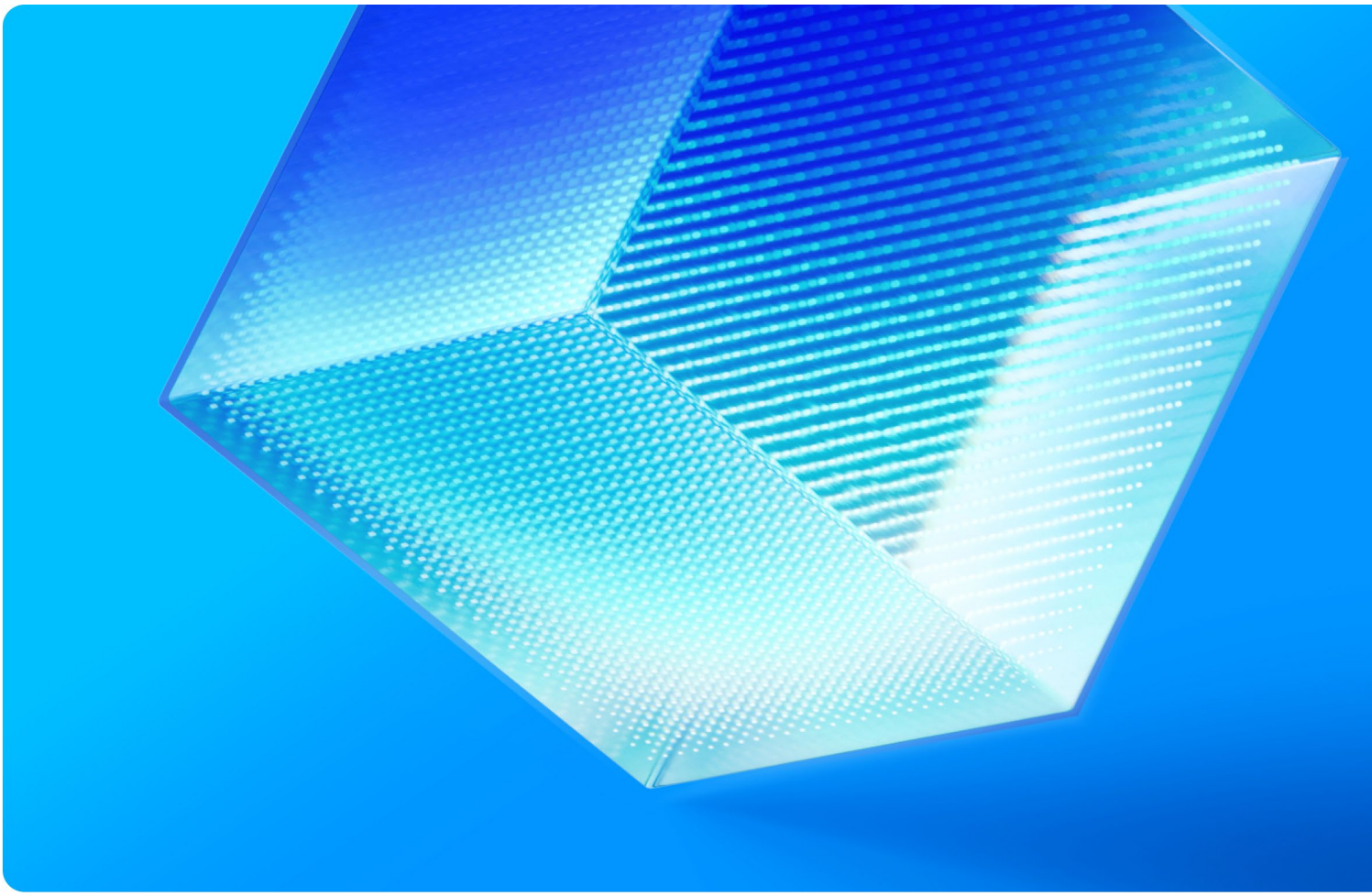
FIELD EFFECT



Field Effect and PCI DSS Compliance

May 2025

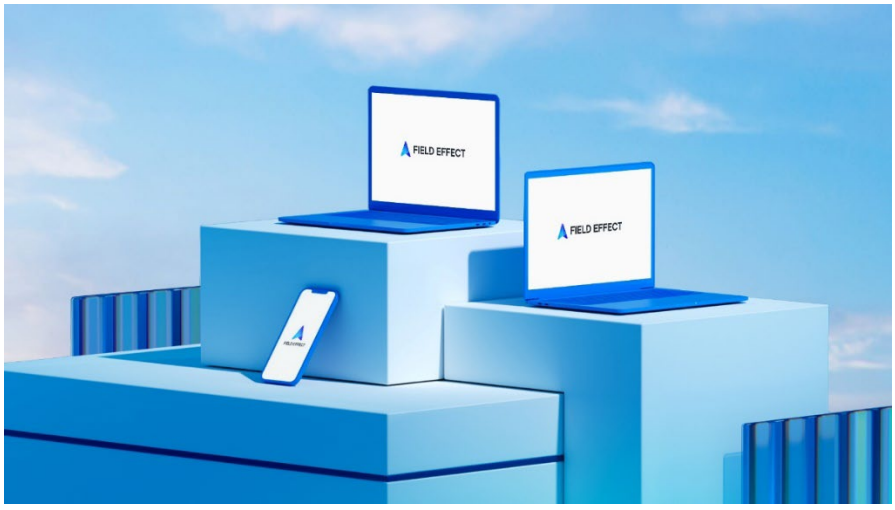
About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Established by the major credit card companies, PCI DSS aims to protect cardholder data and reduce credit card fraud.

Currently on Version 4.0.1 PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. The standard outlines key requirements for data security, including maintaining a secure network, protecting cardholder data, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

Compliance with PCI DSS is overseen by the Payment Card Industry Security Standards Council (PCI SSC). This council provides resources, training, and certification programs to help organizations achieve and maintain compliance. Non-compliance with PCI DSS can result in significant fines, increased transaction fees, and potential loss of the ability to process credit card payments.

Field Effect is pleased to provide this document, which outlines how Field Effect MDR helps support PCI DSS compliance. If you require any further information about Field Effect's security and compliance posture, please contact security@fieldeffect.com or visit the Trust Center.



Field Effect and PCI DSS: A Perfect Match

Managed Detection and Response (MDR) services like Field Effect MDR can play a crucial role in helping organizations meet their PCI DSS compliance goals by providing advanced cybersecurity measures. Field Effect MDR combines cutting-edge technology with human expertise to monitor, detect, and respond to cyber threats in real-time, ensuring that sensitive data, including cardholder data, is protected against unauthorized access and breaches.

Requirement Number	Customized Approach Objective	How we Help
1.2.5	**Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.**	Field Effect MDR comes with one or more 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.**	Field Effect MDR provides world-class anti-malware protection for desktops, laptops, and tablets, protecting these devices from Internet-based attacks to strengthen the security of your organization's CDE.
2.2.4	**System components cannot be compromised by exploiting unnecessary functionality present in the system component.**	Field Effect MDR 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, Field Effect MDR's threat detection and active response capabilities can provide additional security that allows you to accept the increased risk.

Requirement Number	Customized Approach Objective	How we Help
2.2.7	**Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.**	Field Effect MDR 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.**	Field Effect MDR deploys a combination of signature and heuristic based analytics to identify both well-understood and novel threats quickly. In addition, the service provides an Endpoint Devices view which allows customers to ensure the endpoint agent is deployed on all system components.
5.2.2	**Malware cannot execute or infect other system components.**	When Field Effect MDR detects threats to your systems, we can isolate impacted endpoint devices from the network, ensuring all types of malware are contained.
5.3.1	**Anti-malware mechanisms can detect and address the latest malware threats.**	Field Effect MDR auto-updates with new functionality and signatures to detect the latest malware threats, ensuring your network and data stay protected.
6.3.3	**System components cannot be compromised via the exploitation of a known vulnerability.**	When Field Effect MDR detects vulnerabilities, the alert includes both a priority level and CVSS score to allow our customers to remediate threats in accordance with their associated risk.

Requirement Number	Customized Approach Objective	How we Help
5.3.2	**Malware cannot complete execution.**	Field Effect MDR 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), the endpoint agent 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.**	Unlike most other cybersecurity solutions, the Field Effect MDR endpoint agent does not disable Microsoft Defender by default, allowing it to continue its periodic scans.
5.3.5	**Anti-malware mechanisms cannot be modified by unauthorized personnel.**	Field Effect MDR detects and alerts when agent tampering is detected. In addition, the 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 Suspicious Email Analysis Service (SEAS) comes standard with Field Effect MDR. SEAS is a plugin for Outlook and Gmail that provides users with 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.**	Field Effect MDR monitors networks, cloud applications, and endpoint devices to identify technical vulnerabilities, and provides detailed steps on how to address these. With our proprietary approach to alerting known as AROs, all risks are catalogued and triaged by severity.

Requirement Number	Customized Approach Objective	How we Help
6.4.1	**Public-facing web applications are protected against malicious attacks.**	Field Effect's Security Services team provides a full suite of optional services including web-application reviews.
6.4.1	**All actions by all users are attributable to an individual.**	The data returned by Field Effect 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.**	The Field Effect MDR portal 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.**	Field Effect MDR 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.**	Field Effect enhances situational awareness of brute force login attacks by monitoring them on the endpoint, network, and cloud.

Requirement Number	Customized Approach Objective	How we Help
10.4.1	**Potentially suspicious or anomalous activities are quickly identified to minimize impact.**	Field Effect MDR provides 24/7 monitoring of the data 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.**	Our 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.**	Field Effect 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.

About Field Effect

Every business deserves powerful protection from cyber threats.

Field Effect's cybersecurity solutions were purpose-built to prevent, detect and respond to threats for clients of all sizes. We take on the complexity behind the scenes and deliver a solution that's sophisticated where it matters, and simple everywhere else. Consolidate your tech and eliminate the noise while empowering users of all technical backgrounds to confidently navigate cybersecurity and avoid disruptions. Complexity out, clarity in.

Contact our team today.

EMAIL:
letschat@fieldeffect.com

PHONE:
+1 (800) 299-8986