

THINSCALE TECHNOLOGIES

THINKIOSK & SECURE REMOTE WORKER

PCI DSS WHITE PAPER

ROSHAN BOLOOR | QSA, ISO 27001 LEAD AUDITOR/IMPLEMENTOR



C  A L F I R E .

North America | Europe

877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

| | |
|---|-----------|
| Executive Summary | 3 |
| About ThinkKiosk..... | 3 |
| About Secure Remote Worker | 3 |
| Audience..... | 4 |
| Methodology..... | 4 |
| Summary Findings | 5 |
| Assessor Comments | 6 |
| Technical Assessment | 7 |
| Assessment Methods..... | 7 |
| ThinKiosk & Secure Remote Worker Components..... | 7 |
| Assessment Environment..... | 7 |
| Endpoint Diagram..... | 7 |
| Tools and Techniques..... | 9 |
| References..... | 9 |
| APPENDIX A: PCI Requirements Coverage Matrix | 10 |
| PCI DSS Requirements..... | 10 |

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) v4 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 versatile software solution that can transform any Windows endpoint, be it a PC, laptop, or tablet, into a lean, centralized thin client. With its user-friendly interface, ThinKiosk gives users access to their Virtual Desktop Infrastructure (VDI) environments, local applications, and web applications, all while maintaining a secure and centrally managed environment. VDI is a virtualization technology that enables remote access to a desktop on a remote server. ThinKiosk makes it easy for users to enjoy the benefits of VDI without the need for additional hardware or complicated configurations.

ABOUT SECURE REMOTE WORKER

Secure Remote Worker (SRW) is a software-based solution designed for Windows devices outside the corporate network. This innovative tool enables non-corporate devices to function both as a personal device and as a secure thin client for corporate use, all while keeping the underlying Windows OS intact. With Secure Remote Worker, there is no need to make any changes or reconfigurations to the device, nor to reboot, dual boot, or rely on external USB devices.

Secure Remote Worker (SRW) is an innovative software solution that enables users to convert their personal devices into secure, trusted endpoints for remote working or bring-your-own-device (BYOD) scenarios. With SRW, users can connect to the corporate environment in a secure workspace that meets corporate IT standards and security policies.

ThinKiosk & Secure Remote Worker provide a comprehensive solution that locks down the Windows environment to ensure secure access to VDI environments, local applications, and web applications. The solution can be configured to combine remote VDI resources with local applications, while providing secure access to web-based resources through a secure browser. System administrators can customize settings for display resolutions, keyboard and mouse controls, and other Windows features as needed. This powerful tool ensures that users can work efficiently and securely, while meeting corporate IT standards and policies.

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. **Qualified Security Assessors (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 from March 1st, 2023, to March 27th 2023.

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
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 10 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 and Secure Remote Worker offer the above-mentioned restrictions in all three modes of operation - ThinKiosk Shell, Windows Shell, and Secure Remote Worker. Additionally, the software generates comprehensive system logs that enable tracing of malicious activity, as required by PCI DSS regulations.
- To meet PCI DSS Requirement 2, ThinKiosk and Secure Remote Worker provide an administrative password to prevent unauthorized users from disabling the software. This password can be customized and made unique for each installation. Furthermore, the software logs user access in compliance with PCI DSS Requirement 10.
- ThinKiosk and Secure Remote Worker can be tailored to the specific VDI requirements of the Windows system where they are installed. They also check for the status of anti-virus software, turn it on if necessary, and check for the latest Windows patches, security updates, and firewall status.
- Lastly, ThinKiosk and Secure Remote Worker provide Application Execution Prevention and Service Execution Prevention that can be configured to block designated applications and Windows services, enhancing system security and compliance with PCI DSS regulations.

ASSESSOR COMMENTS

During the assessment, ThinKiosk & Secure Remote Worker were evaluated for their compliance with the PCI DSS requirements. While the software can be used to meet technical portions of some PCI DSS requirements, complete compliance with PCI DSS involves multiple factors, including people, process, and technology. Therefore, the use of ThinKiosk & Secure Remote Worker should not be seen as a guarantee of full PCI DSS compliance.

Furthermore, it is important to note that disregarding PCI requirements and security best practices for systems and networks can introduce other security and business continuity risks for merchants and service providers. Therefore, merchants should prioritize security and risk mitigation when selecting security controls.

It should also be noted that ThinScale is not a merchant or a payment application vendor and, therefore, is not subject to certification to the PCI SSC PA-DSS standard. The software does not store, process or transmit card data, and its installation does not adversely impact a merchant's PCI DSS compliance status. Instead, ThinKiosk & Secure Remote Worker should be viewed as a configuration management and hardening mechanism that can support PCI DSS compliance in complex use cases.

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 settings 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 workstation Windows 10. The network environment was segmented from the Coalfire corporate network and the internet by a Cisco ASA 5525x stateful firewall.

Endpoint Diagram

Below is the typical endpoint architecture deployed within a merchant environment.

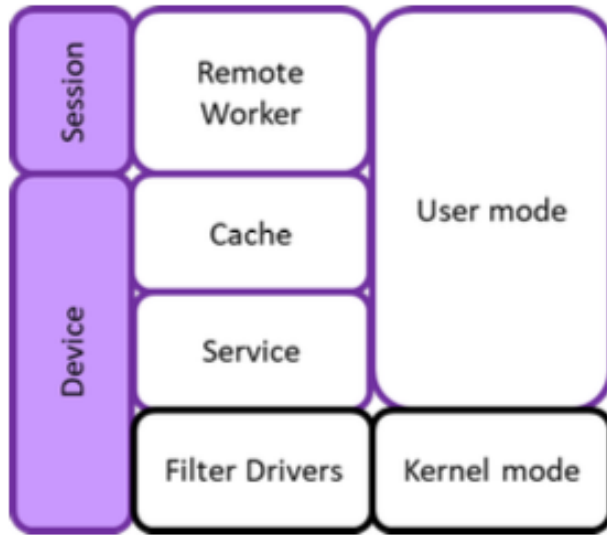


Figure 1: Endpoint Diagram

TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this application security review include:

| TOOL NAME | DESCRIPTION |
|------------------------------|---|
| Windows Administrative Tools | <p>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.</p> <p>The following tools were used, or attempted to access:</p> <ul style="list-style-type: none">• 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 |

**Forensic tool: A tool or method for uncovering, analyzing, and presenting forensic data, which provides robust ways to authenticate, search, and recover computer evidence rapidly and thoroughly.*

REFERENCES

ThinScale website - <https://thinscale.com/>

Documentation provided by ThinScale:



- ThinScale_Architecture_Guide_7_x





PCI Data Security Standard, v4.0 – https://www.pcisecuritystandards.org/document_library/





APPENDIX A: PCI REQUIREMENTS COVERAGE MATRIX



PCI DSS Requirements



Key:

| | |
|---|---|
| Compliance directly supported via use of ThinKiosk & Secure Remote Worker |  |
| Shared responsibility for ThinKiosk & Secure Remote Worker and requires merchant action for full compliance |  |
| Note: All 4.0 requirements that are not listed are not in scope for ThinKiosk and Secure Remote Worker. | |

| PCI REQUIREMENT | COMMENTS | COMPLIANCE SUPPORTED |
|---|--|---|
| 1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. | At present, ThinKiosk & Secure Remote Worker has the capability to detect the presence and status of a firewall on the device where it is installed. When the software is active, it enforces a strict firewall policy on the device. Once ThinKiosk is shutdown or exited, the software will restore the previous firewall policy. |  |
| 2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood. | ThinKiosk & Secure Remote Worker has a robust security feature that does not rely on a default administrative password. Instead, the software mandates the creation of a unique administrative password during installation, in compliance with PCI DSS requirements. The installation manuals provide comprehensive guidelines on how to set up the administrative password. This feature ensures that unauthorized users cannot access the desktop, thereby enhancing the overall security of the system. |  |
| 2.2. System components are configured and managed securely. | ThinKiosk & Secure Remote Worker provides comprehensive lockdown features that prevent any unauthorized access to system configurations from the desktop where the software is installed. This includes restrictions on access to the Control Panel, the Run command, Ctrl+Alt+Del, Task Manager, and Administrative Tools panels like Services and Password Policies. These measures effectively block access to any services that could be abused. Moreover, ThinKiosk & Secure Remote Worker's Service Execution Prevention feature allows for the configuration of designated Windows services to be blocked, further preventing any misuse. |  |
| 2.3 Wireless environments are configured and managed securely. | ThinKiosk & Secure Remote Worker can use WIFI on the enabled devices however Merchants (clients) are responsible for meeting PCI-DSS configuration controls for Wireless Access Points. Workstation wireless configurations are securely managed by ThinKiosk & Secure Remote Worker. It is the responsibility of merchants (clients) to securely configure and manage any wireless access points that are within the scope of PCI-DSS. |  |

| PCI REQUIREMENT | COMMENTS | COMPLIANCE SUPPORTED |
|---|--|---|
| <p>Requirement 3: Protect stored cardholder data</p> | <p>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. However cached configurations are encrypted with AES-256. Merchants (clients) are responsible for meeting PCI-DSS configuration controls for protecting stored CHD.</p> |  |
| <p>Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks</p> | <p>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. The application cannot send any data files because they are not stored on the OS file systems.</p> <p>Merchants (clients) are responsible for meeting PCI-DSS configuration controls for protecting CHD during transmission over open and public networks.</p> |  |
| <p>5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.</p> <p>5.2 Malicious software (malware) is prevented, or detected and addressed.</p> <p>5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.</p> | <p>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.</p> <p>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.</p> <p>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.</p> |  |
| <p>6.3. Security vulnerabilities are identified and addressed.</p> | <p>ThinKiosk & Secure Remote Worker includes a feature that checks if the Windows operating system on the device is up-to-date with the latest patches and updates. The software assesses if the current patches are installed and provides the status on the ThinKiosk Management Console. Additionally, the software verifies the installation of specific Microsoft Knowledge Bases (KBs) and offers remediation guidance if the necessary patches are not installed, preventing the user from proceeding until the issue is resolved. This is run during the boot by SC WindowsUpdates. The application keep a full inventory of versions of application dependencies.</p> |  |

| PCI REQUIREMENT | COMMENTS | COMPLIANCE SUPPORTED |
|---|--|---|
| <p>7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood</p> <p>7.2 Access to system components and data is appropriately defined and assigned.</p> <p>7.3 Access to system components and data is managed via an access control system(s).</p> | <p>ThinKiosk & Secure Remote Worker implements strict access controls that restrict user access to Windows components based on individual access rights and role-based access control (RBAC) requirements. These access controls can be customized to "deny all" for any Windows system components as required by the merchant. Access controls are designed based on the principle of least privilege, ensuring that users only have access to the resources necessary to perform their tasks. Merchants can configure strict access controls for all their users as needed, providing an additional layer of security for their systems.</p> <p>It is the responsibility of the merchants (clients) to adhere to PCI-DSS configuration controls in order to safeguard access to system components and CHD, with the use of RBAC. Merchants are required to review access privileges and ensure that access controls are implemented as needed.</p> |  |
| <p>Requirement 8: Identify and authenticate access to system components</p> | <p>This particular requirement relates to the policies regarding user ID and password when accessing cardholder data. Since ThinKiosk & Secure Remote Worker does not handle, store, or process cardholder data in any way, this requirement is not applicable to the software.</p> <p>The application utilizes user access controls, which require users to input a User ID and password for authentication purposes. This application securely stores passwords on the Windows OS and ensures secure authentication processes.</p> <p>Merchants (clients) are responsible for managing unique user accounts and passwords to access system components. Password parameters and reset procedures must adhere to PCI-DSS requirements and company policies. It is crucial to periodically review and implement joiner-mover-leaver access control reviews to maintain a secure system.</p> |  |
| <p>9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.</p> | <p>ThinKiosk & Secure Remote Worker provides the capability to allow or block Windows Explorer drive letters based on preference. Additionally, the software can be configured to block USB storage devices, while still permitting essential devices like keyboard and mouse, to function properly through USB ports. All data in the ThinKiosk & Secure Remote Worker is stored securely on VM files and encrypted using AES 128.</p> <p>Regarding PCI DSS Requirement 9, it is related to the physical security provided by merchants for places where cardholder data is stored. Since ThinScale is not a merchant and does not store cardholder data, this requirement is not applicable for ThinKiosk & Secure Remote Worker.</p> <p>It is the responsibility of merchants (clients) to securely store, access, distribute, and destroy CHD.</p> |  |
| <p>10.1 Processes and mechanisms for logging and monitoring all access to</p> | <p>ThinKiosk & Secure Remote Worker includes comprehensive logging capabilities that monitor user access and events. The logs record the access of each</p> |  |

| PCI REQUIREMENT | COMMENTS | COMPLIANCE SUPPORTED |
|---|---|---|
| <p>system components and cardholder data are defined and documented.</p> <p>10.2. Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.</p> <p>10.3 Audit logs are protected from destruction and unauthorized modifications.</p> | <p>individual user to the specific components they interact with, and these settings can be customized in the ThinKiosk Profile. Additionally, the software includes an Application Execution Prevention (AEP) feature, which allows for granular control over whitelisted applications, preventing unauthorized processes or applications from executing. AEP can be configured with targeted rule sets, can check for digital signatures, and is similar to PCI DSS Requirement 10.3.4 for file integrity monitoring.</p> | |
| <p>Requirement 11: Test Security of Systems and Networks Regularly</p> | <p>ThinScale, as a provider of ThinKiosk & Secure Remote Worker, does not handle or store cardholder data and is not a merchant, therefore, external and internal penetration testing required by merchants to test the security of their cardholder data environments is not applicable for ThinKiosk & Secure Remote Worker. Merchants (clients) are responsible for conducting regular security tests on their systems and networks. The following tests must be performed as per PCI-DSS requirements:</p> <ul style="list-style-type: none"> • Quarterly wireless rogue detections • Quarterly internal and external vulnerability scans using an Approved Scanning Vendor (ASV) • Annual internal and external penetration testing • Segmentation tests every six months • Conduct vulnerability scans and/or pentests after implementing critical changes. |  |
| <p>12.2 Acceptable use policies for end-user technologies are defined and implemented.</p> | <p>ThinKiosk & Secure Remote Worker offers the ability to configure access to Windows Explorer drive letters based on preference, thereby preventing the storage or copying of any data, including cardholder data, to any local hard drive.</p> <p>ThinKiosk & Secure Remote Worker offer a secure remote connectivity solution that meets the PCI-DSS requirements. Merchants must include ThinKiosk & Secure Remote Worker as critical remote connectivity technologies if they use them for PCI-DSS purposes.</p> <p>As for the remainder of PCI DSS Requirement 12, it pertains to security policies and procedures that merchants must follow. Since ThinScale is not a merchant and does not handle or store any cardholder data, the rest of the requirement is considered not applicable.</p> <p>Merchants (clients) are responsible for defining and implementing an acceptable use policy for end-user technologies, and documenting the policy accordingly.</p> |  |

ABOUT THE AUTHORS

Roshan Boloor | Principal, MBA, MS Cybersecurity, QSA, ISO/IEC 27001 Lead Auditor / Implementor

Roshan Boloor is a Principal IT Security Consultant in the Payments Assurance practice at Coalfire for 10+ years. He advises senior management on how to meet their cybersecurity and IT governance, risk, and compliance (ITGRC) related goals. Roshan has assisted on multiple projects as a lead assessor for PCI DSS, HIPAA, HITRUST, ISO 27001, SOC2, and GDPR. Roshan has also provided support for clients as vCISO, vDPO, CSO, and HIPAA Officer. Roshan lead projects related to Information Technology General Controls (ITGC), IT risk assessments, vulnerability assessments, vendor risk management, social engineering, policy and procedure reviews. Roshan has worked extensively with cloud, software, telecommunication, service, retail, healthcare, financial institutions, and application providers. Roshan has worked closely with Coalfire tier-1 customers to help migrate to AWS, GCP, and Azure cloud environments.

Published April 2023.

ABOUT COALFIRE

Coalfire is the trusted 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 nearly 20 years and has offices throughout the United States and Europe. For more information, visit [Coalfire.com](https://www.coalfire.com).

Copyright © 2014-2013 Coalfire Systems, Inc. Rights Reserved. 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.