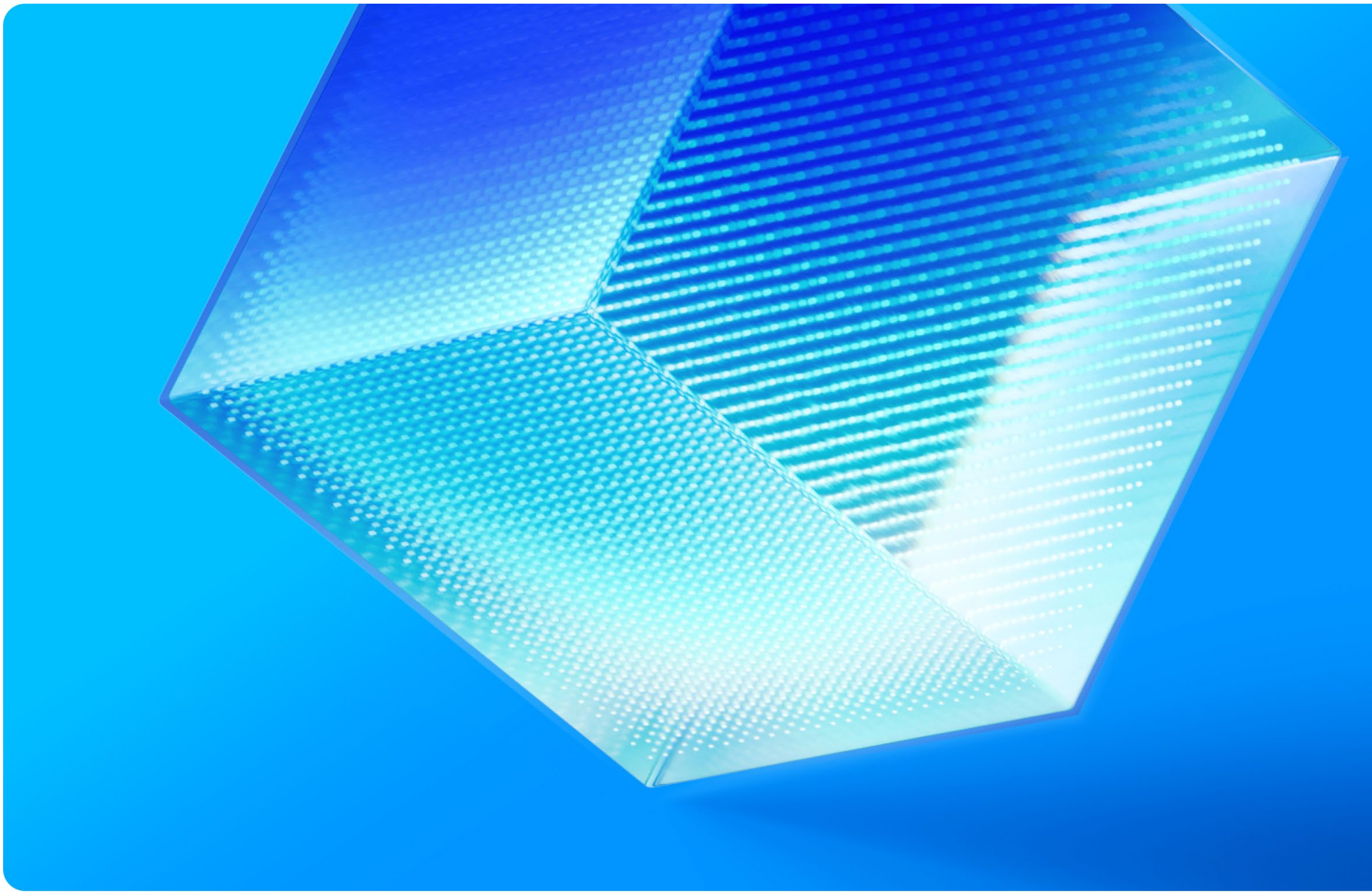
FIELD EFFECT

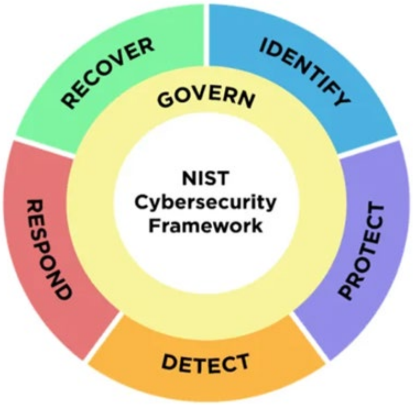


Field Effect and NIST CSF Compliance

May 2025

V2.0

About NIST CSF



The NIST Cybersecurity Framework (CSF) is a comprehensive set of best practices designed to help organizations enhance their cybersecurity posture. The most recent version, NIST CSF Version 2.0, was released in February 2024. Compliance with CSF involves implementing a structured set of cybersecurity practices designed to manage and reduce cybersecurity risks, ensuring the protection of information systems and data throughout their entire lifecycle.

CSF is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, regardless of the maturity level of their cybersecurity programs. The framework includes guidelines on asset management, access control, data protection, and incident response, among other areas.

CSF is voluntary and typically self-assessed. However, some cybersecurity insurance policies or security assessments may refer to it as best practice. Organizations that achieve NIST CSF compliance are demonstrating their commitment to cybersecurity and can leverage this status to build trust with clients and partners.

Field Effect is pleased to provide this document, which outlines how Field Effect MDR helps support NIST CSF 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 CSF: A Perfect Match

Managed Detection and Response (MDR) services like Field Effect MDR can play a crucial role in helping organizations meet their CSF 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 personal data is protected against unauthorized access and breaches.

Subcategory	Topic	How Field Effect Helps
GV.OV-03	**Risk Management Performance Review**	Field Effect MDR provides a monthly Risk Report that includes an overall risk score and helps contextualize software, operating system, and configuration risks across your IT environment.
GV.RM-06	**Risk Assessment Standardization**	See Above.
GV.SC-02	**Cybersecurity Roles Coordination**	As a critical supplier of cybersecurity services, Field Effect can work with your organization to implement your security requirements into your customer agreement.
GV.SC-06	**Supplier Risk Planning**	Field Effect is ISO 27001 certified and has a SOC 2, Type 2 report available for download in the Field Effect Trust Center.

Subcategory	Topic	How Field Effect Helps
GV.SC-08	**Third-Party Incident Inclusion**	If requested, Field Effect can participate in your organization's incident planning and lessons learned sessions.
ID.AM-02	**Software Inventory Management**	Field Effect MDR monitors and reports on risky software installations like Potentially Unwanted Applications (PUAs) and new network administration tools.
ID.AM-08	**Lifecycle Management**	Field Effect provides user and account information along with powerful APIs your organization can leverage to verify the accuracy of your inventories.
ID.RA-01	**Asset Vulnerability Management**	Field Effect MDR can detect network devices not running its endpoint agent to reduce the chances of unauthorized and BYOD devices. In addition, Field Effect APIs can be used to conduct reviews to identify redundant systems, software, and services that unnecessarily increase your organization's attack surface.

Subcategory	Topic	How Field Effect Helps
ID.RA-02	Threat Intelligence Acquisition	Field Effect's dedicated Threat Intelligence team continuously monitors advisories from trusted third-party sources to stay ahead of emerging threat actor tactics and newly disclosed vulnerabilities so this information can be incorporated into the MDR service.
ID.RA-03	Threat Identification	Field Effect performs active threat hunting to look for signs of threat actors within customer environments that may have evaded automated detection.
ID.RA-07	Change and Exception Management	Field Effect MDR detects changes to your environment such as new ports being exposed to the Internet, which can be used to verify that your organization is following procedures for the formal documentation of proposed changes.
ID.RA-10	Supplier Risk Assessment	The Field Effect compliance team can work with your organization to complete your security assessment of the MDR service. You can begin the process now by visiting the Field Effect Trust Center.

Subcategory	Topic	How Field Effect Helps
ID.IM-01	Evaluation-Based Improvements	In addition to MDR services, Field Effect provides penetration testing, phishing simulation, and cybersecurity assessment services. These engagements will enhance your organization’s awareness of your security posture, identify gaps, and provide guidance on how to improve.
ID.IM-02	Security Test-Based Improvements	Field Effect provides Incident Response (IR) preparation and tabletop services that are designed to enhance your organization's cybersecurity readiness by practicing and refining your response to hypothetical cybersecurity incidents in a stress-free and secure setting.
PR.AA-03	Authentication Management	The Field Effect MDR portal allows users to quickly identify cloud accounts without multifactor authentication enabled.
PR.DS-02	Data-in-Transit Protection	When network monitoring is implemented as part of the MDR service, Field Effect will alert on unencrypted and deprecated protocols that pose a risk to data protection.

Subcategory	Topic	How Field Effect Helps
PR.PS-01	Configuration Management	If your organization chooses to run Microsoft Defender alongside the Field Effect endpoint agent, you can manage and enforce Defender settings via the Field Effect MDR portal.
PR.PS-02	Software Lifecycle Management	Field Effect MDR alerts on vulnerable and out-of-date software so that it can be updated or replaced with supported versions.
PR.PS-04	Log Monitoring	As an alternative to using a SIEM, Field Effect MDR acts as a central repository for security event alerting. In addition, Field Effect's physical appliances can be configured as log receivers for devices like firewalls that are unable to install the endpoint agent.
PR.PS-05	Unauthorized Software Prevention	This control involves configuring systems to use approved DNS services that proactively block access to known malicious domains. Field Effect MDR includes a built-in DNS firewall, updated daily with the latest indicators of compromise (IOCs).
DE.CM-01	Network Monitoring	Field Effect's physical appliances perform full PCAP and deep packet inspection on network traffic transiting them to rapidly detect network intrusions.

Subcategory	Topic	How Field Effect Helps
DE.CM-06	**External Service Monitoring**	Field Effect MDR monitors cloud environments for cyber threats and proactively reports cloud configuration issues like MFA disabled for privileged users, unused accounts, and access key rotation. With active response enabled, Field Effect remediates threat actor activities, including suspicious logins, email inbox changes, and access control modifications.
DE.CM-09	**Hardware and Software Monitoring**	Field Effect MDR provides holistic monitoring at the endpoint, network, and cloud to detect threats and proactively report on cyber risk. Additionally, the MDR service includes the Suspicious Email Analysis Service (SEAS), an Outlook add-on that allows users to request automated analysis of suspicious emails.
DE.AE-02	**Adverse Event Analysis**	Field Effect provides log retention and correlation solutions that achieve SIEM outcomes without the complexity and cost of traditional SIEM systems.

Subcategory	Topic	How Field Effect Helps
RS.MA-01	**Incident Response Execution**	Field Effect's 24/7 Security Operations Center (SOC) is always on standby to provide expert incident response support whenever your organization needs it.
RS.MA-02	**Incident Report Validation**	Field Effect's ARO reporting comes in a prioritized, jargon-free format that makes it easy to understand the severity of an incident.
RS.MA-03	**Incident Categorization and Prioritization**	The Field Effect's SOC delivers continuous threat monitoring and rapid response, prioritizing incidents based on their scope and potential impact. Our expert team stands ready to defend your organization around the clock.
RS.MI-01	**Incident Containment**	Field Effect's goal is to contain all cyber incidents in their earliest stages, before they have an impact on your data. With real-time blocking and host isolation capabilities, Field Effect MDR secures thousands of customers worldwide.
RS.MI-02	**Incident Eradication**	When an incident is detected, Field Effect collaborates closely with your organization to ensure complete threat eradication and conducts thorough root cause analysis to help prevent future occurrences.

Complexity out.
Clarity in.

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