MORPHISEC
Moving Target Defense

The Virtual Desktop Infrastructure (VDI) Security Guidebook

Security vulnerabilities in the new Work From Home world

PARTNER READY VMWARE HORIZON

Member of Microsoft Intelligent Security Association
Microsoft

CITRIX®

CONTENTS

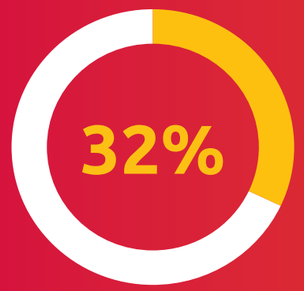
THE RISE OF VIRTUAL DESKTOP INFRASTRUCTURE

With more people working from home than ever before in history, virtual desktop infrastructures have arisen as a fast and cost-effective method to ensure that remote workers can access the applications, they need from wherever they are. In fact, VDI use might soon increase, as Gartner recently found that 74 percent of CFOs intend to shift some positions to working from home permanently because of increased efficiencies.

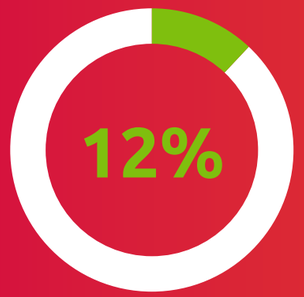
VDI use was on the rise prior to the current environment too. According to Spiceworks research, 32 percent of enterprises currently employ virtual desktops, with 12 percent expecting to implement VDI in the next two years. The adoption statistics become even more impressive among enterprises, with 50 percent already using virtual desktops compared to 24 percent of small and midsize businesses.

This is huge for a technology that barely had roots in the enterprise 10 years ago. Virtual desktops of many varieties, such as cloud-delivered Desktop-as-a-Service as well as server farms running proprietary virtualizations, are used across the business world. For a variety of reasons as well, including:

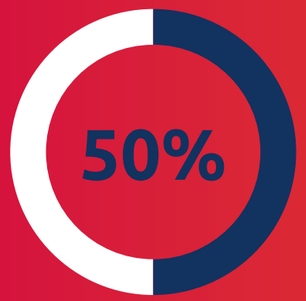
- **Cost-savings and reduced operational TCO –** As the number of virtual instances increases, virtual desktop infrastructure provides a cost-effective way to quickly spin up new desktop access to applications. For companies that have a high numbers of users who require only a limited set of applications, such as in a call center, a virtual desktop infrastructure allows the IT team to quickly and efficiently allow multiple employees to access the tools they need.
- **Improved employee mobility –** Virtual desktops enable workers to log into their specific instance wherever they physically are. What this means in practice is that employees no longer need to carry a bulky laptop or even a tablet with them to have access to information on the go.
- **Increased data privacy controls –** Control over data access is crucial for regulated industries like healthcare (HIPAA) and financial services. A virtual desktop infrastructure centralizes data governance and controls, and is crucial for compliance with rules around handling of personally identifiable information (PII).



of enterprises currently employ virtual desktops



expecting to implement VDI in the next two years



are already using virtual desktops

Source: Spiceworks

MORPHISEC
Moving Target Defense

- **Ability to recycle old technologies –** A thin client terminal used to access a virtualized desktop does not need to be kept as up to date as a traditional physical desktop. As a result of the VDI server being the host of the CPU, memory, and disk resources, old desktops and laptops can easily be repurposed to access virtual machines as needed.
- **Tighter control over installed applications –** With a virtual desktop infrastructure, IT normally has tight administrative control to determine which applications are installed on the system. This avoids the issue of regular end-users installing potentially unwanted applications.
- **Improved patch management processes –** One of the biggest security risks in the modern enterprise is unpatched vulnerabilities. With physical workstations, IT often has to depend on individual users to update their systems. In a virtualized environment, IT can update the golden image--especially valuable for non-persistent VDIs--at the end of the day and then be confident that everything is up to date when users login the next morning.

In the rest of this whitepaper, we will cover the types of virtual desktops, how some organizations use the technology, bust a few myths, and then provide some clearly actionable advice for organizations seeking to secure their virtual desktop infrastructure against cyberattack.

TYPES OF VIRTUAL DESKTOP INFRASTRUCTURE

There are two core types of virtual desktop infrastructure currently on the market. Each has different benefits and drawbacks, and the decision to use each type should depend on your organization's goals and needs.

- **Persistent VDI –** Persistent, or "stateful," VDI is called that because it persists between sessions. It's the most highly customizable type of VDI, and allows for each individual user to have a unique desktop hosted on the hypervisor. Persistent VDI is the closest to a physical desktop in user experience, in that it retains customizations between user sessions. It is also the most expensive form of VDI because of how much memory each virtual desktop requires.
- **Non-persistent VDI –** Non-persistent, also called "pooled" or "stateless," VDI is called non-persistent because it does not persist between user sessions. Once a user logs out of their session, the virtual instance they were using goes back to zero and doesn't retain any customizations the user may have made during the session. When the user logs back in again, they are presented with a generic desktop. Non-persistent desktops are most valuable when users need to access only a standard number of apps and centralized data.

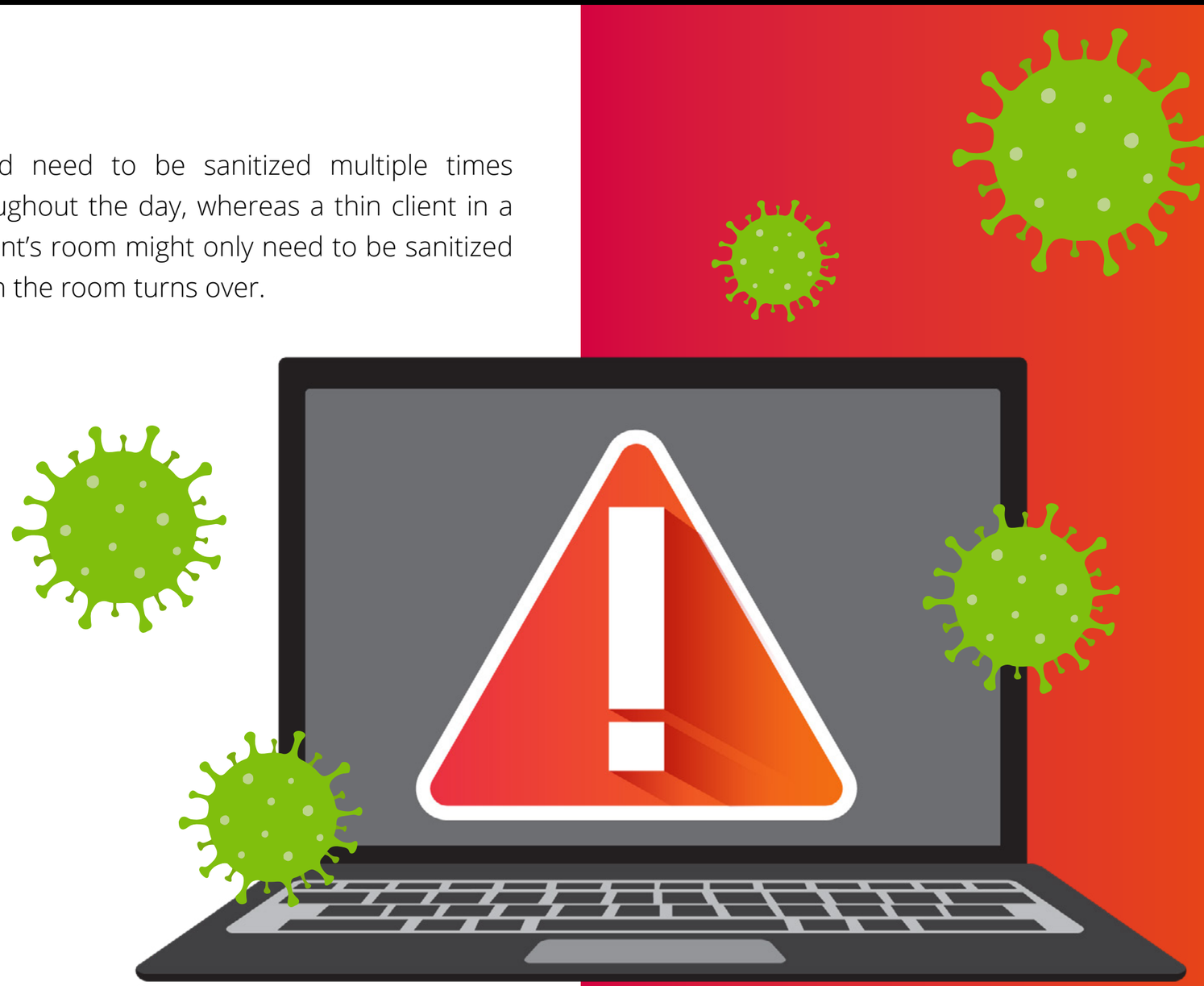
Persistent and non-persistent virtual desktops are both deployed on a centralized host-server, on which runs what's called a hypervisor. The hypervisor then manages the rollout of each virtual instance from a master boot image called the "golden image." This host-server can be on-premises in an enterprise's server room on-site or on the cloud from a server located in rented space in a data center. Another option for deploying VDI is known as desktop-as-a-service or DaaS. As with any "as-a-service" model, DaaS involves a third-party cloud provider hosting the virtual desktop infrastructure and management of the number of desktops falling to the enterprise's IT team.

DaaS is quickly becoming popular as more companies move away from managing their own on-premises systems. It's also somewhat democratized access to desktop virtualization, as enterprises no longer need to manage their own data center either through an on-site server room or colocation. Major providers of DaaS include Microsoft, Amazon Web Services, Citrix, and VMware among others.

VDI USE CASES

Virtual desktops are popular in a wide variety of industries for similar reasons. Organizations that require employees to move around throughout the building especially see the benefit from VDI, as do those who require strict security measures and patch management on employee systems. It's because of the tight control VDI enables from a central IT team that really makes it popular in highly regulated industries such as financial services and healthcare.

In healthcare, Morphisec customer Citizens Medical Center uses non-persistent virtual desktops to ensure that doctors and nurses can log into the applications they need throughout the Victoria, Texas-based hospital's buildings. By doing this, Citizens Medical Center avoids having medical professionals carry bulky laptops throughout their facility. It's also more sanitary in the long-term; a laptop would need to be sanitized multiple times throughout the day, whereas a thin client in a patient's room might only need to be sanitized when the room turns over.



Virtual desktop infrastructure deployed for customer support would ensure that CS reps have only the applications they need.

MORPHISEC
Moving Target Defense

VDI is attractive to financial services because IT teams can limit user access to sensitive data more easily, while also ensuring that virtual endpoints have up-to-date patches installed on their applications. Data accessed via VDI is never present on user endpoints; it's instead accessed on the server, which removes some common attack vectors. The server that hosts the hypervisor and sensitive data can also be locked down more tightly than a physical endpoint, such as through using hardening and whitelisting/blacklisting. IT can also centrally manage patching, thereby ensuring everyone in the organization is working on the most up-to-date software.

Another use-case for VDI is for customer support representatives. In most cases, customer support reps only need to access a few specific applications during the course of their working day. A non-persistent virtual desktop infrastructure deployed for customer support would ensure that CS reps have only the applications they need when they need them, and ensure they are working with the most up-to-date software.

VDI is ultimately hugely beneficial for enterprises from multiple dimensions, including enhanced employee mobility, tighter user access controls in regards to sensitive data, and improved patch management organization-wide. For these reasons, VDI has continued to grow in adoption, and we expect that to continue.

VDI MYTHS BUSTED

With all the benefits that can accrue to virtual desktop infrastructure users, it's nevertheless important to understand the myths that have grown up around the technology.

- **Data accessed via VDI is more secure –** Because no data is stored on a local machine, some IT professionals consider data accessed via VDI to be more secure. This simply isn't true; there isn't any local storage, but a VDI user session is still open to attack. A threat actor could still infiltrate a user session, move laterally to a server, and exfiltrate sensitive data. The lack of local data storage doesn't prevent that from happening. If anything, data being accessed via the host-server might create a higher likelihood of exfiltration.

- **Cancelling a user session cuts off a data breach –** There is a belief, especially in non-persistent VDI deployments, that turning off a session cuts off a data breach at the knees. This myth has prevailed because non-persistent VDI resets to a "clean" state on logout. The reality is that the adversary can establish persistency in the virtual network of the host's data center. A jump server will not save the day either; all it does is present a single point of failure for the adversary to attack. Similarly, deployments conducted rapidly--as in many current work-from-home situations--have security holes in abundance.

- **Virtual desktop instances don't need their own protection –** Because virtual desktop instances are deployed from a hypervisor on a host-server, there is a myth that the protection on the server is enough to secure the child desktops against attack. This isn't true. Virtual endpoints are still endpoints, and need to be protected against threats like remote access trojans (RATs) and lateral movement. On a fundamental level, in fact, virtual endpoints look no different than physical endpoints because most VDIs are virtualizations of a Windows operating system. The threats that face any other Windows machine are still valid against a virtual desktop.

Ultimately, what's important to understand about a virtual desktop infrastructure is that it's no more or less secure than any other IT systems deployed within your organization. Physical endpoints such as computer workstations and servers need to be secured against threat actors, and virtual desktops are no different in that respect.

COMMON ATTACKS FACING VDI

As stated previously, virtual desktops are no different from physical workstations from an operational perspective. Because of this, common attacks on VDI are functionally similar to those focused on physical environments. This includes infostealers, banking trojans, keyloggers, screen scraping, and password recording among others.

A few of the malware Morphisec Labs researchers have seen attack VDI include:

- **Agent Tesla**
- **Formbook**
- **Lokibot**
- **Trickbot**

One Morphisec customer in the healthcare space experienced a Trickbot attack against their virtual desktop infrastructure shortly after implementation. This attack was blocked with Morphisec's moving target defense technology, which was deployed on their VDI golden image and replicated across their non-persistent virtual desktop infrastructure.

Virtual endpoints aren't unique. A user can click on a malicious email link in a virtual desktop the same way that they can click on a malicious email link on a traditional workstation. There is little to no difference between these two security postures, except perhaps that virtual desktops are more likely to be up-to-date with software patches than physical endpoints and it's theoretically easier to harden VDIs against additional threats.

This doesn't, however, mean that virtual desktops are any more protected from zero day attacks than physical endpoints. If a zero day is found in a program installed on a virtual desktop, it is still possible for a threat actor to exploit that vulnerability. Similarly, lateral movement remains a risk for virtual endpoints and, by virtue of VDI running from a centralized server, potentially presents an even greater risk.

COMMON CHALLENGES OF SECURING VDI

Despite the obvious benefits of implementing a virtual desktop infrastructure, which we've already covered in a previous section, there are also some fairly significant challenges when it comes to securing VDI against the worst cyberattacks. These include limited memory and CPU resources, the risk of a "boot storm" from lagging updates, unreliable endpoint telemetry, and network limitations.

LIMITED MEMORY AND CPU RESOURCES

When a new virtual instance is created, the hypervisor assigns precisely the amount of memory and CPU required to operate the virtual desktop for maximum density. This takes into account all the needed applications within the virtual environment, as well as the number of virtual environments that need to be created at any given time. This is an especially important calculation when it comes to non-persistent desktops that need to be reallocated with each new user session. This is critical to gain the most ROI from a VDI deployment, as the best way to save on cost is to maximize the number of instances that each host-server can run at any given time.

The agents for most antivirus platforms, especially the ones that use machine learning for detection, tend to consume significant memory. As a result, deploying one of these agents on child desktops often reduces the number of virtual instances that can be run on the host-server. It's because of this that deploying antivirus on child desktops often leads to an increase in costs; fewer desktops can be deployed on each host-server, requiring additional infrastructure be installed to meet the same needs. Without these agents included, IT teams can deploy many more virtual instances on each host-server.

ANTIVIRUS "BOOT STORM"

Further, antivirus products require regular updates to their signature database to function properly. Even next-generation antivirus products, which often leverage machine learning algorithms, require regular updates and a reliable connection to the internet to receive them. The resource limitations of most virtual desktops mean that they are ill-suited for regular updates. Ideally, all signature or algorithm updates should occur on the golden image at the hypervisor level prior to spinning up new virtual instances.

Without regular updates of the golden image, there's a risk of an antivirus "boot storm" where multiple signature database updates are downloaded when the non-persistent virtual desktop is booted up. If this happens, there is a major impact on user experience and a massive spike in network traffic. VDI vendors VMware and Citrix, in fact, recommend turning off automatic updates for antivirus products on non-persistent desktops to avoid having a boot storm occur.

UNRELIABLE ENDPOINT TELEMETRY

Endpoint detection and response solutions require an agent to be installed on each endpoint, constantly sending telemetry back to a central console. In a physical endpoint environment, this means an agent on each workstation that then delivers the needed information back into the analytics engine.

In a virtual environment, this means putting an agent on every virtual desktop as well as the host server. Putting a single EDR agent on the hypervisor/host server extremely limited visibility into child desktops, which the IT team would need to fully monitor all endpoints.

The data that an EDR solution ingests from all these agents is enormous, which would consume needed resources on each virtual desktop as well as cause major network traffic at the same time. Consider that each virtual endpoint needs to send this same data back to the EDR solution; as the virtual desktop instances spins up or down, that network traffic becomes highly variable. Additionally, when the user logs out at the end of a non-persistent desktop session, that endpoint vanishes along with its monitoring agent.

This network traffic isn't like the boot storm that could happen when an AV signature database updates. It would be a consistent flow of traffic and endpoint data back from every single virtual desktop all the time, which results in huge data storage requirements for all this information.

Virtual desktop instances aren't designed to function the way an EDR platform needs them to. The sheer amount of network traffic that an EDR agent generates would overwhelm the virtual desktop and consume much of the memory needed to operate a VDI. As a result, EDR wouldn't provide any security benefits to a virtual desktop infrastructure.

NETWORK LIMITATIONS

Network traffic in general is expensive, and as virtual desktops are spun up or down there is a highly variable network load. Every additional agent–both monitoring and detection–creates additional variable load on the network. It's very easy to overload the virtual desktop and consume necessary compute resources with a monitoring and detection agent.

As such, to limit the network load, detection solutions might limit the traffic heading to the VDI. This means there is a bigger time window when a virtual desktop isn't updated for an attacker to strike and effect their attack; this can be lateral movement, credential theft, or any number of other goals.

To account for this, some VDI vendors have introduced the ability to only update signatures based on what the specific virtual desktop is missing in the moment. Others advise to update the golden image regularly to ensure that child desktops have the most up-to-date information. This limits network load, which can very easily increase exponentially depending on the number of virtual instances looking to be updated. Detection and monitoring solutions further will take necessary CPU resources, which additionally increases costs commensurate with the amount of resources consumed.

WHAT YOU NEED TO SECURE A VIRTUAL DESKTOP INFRASTRUCTURE

When it comes to securing a virtual desktop infrastructure against the worst cyber threats, there are a few key requirements that come to mind:

- **A lightweight agent –** Virtual desktops are already tight on memory and CPU resources, so the heavy agents of traditional endpoint protection solutions are ill-suited for virtual environments. What's needed is a lightweight agent that doesn't consume a lot of resources, thus enabling virtual instances to be spun up or down quickly as well as utilizing the full number of virtual desktop instances to better preserve density. This also enables child desktops to be "born secure" at the moment of creation.
- **A platform that doesn't require updates –** With antivirus boot storm a real problem, the golden standard for protection is a platform that doesn't require updating on boot. You can get around boot storm by keeping the golden image updated, but that only secures you against known threats; for unknown threats, the best option is a platform that doesn't require updates to secure VDI against advanced evasive malware.
- **A hardening solution to limit the attack surface –** Hardening is one of the best ways to add security to an endpoint. It's next to impossible to harden a physical endpoint past a certain point, largely because of the greater need for flexibility. Not so with a virtual desktop. Virtual desktops, especially non-persistent ones, can be more readily hardened compared to physical workstations. A solution that offers hardening capabilities is thus hugely beneficial.

One additional security measure that some solutions offer is user analytic behavior. This is an easier lift in a virtual desktop infrastructure largely because there's more administrative control and deeper visibility into what users are actually doing on their desktop. With the golden image on the hypervisor, and visibility into activity on child desktops, it's far easier to understand what is deviation from normal user behavior than on a physical machine.

CONCLUSION

THE FUTURE OF VDI SECURITY

Morphisec's moving target defense technology was built to secure critical systems with a lightweight agent that doesn't consume vital CPU or memory resources. The platform also doesn't require updates to deterministically block advanced evasive malware from infecting critical systems. Further, deploying the Morphisec agent at the host-server level and the golden image means that our application memory morphing system is replicated on every child desktop, automatically hardening all non-persistent or "pooled" VDI against advanced cyber attack.

Virtual desktops are only going to grow in popularity as more people continue to work from home. As a result, enterprises of all sizes are going to need to secure their virtualized infrastructures against advanced evasive malware and will need to do so with a security solution that avoids antivirus boot storm, doesn't consume memory or CPU resources, doesn't require frequent updates, and avoids the need for EDR-like endpoint telemetry. The future of VDI security is now... will you be able to secure it?

MORPHISEC
Moving Target Defense

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology – placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.