FIELD EFFECT

Covalence Compliance Series

MAPPING GUIDE

NIST CSF v01.1

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 NIST CSF

The NIST Cybersecurity Framework (CSF) was originally released in 2014 as a guide for operators of critical infrastructure. Currently on version 1.1, CSF is a voluntary framework designed to leverage existing standards and to assist organizations in reducing their overall cybersecurity risk. It was also designed to assist communication among both internal and external stakeholders. A new version of the framework is scheduled for release in early 2024.

This document, which shows how Covalence aligns to relevant cybersecurity controls within the CSF can help streamline the implementation and audit processes.

* 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.

Function	Subcategory	Description	Covalence Coverage	Description
Identify (ID)	ID.AM-1	Physical devices and systems within the organization are inventoried	○ Support	Covalence provides an Endpoint Devices view which allows customers to quickly perform spot checks against their inventory of assets.
Identify (ID)	ID.RA-1	Asset vulnerabilities are identified and documented	◐ Partial	Covalence monitors networks, cloud applications, and endpoint devices to identify technical vulnerabilities, and provides detailed steps on how to address them.
Identify (ID)	ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	● Complete	Covalence employs industry-standard indicators of compromise (IOCs) along with our own threat intelligence to identify malicious systems, domains, botnets, ransomware, and other threats to your environment.
Identify (ID)	ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	◐ Partial	Field Effect's proprietary ARO system of Actions, Recommendations, and Observations provides timely, detailed information on the vulnerabilities and risks to a network.
Protect (PR)	PR.DS-5	Protections against data leaks are implemented	◐ Partial	Covalence monitors for unauthorized disclosure and extraction of information (e.g. SharePoint sites, removable media) and has the ability to lock cloud accounts and endpoint devices as a data leakage prevention measure.

● **Complete**

Covalence covers > 90% of this safeguard

◐ **Partial**

Covalence partially covers this safeguard

○ **Support**

Covalence can detect failures in this safeguard or can be leveraged to streamline monitoring

Function	Subcategory	Description	Covalence Coverage	Description
Protect (PR)	PR.IP-12	A vulnerability management plan is developed and implemented	○ Support	You organization's vulnerability management plan can be built around Covalence's detection and notification of technical vulnerabilities.
Protect (PR)	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	◐ Partial	Covalence collects event logs from endpoints and the cloud for analysis and alert generation. Field Effect analysis includes comparing logs against available threat intelligence, known behaviour patterns, and malware signatures. The Covalence appliance can be configured as a syslog receiver for devices like firewalls that are unable to install the endpoint agent. Once collected by Covalence, log files are protected against editing and deletion by the originator.
Protect (PR)	PR.PT-2	Removable media is protected and its use restricted according to policy	◐ Partial	Covalence can maintain an allow/block list of USB media, ensuring USB media are only leveraged when there's an organizational reason for their use.
Detect (DE)	DE.AE-2	Detected events are analyzed to understand attack targets and methods	● Complete	Field Effect's team of experienced cyber analysts manage alert events and place them into context with your organization to develop a complete understanding of the methods and targets of the attack.

● **Complete**

Covalence covers > 90% of this safeguard

◐ **Partial**

Covalence partially covers this safeguard

○ **Support**

Covalence can detect failures in this safeguard or can be leveraged to streamline monitoring

Function	Subcategory	Description	Covalence Coverage	Description
Detect (DE)	DE.AE-3	Event data are collected and correlated from multiple sources and sensors	● Complete	One of the benefits of the holistic cyber protection that Covalence collects and correlates event data from the endpoint, network, and cloud to fully understand events and incidents.
Detect (DE)	DE.AE-4	Impact of events is determined	● Complete	Drawing on our deep understanding of cybersecurity, Field Effect's team of experts quickly assess the impact of events on your network to ensure they are contained with minimal impact.
Detect (DE)	DE.AE-5	Incident alert thresholds are established	● Complete	Field Effect's ARO system categorizes and prioritizes information security events.
Detect (DE)	DE.CM-1	The network is monitored to detect potential cybersecurity events	● Complete	Covalence conducts full PCAP and deep packet inspection on network traffic transiting it.
Detect (DE)	DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	◐ Partial	The data returned by Covalence includes information that can be used to associate actions with individual system users (e.g. username, timestamp, source address, destination address).
Detect (DE)	DE.CM-4	Malicious code is detected	● Complete	Covalence provides world-class, holistic protection against malware on the endpoint, network, and cloud.

● **Complete**
Covalence covers > 90% of this safeguard

◐ **Partial**
Covalence partially covers this safeguard

○ **Support**
Covalence can detect failures in this safeguard or can be leveraged to streamline monitoring

Function	Subcategory	Description	Covalence Coverage	Description
Detect (DE)	DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	◐ Partial	Covalence cloud integrations help manage the information security risks associated with the use of cloud services, and can detect cybersecurity events.
Detect (DE)	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	◐ Partial	See above.
Detect (DE)	DE.CM-8	Vulnerability scans are performed	○ Support	Covalence detects vulnerabilities on enterprise and externally exposed assets to complement active vulnerability scans.
Respond (RS)	RS.AN-1	Notifications from detection systems are investigated	● Complete	Field Effect analysts manage alerts and investigations for Covalence, keeping the number of ARO reports and false-positives to a minimum.
Respond (RS)	RS.AN-2	The impact of the incident is understood	◐ Partial	Covalence AROs contain detailed information and insights so that the impact and scope of cyber security incidents is easily understood.
Respond (RS)	RS.AN-3	Forensics are performed	● Complete	In the unlikely event that forensics are required to investigate and contain an incident, Field Effect will provide instructions and analytic support.

● **Complete**
Covalence covers > 90% of this safeguard

◐ **Partial**
Covalence partially covers this safeguard

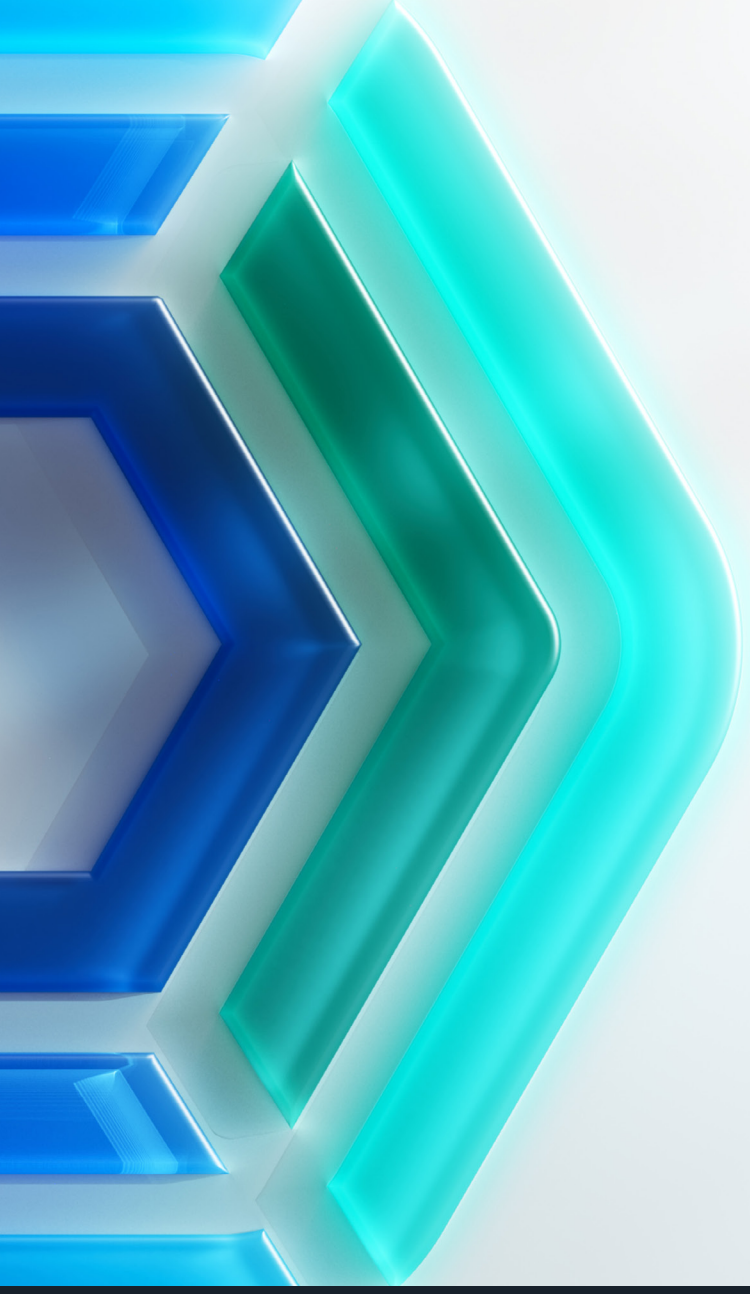
○ **Support**
Covalence can detect failures in this safeguard or can be leveraged to streamline monitoring

Function	Subcategory	Description	Covalence Coverage	Description
Respond (RS)	RS.AN-4	Incidents are categorized consistent with response plans	● Complete	The Covalence ARO system categorizes and prioritizes information security events.
Respond (RS)	RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	● Complete	Our threat intelligence team monitors security bulletins, vulnerability notifications, and posts from security researchers to ensure Covalence detects the latest threats and that your network and data stay protected.
Respond (RS)	RS.MI-1	Incidents are contained	● Complete	Covalence ensures cyber incidents are detected and mitigated quickly so that they have a minimal impact on your organization.
Respond (RS)	RS.MI-2	Incidents are mitigated	● Complete	See above.
Respond (RS)	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	○ Support	Covalence monitors networks, cloud applications, and endpoint devices to identify technical vulnerabilities, and provides detailed steps on how to address them.

● **Complete**
Covalence covers > 90% of this safeguard

◐ **Partial**
Covalence partially covers this safeguard

○ **Support**
Covalence can detect failures in this safeguard or can be leveraged to streamline monitoring



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