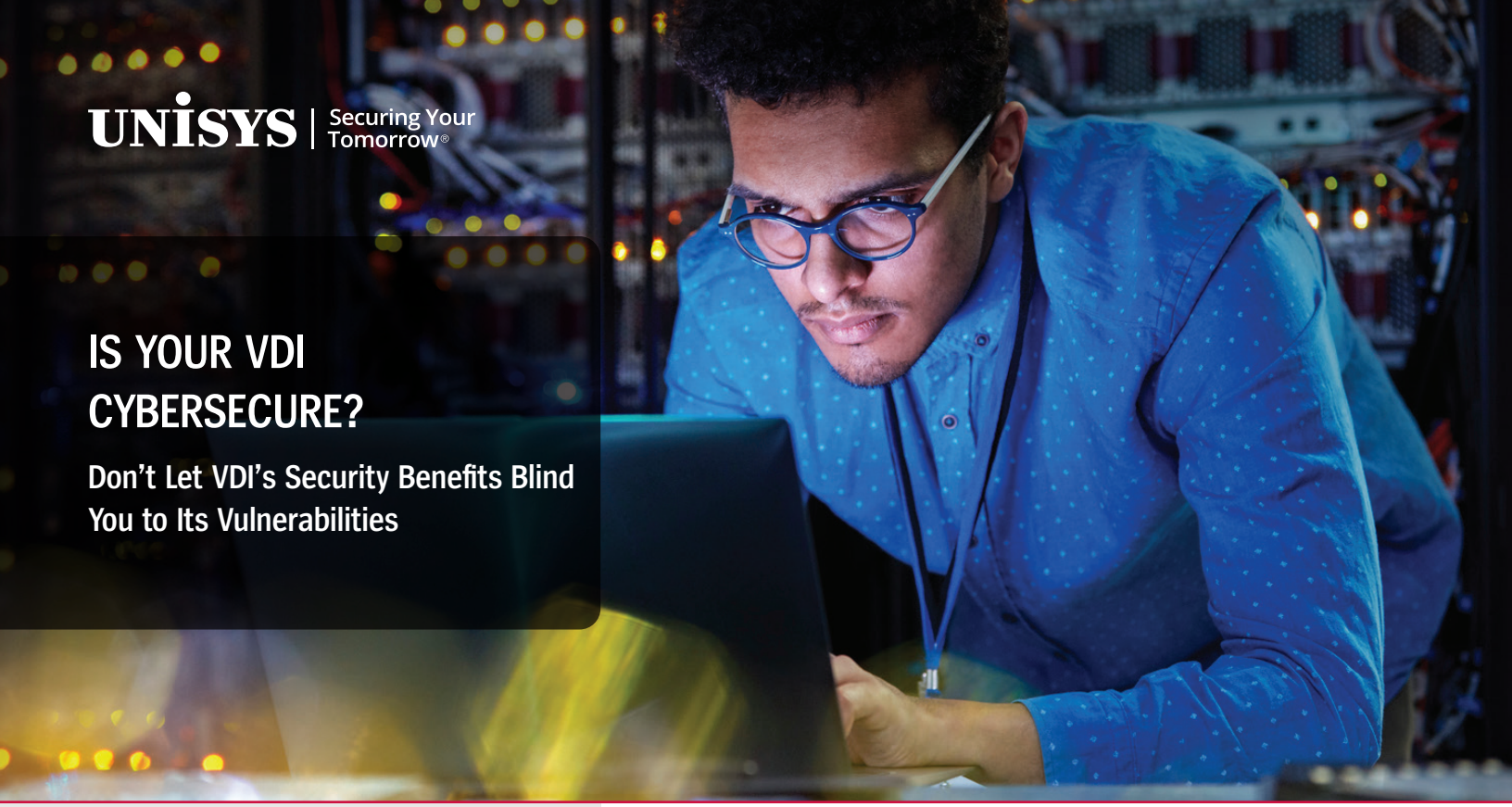

UNISYS | Securing Your Tomorrow®

IS YOUR VDI CYBERSECURE?

Don't Let VDI's Security Benefits Blind You to Its Vulnerabilities

SOLUTION HIGHLIGHTS

- *Protection from hackers who penetrate your end users' BYOD*
- *Protection for users who leave your VDI and then return, potentially infecting it*
- *A Zero Trust basis for allowing access to your network*
- *Immediate detection of an intrusion of your VDI environment*
- *Rapid isolation of the intruder to prevent lateral movement and data exfiltration*
- *Compliance with industry cybersecurity standards*
- *Swift, efficient deployment into your organization*

Chances are you did not expect that your deployment of Virtual Desktop Infrastructure (VDI) would have grave security implications because of VDI's enhanced centralization and isolation. But as many organizations are discovering, it would be a mistake to let the security benefits of VDI diminish your vigilance. Better protections against phishing, viruses, and malware have hackers looking for new targets, including VDI.

Your VDI is no doubt serving its main purposes: reducing strain on your IT resources and improving your end users' experience. IT can add and subtract desktops faster and spend less time managing them. They can troubleshoot them quickly and remotely. With employees' resources centralized in the data center or on the cloud, updates and patches are simpler.

In the meantime, your users get the exact desktop they need with high-bandwidth networking and swift response time, enabling them to work more efficiently and productively.

To be sure, it is safer to use VDI to store critical data at the data center or on the cloud, where your security measures are bound to be top-quality, rather than on each individual user's endpoint.

But there are still areas of vulnerability for your VDI environment.

VDI Vulnerabilities

External Site - In the normal course of their work, your end users most likely leave your VDI environment to access websites that lie outside of it, e.g., corporate partner resources such as employee benefits websites, search engines, competitor's websites, corporate tools like Workday or BambooHR, even your Human Resources intranet set, as well as permitted social media and e-commerce shopping sites.

If the communication path to these resources is not fully secured, as it often is not, the end user can be compromised and, upon returning to your VDI environment, infect your network and other users.

BYOD Remotely - At many organizations, Bring Your Own Device (BYOD) policies have not kept pace with the growing cybersecurity threats. BYOD has been growing rapidly in response to employee preference, employer permission, and the increased productivity BYOD often yields, and the pandemic's explosive impact on work-from-home policies has furthered the practice. In addition, employers are increasingly enabling BYOD for contractors, partners, customers, and suppliers. The result of this proliferation of BYOD is a vastly expanded attack surface and fresh opportunities for hackers to take advantage of such conditions to target unwary users of BYOD devices. Cybersecurity experts concur: With the high rate of hacking attempts and the fact that a simple error on the part of an end user can permit penetration, breaches cannot be entirely prevented, as Unisys CEO Peter Altabef explained. So it is important to keep in mind that BYOD policies can adversely affect the security of your VDI environment.

How to Secure Your VDI Environment

You cannot control or secure everywhere your data must go in today's world. You cannot secure every BYOD device that attempts to access your network. Instead, your VDI environment needs to be protected by a security approach that can quickly detect an intrustion, rapidly isolate it from the rest of the network and from other devices, and prevent data exfiltration and malware penetration and proliferation.

To do this, you need Unisys Stealth® deployed on all endpoints that may leave and return to your VDI. Stealth™ operates on these four principles:

- ***Zero Trust:*** Assume every access request is unauthorized until the requestor is authenticated.
- ***Software-Defined Perimeter:*** Instead of a hardware-dependent perimeter, adopt seamless, least-privilege access and a reduced attack surface.

- ***Micro-segmentation:*** Create micro-perimeters that conceal endpoints, restrict lateral data access from unauthorized traffic, and cloak personal and transactional information from intruders.
- ***End-to-End Encryption:*** Protect data in transit, no matter the underlying infrastructure. Reduce the attack surface and ensure confidentiality, integrity, and access to data.
- ***Dynamic Isolation:*** Remove a device or user from the network in as little as 10 seconds and bring it back just as quickly, automatically or with one click.

WHY UNISYS?

At Unisys, security is in our DNA. We took years to develop Stealth so that you can deploy it in just hours. To make Stealth ready for your organization, we Stealth-secured our own first. Today Stealth protects our entire organization, end to end. Stealth also protects the assets and reputations of thriving organizations across the globe – government agencies, financial institutions, and leading corporations. Our deeply experienced cybersecurity consultants can ensure a smooth, efficient deployment.

Contact us today at Stealth@unisys.com, or visit us at www.unisys.com/stealth

For more information visit www.unisys.com