Framework Mapping: Identity Services Engine (ISE) + NIST CSF 2.0

Overview of the NIST Cybersecurity Framework 2.0

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

In February 2024, NIST released the 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. The 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.

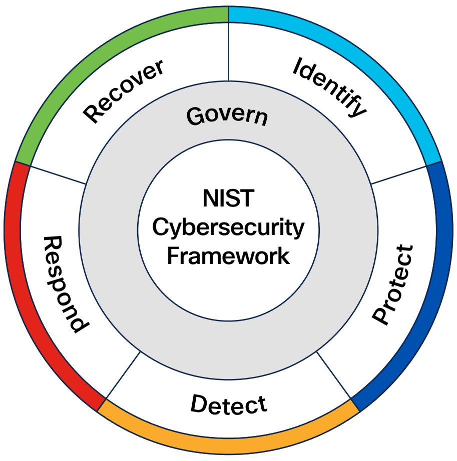
Guiding Cybersecurity Programs: Establishing or improving cybersecurity strategies in alignment with organizational goals.

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.

Key Components of the NIST Cybersecurity Framework 2.0

The 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, and maintenance

🟧 **DETECT:**

Establish systems to identify cybersecurity events or anomalies in a timely manner.

Examples: Continuous monitoring, intrusion detection, and threat intelligence

🟥 **RESPOND:**

Develop and implement appropriate actions to mitigate the effects of a detected cybersecurity event.

Examples: Incident response planning, mitigation strategies, and communication

🟩 **RECOVER:**

Develop plans to restore operations and reduce the impact of cybersecurity incidents.

Examples: Disaster recovery, business continuity planning, and 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 the NIST CSF 2.0 for several reasons:

Flexibility: Its non-prescriptive 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 the NIST Cybersecurity Framework (CSF) 2.0 with other standards like 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 Firewalls, 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.

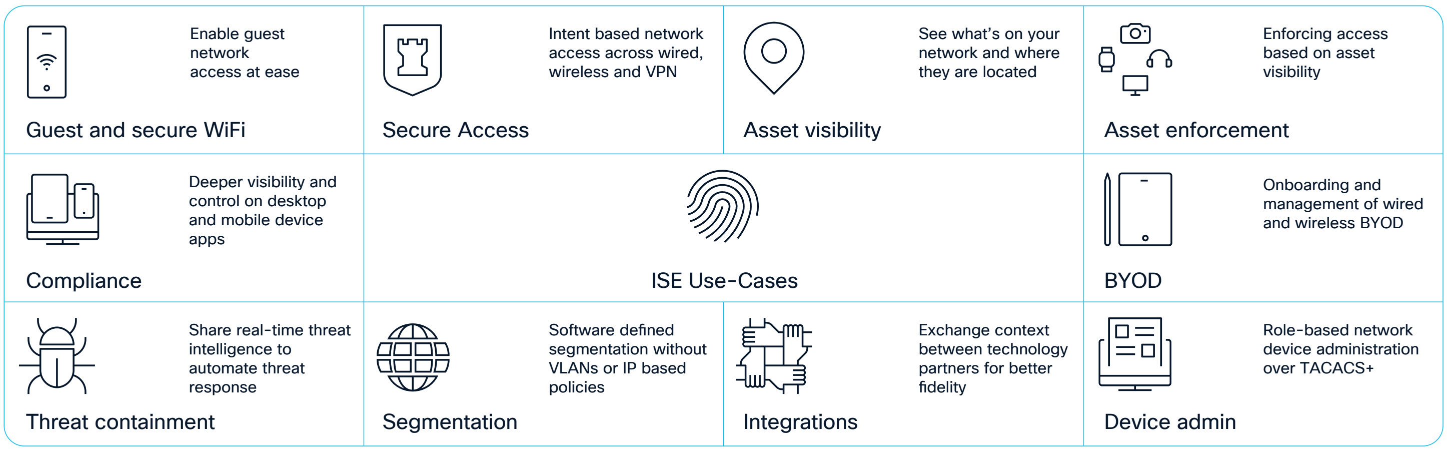
Understanding Cisco Identity Services Engine

As network environments become more dynamic and complex, traditional access control methods may no longer provide adequate security or visibility. Cisco Identity Services Engine (ISE) is designed to address modern access and policy challenges by offering comprehensive identity-based network access control. By integrating authentication, authorization, and accounting (AAA) with advanced profiling and policy enforcement capabilities, Cisco ISE enables organizations to secure their networks, ensure compliance, and streamline user and device access—all from a unified platform.

What is ISE?

Cisco Identity Services Engine (ISE) is a comprehensive identity-based network access control solution that enables organizations to enforce security policies across wired, wireless, and VPN connections. ISE extends beyond traditional access control by providing advanced features such as device profiling, context-aware policy enforcement, guest access management, and integration with threat intelligence platforms.

Cisco ISE leverages automation, dynamic policy application, and real-time visibility to help organizations identify users and devices, control access, and respond quickly to security threats. As part of Cisco's security portfolio, ISE is designed to scale from small businesses to large enterprises, offering unified management, flexible deployment options, and robust compliance capabilities—all while maintaining network performance and user experience.



ISE Use-Cases

Guest and secure WiFi: Enable guest network access at ease

Secure Access: Intent based network access across wired, wireless and VPN

Asset visibility: See what's on your network and where they are located

Asset enforcement: Enforcing access based on asset visibility

Compliance: Deeper visibility and control on desktop and mobile device apps

BYOD: Onboarding and management of wired and wireless BYOD

Threat containment: Share real-time threat intelligence to automate threat response

Segmentation: Software defined segmentation without VLANs or IP based policies

Integrations: Exchange context between technology partners for better fidelity

Device admin: Role-based network device administration over TACACS+

Use Case Overview

Guest and Secure Wireless Access

Many organizations provide free internet access to guests visiting their organization for a short period. These guests include vendors, retail customers, short-term vendors or contractors, and so on. Cisco ISE provides the ability to create accounts for these visitors and authenticate them for audit purposes. There are three ways in which Cisco ISE can provide Guest access: via a hotspot (immediate noncredentialled access), self-registration, or sponsored Guest Access. Cisco ISE also provides a rich set of APIs to integrate with other systems such as vendor management systems to create, edit, and delete Guest accounts. Further, the various portals that the end user sees can be completely customized with the right font, color, themes, and so on to match the look and feel of the customer's brand.

Asset Visibility

Understanding the device type is often a critical element in determining the type of network access that should be granted to the device. For example, a building management system such as an IP camera or an elevator should be given access to a specific part of the network (such as the building management services network), while a printer should be given access to another part of the network (such as IT services). Having visibility helps the IT administrator determine the types of devices on the network and how to provide them with the right level of permissions. Basic asset visibility profiles endpoints by matching their network attributes to known profiles. Advanced asset visibility performs deeper analysis of the different conversations that applications on these devices have with other endpoints and servers on the network through Deep Packet Inspection (DPI). While basic asset visibility will provide you with visibility into most of your network, especially your traditional devices (printers, mobile phones, etc.), advanced asset visibility will provide you with visibility into more vertical-specific and IoT-types of devices.

Compliance

Saboteurs focus on intentional data corruption (ransomware) and data exfiltration, which compromises endpoints on a network. The most effective and well-publicized compromises take advantage of known issues that would have been simple to remediate but were overlooked. Compliance visibility allows organizations to view how user endpoints comply with corporate policy through the use of posture and/or integration with Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) systems (supported MDM/EMM systems can be found in Cisco ISE Network Component Compatibility). Using either Cisco ISE's Posture engine or an MDM, an organization can evaluate how many endpoints are compliant and ensure that noncompliant software is not installed and/or running.

Secured Wired Access

Securing the wired network is essential to prevent unauthorized users from connecting their devices to the network. Using Cisco ISE, network administrators can provide secure wired network access by authenticating and authorizing users and devices. Authentication can be active or passive. An active authentication is done using 802.1X when Cisco ISE authenticates the user against an identity source. Passive authentication involves Cisco ISE learning the user's identity via Active Directory domain logins or other indirect means. Once the user or device authenticates successfully, authorization takes place. Authorization can be achieved by assigning the endpoint's network access session a dynamic VLAN, a downloadable ACL, or other segmentation methods.

Bring Your Own Device (BYOD)

Many organizations have instituted a policy that allows employees to connect their personal devices such as smartphones to the corporate wireless network and use it for business purposes. This is referred to as a Bring-Your-Own-Device (BYOD) policy. However, since these devices are owned by the individuals, they don't like to install management software that allows organizations to "manage" the endpoint. In such situations, Cisco ISE provides a very streamlined method to automate the entire BYOD onboarding process, from device registration and supplicant provisioning to certificate installation. This can be done on devices across various OS platforms such as iOS, Android, Windows, macOS, and ChromeOS. The Cisco ISE My Devices Portal, which is completely customizable, allows end users to onboard and manage various devices.

Cisco ISE provides multiple elements that help automate the entire onboarding aspect for BYOD. This includes a built-in Certificate Authority (CA) to create and help distribute certificates to different types of devices. The built-in CA provides a complete certificate lifecycle management. Cisco ISE also provides a My Devices Portal, an end-user-facing portal that allows the end user to register their BYOD endpoint as well as mark it as being lost and block it from the network. BYOD onboarding can be accomplished either through a single-SSID or dual-SSID approach. In the single-SSID approach, the same SSID is used to onboard and connect the end user's device, while in the dual-SSID approach, an open SSID is used to onboard the devices, but the device connects to a different, more secure SSID after the onboarding process. For customers that want to provide a more complete management policy, BYOD can be used to connect the end user to the MDM onboarding page as well.

Rapid Threat Containment

Cisco Rapid Threat Containment makes it easy to get fast answers about threat on your network and to stop them even faster. It uses an open integration approach of Cisco security products, technologies from Cisco partners, and the extensive network control of Cisco ISE.

With integrated network access control technology, you can manually or automatically change our users' access privileges when there is suspicious activity, a threat, or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their user can keep working on less-critical applications.

Upon detecting a flagrant threat on an endpoint, a pxGrid ecosystem partner can instruct ISE to contain the infected endpoint, either manually or automatically. The containment can involve moving the device to a sandbox for observation, moving it to a remediation domain for repair, or removing it completely. ISE can also receive the standardized Common Vulnerability Scoring System (CVSS) classifications as well as the Structured Threat Information Expression (STIX) threat classifications, so that manual or automatic changes to a user's access privileges can be made based on their security score.

Segmentation

Network segmentation is a proven concept to protect critical business assets, but traditional approaches are complex. Cisco Group-Based Policy/TrustSec software-defined segmentation is simpler to enable than VLAN-based segmentation. Policy is defined through security groups. It is an open concept in IETF, available within Open Daylight, and supported on third-party and Cisco platforms. Cisco ISE is the segmentation controller, which simplifies the management of switch, router, wireless, and firewall rules. Group-Based Policy/TrustSec segmentation provides better security at a lower cost compared to traditional segmentation. Forrester Consulting found in an analysis of customers that operational costs are reduced by 80% and policy changes are 98% faster.

Security Ecosystem Integrations

Cisco ISE builds contextual data about endpoints in terms of their device type, location, time of access, posture, user(s) associated to that asset, and much more. Endpoints can be tagged with SGTs based on these attributes. This rich contextual insight can be used to enforce effective network access control policies and can also be shared with ecosystem partners to enrich their services. For example, in the Cisco Next-Generation Firewalls (NGFW), policies can be written based on the identity context, such as device type, location, user groups, and others, received from Cisco ISE. Inversely, specific context from third-party systems can be fed into the Cisco ISE to enrich its sensing and profiling capabilities, and for threat containment. The context exchange between the platforms can be done via Cisco pxGrid (including pxGrid Cloud and pxGrid Direct) or REST APIs.

Device Administration (TACACS+)

Network and security administrators typically own the task of administering and monitoring network and security devices in an enterprise. When there are a limited number of devices, keeping track of admin users, privileges, or changes in configuration can be easy. However, as the network grows to tens, hundreds, or even thousands of devices, it becomes exceedingly complex to manage devices without automation and a smooth workflow. Cisco ISE provides the capability to automate device administration tasks with clean workflows and monitoring capabilities with TACACS+ within a controlled space in the UI.

Workload Connector

Zero Trust access from anywhere requires consistent access and segmentation policies between users, devices, and application workloads. Cisco ISE collects contextual data from workloads using Workload Connectors. Workloads can be classified with Security Group Tags (SGTs) based on this imported context from the data center and cloud providers. This context can be used to create and enforce effective network access control policies and can also be shared with ecosystem partners to enrich their services. For example, in the Cisco Secure Firewall, policies can be written based on the identity context, which has been assigned by ISE utilizing attributes such as device type, location, owner, the ACI Endpoint Group, and others.

Benefits of ISE

Cisco Identity Services Engine (ISE) provides several key advantages for organizations seeking to secure and simplify network access:

- **Centralized Access Control**: By unifying authentication, authorization, and accounting (AAA) functions, Cisco ISE enables organizations to consistently enforce security policies across all users and devices.
- **Dynamic Policy Enforcement:** Real-time context awareness and adaptive policies allow ISE to automatically adjust access rights based on user roles, device type, location, and security posture.
- **Operational Efficiency:** Automated workflows, streamlined onboarding, and centralized management help reduce administrative effort, freeing IT teams to focus on strategic projects.
- **Comprehensive Visibility:** ISE delivers deep visibility into who and what is connected to the network, enabling faster identification and response to potential risks.
- **Scalable and Future-Ready:** Designed to integrate with Cisco's broader security ecosystem, Cisco ISE supports evolving organizational needs, compliance requirements, and emerging security challenges.

ISE Deployment Options

Cisco Identity Services Engine (ISE) Deployment Options
Cisco offers flexible deployment options for ISE to suit a wide range of network environments and organizational needs:

- **Physical Appliances:** Dedicated Cisco ISE hardware appliances provide robust performance and reliability for on-premises deployments in enterprise networks.
- **Virtual Appliances:** Cisco ISE is available as a virtual appliance, allowing organizations to deploy it on their existing virtualization infrastructure in private data centers or cloud environments.
- **Cloud-Managed and Hybrid Deployments:** Cisco ISE supports integration with cloud services and hybrid environments, enabling centralized policy management and secure access across distributed networks.

ISE Technical Features

Cisco Identity Services Engine (ISE) offers a comprehensive set of features designed to secure network access, enhance visibility, and enforce consistent policies across modern networks. Key capabilities include:

- **Identity and Access Control**
  Cisco ISE delivers centralized authentication, authorization, and accounting (AAA) services, enabling organizations to define and enforce detailed access policies based on user, device, location, and security posture.
- **Device Profiling**
  ISE automatically detects, classifies, and profiles devices connecting to the network, providing granular visibility into endpoints—including BYOD, IoT, and guest devices—without requiring manual intervention.
- **Context-Aware Policy Enforcement**
  With context-aware capabilities, ISE dynamically applies policies based on real-time information such as user identity, device type, connection method, time, and posture assessment, ensuring secure and appropriate access.
- **Guest Access Management**
  ISE simplifies the process of providing secure Guest Access with customizable portals, self-registration workflows, and sponsor approval, while maintaining complete visibility and control over guest users.
- **Posture Assessment and Remediation**
  ISE evaluates the security posture of endpoints before granting network access. Non-compliant devices can be automatically directed to remediation resources or assigned restricted access, helping maintain compliance and reduce risk.
- **Integration with Threat Intelligence and Security Ecosystem**
  ISE integrates with Cisco and third-party security solutions, such as Cisco Secure Network Analytics, Cisco Secure Firewall, and Cisco XDR, to share contextual information and orchestrate automated threat response.
- **Network Segmentation and Policy Enforcement**
  ISE enables dynamic network segmentation by assigning users and devices to appropriate VLANs or security groups using Security Group Tags (SGTs), supporting Zero Trust and minimizing lateral movement of threats.
- **Automated Device Onboarding**
  ISE streamlines the onboarding process for new users and devices, supporting certificate-based authentication, 802.1X, and flexible onboarding workflows for various device types and use cases.
- **Scalability and High Availability**
  Cisco ISE is built for enterprise-scale environments, supporting distributed deployments, high availability, and redundancy to ensure consistent performance and uptime.
- **Centralized Management and Reporting**
  ISE provides unified management, detailed reporting, and real-time monitoring from a single interface, allowing administrators to track user and device activity, compliance status, and policy enforcement across the network.

For more detailed information check out the ISE Data Sheets.

Mapping Cisco ISE to NIST CSF 2.0

		Cisco ISE NIST CSF 2.0 Mapping		Cisco ISE NIST 800-53 Mapping	
Function	**Category**	**Yes**	**Supports**	**Yes**	**Supports**
Govern (GV)		Non-technical controls			
Identify (ID)	Asset Management (ID.AM)	ID.AM-08	ID.AM-01, ID.AM-02	CM-09, CM-13, MA-02, MA-06, PL-02, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12	CM-08, PM-05, AC-20, SA-05, SA-09
	Risk Assessment (ID.RA)		ID.RA-01, 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, 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-01, PR.AA-03, PR.AA-04, PR.AA-05		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, IA-13, AC-03, AC-05, AC-06, AC-07, AC-10, AC-12, IA-13, AC-16, AC-17, AC-18, AC-19, AC-24	
	Awareness and Training (PR.AT)	Non-technical controls			
	Data Security (PR.DS)	PR.DS-01, PR.DS-02	PR-DS-02	CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11	CP-06, CP-09
	Platfrom Security (PR.PS)	PR.PS-01, PR.PS-04, PR.PS-05	PR.PS-01, 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, AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, SC-34, AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, CM-07(02), CM-07(04), CM-07(05), SC-34	CM-11, MA-03(06), SA-10(01), SI-02, SI-07, SA-03, SA-08, SA-10, SA-11, SA-15, SA-17
	Technology Infrastructure Resilience (PR.IR)	PR.IR-01, PR.IR-03, PR.IR-04		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	
Detect (DE)	Continuous Monitoring (DE.CM)	DE.CM-01, DE.CM-06	DE.CM-03, DE.CM-09	AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04, PS-07, SA-04, SA-097	AC-02, AU-12, AU-13, CA-07, CM-10, CM-11, AC-04, AC-09, AU-12, CM-03, CM-06, SC-34, SC-35, SI-04, SI-07
	Adverse Event Analysis (DE.AE)		DE.AE-03, DE.AE-06, DE.AE-07, DE.AE-08		AU-07, IR-04, AU-07, IR-04, IR-06, IR-08, RA-03, RA-07
Respond (RS)	Incident Management (RS.MA)	Non-technical controls			
	Incident Analysis (RS.AN)		RS.AN-03, RS.AN-07, RS-AN.08		AU-07, IR-04, AU-07, IR-04, IR-06
	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)	None	RC.RP-03	None	CP-02, CP-04, CP-09
	Incident Recovery Communication (RC.CO)	Non-technical controls			

Conclusion

The NIST Cybersecurity Framework 2.0 continues to provide a robust foundation for managing cybersecurity risk, adapting to new threats, and supporting organizational resilience. Its flexible, scalable, and comprehensive structure enables organizations to strengthen their security posture, meet regulatory requirements, and ensure the continuity of critical operations.

Cisco Identity Services Engine (ISE) is a powerful solution that empowers organizations to enforce identity-based access controls, gain deep visibility into users and devices, and automate policy enforcement across complex network environments. By integrating authentication, authorization, device profiling, and dynamic policy management, Cisco ISE helps organizations protect their networks from evolving threats and support Zero Trust initiatives.

Aligning Cisco ISE with the NIST CSF 2.0 enables organizations to effectively manage network access risks, enhance compliance, and facilitate clear communication between technical teams and leadership. With its scalability, unified management, and integration with Cisco's broader security ecosystem, Cisco ISE is an asset for organizations implementing the NIST CSF 2.0—whether establishing foundational controls or refining a mature cybersecurity program.