Framework Mapping: Cisco Secure Workload + NIST CSF 2.0

Overview of the NIST Cybersecurity Framework 2.0

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 is a voluntary set of guidelines developed to help organizations manage and reduce cybersecurity risks. While these guidelines are voluntary, their adoption can significantly improve an organization's security posture by offering a structured approach to risk management.

In February 2024, NIST released CSF 2.0, updating version 1.1 from April 2018. This update incorporates feedback from various industries and stakeholders, enhancing the framework's flexibility, applicability, and relevance. NIST CSF 2.0 continues to serve as a voluntary, risk-based framework designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks, foster resilience, and align with best practices.

Purpose of the framework

The NIST Cybersecurity Framework provides a structured yet flexible approach to improving an organization's cybersecurity posture. It is used for:

- **Assessing risks:** Identifying, analyzing, and prioritizing cybersecurity risks.
- **Guiding cybersecurity programs:** Establishing or improving cybersecurity strategies in alignment with organizational goals.
- **Enhancing communication:** Facilitating clear communication about cybersecurity risks and strategies between technical teams, leadership, and external stakeholders.

The framework is particularly valuable for organizations that lack formalized cybersecurity programs or resources, though it is robust enough to benefit even the most mature organizations.

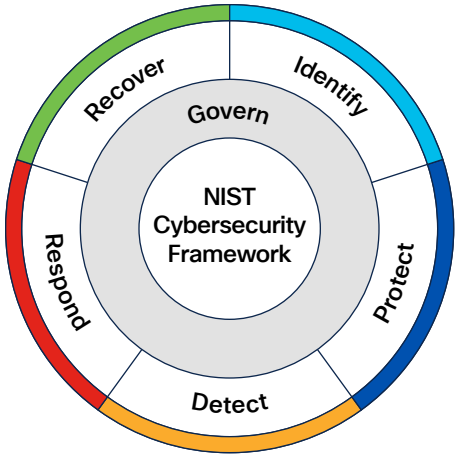

Figure 1. Components of the NIST CSF 2.0

Key components of the NIST Cybersecurity Framework 2.0

NIST CSF 2.0 maintains the foundational structure of the original framework while introducing several enhancements. Its key components are:

Core functions

The framework core outlines six **high-level functions** that provide a strategic view of cybersecurity risk management. These functions remain foundational in CSF 2.0 and are as follows:

- **Govern:** Establish and oversee policies, roles, processes, and accountability to align cybersecurity efforts with organizational objectives and regulatory requirements.

  Examples: Risk management policies, executive accountability, cybersecurity governance framework

- **Identify:** Develop an understanding of cybersecurity risks to systems, assets, data, and capabilities. This involves identifying critical resources, threats, and vulnerabilities.

  Examples: Asset management, governance, risk assessments

- **Protect:** Implement safeguards to ensure the delivery of critical services and mitigate risks.

  Examples: Access control, data protection, training, maintenance

- **Detect:** Establish systems to identify cybersecurity events or anomalies in a timely manner.

  Examples: Continuous monitoring, intrusion detection, threat intelligence

- **Respond:** Develop and implement appropriate actions to mitigate the effects of a detected cybersecurity event.

  Examples: Incident response planning, mitigation strategies, communication

- **Recover:**
  Develop plans to restore operations and reduce the impact of cybersecurity incidents.

  Examples: Disaster recovery, business continuity planning, lessons learned

Implementation tiers

The framework includes **implementation tiers** to help organizations evaluate their current cybersecurity practices and set goals for improvement. These tiers reflect the degree to which an organization's cybersecurity practices are informed by risk management processes, integrated with business needs, and adaptive to evolving risks:

Tier 1 (Partial): Limited awareness and ad hoc implementation of cybersecurity practices.

Tier 2 (Risk-Informed): Risk management practices are formally defined but not fully integrated.

Tier 3 (Repeatable): Cybersecurity practices are consistently applied and documented across the organization.

Tier 4 (Adaptive): Practices are continuously improved and proactively adapted to changing risks.

Profiles

The **framework profiles** allow organizations to align the framework to their specific goals, resources, and risk tolerance. A profile compares the current state of an organization's cybersecurity practices to its desired state, serving as a roadmap for improvement.

Why use the NIST Cybersecurity Framework?

Organizations adopt NIST CSF 2.0 for several reasons:

Flexibility: Its nonprescriptive nature allows organizations to tailor it to their unique needs.

Widely recognized: The framework is globally acknowledged as a standard for cybersecurity best practices.

Risk Management: It helps organizations prioritize risks and allocate resources effectively.

Compliance alignment: While voluntary, the framework aligns with various regulatory requirements and standards, simplifying compliance efforts.

Mapping to other frameworks

The NIST National Online Informative References (OLIR) Program provides a framework for organizations to map cybersecurity standards, guidelines, and frameworks. By leveraging OLIR, Cisco can cross-reference NIST CSF 2.0 with other standards, such as NIST SP 800-53, simplifying compliance and security alignment. This approach eliminates the need for separate mappings, saving time and effort while ensuring traceability across frameworks.

For Cisco, this means that once its security solutions, such as Cisco® Secure Workload, are mapped to NIST CSF 2.0, these mappings can be extended through NIST OLIR to align with other frameworks. This capability is particularly beneficial for public sector and regulated industries, where compliance with multiple frameworks is often required. By using NIST CSF 2.0 as a common backbone, Cisco helps customers achieve compliance efficiently while demonstrating how its solutions align with best practices and regulatory mandates.

This cross-mapping capability strengthens Cisco's position as a strategic enabler of cybersecurity compliance, providing customers with a clear understanding of how its solutions fit into their broader compliance and risk management strategies.

Understanding Cisco Secure Workload

Cisco Secure Workload formerly known as Cisco Tetration®, is a comprehensive workload protection platform designed to provide visibility, security, and compliance across hybrid, multicloud, and on-premises environments. It enables organizations to monitor application behaviors, map application dependencies, and enforce microsegmentation policies to limit lateral movement and reduce the attack surface. By leveraging advanced analytics and machine learning, Cisco Secure Workload detects anomalies, identifies unauthorized activities, and simplifies policy creation and enforcement. Its capabilities help organizations enhance their security posture, meet compliance requirements, and protect workloads throughout their lifecycle.

Deployment options

Cisco Secure Workload offers flexible deployment options to address the diverse needs of organizations, whether they operate in on-premises data centers, public or hybrid clouds, or containerized environments. Its ability to integrate seamlessly with existing infrastructure and adapt to evolving IT environments makes it a powerful solution for securing workloads across the enterprise. By tailoring the deployment to their unique requirements, organizations can maximize security, reduce risks, and maintain a consistent security posture across all environments.

On-premises option

Cisco Secure Workload can be deployed in an organization's on-premises data center, providing full workload visibility and security within private infrastructure.

Use case: Ideal for organizations with strict data sovereignty, compliance, or security requirements that mandate keeping workloads on-premises.

Deployment details:

- Requires physical and virtual infrastructure to run the Cisco Secure Workload platform.
- Sensors (agents) are deployed on workloads (e.g., servers, virtual machines) to collect telemetry and enforce security policies.
- For workloads where it is not possible to install an agent, telemetry and discovery can be done using common network telemetry protocols such as NetFlow, IPFIX, Encapsulated Remote Switch Port Analyzer (ERSPAN) and NetFlow Secure Event Logging (NSEL).
- Integration with existing on-premises tools such as firewalls, network management solutions, and Security Information and Event Management (SIEM) systems is supported.

Benefits:

- Full control over data and infrastructure.
- Enhanced security for workloads operating within private data centers.

Software-as-a-Service (SaaS) option

Cisco Secure Workload can also be delivered as a SaaS offering, reducing the operational overhead of managing the platform infrastructure.

Use case: Ideal for organizations seeking a fully managed solution that simplifies deployment and maintenance.

Deployment details:

- Cisco hosts and manages the platform infrastructure, while organizations deploy sensors on their workloads or consume network telemetry for workload discovery.
- SaaS deployment supports hybrid, multicloud, and on-premises workloads.
- Updates, scaling, and availability are handled by Cisco.

Benefits:

- Faster time to value with minimal operational burden.
- Fully managed by Cisco, helping ensure the latest features and security updates.
- Scales to meet the needs of dynamic environments.

Support for workload form factors

Cisco Secure Workload provides holistic coverage of workload form factors such as bare metal, virtualized workloads (regardless of hypervisor), public cloud workloads, and modern cloud-native workloads. It also has extensive support for multiple operating systems such as Windows OS, Linux, and Unix.

Bare-metal and virtualized workloads

Cisco Secure Workload supports deployment on both bare-metal servers and virtualized infrastructure.

Use case: Provides flexibility for organizations using traditional IT environments or virtualized platforms.

Deployment details:

- Sensors (agents) can be installed on bare-metal servers and virtual machines.
- Additionally, workloads without sensors (agentless) can be discovered and onboarded with network telemetry.
- Virtualized environments, such as VMware vSphere, Microsoft Hyper-V, and KVM, are fully supported.
- Granular telemetry and policy enforcement extend to both bare-metal and virtualized workloads.

Benefits:

- Versatility across diverse IT environments.
- Protects legacy systems and modern virtualized infrastructures.

Public cloud workloads

Cisco Secure Workload supports cloud workloads regardless of the cloud service provider. Examples of cloud service providers include AWS, Microsoft Azure, and Google Cloud Platform.

Use case: Suitable for organizations adopting public cloud infrastructure or operating cloud-native workloads.

Deployment details:

- Sensors (agents) are deployed on cloud workloads (e.g., instances, virtual machines) to monitor application behaviors and enforce security policies.
- Additionally, workloads without sensors (agentless) can be discovered and onboarded using cloud flow logs.
- Enforcement can be done with the host-native firewall of the workloads or using cloud built-in controls, such as security groups.
- Visibility extends to workload communication within and across cloud environments.

Benefits:

- Supports cloud scalability and dynamic workload environments.
- Simplifies security for distributed and containerized workloads.
- Provides consistent security policies across hybrid infrastructures.

Cloud-native: Containerized and Kubernetes workloads

Cisco Secure Workload supports modern application architectures, including containerized workloads and Kubernetes-based deployments.

Use case: Designed for organizations using microservices and containers in their development and production environments.

Deployment details:

- Sensors (agents) are deployed within Kubernetes clusters.
- Integrates with Kubernetes-native tools for workload orchestration and management.
- Integrates with cloud-managed Kubernetes services, such as Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS), and Google Kubernetes Engine (GKE).
- Provides visibility into container-to-container communication and enforces security policies at the container level.

Benefits:

- Provides granular visibility into containerized workloads.
- Security is aligned with DevSecOps practices.
- Helps ensure compliance and reduces risk in containerized environments.

Key technical features of Cisco Secure Workload

Cisco Secure Workload delivers a robust set of technical features designed to secure workloads in complex and dynamic environments. Its ability to integrate with diverse infrastructure, automate security policy enforcement, and provide deep visibility makes it a key solution for organizations aiming to strengthen their workload security posture.

Comprehensive workload visibility

Description: Provides deep visibility into workload behaviors, application dependencies, and network communications across on-premises, hybrid, and multicloud environments.

Benefits: Enables organizations to understand how workloads interact, identify vulnerabilities, and gain insights into their IT environment for better decision-making and security posture.

Application dependency mapping

Description: Automatically maps application dependencies by analyzing communication patterns between workloads and applications.

Benefits: Simplifies the creation of security policies, supports troubleshooting, and helps ensure secure application behavior by understanding interdependencies.

Microsegmentation

Description: Enables granular policy enforcement to segment workloads and limit lateral movement of threats within the environment.

Benefits: Reduces the attack surface by restricting unauthorized communications between workloads and ensuring adherence to the principle of least privilege.

Near-real-time anomaly detection

Description: Leverages advanced machine learning and analytics to identify deviations from baseline workload behaviors and detect suspicious activities.

Benefits: Provides early warning of potential threats or misconfigurations, enabling faster responses and reducing dwell time for attackers.

Policy automation

Description: Automates the generation and enforcement of security policies based on observed workload behaviors and application dependencies.

Benefits: Simplifies security management, reduces the risk of human error, and helps ensure consistent application of policies across diverse environments, improving operational efficiency.

Multicloud and hybrid cloud support

Description: Offers seamless integration with public cloud platforms (e.g., AWS, Azure, GCP), private cloud, and on-premises environments.

Benefits: Provides consistent visibility and security policy enforcement across all environments, allowing organizations to adopt a unified security approach regardless of where workloads are deployed.

Integration with Kubernetes and container environments

Description: Supports containerized workloads and integrates with Kubernetes clusters, providing visibility and policy enforcement at the container pod level.

Benefits: Secures modern microservices-based applications and aligns with DevSecOps practices to help ensure security in dynamic containerized environments.

Continuous telemetry and monitoring

Description: Collects real-time telemetry from workloads to monitor application traffic, workload behavior, and network flows.

Benefits: Provides actionable insights into security events and enables comprehensive monitoring for compliance and threat detection.

Threat intelligence integration

Description: Supports integration with external threat intelligence platforms to enhance detection and response to known threats.

Benefits: Improves situational awareness and strengthens defenses by correlating workload activity with external threat data.

Secure API integration

Description: Provides APIs for integration with third-party tools such as SIEM (e.g., Splunk®), Security Orchestration Automation and Response (SOAR), Endpoint Detection and Response (EDR), and orchestration platforms.

Benefits: Enhances interoperability and allows organizations to build a cohesive security ecosystem.

Compliance and audit support

Description: Tracks workload behaviors and generates detailed audit trails that demonstrate compliance with security frameworks and regulations (e.g., NIST, GDPR, PCI-DSS).

Benefits: Simplifies compliance reporting and enhances transparency for internal and external audits, helping organizations meet regulatory requirements.

Scalability and performance

Description: Designed to scale with growing environments, from small deployments to large, complex enterprises with thousands of workloads.

Benefits: Provides consistent security and visibility as organizations expand their IT infrastructure, adapting to evolving IT and security landscapes.

Role-Based Access Control (RBAC)

Description: Provides role-based access control for administrators and users of the platform.

Benefits: Protects sensitive security configurations and limits access to authorized personnel only, reducing insider threats.

Behavioral baselines

Description: Builds baseline profiles of normal workload and application behaviors over time.

Benefit: Helps detect anomalies and suspicious activity by identifying deviations from established norms.

Enforcement via agents (sensors)

Description: Agents (lightweight sensors) are deployed on workloads to collect telemetry and enforce security policies in real time.

Benefits: Provides continuous monitoring and helps ensure that security policies are applied directly at the workload level.

Enforcement via network (agentless)

Description: Collection of telemetry is done using common network telemetry protocols such as ERSPAN, NetFlow, IPFIX, and NSEL, as well as cloud flow logs. Native enforcement can be done using firewalls, load balancers, cloud built-in controls, and infrastructure devices via integration with third-party policy orchestrators.

Benefits: Provides continuous monitoring and helps ensure that security policies are applied directly at the workload level.

Encrypted communications

Description: Supports encrypted communications between workloads and the Secure Workload platform to help ensure data confidentiality.

Benefits: Protects sensitive telemetry data and helps ensure secure interactions between platform components.

Incident investigation support

Description: Provides detailed telemetry and historical data to support post-incident analysis and forensic investigations.

Benefits: Helps identify root causes, scope of impact, and areas requiring remediation after security incidents.

Support for legacy, modern, and cloud-native environments

Description: Works across bare-metal servers, virtual machines, and containerized environments.

Benefit: Provides consistent security across traditional IT systems, modern cloud-native applications, and hybrid architectures.

Centralized management

Description: Offers a single management console for policy configuration, monitoring, and reporting.

Benefits: Simplifies operations and provides a unified view of workloads across the entire IT environment, contributing to improved operational efficiency.

Event correlation and reporting

Description: Correlates events across workloads and provides detailed reports on security incidents and policy violations.

Benefits: Enhances situational awareness and simplifies the communication of security posture to stakeholders.

Mapping Cisco Secure Workload to NIST CSF 2.0

Cisco Secure Workload Capability Mapping to NIST CSF 2.0 and NIST 800-53

Function	Category	Cisco Secure Workload NIST CSF 2.0 Mapping (Meets)	Cisco Secure Workload NIST CSF 2.0 Mapping (Supports)	Cisco Secure Workload NIST 800-53 Mapping (Meets)	Cisco Secure Workload NIST 800-53 Mapping (Suports)
Govern (GV)		Non-technical controls			
Identify (ID)	Asset Management (ID.AM)	ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05	ID.AM-01, ID.AM-07, ID.AM-08	AC-20, CM-08, PM-05, SA-05, SA-09, AC-04, CA-03, CA-09, PL-02, PL-08, PM-07, AC-20, SR-02, RA-03, RA-09, RA-02	CM-08, PM-05, CM-12, CM-13, SI-12, CM-09, MA-02, MA-06, PL-02, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-18, SR-05, SR-12
	Risk Assettment (ID.RA)	ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06	ID.RA-09	CA-02, CA-07, CA-08, RA-03, RA-05, SA-11(02), SA-15(07), SA-15(08), SI-04, SI-05, SI-05, PM-15, PM-16, PM-12, SI-05, PM-09, PM-11, RA-02, RA-08, RA-09, RA-02, PM-18, PM-30, RA-07	SA-04, SA-05, SA-10, SA-11, SA-15, SA-17, SI-07, SR-05, SR-06, SR-10, SR-11
	Improvement (ID.IM)	Non-technical controls			
Protect (PR)	Identity, Management, Authentication, and Access Control (PR.AA)	PR.AA-03, PR.AA-05	PR.AA-01	AC-07, AC-12, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11, AC-01, AC-02, AC-03, AC-05, AC-06, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13	AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11
	Awareness and Training (PR.AT)	Non-technical controls			
	Data Security (PR.DS)	PR.DS-01, PR.DS-11	PR.DS-02, PR.DS-10	CA-03, CP-09, MP-08, SC-04, SC-07, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-03, SI-04, SI-07, CP-06	AU-16, CA-03, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-03, SI-04, SI-07, AC-02, AC-03, AC-04, AU-09, AU-13, CP-09, SA-08, SC-24, SC-32, SC-39, SI-10, SI-16
	Platfrom Security (PR.PS)	PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-05, PR.PS-06		CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11, MA-03(06), SA-10(01), SI-02, SI-07, CM-07(09), SA-10(03), SC-03(01), SC-39(01), SC-49, SC-51, AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, CM-07(02), CM-07(04), CM-07(05), SA-03, SA-08, SA-10, SA-11, SA-15, SA-17, SC-34	
	Technology Infrastructure Resilience (PR.IR)	PR.IR-01, PR.IR-03, PR.IR-04	PR.IR-02	AC-03, AC-04, SC-04, SC-05, SC-07, CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13, CP-06, CP-07, CP-08, PM-03, PM-09	CP-02, PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18, PE-23
Detect (DE)	Continuous Monitoring (DE.CM)	DE.CM-01, DE.CM-09	DE.CM-03, DE.CM-06	AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04, AC-04, AC-09, CA-07, CM-06, CM-10, CM-11, SC-34, SC-35, SI-07	AC-02, AU-12, AU-13, CA-07, CM-10, CM-11, CA-07, PS-07, SA-04, SA-09, SI-04
	Adverse Event Analysis (DE.AE)	DE.AE-02, DE.AE-03, DE.AE-07	DE.AE-04, DE.AE-06, DE.AE-08	AU-06, CA-07, IR-04, SI-04, AU-06, CA-07, PM-16, IR-04, IR-05, IR-08, SI-04, PM-16, RA-03, RA-10	PM-09, PM-11, PM-18, PM-28, PM-30, IR-04, PM-15, PM-16, RA-03, RA-10, IR-04, IR-08
Respond (RS)	Incident Management (RS.MA)	Non-technical controls			
	Incident Analysis (RS.AN)	RS.AN-07	RS.AN-03, RS.AN-08	AU-07, IR-04, IR-06	AU-07, IR-04, IR-08, RA-03, RA-07
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls			
	Incident Mitigation (RS.MI)	RS.MI-01, RS.MI-02		IR-04	
Recover (RC)	Incident Recovery Plan Execution (RC.RP)	RC.RP-03, RC.RP-05		CP-02, CP-04, CP-09, CP-10	
	Incident Recovery Communication (RC.CO)	Non-technical controls			

Conclusion

The NIST Cybersecurity Framework 2.0 builds on the strengths of the original framework while addressing the dynamic nature of cybersecurity challenges. By providing a flexible, scalable, and comprehensive approach to risk management, the framework empowers organizations to enhance their cybersecurity posture, improve resilience, and ensure the continuity of critical operations. Whether an organization is just beginning its cybersecurity journey or looking to refine an established program, CSF 2.0 serves as a robust guide for navigating today's complex threat landscape.

Cisco Secure Workload is a powerful and versatile workload protection platform that delivers comprehensive visibility, advanced security, and policy enforcement across on-premises, hybrid, and multicloud environments. By leveraging application dependency mapping, real-time telemetry, behavioral analytics, and microsegmentation, it empowers organizations to reduce their attack surface, prevent lateral movement of threats, and respond swiftly to anomalies. Its seamless integration with diverse environments, including containerized and Kubernetes-based architectures, makes it an essential tool for modern organizations seeking to secure their workloads while maintaining operational efficiency and scalability.

Aligning to NIST CSF 2.0 provides organizations with a structured and comprehensive approach to managing cybersecurity risks and improving their overall security posture. By mapping Cisco Secure Workload to NIST CSF, organizations can effectively address critical aspects of identifying, protecting, detecting, responding to, and recovering from cybersecurity threats. This alignment not only helps organizations meet compliance requirements and industry best practices but also strengthens their ability to adapt to an evolving threat landscape, helping ensure long-term resilience and robust defense mechanisms.

Resources

Cisco Secure Workload

Cisco Secure Workload At-a-Glance

Cisco Secure Workload data sheet