THINSCALE

ThinScale's guide to

Protecting your VDI / DaaS from Data Loss & Unauthorized Access

Virtual Desktops & Security

www.thinscale.com

Table Of Content

Introduction

Virtual Desktop Infrastructure (VDI) and Desktop as a Service (DaaS) have become crucial tools for organizations managing remote work setups. Post-pandemic, these virtual environments are no longer a luxury but a necessity. However, the rapid adoption of VDI/DaaS often outpaced the implementation of robust security measures.

Many organizations, in the haste to facilitate remote work, relied solely on a Virtual Private Network (VPN) or, in some cases, neglected security altogether.

This short ebook is a practical resource for those looking to strengthen the security posture of their virtual environment. Our goal is to equip you with the knowledge and practices needed to effectively safeguard your virtual assets.

In the following chapters, we'll break down the threats to virtual infrastructures, untangle the complexities of access management in a work-from-home setting, and navigate the landscape of malware prevention. We'll also dive into the vulnerabilities of endpoints and explore cutting-edge technologies to enhance virtual desktop security.

Along the way, we'll stress the importance of constructing a robust security perimeter and provide practical insights into implementing multi-layered defence strategies.

Chapter 1
Understanding the Threats to Virtual Environments

The widespread adoption of VDI and DaaS brings with it a range of potential threats to virtual infrastructures. In this chapter, we'll shed light on the risks and vulnerabilities associated with virtual environments.

Identifying Threats

In the context of VDI/DaaS, threats can manifest in various forms, jeopardizing the confidentiality, integrity, and availability of virtual environments. Unauthorized access, data breaches, and system vulnerabilities are common concerns. By pinpointing potential threats specific to your virtual infrastructure, you can tailor security measures to address these challenges effectively.

Key considerations include:

- Unauthorized access attempts and their implications.
- The risk of data breaches and the potential impact on sensitive information.
- Vulnerabilities in the virtual environment that may be exploited by malicious actors.

Assessing Risks and Vulnerabilities

An effective security strategy demands a thorough assessment of risks and vulnerabilities associated with VDI/DaaS environments. This involves a pragmatic analysis of potential weak points that adversaries could exploit. By understanding these risks, organizations can prioritize security efforts and allocate resources where they are most needed.

Critical aspects to explore include:

- Identifying vulnerabilities in virtual infrastructure components.
- Analyzing potential points of entry for malicious actors.
- Evaluating the impact of successful exploitation of these vulnerabilities on overall security.

Proactive Security Approach

Taking a proactive stance involves more than just reacting to security incidents. It requires anticipating potential threats and implementing preventive measures. A proactive security approach for VDI/DaaS environments includes continuous monitoring, timely updates, and the establishment of resilient security protocols to thwart threats before they escalate.

Key elements of a proactive security approach:

- Continuous monitoring of virtual infrastructure for anomalous activities.
- Timely implementation of security updates and patches.
- Establishing a resilient security framework that anticipates evolving threats.

The Major Threats to VDI/DaaS Infrastructures

Lack of Endpoint Control

When organizations lack control or fail to protect their endpoints, it opens the door to untrusted devices connecting to VDI and DaaS environments. This can lead to vulnerabilities that may compromise the overall security posture.

Hacking and Exploitative Social Engineering

We see malicious actors often employ hacking techniques and social engineering tactics to extract user credentials, which they can then utilize to gain unauthorized access. Recognizing these threats is vital to prevent security breaches.

Inadequate Data Safeguards

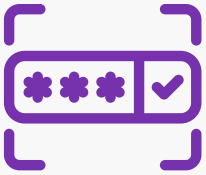
The absence of policies and controls in place to safeguard data can result in potential data exfiltration via VDI and DaaS channels. Ensuring robust data protection measures are in place is critical to mitigate this risk.

Zero-Day Exploits

The ever-present threat of zero-day exploits can potentially compromise devices both inside and outside of the VDI and DaaS environments. Staying vigilant and proactive in addressing these vulnerabilities is essential for maintaining a secure environment. The best model to switch to is a trust-nothing approach.

Security Threats for VDI/DaaS Environments

Endpoint Vulnerabilities



Credential Theft

Zero-Day Exploits

Lack of Endpoint Security

No Data Protection

No Access Control

BYOD & Unmanaged Device Risks

No Device Trustworthiness

Chapter 2

Access Management in the Work-From-Home Era

The demands of a distributed workforce have introduced unique challenges that forced IT leaders to re-assess their access management strategies and policies.

This chapter delves into the intricacies of managing access in the work-from-home era, emphasizing the need for proactive measures to secure virtual environments effectively.

The Shift to Remote Work

The widespread adoption of remote work has transformed the traditional office landscape, presenting both opportunities and challenges. Understanding the specific challenges posed by a distributed workforce is crucial for developing tailored access management solutions. Key considerations include the diversity of devices, network connections, and potential vulnerabilities inherent in remote setups.

Exploring Challenges:

- Variability in the quality and security of home network connections.
- Diverse devices accessing virtual environments, each with its own security profile.
- Balancing the convenience of remote work with the need to maintain a secure virtual environment.

Proactive Access Management

Proactive access management is paramount in mitigating the risks associated with unauthorized access. This section focuses on proven approaches that organizations can implement to bolster their access management protocols.

Key components of proactive access management:

- Regularly reviewing and updating user access privileges.
- Implementing least privilege principles to restrict unnecessary permissions.
- Utilizing multi-factor authentication to add an additional layer of security.
- Monitoring and logging access activities for potential anomalies.

Importance of Robust Authentication Mechanisms:

Authentication lies at the heart of access management. This section underscores the critical importance of robust authentication mechanisms in ensuring that only authorized personnel gain entry to virtual environments.

We recommend:

- Implementing strong password policies.
- Advanced MFA methods such as biometric authentication methods for enhanced security.
- Employing single sign-on (SSO) solutions for streamlined yet secure access.

Setting up Host Checks in Work-From-Home Environments

Setting up host checks for devices accessing virtual environments in a WFH environment is crucial for ensuring security and compliance. Host checks help verify the health and security posture of the devices connecting to the virtual desktop environment, minimizing the risk of unauthorized access and potential threats. Here's a guide on how to implement effective host checks:

Define Compliance Policies

Clearly outline the compliance policies that devices must adhere to before gaining access to the VDI/DaaS environment. This includes requirements such as updated antivirus software, operating system patches, and specific security configurations.

Use Endpoint Security Solutions

Implement endpoint security solutions that offer host checking capabilities. These

solutions can assess the device's compliance with predefined policies, ensuring it meets the security standards set for accessing the virtual desktop infrastructure.

Network Access Control (NAC)

Integrate Network Access Control mechanisms to evaluate devices attempting to connect to the VDI/DaaS. NAC verifies the device's health status, compliance with security policies, and ensures that only authorized and secure devices can access the network.

Device Auditing

Employ device profiling to gather information about connecting devices. This includes details such as device type, operating system version, and security software. Profiling assists in identifying and allowing only trusted devices to access the virtual desktop environment.

Multi-Factor Authentication (MFA)

Enhance security by implementing multi-factor authentication. In addition to host checks, MFA adds an extra layer of verification, reducing the risk of unauthorized access even if a device passes the initial compliance checks.

Continuous Monitoring

Establish continuous monitoring mechanisms to track changes in device status. Periodic re-evaluation ensures that devices maintain compliance throughout their connection to the VDI/DaaS, responding to any alterations in the device's security posture.

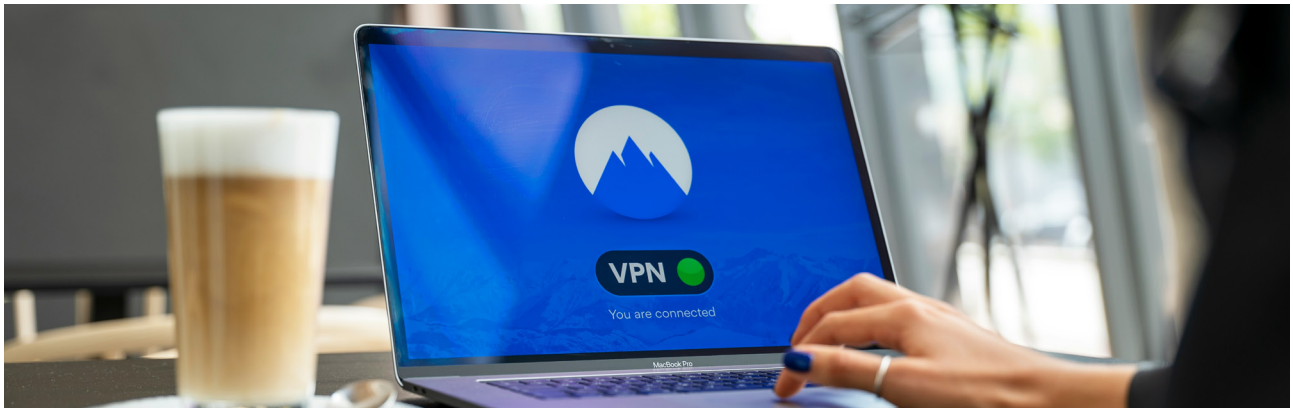
User Education & Communication

Educate users on the importance of maintaining a secure device and the role of host checks in safeguarding the virtual desktop environment. Clear communication helps users understand their responsibility in maintaining a secure work environment.

ThinScale's VDA and device vetting tools help to ensure that only authorized and policy compliant devices are given access to your virtual environment.

5 Threats Associated with VPNs

VPNs often play a crucial role in securing access to VDI environments, particularly in the context of WFH. However, VPNs, when used as the primary or even sole, access security layer are vulnerable to several threats.



Here are the 5 major ones, and what you can do to prevent them:

Unauthorized access via VPN

One of the main risks is the possibility of unauthorized access by malicious actors who obtain VPN credentials. If an attacker gains access to valid VPN credentials, most likely through a phishing exercise, they can potentially use the VPN to connect to the VDI environment.

→ **Required action:**

Organizations must implement robust authentication measures, such as multi-factor authentication (MFA), to mitigate this risk.

Insider threats

The danger of internal actors misusing VPN access cannot be overlooked. If an employee with legitimate access decides to act maliciously, they could use the VPN to connect to the VDI environment from an unauthorized device.

→ **Required action:**

Organizations must implement stringent VDI access controls, regularly monitor VPN logs, and conduct thorough background checks to minimize the risk of insider threats.

VPN software vulnerabilities

Like any software, VPNs can have vulnerabilities that could be exploited by hackers. If a bad actor discovers and exploits a vulnerability in the VPN, they may gain unauthorized access to the VDI environment.

→ **Required action:**

Regularly updating and patching VPN software is crucial to address known vulnerabilities and ensure the security of the connection.

Compromised endpoints

If the endpoint device used for VPN access is compromised, either through malware or other security breaches, the security of the VPN connection is jeopardized. Hackers could potentially use the compromised device as a gateway to access the VDI environment.

→ **Required action:**

Employing endpoint security measures, such as device lockdown, antivirus software and regular security audits, helps mitigate this risk.

Man-in-the-middle attacks

VPNs are susceptible to man-in-the-middle (MitM) attacks, where an attacker intercepts and potentially alters the communication between the user and the VDI environment.

→ **Required action:**

Utilize strong encryption protocols and secure key exchange mechanisms within the VPN implementation.

Chapter 3

Building a Secure Perimeter Around Your Virtual Desktop Environment

Building a secure perimeter is never a one-size fits all approach. In fact, some IT thought-leaders have suggested that the notion of a perimeter itself is out-dated. Instead, they argue that we should focus on the concept of zero-trust architecture.

But in many ways, this is just semantics- a perimeter can also be built on the principle of “trust no-one”. So, let’s look at how you can embed this into your security posture.

Keys to Zero Trust Architecture:

Assume Breach

Zero trust challenges the notion that internal networks are safe by default. Every user, device, and application is treated as untrusted until proven otherwise.

Micro-Segmentation

Implementing micro-segmentation is a fundamental aspect of zero trust. This involves dividing the network into small, isolated segments, limiting lateral movement in case of a breach.

Integrating Solutions

True zero trust requires a blend of solutions into a multi-layered defense that emphasizes constant monitoring, continuous verification, and strict access controls.

How ThinScale ensures secure access

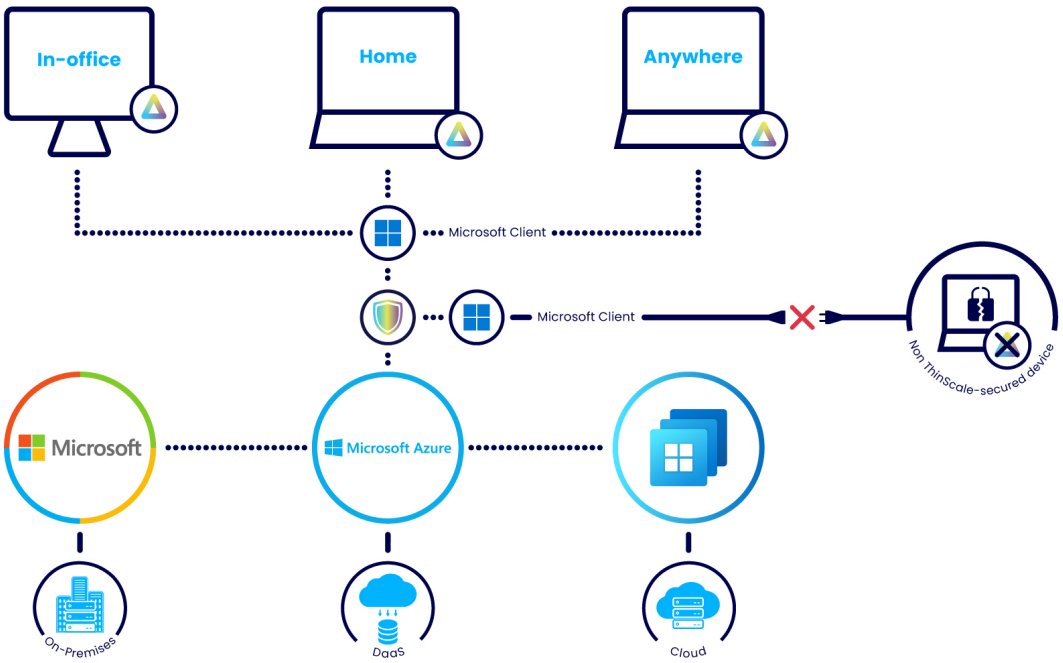
01. ThinScale’s Virtual Desktop Agent (VDA) intercepts all attempts to access your virtual desktop environment.

02. It performs a number of policy checks and confirms whether or not the device requesting access is running a secure, ThinScale session.

03. If the device is secured with ThinScale then access to the virtual environment is granted.

04. If the device is unsecured then access to it is denied.

05. Not only does it prevent users from inadvertently exposing your environment to malware sitting on the device, it also helps prevent phishing-based attacks as obtaining a user's log-in credentials or even using the same VPN is no longer sufficient.



An overview of how ThinScale's VDA works. It is shown here with Azure Virtual Desktop, but it is compatible with all major virtualization vendors- VMWare, Citrix etc.

Secure your VDI & DaaS Deployments

Virtualized deployments offer IT teams more security, control and better ease of use than other deployment methods. However, they do very little to protect the endpoint from things like malware, the infiltration and exfiltration of confidential data, and even user-initiated risk.

This is why endpoint security solutions are almost always used with VDI or DaaS deployments as a best practice because it provides the organization with true end-to-end security and control. This ensures that the cost committed to implementing a VDI or DaaS deployment is not made irrelevant by unsecured endpoints.

How Does ThinScale Secure & Enhance your VDI & DaaS Deployments?

Secure & control endpoint access

Protect your virtual resources by enforcing a zero-trust security framework on your endpoints - controlling what employees can access.

Data leakage prevention

ThinScale's encrypted temporary storage can only be accessed by someone with valid credentials. Further, features like write filtering, USB device blocking, and application blocking ensures that no unwanted infiltration or exfiltration of data can occur.

Accelerate VDI & DaaS deployments

Centrally convert and manage endpoints as secure workspaces, preconfigured and packaged with any client authentication settings needed for your employees to quickly access their virtual resources.

Centrally update your VDI clients

ThinScale also provides a streamlined way for IT teams to deploy updates to their VDI & DaaS clients through the ThinScale Management Platform's Software Packages functionality.

Contact us

THINSCALE | V8

learn more **thinscale.com**