FIELD EFFECT

Covalence Compliance Series

MAPPING GUIDE

PCI DSS v4.0

FIELD EFFECT

About Field Effect

Field Effect, a global cybersecurity company, is revolutionizing the industry by bringing advanced cybersecurity solutions and services to businesses of all sizes. After years of research and development by the brightest in the business, we have pioneered a holistic approach to cybersecurity.

Our complete Managed Detection and Response (MDR) solution, flexible simulation-based training platform, and expert-led professional services form a unified defense that results in superior security, less complexity, and immediate value. We build solutions that are sophisticated, yet easy to use and manage, so every business owner can get the hands-free cybersecurity they expect. For more information, visit fieldeffect.com.

About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements established by credit card companies to protect cardholder data during payment transactions, ensuring secure handling, processing, and storage of sensitive information. Compliance with PCI DSS helps prevent data breaches and maintains consumer trust in the payment card industry. The latest version of the standard (Version 4.0) was released in March 2022. Field Effect is happy to support our customers with this guide, which shows how our flagship product (Covalence) can satisfy certain PCI DSS requirements and help streamline the audit process.

* This document is intended to help readers better understand the regulatory compliance landscape and its potential obligations, and does not replace or negate official guidance from an auditor. Consulting a regulatory auditor or similar authority is recommended for specific guidance on your organization's compliance requirements.

PCI DSS Requirement	PCI DSS Customized Approach Objective	Covalence Description
1.2.5	**Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.**	Covalence detects the usage of insecure services such as FTP and Telnet, and has network sensors that can be deployed to key locations such as Cardholder Data Environment (CDE) gateways.
1.5.1	**Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.**	Covalence provides world-class anti-malware protection for desktops, laptops, and tablets, protecting these devices from Internet-based attacks and ensuring they don't compromise the security of your organization's CDE.
2.2.4	**System components cannot be compromised by exploiting unnecessary functionality present in the system component.**	Covalence provides in-depth situational awareness of your network, allowing you to audit system configurations to ensure only necessary functionality is enabled.
2.2.5	**System components cannot be compromised by exploiting insecure services, protocols, or daemons.**	If your organization must run insecure services, protocols, or daemons, Covalence's detection and active response capabilities may provide the additional security that allows you to accept the increased risk.
2.2.7	**Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.**	Covalence detects the usage of insecure protocols like FTP and Telnet which can compromise the security of your network and cardholder data.
5.2.1	**Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.**	Covalence deploys a combination of signature and heuristic-based analytics. This combined approach ensures that well-understood threats are identified quickly and efficiently, while novel or emerging threats are also detected. In addition, Covalence provides an Endpoint Devices view which allows customers to ensure it's deployed on all system components.
5.2.2	**Malware cannot execute or infect other system components.**	When Covalence detects threats to your systems, it can isolate impacted endpoint devices from the network, ensuring all types of malware are contained.

PCI DSS Requirement	PCI DSS Customized Approach Objective	Covalence Description
5.3.1	**Anti-malware mechanisms can detect and address the latest malware threats.**	Covalence auto-updates with new functionality and signatures to detect the latest malware threats, ensuring your network and data stay protected.
5.3.2	**Malware cannot complete execution.**	Covalence performs continual behavioral analysis at the endpoint, network, and cloud layers to provide holistic security. When malicious behavior is detected (e.g. a user clicking on a malicious document), Covalence can take immediate action to prevent execution.
5.3.2.1	**Scans by the malware solution are performed at a frequency that addresses the entity's risk.**	Instead of performing periodic scans of files at rest which can impact system performance, Covalence scans devices as required by system activity.
5.3.3	**Malware cannot be introduced to system components via external removable media.**	Covalence can maintain an allow/block list of USB media, which helps customers ensure USB media are only leveraged when there's an organizational reason for their use. In addition, Covalence conducts continuous behavioral analysis of systems, including when media is inserted or logically mounted.
5.3.5	**Anti-malware mechanisms cannot be modified by unauthorized personnel.**	Covalence has protections in place that trigger alerting when agent-tampering is detected. In addition, the Covalence endpoint agent runs in kernel mode and requires administrative access to disable.
5.4.1	**Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.**	The Covalence Suspicious Email Analysis Service (SEAS) is an Outlook plug-in that provides users the ability to request automated analysis of suspicious email to help them recognize social engineering attacks such as phishing.
6.3.1	**New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.**	Covalence monitors networks, cloud applications, and endpoint devices to identify technical vulnerabilities, and provides detailed steps on how to address these. Through Field Effect's proprietary ARO (Actions, Recommendations, and Observations) reporting, these vulnerabilities are easily visible for triaging.

PCI DSS Requirement	PCI DSS Customized Approach Objective	Covalence Description
6.3.3	System components cannot be compromised via the exploitation of a known vulnerability.	When vulnerabilities are reported via Covalence AROs, they include both a priority level and CVSS score to allow our customers to remediate them in accordance with their associated risk.
6.4.1	Public-facing web applications are protected against malicious attacks.	Field Effect's Security Services team provides a full-suite of services including penetration testing, phishing exercises, and web-application reviews.
8.2.1	All actions by all users are attributable to an individual.	The data returned by Covalence for analysis includes information that can be used to associate actions with individual system users (e.g. username, timestamp, source address, destination address).
8.2.2	All actions performed by users with generic, system, or shared IDs are attributable to an individual person.	Covalence provides an Endpoint Devices view which can be leveraged to help verify that the use of shared accounts is limited and approved.
8.3.1	An account cannot be accessed except with a combination of user identity and an authentication factor.	Covalence identifies third-party cloud application accounts where MFA has not been observed, allowing customers to verify the implementation of MFA.
8.3.4	An authentication factor cannot be guessed in a brute force, online attack.	Covalence enhances situational awareness of brute force login attacks by monitoring for them on the endpoint, network, and cloud.
10.2.1	Records of all activities affecting system components and cardholder data are captured.	As an alternative to using a SIEM, the Covalence appliance acts as a central repository for security event alerting. The Covalence appliance can also be configured as a short-term log receiver for devices, like firewalls, that are unable to install the endpoint agent.
10.2.1.2	Records of all actions performed by individuals with elevated privileges are captured.	Covalence collects event logs from endpoints and the cloud for analysis and alert generation, including for users with elevated privileges.
10.2.1.7	Records of alterations that indicate a system has been modified from its intended functionality are captured.	Covalence can detect malware attempting to create or replace system-level objects, and can prevent it from taking control of a particular function or operation on that system.

PCI DSS Requirement	PCI DSS Customized Approach Objective	Covalence Description
10.2.2	Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.	The login data collected by Covalence contains all the details necessary to perform a thorough analysis of the event, including event type, date and time, result, origin, and user.
10.3.1	Stored activity records cannot be accessed by unauthorized personnel.	Once collected by Covalence, all data and log files are protected against editing and deletion by non-Field Effect personnel.
10.3.2	Stored activity records are secured and preserved in a central location to prevent unauthorized modification.	The Covalence appliance provides a central location for short-term log and data collection and protects all data against unauthorized modification, including editing and deletion.
10.4.1	Potentially suspicious or anomalous activities are quickly identified to minimize impact.	Covalence provides 24/7 monitoring of the data and logs collected to ensure that any security events are identified quickly and contained, minimizing impact on your network and data.
10.7.1 & 10.7.2	Failures in critical security control systems are promptly identified and addressed.	The Covalence MDR service is monitored 24/7 by Field Effect operational personnel for processing failures.
11.3.1	The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.	Covalence detects vulnerabilities on enterprise and externally exposed assets to complement active scanning tools.
11.4	A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.	Field Effect's Security Services team provides a full-suite of services including penetration testing, phishing exercises, and web-application reviews.

The most sophisticated cyber threat monitoring on the planet, made simple.

Covalence is an award-winning cybersecurity solution that provides transparent, holistic managed detection and response for your whole IT infrastructure in one platform, no matter where you are or where your endpoints are located. No add-ons, no modules, and no gaps in your security. Learn more about Covalence.

Covalence

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cybersecurity solutions to protect them.

Our threat monitoring, detection, and response platform, along with our training and compliance products and services are the result of years of research and development by the brightest talents in the cybersecurity industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:

CANADA + UNITED STATES
+1 (800) 299-8986

UNITED KINGDOM
+44 (0) 800 086 9176

AUSTRALIA
+61 1800 431418