WHITE PAPER

THINKIOSK & SECURE REMOTE WORKER

GDPR 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 leading independent industry provider of IT security, governance, and regulatory compliance services, to conduct an independent technical assessment of their ThinKiosk (ThinKiosk) & Secure Remote Worker (Secure Remote Worker) product to determine the solution's suitability to meet the General Data Protection Regulation (GDPR) for protection of personal data. Coalfire conducted assessment activities including technical testing, architectural review, and compliance validation.

The following is discussed within this white paper:

- Coalfire describes how either the ThinKiosk or Software Remote Worker software can be part of the 'appropriate technological measures' specified in Article 32, in addition to Recitals 78 and 83, to support meeting the requirements of the GDPR for protecting personal data (examples include name, email address, date of birth, password, social security number, bank details, or confidential health records) based on the sample testing and evidence gathered during this assessment.
- Coalfire describes how either the ThinKiosk or Software Remote Worker software can be leveraged to assist with meeting Article 33 'Notification of a personal data breach to the supervisory authority' and Article 34 'Communication of a personal data breach to the data subject'.
- This paper briefly describes the origin of the GDPR, presents the features of the solution that can be leveraged for suitability and compliance with the GDPR, and provides a mapping of available features in the solution specific to the GDPR and cybersecurity best practices.

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. 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 OR SECURE REMOTE WORKER

Either ThinKiosk or Secure Remote Worker, depending on whether your endpoints are in-house or remote, 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.

Both 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.

GENERAL DATA PROTECTION REGULATION (GDPR)

The European Union (EU) GDPR replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy.

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation took effect after a two-year transition period, meaning it started being enforced on May 25, 2018.

The GDPR not only applies to organizations located within the EU, but also applies to organizations located outside of the EU if they offer goods or services to or monitor the behavior of EU data subjects. It also applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.

Organizations can be fined up to 4% of annual global turnover for breaching the GDPR or €20 million, whichever is greater. This is the maximum fine that can be imposed for the most serious infringements, including not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines; a company can be fined only 2% for not having their records in order (Article 28), not notifying the supervising authority and data subject about a breach (Article 33), or not conducting an impact assessment (Article 35). It is important to note that these rules apply to both Controllers and Processors as defined by the GDPR - meaning 'cloud' environments will not be exempt from GDPR enforcement.

The GDPR defines Controllers as entities that collect and use personal data. More specifically, Controllers determine what data is collected and the means and purposes for processing. If an organization uses a web site, for example, that uses the data for marketing or analytics services, it would be considered a Controller under the GDPR. A Processor is an organization that processes data under contract to the Controller. If the Controller collecting and using the data actually outsources the analysis of the data to a third-party, that third-party becomes the Processor, as defined by the GDPR.

In addition, the GDPR identifies a Supervisory Authority as the body responsible for monitoring GDPR compliance in a given country. Supervisory Authorities are member state organizations responsible for enforcement within the member state.

The GDPR is categorized in various Chapters, Articles, and Recitals format. Articles and Recitals are essential to understanding the GDPR. Supervisory Authorities have implemented a number of Recitals that are part of the legislation and provide guidance to interpret the Articles.

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 & Secure Remote Worker solutions and its components.
2. Implementation of the software in the Coalfire lab environment on the following Operating Systems:
   a. Windows 10
   b. Windows 8.1
   c. Windows 8
   d. Windows 7
3. Testing of the software, which runs in the following three modes:
   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, attempting access 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. ThinKiosk AEP feature
   o. ThinKiosk Service Execution Prevention feature

5. Installing a controlled sample of malware 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, either ThinKiosk or Secure Remote Worker can provide coverage for GDPR Article 32, Article 33, and Article 34, in addition to GDPR Recitals 78 and 83. However, implementing either ThinKiosk or Secure Remote Worker alone is not sufficient for a Controller or Processor to achieve compliance with these Articles and Recitals. It contributes to compliance by improving endpoint security through reducing the risk of breaches and logging activities related to breaches.
- Many GDPR requirements fall outside of the scope of either ThinKiosk or Secure Remote Worker. Those requirements are not technical in nature and would not be handled by the software itself. They would be administrative requirements handled by the company or organization installing either ThinKiosk or Secure Remote Worker on their systems.
- Either ThinKiosk or Secure Remote Worker were 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
- Either ThinKiosk or Secure Remote Worker AEP successfully blocked an application that they were configured to block
- Either ThinKiosk or Secure Remote Worker Service Execution Prevention successfully blocked a Windows service that it was configured to block
- Either ThinKiosk or 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
- Either ThinKiosk or Secure Remote Worker provided the above restrictions in all three modes of operation (ThinKiosk Shell, Windows Shell, and Secure Remote Worker).
- Either ThinKiosk or Secure Remote Worker adequately generated system logs of events such that malicious activity could be traced in accordance with GDPR Article 32 and Article 33.

- Either ThinKiosk or 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 GDPR Article 32. The software also logged user access, per GDPR Article 32 and 33.
- Either ThinKiosk or 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.
- Either ThinKiosk or Secure Remote Worker checks if anti-virus software is enabled and can 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.
- Either ThinKiosk or Secure Remote Worker AEP 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 either ThinKiosk or Secure Remote Worker in an environment, specifically one that included personal data. ThinKiosk or Secure Remote Worker, when properly implemented following guidance from ThinScale, can contribute to a comprehensive security and privacy program to meet the requirements of the GDPR for protecting personal data. However, as most computing environments and configurations vary drastically, complete compliance with the GDPR is a combination of multiple elements of people, process, and technology.

It should not be construed that the use of either ThinKiosk or Secure Remote Worker guarantees full compliance with the GDPR. Disregarding other GDPR requirements and security best practice controls for systems and networks 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 Controller nor a Processor, as defined by the GDPR. It does not collect any personal data, and is only part of the endpoint where the data is input to systems run by a Controller or Processor. The software does not store, process, or transmit any personal data. Installation of the software does not adversely impact the GDPR status for a Controller or Processor. It should be seen as a configuration management and hardening mechanism a Controller or Processor can use to support GDPR compliance in an often complex use case.

TECHNICAL ASSESSMENT

ASSESSMENT METHODS

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

1. Analysis of the architecture and configuration of the solution in accordance with vendor guidelines.
2. Deployment of the ThinKiosk or 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 or Secure Remoter Worker. ThinKiosk or 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, both ThinKiosk & Secure Remote Worker function as a fully-featured standalone client. The management server is a web-based platform secured by HTTP/S.

ASSESSMENT ENVIRONMENT

Both 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 both 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: • Control Panel • Ctrl+Alt+Del • Services Panel of Administrative Tools • Password Policies panel of Administrative Tools • Windows Explorer • Task Manager • Windows Event Logs • User Accounts • Run Command Textbox in Start Menu • Internet Settings • Remote Desktop • 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

EU GDPR – https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN and https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

APPENDIX A: GDPR REQUIREMENTS COVERAGE MATRIX

GDPR REQUIREMENTS

NOTE: The below requirements/configurations apply only to the ThinKiosk & Secure Remote Worker-protected endpoints. The Controller or Processor in scope for the GDPR must still configure all their other backend and virtual environments for GDPR compliance.

ARTICLE 32

Security of Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 32 requires organizations to implement appropriate security measures to protect personal data, which refers to ‘encryption of personal data’ as one way to meet the requirement. In order to ensure there is ongoing confidentiality, integrity, availability, and resilience of processing systems and services, the protection of systems storing this data is important.

The following is either implemented by, or out-of-scope for, both ThinKiosk & Secure Remote Worker to provide partial support for compliance with Artilce 32 of the GDPR for the Controller or Processor installing the software:

(a) Both ThinKiosk & Secure Remote Worker do not transmit any personal data, over either public or private networks. The device running either ThinKiosk or Secure Remote Worker may have access to view card data in a Controller’s or Processor's data environment, but that data is never transmitted back to the device or to either ThinKiosk or Secure Remote Worker. The personal data would only be accessible to view and, even then, just in read-only mode. Therefore, this requirement would be out-of-scope for Article 32.

(b) Both ThinKiosk & Secure Remote Worker can be configured “*to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services”* via the following*:*

- Both ThinKiosk & Secure Remote Worker can check if a firewall is installed or running on the device where it is installed and apply a restrictive firewall policy.
- Both 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.
- The Service Execution Prevention feature added to both ThinKiosk & Secure Remote Worker can be configured to block designated Windows services and device drivers to prevent misuse.
- Both ThinKiosk & Secure Remote Worker currently checks if anti-virus software is running and up-to-date on the device where it is installed. When the software starts up

and locks down the device, Both ThinKiosk & Secure Remote Worker turn on anti-virus software that is turned off. The software prevents the user from continuing if the configured policy rules are not met. For example, for anti-virus software, both ThinKiosk & Secure Remote Worker would check whether the anti-virus is running and up-to-date. Both ThinKiosk & Secure Remote Worker then displays remediation advice. If the anti-virus software is running, it would be required to be set to run periodic scans by default. The software also maintains audit logs within the anti-virus software itself to keep track of incidents.

- Both ThinKiosk & Secure Remoter Worker detect if a Windows system has the most recent patches and updates.
- Both ThinKiosk & Secure Remote Worker restrict 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.
- Both ThinKiosk & Secure Remote Worker include, through its AEP feature, whitelisting of applications that can be configured to prevent unauthorized processes or applications to be executed.

(c) Both ThinKiosk & Secure Remote Worker do not restore availability or access to personal data. This would be the responsibility of the Controller or Processor using the software. Therefore, this requirement would be out-of-scope for Article 32.

(d) Both ThinKiosk & Secure Remote Worker are not a testing tool for regularly evaluating security controls. This would be the responsibility of the Controller or Processor using the software. Therefore, this requirement would be out-of-scope for Article 32.

ARTICLE 33 AND 34

Article 33 Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Article 34 Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

If a company loses data in a cyberattack or by any other means, the company is obliged to deliver a breach notification. This breach notification should include the type of data, number of compromised users as a result of the incident, or the approximate number of personal data records affected.

Both ThinKiosk & Secure Remote Worker supports GDPR Articles 33 and 34 by recording any relevant activities (detected or blocked) that could result in a breach.

Both ThinKiosk & Secure Remote Worker contains logs that monitor user access and events, including logging settings set in either the ThinKiosk Profile or Secure Remote Worker Profile. These logs match the access of every individual user of both ThinKiosk & Secure Remote Worker to the component being accessed.

The logging feature, together with all of the features listed in support of Article 32 above, can assist an organization to analyze data breach issues and gather information to quickly notify the Supervisory Authority.

RECITAL 78

Appropriate technical and organisational measures

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.
This recital ties to GDPR Article 32, which can assist organizations in implementing appropriate technical and organizational measures for data protection. The development of policies, and the adoption and implementation of those policies, remains the responsibility of the Controller or Processor, which would not include ThinScale.
RECITAL 83
Security of processing *In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected*
This recital tied to Article 32 would not be in scope for both ThinKiosk & Secure Remote Worker, since it is neither a Controller or a Processor, as defined by the GDPR. It does not collect any personal data, and is only part of the endpoint where the data is input to systems run by a Controller or Processor. However, information gathered from both ThinKiosk & Secure Remote Worker application logs by the Controller or Processor installing the software can be used for determining, evaluating, and mitigating security risks.

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 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

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

ThinKiosk & Secure Remote Worker – GDPR Compliance January 2019