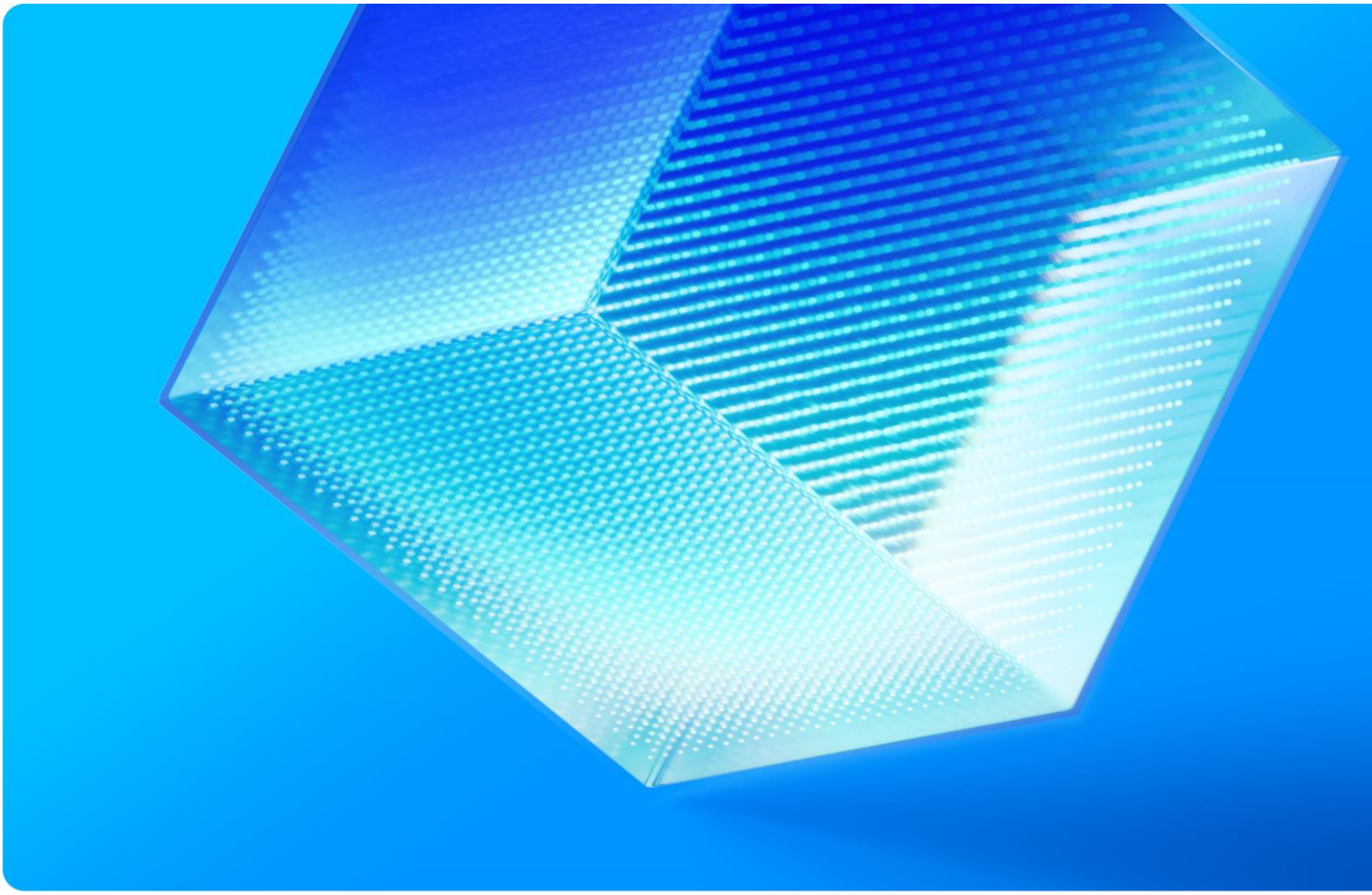
FIELD EFFECT



# MDR Compliance Series

## NIST Cybersecurity Framework (CSF)

Version 2.0

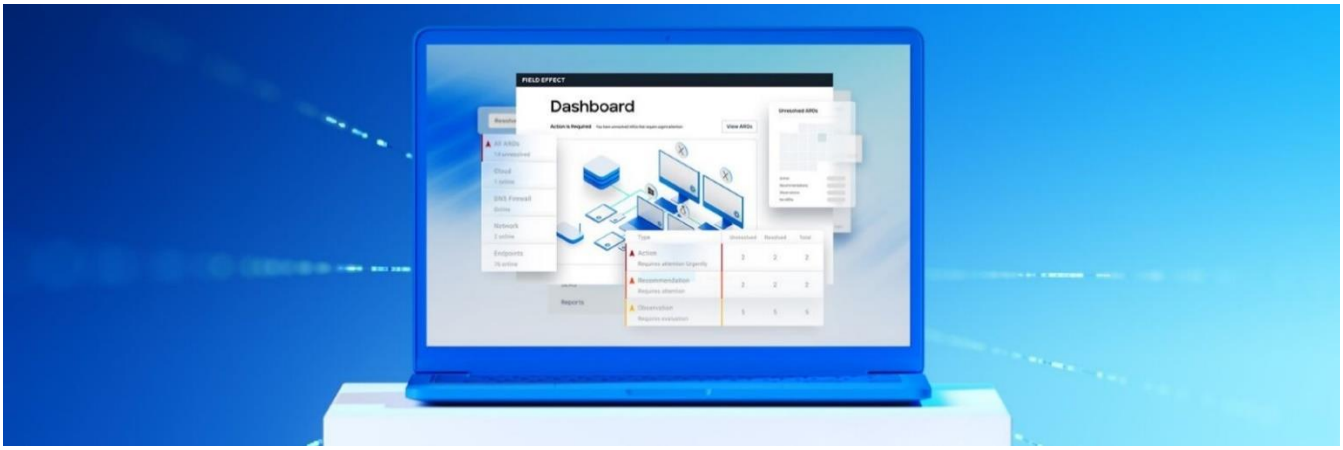
# About Field Effect

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 initially introduced in 2014 to guide critical infrastructure operators and to serve as a voluntary framework aiding organizations in mitigating cybersecurity risks. In its latest iteration (Version 2.0) released in February 2024, the CSF explicitly extends its assistance to all organizations, regardless of their size or sector.

Noteworthy enhancements include an expanded scope, a renewed emphasis on governance, and improved reference documentation. The goal of this document is to outline how Covalence aligns with relevant cybersecurity controls within the CSF and facilitates the implementation and audit processes.[1]




[1] 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.

# Govern (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

| Subcategory | Description | How we help |
|---|---|---|
| **GV.RM-01** | Risk management objectives are established and agreed to by organizational stakeholders | Our monthly reporting helps organizations establish and monitor measurable objectives for cybersecurity risk management. |
| **GV.RM-03** | Cybersecurity risk management activities and outcomes are included in enterprise risk management processes | Field Effect MDR automatically identifies and assesses several categories of cybersecurity risks across endpoints, network, and cloud services, so you can properly document and prioritize them. |
| **GV.RM-06** | A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks | By monitoring your organization's endpoints, network, and cloud workloads, our MDR service helps identify risks so you can properly document and prioritize them. |
| **GV.RR-03** | Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies | Field Effect MDR empowers your team with expert-led support so you can achieve ample resourcing at a fraction of the price of developing this capability internally. |

# Identify (ID)

The organization's current cybersecurity risks are understood.

| Subcategory | Description | How we help |
|---|---|---|
| **ID.AM-01** | Inventories of hardware managed by the organization are maintained | Our Endpoint Devices view allows customers to quickly perform spot checks against their asset inventory. |
| **ID.AM-02** | Inventories of software, services, and systems managed by the organization are maintained | Field Effect MDR monitors for software and service inventory changes and alerts on potentially unwanted applications. |
| **ID.RA-01** | Vulnerabilities in assets are identified, validated, and recorded | Our MDR service not only identifies technical vulnerabilities on your computers, networks, and cloud applications, but its automated reporting provides detailed steps on how to address them. |
| **ID.RA-02** | Cyber threat intelligence is received from information sharing forums and sources | Field Effect securely ingests threat intelligence feeds and advisories to alert on threats and develop analytics to detect the latest tactics, techniques, and procedures (TTPs). |
| **ID.RA-03** | Internal and external threats to the organization are identified and recorded | Our threat hunters and intelligence analysts maintain awareness of new threats and constantly scan our customer networks for them. |

| | | |
|---|---|---|
| **ID.RA-5** | Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization | Our proprietary ARO system provides timely, detailed information on the vulnerabilities and risks to your devices and networks. |
| **ID.IM-01** | Improvements are identified from evaluations | Our MDR service provides an automated mechanism to constantly evaluate your compliance with cybersecurity requirements and identify areas for improvement. |
| **ID.IM-02** | Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties | Field Effect provides a full suite of cybersecurity services including vulnerability assessments, phishing exercises, and tabletop exercises. |

# Protect (PR)

Safeguards to manage the organization's cybersecurity risks are used.

| Subcategory | Description | How we help |
|---|---|---|
| **PR.AA-03** | Users, services, and hardware are authenticated | Field Effect MDR detects legacy encryption protocols and authentication mechanisms, and reports on cloud accounts with MFA disabled. |
| **PR.AT-01** | Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with security risks in mind | The Suspicious Email Analysis Service (SEAS), included with our MDR solution, reduces the risk of phishing by helping users recognize social engineering attempts and providing a mechanism to report suspicious activity. |
| **PR.DS-01** | The confidentiality, integrity, and availability of data-at-rest are protected | Our MDR service reports on USB device use and can maintain an allow/block list of removable media, ensuring they are only leveraged where there's an organizational reason for their use. |
| **PR.DS-02** | The confidentiality, integrity, and availability of data-in-transit are protected | Organizations can create custom blocklists in the DNS firewall to prevent access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems. |

| | | |
|---|---|---|
| **PR.PS-02** | Software is maintained, replaced, and removed commensurate with risk | Our service detects end-of-life software and operating systems so they can be quickly replaced with supported, maintained versions. |
| **PR.PS-05** | Installation and execution of unauthorized software are prevented | Field Effect MDR comes equipped with a DNS Firewall that automatically updates with the latest threat intelligence to provide additional protection from phishing and block access to known malicious domains. |

# Detect (DE)

Possible cybersecurity attacks and compromises are found and analyzed.

| Subcategory | Description | How we help |
|---|---|---|
| **DE.CM-01** | Networks and network services are monitored to find potentially adverse events | Our MDR services comes with an optional network appliance that conducts full PCAP and deep packet inspection of traffic transiting it to detect cybersecurity events and identify technical vulnerabilities. |
| **DE.CM-03** | Personnel activity and technology usage are monitored to find potentially adverse events | The data returned by our MDR service includes system and cloud logs that are analyzed to find unusual access patterns and failed access attempts. |
| **DE.CM-06** | External service provider activities and services are monitored to find potentially adverse events | Field Effect MDR ingests telemetry from cloud infrastructure, employing behavioral analytics to detect unusual activity, such as unauthorized account access from suspicious ISPs. |
| **DE.AE-02** | Potentially adverse events are analyzed to better understand associated activities | Our MDR 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. |
| **DE.AE-03** | Information is correlated from multiple sources | Field Effect MDR collects and correlates event data from the endpoint, network, and cloud to fully understand events and incidents. |

| | | |
|---|---|---|
| **DE.AE-04** | The estimated impact and scope of adverse events are determined | Our AROs come packed with useful information on the scope and possible impacts of the cyber events we detect, all without having to deploy expensive SIEM technology. |
| **DE.AE-06** | Information on adverse events is provided to authorized staff and tools | Not only do we function as your security operations center (SOC), but the Field Effect portal allows us to alert your organization when certain types of alerts occur. |
| **DE.AE-07** | Cyber threat intelligence and other contextual information are integrated into the analysis | Whether it's comparing the latest threat intelligence to activity on your network, or rapidly acquiring and analyzing vulnerability disclosures, Field Effect takes care of this requirement. |
| **DE.AE-08** | Incidents are declared when adverse events meet the defined incident criteria | Our service drastically reduces false-positives and alert fatigue, allowing you to act with confidence when declaring incidents. |

# Respond (RS)

Actions regarding a detected cybersecurity incident are taken.

| Subcategory | Description | How we help |
|---|---|---|
| **RS.MA-01** | The incident response plan is executed in coordination with relevant third parties once an incident is declared | Field Effect can work with you to develop an incident response plan, and as your third-party MDR provider we'll be there every step of the way should a cybersecurity incident be declared. |
| **RS.MA-02** | Incident reports are triaged and validated | Our award-winning AI and experienced analysts handle the majority of triage and prevent alert fatigue. In addition, all AROs are compared against set criteria and labelled with an incident severity. |
| **RS.MA-03** | Incidents are categorized and prioritized | All AROs come categorized, prioritized, and written in jargon-free language designed to be understood by everyone. |
| **RS.MA-04** | Incidents are escalated or elevated as needed | The Field Effect portal allows you to update the status of ongoing incidents, coordinate with internal stakeholders, and request further assistance from us. |
| **RS.AN-03** | Analysis is performed to determine what has taken place during an incident and the root cause of the incident | AROs contain detailed information and insights so that the impact, scope, and root cause of incidents can be easily understood. |

| | | |
|---|---|---|
| **RS.AN-06** | Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved | All MDR commands are recorded for audit purposes, so that a detailed history of actions performed during investigations and incidents can be reviewed and preserved if necessary. |
| **RS.AN-07** | Incident data and metadata are collected, and their integrity and provenance are preserved | Any data or metadata collected by our MDR service is immediately brought back to the appliance where it's protected from deletion and alteration. |
| **RS.AN-08** | An incident's magnitude is estimated and validated | When an incident occurs, Field Effect analysts proactively look for indicators of compromise and evidence of persistence to ensure the full magnitude of the event is understood. |
| **RS.MI-01** | Incidents are contained | Our MDR service can block well-known hacking techniques, isolate infected endpoints, and disable compromised cloud accounts, allowing us to quickly contain incidents. |
| **RS.MI-02** | Incidents are eradicated | By containing and eradicating incidents quickly, we ensure they have minimal impact on your organization. |

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

Field Effect MDR 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.

## 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.

FIELD EFFECT

## Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
CANADA + UNITED STATES
+1 ( 800) 2 99 - 8986

UNIT ED KINGDOM
+44 (0 ) 800 086 9176

AUSTRALIA
+61 1800 431418