WHITE PAPER

# THINKIOSK & SECURE REMOTE WORKER

## PCI DSS COMPLIANCE WHITE PAPER

## ThinScale Technology

**Joel Dubin** | CISSP, QSA, PA-QSA
**Nick Trenc** | QSA, PA-QSA, CISSP, CISA

COALFIRE

North America | Europe
877.244.8077 | info@coalfire.com | Coalfire.com

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

ThinScale Technology (ThinScale) engaged Coalfire Systems Inc. (Coalfire), a respected Qualified Security Assessor (QSA) for the Payment Card Industry (PCI) and Payment Application Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of their ThinKiosk (ThinKiosk) & Secure Remote Worker (Secure Remote Worker) product. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire will describe which requirements of the PCI Data Security Standard (PCI DSS) v3.2 were applicable and supported by the ThinKiosk & Secure Remote Worker software based on the sample testing and evidence gathered during this assessment. The requirements that were not applicable have been included in the matrix in Appendix A.

## ABOUT THINKIOSK

ThinKiosk is a software-only solution for any Windows endpoint, including PCs, laptops, and tablets, that converts the endpoint into a thin client. It creates a centrally managed and secure thin client with a lightweight user interface that provides users access to their Virtual Desktop Infrastructure (VDI) environments, local applications and web applications. VDI is a virtualization technology that allows a user to remotely access a desktop on another server.

## ABOUT SECURE REMOTE WORKER

Secure Remote Worker is a software-only solution for non-corporate Windows devices, that allows them to be used as a personal device as well as a secure corporate thin client all without the need to change or reconfigure the underlying Windows OS. It is achieved without the need to reboot, dual boot or use a USB device.

When enabled, SRW will convert users' personal devices into secure, trusted endpoints allowing them to be used for remote working or BYOD. SRW provides a secure workspace allowing them to connect to the corporate environment, all while ensuring corporate IT standards and security policies are met.

ThinKiosk & Secure Remote Worker locks down the Windows environment where it is installed, providing users with the access they need to access their VDI environments, local applications and web applications. The solution can be configured to combine remote VDI resources with local applications while providing access to web-based resources through the secure browser. Other Windows settings, as needed, can be configured by system administrators for adjustment of display resolutions, keyboard, and mouse controls.

ThinKiosk & Secure Remote Worker have some key functionality in enabling personal & corporate devices to become PCI compliant including;

- Windows Patch Management
- Windows Firewall Control
- Windows Security Centre Detection
- USB Device Blocking
- Application Execution Prevention (AEP)
- Service Execution Prevention (SEP)
- Restricted access to key operating system components

For more detailed descriptions of these functionalities see the ThinScale website here.

## AUDIENCE

This assessment white paper has three target audiences:

1. **QSA and Internal Audit Community:** This audience may be evaluating ThinKiosk or Secure Remote Worker to assess a merchant or service provider environment for PCI DSS.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating ThinKiosk or Secure Remote Worker for use within their organization for compliance requirements for both PCI DSS and other security standards.
3. **Merchant and Service Provider Organizations:** This audience may be evaluating ThinKiosk or Secure Remote Worker for deployment in their cardholder data environment and what PCI DSS benefits could be achieved from using this solution.

## METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using the below industry and audit best practices. Coalfire conducted technical testing in their Colorado lab from September 18, 2017 to September 29, 2017, on February 13, 2018 and then again from December 20, 2018 to December 28, 2018.

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full ThinKiosk and Secure Remote Worker solution and its components.
2. Implementation of the software in the Coalfire lab environment on the following OSs:
    a. Windows 10
    b. Windows 8.1
    c. Windows 8
    d. Windows 7
3. The software runs in the following three modes, all of which were tested:
    a. ThinKiosk Shell – The desktop is completely empty except for the ThinKiosk panel
    b. Windows Shell -- A full Windows desktop displayed, but with limited functionality
    c. Secure Remote Worker -- Similar to the ThinKiosk Shell, with only the ThinKiosk panel on the desktop. This mode is the most common implementation.
4. During testing, access was attempted to the following Windows features, both by accessing the feature directly as it was intended to be used and by unconventional means that might be employed by a malicious user:
    a. Command Prompt
    b. Windows Explorer
    c. Control Panel
    d. Internet Settings
    e. Remote Desktop
    f. Task Manager
    g. Ctrl+Alt+Del
    h. Run command textbox in Start Menu
    i. USB mass storage device access
    j. Administrative Tools – Services and Password Policies
    k. User accounts
    l. Windows Event Logs
    m. Malware detection and anti-virus protection

n. Attempting to run an application configured to be blocked by the ThinKiosk & Secure Remote Worker Application Execution Prevention feature
o. Attempting to run a Windows service configured to be blocked by the ThinKiosk Service Execution Prevention and Windows Service/Device Driver Validation feature

5. A controlled sample of malware was installed on the Windows 7 test system to observe how ThinKiosk & Secure Remote Worker handled malware detection and protection. In addition, anti-virus software was turned off for one test to monitor how ThinKiosk & Secure Remote Worker managed anti-virus software and updates.

## SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- When properly implemented following vendor guidance, ThinKiosk & Secure Remote Worker provides coverage for the PCI DSS requirements listed in the Appendix A based on the sample testing and evidence gathered during this assessment.
- Many PCI DSS requirements fall outside of the scope of ThinKiosk & Secure Remote Worker. Those requirements are also listed along with the reasoning behind them not being in scope.
- ThinKiosk & Secure Remote Worker was able to lockdown systems, as described in the documentation, preventing complete access to the following Windows features:
  - Command Prompt
  - Run command from the Start Menu
  - Ctrl+Alt+Del
  - USB mass storage device access
  - Addition of new users
  - Task Manager
  - Administrative Tools – Services and Password Policies
  - Application Execution Prevention successfully blocked an application that it was configured to block
  - Service Execution Prevention successfully blocked a Windows service that it was configured to block
- ThinKiosk & Secure Remote Worker were able to allow limited access to the following Windows features, but restricted the ability to change configurations to allow running software, other than ThinKiosk & Secure Remote Worker, on the test systems:
  - Control Panel
  - Internet Settings
  - Remote Desktop
  - Windows Explorer
- ThinKiosk & Secure Remote Worker provided the above restrictions in all three modes of operation (ThinKiosk Shell, Windows Shell and Secure Remote Worker).
- ThinKiosk & Secure Remote Worker adequately generated system logs of events such that malicious activity could be traced in accordance with PCI DSS requirements.
- ThinKiosk & Secure Remote Worker has an administrative password to prevent the software from being disabled by unauthorized users. The password can be set up by an administrator and made unique for

each software installation, as required by PCI DSS Requirement 2. The software also logged user access, per PCI DSS Requirement 10.

- ThinKiosk & Secure Remote Worker configurations can also be customized to the type of VDI required to be accessed from the Windows system, where it is installed.
- ThinKiosk & Secure Remote Worker checks if anti-virus software is enabled and can it turn it on, if it has been turned off. The software also checks if the system has the latest Windows patches or other security updates and if the firewall has been turned off.
- ThinKiosk & Secure Remote Worker Application Execution Prevention and Service Execution Prevention can be configured to successfully block designated applications and Windows services.

## ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of ThinKiosk & Secure Remote Worker in a PCI DSS environment, specifically to include its impact on all the PCI DSS requirements. ThinKiosk & Secure Remote Worker, when properly implemented following guidance from ThinScale, can be utilized to meet the technical portions of several PCI DSS requirements for a merchant/service provider. However, as most computing environments and configurations vary drastically, complete compliance with PCI DSS is a combination of multiple elements of people, process and technology.

It should not be construed that the use of ThinKiosk & Secure Remote Worker guarantees full PCI DSS compliance, as disregarding PCI requirements and security best practice controls for systems and networks inside or outside of PCI DSS scope can introduce many other security or business continuity risks to merchants and service providers. Security and business risk mitigation should be any merchant's goal and focus for selecting security controls.

In summary, ThinScale is neither a merchant, which would be in scope for PCI DSS, nor a payment application vendor, which would be in scope for the PCI SSC Payment Application Data Security Standard (PA-DSS). The software is not eligible to be certified to the PA-DSS standard, as it doesn't store, process or transmit card data. Installation of the software does not adversely impact the status of PCI DSS compliance for a merchant. It should be seen as a configuration management and hardening mechanism a merchant/service provider can use to support PCI DSS compliance in an often complex use case.

# TECHNICAL ASSESSMENT

## ASSESSMENT METHODS

The assessment used the following methods to assess the potential PCI DSS coverage of the solution:

1. Analysis of the architecture and configuration of the solution in accordance with vendor guidelines.
2. Deployment of ThinKiosk & Secure Remote Worker software to test machines along with enablement of strict policies to enforce lockdown of the Windows endpoints. Examination of the software configuration to confirm protection cannot be turned off by non-administrators.
3. Review of configurations and setting on each Windows test system while the software was deployed and running to verify all Windows features listed above were locked down.
4. Unlocking of the test systems using an administrative password to verify what had actually been inaccessible when the systems were locked down. The software was then turned on and the systems were locked down again to verify the same Windows features were once again inaccessible.

## THINKIOSK & SECURE REMOTE WORKER COMPONENTS

ThinKiosk & Secure Remote Worker consists of the following components:

1. ThinKiosk & Secure Remote Worker Client – The client interface for software, which is installed on the PC. The GUI consists of a control panel that can be opened and displayed on the PC desktop or can be run minimized. When run as a non-administrative user, the GUI only provides access to the allowed Windows features and the VDI environment. When unlocked by an administrative user, the GUI allows full access to all previously blocked Windows functionality. The client also runs as a background process with the user interface minimized with a notification tray-based icon.
2. ThinScale Management Server 3.1 – The management server is an optional component that can be installed on a backend server in the merchant network. It can be used to manage multiple devices hosting ThinKiosk & Secure Remote Worker. ThinKiosk & Secure Remote Worker can be configured upon installation to use a local profile on the device where it is installed or to connect to and use a profile on the management server. When the management server is not deployed, ThinKiosk & Secure Remote Worker functions as a fully-featured standalone client. The management server is a web-based platform secured by HTTP/S.

## ASSESSMENT ENVIRONMENT

ThinKiosk & Secure Remote Worker were installed in Coalfire's lab and implemented on four Virtual Machines running Windows 7, Windows 8, Windows 8.1, and Windows 10. Each system was running Windows Defender antivirus with auto-update enabled, which was turned on and off, as needed, during testing. The network environment was segmented from the Coalfire corporate network and the internet by a Cisco ASA 5525x stateful firewall.

## TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this technical assessment included:

| TOOL NAME | DESCRIPTION |
|---|---|
| Windows Administrative Tools | The suite of native tools included with Windows were used to test ThinKiosk & Secure Remote Worker and verify that it locked down the PCs where it was installed. |

| TOOL NAME | DESCRIPTION |
| --- | --- |
| | The following tools were used, or attempted to access:<br>• Control Panel<br>• Ctrl+Alt+Del<br>• Services Panel of Administrative Tools<br>• Password Policies panel of Administrative Tools<br>• Windows Explorer<br>• Task Manager<br>• Windows Event Logs<br>• User Accounts<br>• Run Command Textbox in Start Menu<br>• Internet Settings<br>• Remote Desktop<br>• Command Prompt |

## REFERENCES


ThinScale website - https://thinscale.com/

Documentation provided by ThinScale:

- ThinKiosk Client Admin Guide
- ThinKiosk Profile Configuration Guide
- ThinScale Management Console 3.1.x Admin Guide
- ThinScale Management Server 3.1.x Admin Guide

PCI Data Security Standard, v3.2 – https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

# APPENDIX A: PCI REQUIREMENTS COVERAGE MATRIX

### PCI DSS REQUIREMENTS

**Key:**

Compliance directly supported via use of ThinKiosk & Secure Remote Worker = ✓

Out of scope for ThinKiosk & Secure Remote Worker and requires merchant action for full compliance = ✓

NOTE: The below requirements/configurations apply to the ThinKiosk & Secure Remote Worker-protected endpoints. All backend and virtual environments must also be configured for PCI compliance.

| PCI REQUIREMENT | COMMENTS | COMPLIANCE SUPPORTED |
|---|---|---|
| **1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment.** | ThinKiosk & Secure Remote Worker currently checks if a firewall is installed or running on the device where it is installed. The software applies a restrictive firewall policy on the device while the software is running. When ThinKiosk will be turned off or unlocked, the software will reset the firewall policy. | ✓ |
| **2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.** | ThinKiosk & Secure Remote Worker does not have a default administrative password. The software requires an administrative password for unlocking the desktop. The installation manuals contain detailed instructions for creating an administrative password that is unique for each installation, as required by PCI DSS. | ✓ |
| **2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.**<br>**2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.**<br>**2.2.4 Configure system security parameters to prevent misuse.**<br>**2.2.5 Remove all unnecessary functionality,** | ThinKiosk & Secure Remote Worker completely locks down access to any configuration for changing daemons, required services, and protocols from the desktop where the software is installed. The software limits access to the Control Panel, the Run command in the Start Menu, Ctrl+Alt+Del, Task Manager, and the Services and Password Policies panels in Administrative Tools, effectively blocking access to services that could be misused.<br><br>In addition, the Service Execution Prevention feature added to ThinKiosk & Secure Remote Worker can be configured to block designated Windows services to prevent misuse. | ✓ |

| | | |
|---|---|---|
| **such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.** | | |
| **Requirement 3: Protect stored cardholder data** | ThinKiosk & Secure Remote Worker does not store cardholder data and, as a result, does not require encryption or any other protection of cardholder data as mandated by this requirement. | ✓ |
| **Requirement 4: Encrypt transmission of cardholder data across open, public networks** | ThinKiosk & Secure Remote Worker does not transmit any cardholder data, over either public or private networks. The device running ThinKiosk & Secure Remote Worker may have access to view card data in a merchant's cardholder data environment, but that data is never transmitted back to the device or to ThinKiosk. The cardholder data would only be accessible to view and, even then, just in read-only mode. | ✓ |
| **5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).**<br>**5.2 Ensure that all anti-virus mechanisms are maintained as follows:**<br>• **Are kept current,**<br>• **Perform periodic scans**<br>• **Generate audit logs which are retained per PCI DSS Requirement 10.7.**<br>**5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.** | ThinKiosk & Secure Remote Worker currently checks if anti-virus software is either running or up-to-date on the device where it is installed. In addition, when the software starts up and locks down the device, ThinKiosk & Secure Remote Worker turns on anti-virus software that is turned off.<br><br>The status of the anti-virus software is displayed on the Management Console for ThinKiosk. The software prevents the user from continuing if the configured policy rules are not met. For example, for anti-virus software, ThinKiosk & Secure Remote Worker would check whether the anti-virus is running and up-to-date. ThinKiosk then displays remediation advice.<br><br>For Requirement 5.2, specifically, ThinKiosk & Secure Remote Worker supports PCI compliance by checking if the anti-virus software is current and running. If the anti-virus software is running, it would be required to be set to run periodic scans by default. In addition, the audit logs for this requirement are configured within the anti-virus software itself, which would not be a feature of ThinKiosk & Secure Remote Worker. | ✓ |
| **6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.** | ThinKiosk & Secure Remote Worker currently detects if a Windows system has the most recent patches and updates.<br><br>The software detects if the Windows system on the device has all current patches installed and displays the status on the ThinKiosk Management Console. The software verifies if particular Microsoft Knowledge Bases (KBs) were installed and prevents the user from continuing, instead displaying remediation advice. | ✓ |
| **7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.** | ThinKiosk & Secure Remote Worker restricts access to Windows components and can be configured based on individual access rights for a particular user. It can also be set to "deny all" for any Windows system components. | ✓ |

| | | |
|---|---|---|
| **7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.** | | |
| **Requirement 8: Identify and authenticate access to system components** | This requirement pertains to user ID and password policies for access to cardholder data. ThinKiosk & Secure Remote Worker does not store, transmit, or process cardholder data in any form, making this requirement out of scope. | ✓ |
| **9.5 Physically secure all media.** | ThinKiosk & Secure Remote Worker can be configured to block or allow Windows Explorer drive letters based on preference.<br><br>Starting with version 5.2, ThinKiosk can be configured to block USB storage devices, while still allowing essential devices using USB ports, such as a keyboard and mouse, to run.<br><br>The rest of PCI DSS Requirement 9 relates to physical security provided by merchants for locations where cardholder data is stored. This is out of scope for ThinKiosk & Secure Remote Worker, since ThinScale is not a merchant nor does it store cardholder data. | ✓ |
| **10.1 Implement audit trails to link all access to system components to each individual user.** | ThinKiosk & Secure Remote Worker contains logs that monitor user access and events, including logging settings set in the ThinKiosk Profile. These logs match the access of every individual user of ThinKiosk & Secure Remote Worker to the component being accessed.<br><br>ThinKiosk & Secure Remote Worker also includes, through its AEP feature, whitelisting of applications that can be configured to prevent unauthorized processes or applications to be executed. AEP is granular down to the application level and can also be configured by targeted rule sets or can check if an application has a digital signature. This is similar to PCI DSS Requirement 10.5.5 for file integrity monitoring. | ✓ |
| **Requirement 11: Regularly test security systems and processes.** | This requirement pertains to external and internal penetration testing required by merchants to test the security of their cardholder data environments. ThinScale is not a merchant and does not store or handle credit card data in any form, so this requirement is out of scope. | ✓ |
| **12.3 Develop usage policies for critical technologies and define proper use of these technologies.**<br>**12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and** | ThinKiosk & Secure Remote Worker can be configured to block or allow Windows Explorer drive letters based on preference. This would prevent the copying and storage of any data, including cardholder data, to any local hard drive.<br><br>The rest of PCI DSS Requirement 12 pertains to security policies and procedures for merchants. Since ThinScale is not a merchant and does not store or handle any cardholder data, the remainder of the requirement is out of scope. | ✓ |

| | | |
|---|---|---|
| **removable electronic media, unless explicitly authorized for a defined business need.** | | |

## ABOUT THE AUTHORS

**Joel Dubin** | Senior Consultant

Joel Dubin (jdubin@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire. Joel has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including application security, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, QSA, and PA-QSA.

QA:
**Nick Trenc** | Director

Nick Trenc (ntrenc@coalfire.com) is the Director of the Solution Validation team with Coalfire. Nick has several years of experience working in Information Security. Nick has an in-depth understanding of application, network, and system security architectures and has authored and spoken on multiple security topics including mobile security, application security, virtualization, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance.

Published March 2018 and Updated January 2019.

## ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com