

# THINKIOSK

## Secure and easy to manage corporate endpoints

TECHNICAL DATASHEET



THINSCALE

# Solving the Challenges of Working from Anywhere

Organizations around the world are choosing to implement a Work from Anywhere policy, which benefits both the employee and the company. However, there are several factors to consider:

- ✔ Security and compliance
- ✔ Ease of management
- ✔ Scalability
- ✔ Control and supportability
- ✔ Cost
- ✔ Speed of deployment
- ✔ Employee experience

ThinKiosk addresses these challenges by enabling employees to work easily and securely from any location, and any device. All are managed from an easy-to-use centralized platform. All while reducing costs and boosting ROI on existing hardware.

## ThinKiosk Benefits



### Deliver PCI and HIPAA Compliance

ThinKiosk enables organizations to meet the stringent compliance requirements demanded by QSAs for PCI, HIPAA, and GDPR compliance.



### Convert any Windows Device

ThinKiosk allows employers to use new and existing Windows devices. This ensures compatibility with all hardware and applications that IT teams and end-users are accustomed to.



### Full Device Lockdown

Secure corporate machines by locking them down with a centralized policy preventing them from accessing the underlying OS.



### Dynamic Workspace Environment

ThinKiosk gives employees a secure workspace that can be accessed from any ThinScale device from where they can access their IT-curated apps and services.



### Familiar Employee Experience

ThinKiosk delivers a familiar and intuitive user interface, with a Windows look and feel, along with enhanced productivity features.



### Centralized Management

Manage your entire remote device estate using a single management platform with a single administrative console.



### Simplified work from anywhere support

With authentication integration and user-based profiles, users simply need their credentials to access their environment. Time-consuming re-imaging is also eliminated. Drastically reducing IT workload.



### Reduce Cost, Increase ROI

ThinKiosk enables organizations to reduce the cost of hardware acquisition, by allowing the repurposing of older hardware, increasing the lifespan of machines by an average of 5 years.

# Endpoint Security and Compliance



## ✔ Full Lockdown of Corporate Devices

ThinKiosk denies access to the underlying Windows operating system, disabling the OS. Instead, an employee will access the ThinKiosk workspace, a simple and easy-to-navigate user interface from where they can connect to their corporate resources securely, with access to nothing unapproved by IT.

## ✔ Prevent USB Mass Storage Devices from Being Accessed

USB devices are often seen as one of the main causes of security breaches and data leakage within an organization. ThinKiosk can prevent these devices from being used while maintaining compatibility with USB hardware (e.g. headsets) with its USB device blocking feature.

## ✔ Prevent Unauthorized Apps from Being Launched

The ThinKiosk Application Execution Prevention (AEP) feature adds an additional layer of security by preventing the execution of unauthorized applications. Employing a rules-based system, IT admins can create white/blacklists to configure exactly which apps employees are allowed to launch on their ThinKiosk device.

## ✔ Prevent Unauthorized Services from Running

The Service Execution Prevention (SEP) feature of ThinKiosk allows you to control which Windows services are allowed to run on your ThinKiosk corporate machines. If a service attempts to run and it does not match the defined Service Execution Prevention policies, then the service will be unable to run.

## ✔ Securing the Employees' Browsing Experience

An integrated secure web browser is included as part of ThinKiosk, enabling employees to securely browse internet sites or access virtual resources via HTML, based on policy set by the IT department, who can dictate the entire browsing experience, all with the full support of URL white/blacklisting.

## ✔ Ensuring Devices are Protected and Monitored

ThinKiosk proactively monitors the security components of the device OS, such as Firewall Protection, Anti Virus, and much more. If one of these components is not compliant or configured correctly, ThinKiosk can take the appropriate action for remediation, ensuring that issues are quickly resolved.

## ✔ Prevent Data Leakage on Corporate machines

ThinKiosk's temporary storage prevents data leakage entirely on the corporate machine. Automatically creating a Virtual File System (VFS) that intercepts all write requests made to the volume, the Write Filter ensures a clean slate for ThinKiosk whenever the machine is booted up.

## ✔ Control Virtual Machine access with Contextual Security

ThinKiosk can also prevent employees from accessing virtual/remote resources from other unsecured endpoints using the Virtual Desktop Agent (VDA). VDA detects an employee is connecting from outside a ThinKiosk machine, and will carry out remediation based on IT policy.

## ✔ Wired network enforcement and Wi-Fi detection

ThinKiosk can be set to enforce connection only through wired network connections, or only through defined, trusted wi-fi networks. This ensures against malicious actors being introduced in scenarios where users bring their corporate devices to unknown areas and attempt to connect to untrustworthy internet hotspots.

# Enhanced Workplace Efficiency



## ✔ Device and Environmental Health Checks

ThinKiosk includes a unique solution that enables IT admins to enforce frequent checks on the health and status of the corporate device and its external environment, ensuring that both meet the minimum requirements set by your company.

## ✔ Simple and Familiar User Experience

The employee experience is key to productivity. ThinKiosk delivers a familiar Windows look and feel, coupled with an intuitive and customizable user interface that enables fast and easy access to corporate resources. ThinKiosk also passes through local Ctrl +Alt +Del and other keystrokes through to remote environments, just as if the employee is working locally on their device.

## ✔ Centralized Deployment

ThinKiosk can be easily deployed remotely as a simple to install MSI file, meaning your IT team can quickly get your corporate machines up and running, requiring very little from IT to actually secure your corporate environment.

## ✔ Scalable Enterprise Architecture

ThinKiosk can scale to deliver secure and managed workspace environments for thousands of remote Windows-based PCs, laptops, and thin clients, all managed from the ThinScale Management Platform. As a software-only solution, ThinKiosk delivers flexible scalability and as such, it supports any Windows-based device from any vendor, meaning IT teams are not dependent on a single hardware vendor.

# Centralized management and control



## ✔ Ensuring Windows is Always Secure and Up To Date

ThinKiosk enables IT departments to easily manage Windows updates, ensuring that the employees are up to date with all the relevant patches before connecting to the corporate environment. For IT, this means they can configure how often the client devices check for any updates and then decide when and if to apply them.

## ✔ Manage Network Security

ThinKiosk allows IT admins to fully configure the Windows Firewall feature internally. They can edit or remove any existing firewall rules, or configure new firewall rules, and manage this centrally from the ThinScale Management Platform and ThinKiosk's profile editor.

## ✔ Third Party Software Deployment and Installation

Through the ThinScale Management Platform, IT can centrally create, save and deploy software packages across their whole environment to be installed locally at the employee's endpoint. Anything from VDI clients, applications, and security certificates can all be deployed as software packages.

## ✔ Simplified Management, Support, and Onboarding

As ThinKiosk is a software-only solution, IT simply needs to deploy the software by whatever means they wish and can get their corporate machines secured and ready for use in a matter of hours as opposed to days. IT admins have the ability to manage the secure workspace environment remotely, allowing them to update security policies on the fly, with no need for a deskside visit or employees to travel in or send devices back.

# Solution Brief

## What is ThinKiosk?

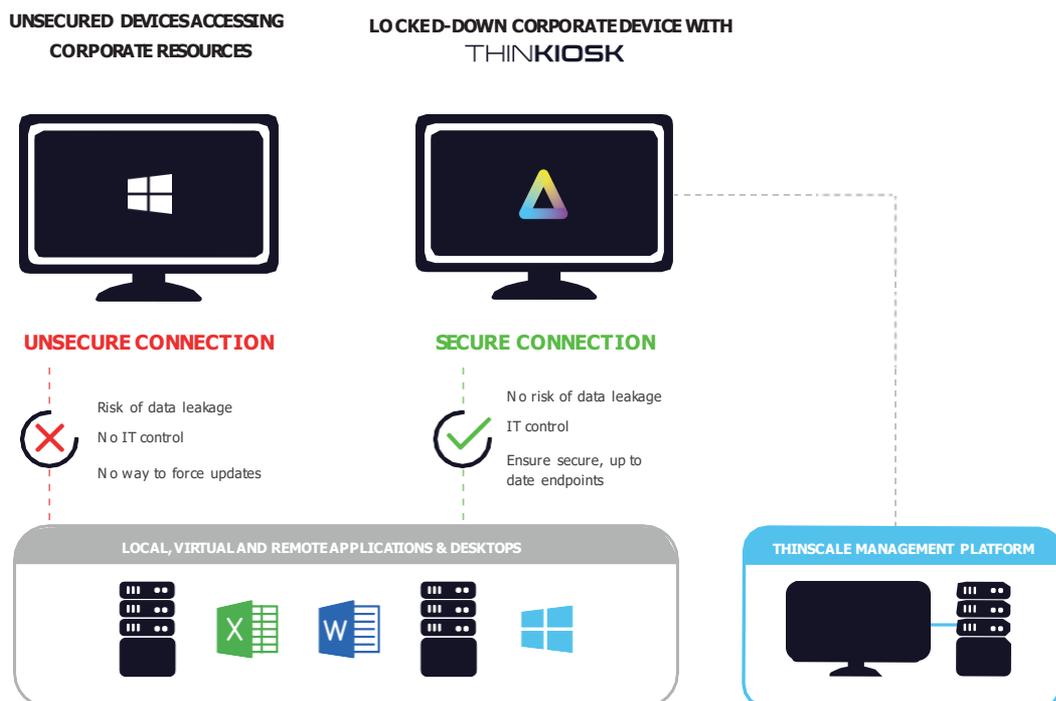
ThinKiosk is a Windows application that is installed on corporate Windows devices. Upon installation, it converts the Windows device into a fully locked down corporate device.

## What isn't ThinKiosk?

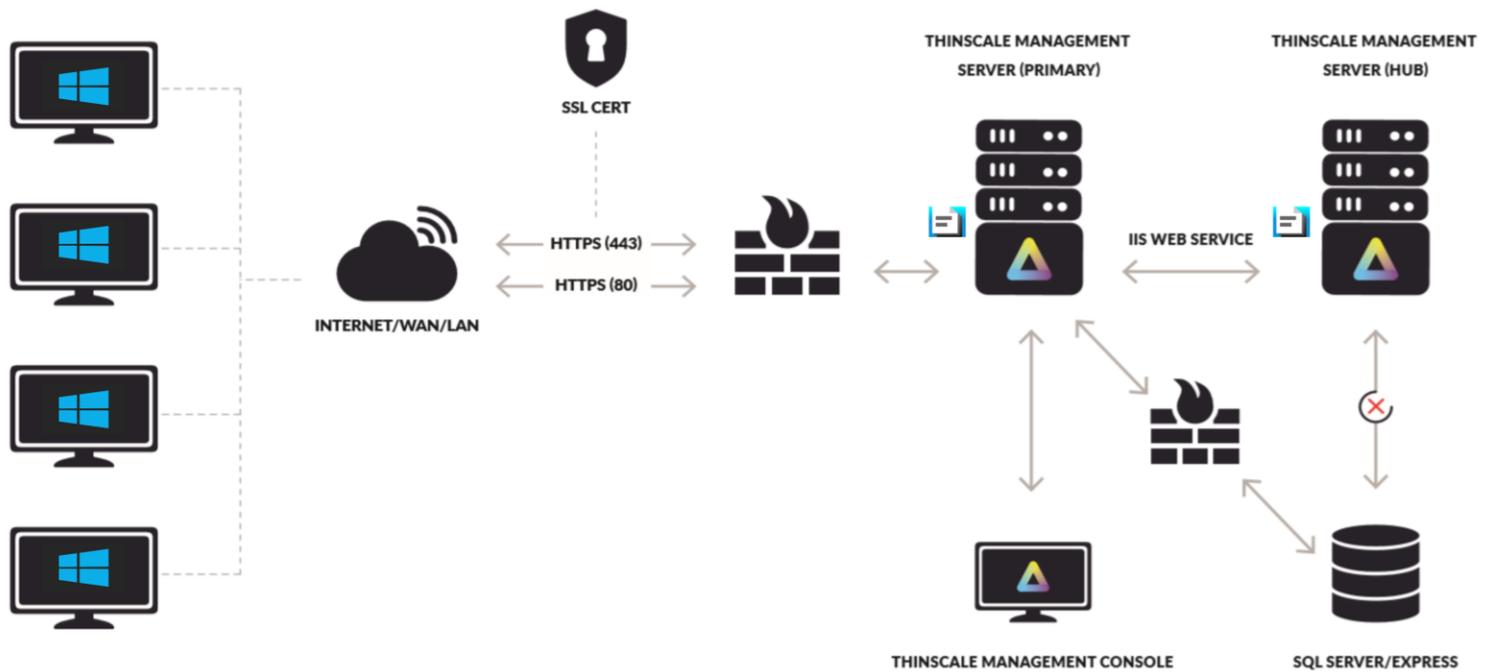
ThinKiosk is not a hardware-defined Thin client, nor a ThinOS. It runs on top of the existing Windows operating system and does not use container or virtualization technology to run another operating system instance.

## How ThinKiosk Works

- Blocks the Windows OS and runs a low permission ThinKiosk Shell persistently on top
- Access policies are evaluated ensuring the personal PC meets security requirements
- Windows Patches are installed
- AV/AS are installed and running FW policies are applied
- Not running inside a virtual machine
- Applies Windows policy settings to prevent access to the underlying OS
- Creates temporary storage to prevent data leakage
- Enables its Application Execution Prevention (AEP) and Service Execution Prevention (SEP) technologies to prevent the execution of unauthorized applications
- Blocks USB storage devices at driver level to ensure no data can be manually removed



## THINSCALE MANAGEMENT PLATFORM ARCHITECTURE



### TECHNICAL SPEC

## ThinKiosk Components



### ✔ ThinKiosk Client

A lightweight application that installs the ThinKiosk shell and blocks the underlying Windows OS on corporate devices, compatible with all Windows x64/86 devices.

### ✔ ThinScale Management Platform

The ThinScale Management Platform provides easy management and control over your entire endpoint environment.

### ✔ Virtual Desktop Agent

Installs on the VM/RDSH and performs checks on the connecting device and performs actions based on whether the connecting device is running ThinKiosk.

## THINKIOSK REQUIREMENTS

<b>ThinKiosk Client</b>	<ul style="list-style-type: none"> <li>• .NET Framework 4.7.2 or above</li> <li>• Windows 8.1 or higher</li> <li>• Firewall rule allowing ThinKiosk to take inbound connections (created by the installer)</li> <li>• Internet Explorer 7 or higher</li> </ul>
<b>Management Server</b>	<ul style="list-style-type: none"> <li>• Windows Server 2012 or above</li> <li>• .NET Framework 4.7.2 or above</li> <li>• .NET Core 5.0.5 Runtime specific               <ul style="list-style-type: none"> <li>• <a href="https://dotnet.microsoft.com/download">https://dotnet.microsoft.com/download</a></li> <li>• <i>Note: it will be installed automatically during installation, if not present</i></li> </ul> </li> <li>• Internet Information Services (IIS)               <ul style="list-style-type: none"> <li>• 8.5 for Server 2012 R2</li> <li>• 10.0.14393.0 for Server 2016</li> <li>• 10.0.17763.1 for Server 2019</li> </ul> </li> <li>• 3GB of RAM or above</li> <li>• 1GB of FREE Space or above</li> <li>• SQL Server 2012 or above (if using SQL for your database)               <ul style="list-style-type: none"> <li>• 1GB minimum DB size ~ 4,000 devices require at least 2 GB, but it also depends on how long your data retention is set to.</li> </ul> </li> <li>• SQL Express is also supported</li> <li>• BitLocker Drive Encryption</li> <li>• BitLocker Network Unlock</li> <li>• Evergreen Bootstrapper distribution (7.2 only)</li> </ul>
<b>Management Console</b>	<ul style="list-style-type: none"> <li>• Windows 2008 / Vista (or above)</li> <li>• .NET Framework 4.6.1 (or above)</li> <li>• 500MB minimum disk free space</li> </ul>
<b>Virtual Desktop Agent</b>	<ul style="list-style-type: none"> <li>• Windows 7 / Windows Server 2012 (or above)</li> <li>• .NET Framework 4.5 (or above)</li> </ul>

## THINKIOSK FEATURE LIST

<p><b>Central Management</b></p>	<ul style="list-style-type: none"> <li>• ThinScale Management Server</li> <li>• ThinScale Management Console</li> <li>• Software Package Installation</li> <li>• Secure Session Apps Installation</li> <li>• Scripting Functionality</li> <li>• Roles-Based Administration</li> <li>• Windows Patching Management</li> <li>• Firewall Control Management</li> <li>• User-based profile assignment</li> <li>• Azure AD, Ping &amp; Okta Authentication support</li> <li>• Device Activity Auditing</li> <li>• Central deployment</li> </ul>
<p><b>Control</b></p>	<ul style="list-style-type: none"> <li>• Local Application Access</li> <li>• Internal VDI/RDSH Connection (Citrix, VMware, RDS, WVD)</li> <li>• Whitelist and Blacklist URLs</li> <li>• Wi-Fi detection</li> </ul>
<p><b>User Experience</b></p>	<ul style="list-style-type: none"> <li>• Configuration of Local Settings</li> <li>• Access Policies</li> <li>• Browser Multi-Tab Implementation</li> <li>• Support for Magic Filter</li> <li>• LDAP Integration</li> <li>• Support for 4K Display, DPI Scaling, Duplicate, Extends and Identify</li> </ul>
<p><b>Security</b></p>	<ul style="list-style-type: none"> <li>• Endpoint Protection Features</li> <li>• Endpoint Security Features</li> <li>• Secure Browser</li> <li>• Windows Security Center Detection</li> <li>• Virtual Machine Detection</li> <li>• Anti Virus Definition Detection</li> <li>• Anti Spyware Definition Detection</li> <li>• WiFi Detection</li> <li>• Application Execution Prevention (AEP) Implementation</li> <li>• Service Execution Prevention (SEP) Implementation</li> <li>• USB Mass Storage blocking</li> <li>• ThinScale Virtual Desktop Agent (VDA)</li> </ul>



The Media Cube, IADT,  
Kill Avenue, Dún Laoghaire,  
Co. Dublin,  
Ireland, A96 X6X3

**+353 1906 9250**  
**[hello@thinscale.com](mailto:hello@thinscale.com)**