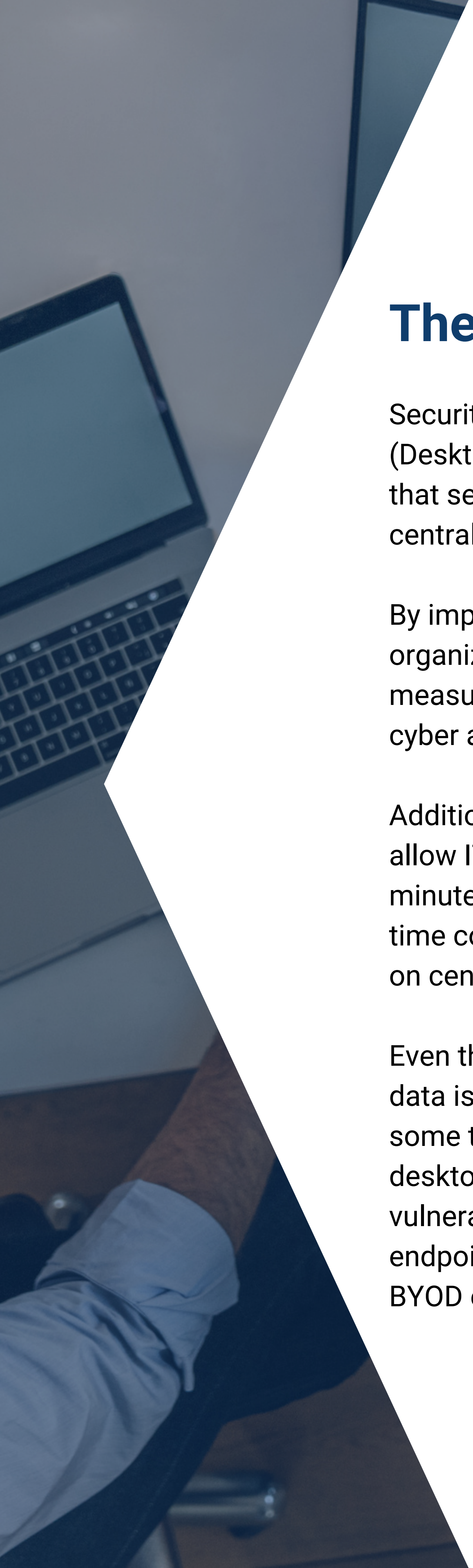
stratodesk

4 Security Obstacles IT Admins Face When Implementing VDI/DaaS

The four largest VDI security challenges and how to better protect your endpoints



The Innate Security of VDI/ DaaS

Security is one of the key concerns facing VDI/DaaS (Desktop-as-a-Service) deployments, yet it could be argued that security is the main reason for switching to a centralized or cloud-hosted infrastructure.

By implementing VDI or taking advantage of DaaS, organizations can strengthen their overall security measures, protect sensitive data, and minimize the risk of cyber attacks.

Additionally, on-premise or cloud-hosted desktop solutions allow IT Ops teams to set up many virtual desktops in just minutes and make the management of these easier and less time consuming. All desktop data and applications remain on central servers, reducing physical desktop security risks.

Even though the whole desktop with all its applications and data is living on a central server or on the cloud, users need some type of physical endpoint device to connect to “their” desktop. A physical endpoint, no matter how thin, is vulnerable and remains a security risk without the right endpoint security strategy especially in a hybrid work or BYOD environment.

The Endpoint Security Obstacles Facing IT Teams

Along with other tasks and systems to manage, IT teams face several obstacles as they balance VDI/DaaS support, reliability, while reducing complexity and increasing endpoint security for their in-office, hybrid, or remote desktop users.

1 Local Windows OS

The first obstacle to overcome is the local Windows issue. Even if users connect to VDI or DaaS, the IT team must run Windows installations on each of their endpoint devices. The IT team must invest additional hours to maintain these devices and apply patches when security vulnerabilities are found.

Not to mention, IT must also provide antivirus and malware protection for each and every endpoint device. To make things worse, different devices house different versions of Windows, which creates even more complexity.

Not if, but when the next Windows OS vulnerability is discovered, most organizations do not have a solid plan for quickly patching or locking down affected devices. With employees on vacation or extended leave, organizations cannot rely on the end-user to update and patch in timely manner. These unpatched endpoints leave huge security gaps for the organization.

2 Security vs. Work Efficiency

Along with the Windows problem is the matter of security. As previously mentioned, endpoint security is a key concern for virtual deployments – System Admins must not only increase and maintain a high security standard while also decreasing login times, they must enable hardened security standards for the safety of confidential data and information.

At the same time, they must allow staff to access all of the apps and data they need from any device, wherever they are. This causes great concern for IT managers who now have an equally high demand put not only on budget and security but also on ensuring convenience and flexibility for employees at the same time.

Reliability is crucial for employee work efficiency. Without an endpoint solution in place that is hassle free and one that offers a seamless user experience, employees cannot function at peak performance. If there is any hassle at all on the end user, you can quickly lose the benefit of VDI or DaaS as IT resources are redirected towards aiding and assisting employees.

3 Sometimes 'The Worst' Happens

If an endpoint device is lost or stolen, how can IT leaders be assured that no confidential information is then accessible from the endpoint device? What about potential "evil maid" attacks? In reality, too many attack vectors exist that target the endpoint devices themselves.

4 BYOD and Flexible Work Policies

Many enterprises and organizations of all sizes and across multiple industries are facing a growing problem: the trend of faculty and staff bringing personal devices into the office, or using their personal devices to work from home.

Employees want and expect to perform integral tasks on personal devices, either at home, in the office, or on the go. But how can this be done without opening up your network to the possibility of threats? Organizations have virtually zero control over endpoint devices themselves once they are in an employee's possession. If they are compromised, lost or stolen, these devices can pose a significant threat to your corporate network if the proper solutions are not put in place.

Better Protection for your Virtual Desktop and DaaS Workspaces

With these endpoint security considerations in mind, there are certainly other factors that will play into your organization's virtual desktop strategy. However, one way to address all four challenges in one solution is to virtually implement a secure operating system(OS) on the endpoint that equips employees with access to their virtual desktop and apps, while giving IT full manageability.

Since 95% of malware attacks target Windows OS, you can significantly reduce the attack surface for each endpoint that you install the read-only OS on. In addition to improving security, you can also cut costs and time spent managing local Windows updates/patches, local device antivirus and malware detection tools, and one-on-one device troubleshooting. And your employees can still use all the Microsoft apps and tools they like in the cloud or on the on-prem server without all the endpoint security risks.

Windows OS alternatives can also offer a flexible endpoint management and deployment platform to manage, update, and monitor your users' endpoints no matter where they are working. Your employees can get up and running quickly regardless of location, time zone, or their personal IT skills and their endpoints stay secure due to their Linux-based OS such as Stratodesk NoTouch.

Sources:

https://www.theregister.com/2021/10/14/googles_virustotal_malware/

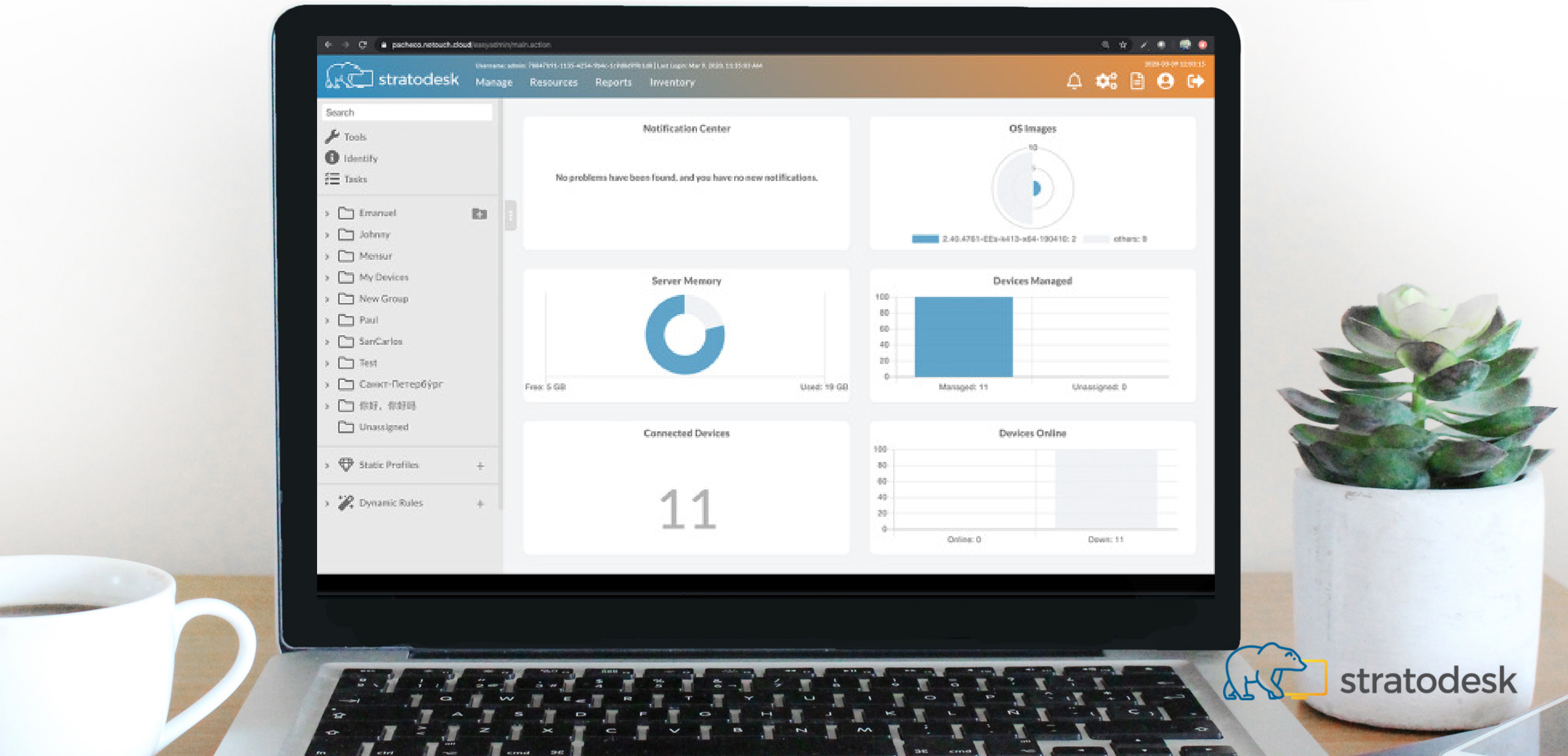
https://www.stratodesk.com/

Get a Free Trial of Stratodesk Today

NoTouch OS is an ultra-secure endpoint operating system (OS) crafted with precision to meet the unique demands of modern enterprises. With zero-trust architecture embedded in its core, NoTouch OS is the market-leading endpoint OS for VDI, DaaS, SaaS, Secure Browsing, IIoT, and Automation use cases.

This pioneering enterprise OS streamlines IT operations and endpoint administration, resulting in significant CAPEX and OPEX reductions, promotes sustainability by extending hardware life cycles and revolutionizes user experience and productivity while ensuring unparalleled endpoint security across all devices and locations.

Claim Free License



No problems have been found, and you have no new notifications.