Cisco and the NIST Cybersecurity Framework

Effective Cybersecurity Risk Management

From the largest federal agency to the smallest school district, every organization today is faced with managing cybersecurity risks efficiently and effectively. Can yours benefit from an innovative, best practices approach to cybersecurity?

Cybersecurity can seem overwhelming, and there's plenty of long to-do lists. The Center for Internet Security (CIS) has the Critical Security Controls, the International Organization for Standardization (ISO) has its 27000-series publications, and ISACA manages its COBIT 5 framework. Layer those atop compliance mandates like the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) -- and it's often hard to know where to start.

That's why the National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF). It enables organizations of all sizes to discuss, address, and manage cybersecurity risk. And without reinventing the cyber wheel, it references existing best practices through its Core functions: Identify, Protect, Detect, Respond, and Recover. The CSF Profiles and Tiers work with the Core to drive a simple yet effective cybersecurity risk management process that can plug into existing governance and risk management processes.

However, even with the NIST Cybersecurity Framework, many organizations still need more help. Critical tasks like risk assessment, gap analysis, and action planning are left to you. Then there's a dizzying array of security products on the market today from which to select. Often they have overlapping or missing capabilities and, worse, don't integrate with one another. There are simply not enough skilled cybersecurity professionals available to configure and manage all of those tools, let alone analyze and act on their output. Where can you get the solutions and guidance you really need for a truly effective cybersecurity program?

Let Cisco help

In the next few pages, we'll show how Cisco's effective security aligns with the NIST Cybersecurity Framework. We'll list each Framework function and category, and explain exactly how Cisco products and services help you accomplish each specific Framework goal. Our solutions are simple, open, and automated to interoperate at every level of the security stack, not only across the Cisco portfolio but also with other vendors' products. Furthermore, our solutions build industry-leading, actionable Talos threat intelligence directly into them. With Cisco, you can take a new approach to cybersecurity, adopt the Framework, and bolster cyber defenses and readiness.

Cybersecurity Framework Basics

The best source of Framework information is NIST itself, and the complete Framework document, newsletters, and other resources are freely available from www.nist.gov/cyberframework. Figure 1 summarizes the Framework's core structure for convenience, but please refer to the NIST Framework document for complete details.

Figure 1: Framework Core Structure

Cisco Security and the NIST Cybersecurity Framework		Technical Controls	Non-technical Controls
		Cisco	Cisco Services or Technology Partners
ID	Asset Management	✓	
	Business Environment		✓
	Governance		✓
	Risk Assessment	✓	✓
	Risk Management		✓
	Supply Chain	✓	✓
PR	Access Control	✓	✓
	Awareness Training		✓
	Data Security	✓	
	Info Protection Process		✓
	Maintenance		✓
	Protective Technology	✓	
DE	Anomalies and Events	✓	
	Continuous Monitoring	✓	
	Detection Process		✓
RS	Response Planning		✓
	Communications		✓
	Analysis	✓	
	Mitigation	✓	
	Improvements		✓
RC	Recovery Planning		✓
	Improvements		✓
	Communications		✓

Each Category has several Subcategories and multiple Informative Resources, so the entire Framework Core cannot fit into small summary table. That's why Figure 1 shows only the Subcategories and Informative Resources column headings but the fields are blank. Please see the Framework document's Appendix A, "Framework Core" for complete details.

Cisco Supports the NIST Cybersecurity Framework

Cisco's comprehensive cybersecurity product and services portfolio defends organizations throughout the world against today's advanced threats. Figure 2 shows how our cybersecurity products map to the NIST Cybersecurity Framework:

Figure 2: Cisco Security Product Aligns with the Framework

		AMP/ Threat Grid	Stealthwatch (with Cognitive)	Cloudlock	Web/ Email	Umbrella	Firepower	ISE/ Trustsec	Duo	AnyConnect	Meraki SM	Cisco Services
ID	Access Management	■	■	■			■	■	■		■	■
	Business Environment	Non-technical control area										■
	Governance	Non-technical control area										■
	Risk Assessment	■	■				■	■		■		■
	Risk Management	Non-technical control area										■
	Supply Chain	Cisco Security and Trust Organization (S&TO)										
PR	Access Control	■		■			■	■	■	■	■	■
	Awareness Training	Non-technical control area										■
	Data Security	■	■	■	■	■	■	■		■	■	■
	Info Protection Process	Non-technical control area										■
	Maintenance		■					■	■	■	■	■
	Protective Technology	■			■		■	■	■	■	■	■
DE	Anomalies and Events	■	■	■	■	■	■					■
	Continuous Monitoring	■	■	■	■	■	■		■	■		■
	Detection Process	Non-technical control area										■
RS	Response Planning	Non-technical control area										■
	Communications	Non-technical control area										■
	Analysis	■	■	■	■	■	■					■
	Mitigation	■		■	■	■	■	■				■
	Improvements	Non-technical control area										■
RC	Recovery Planning	Non-technical control area										■
	Improvements	Non-technical control area										■
	Communications	Non-technical control area										■

The green boxes show where Cisco Security products supports the Framework's desired outcomes. For example, Cisco Identity Services Engine (ISE) profiles and categorizes devices when they attempt to connect to the network. Knowing what's on the network is a key step toward effective Asset Management (Identify function). And Cisco Stealthwatch baselines network traffic patterns and detect suspicious activity, critical capabilities for the Anomalies and Events category (Detect function).

Cybersecurity products alone cannot cover the entire Framework. For example, the Awareness and Training category (Protect function) ensures that people are provided with cybersecurity awareness education and are adequately trained to perform their duties. The Detection Processes category (Detect function) ensures that people understand their roles; that detection processes are tested and improved; and event detection information is communicated and reported properly. Therefore, Figure 2 shows the non-technical control areas; that is, those categories where people and process related controls (and not technical controls) are required.

Cisco Security Services can help with all areas of the Framework, including the non-technical controls. We can help your organization adopt the Framework and use it to effectively manage cybersecurity risk. Figure 3 shows how our Advisory, Integration and Managed services can help you adopt the NIST Cybersecurity Framework:

Figure 3: Cisco Security Services: NIST CSF Alignment

		Advisory	Integration	Managed
ID	Access Management	✓	✓	✓
	Business Environment	✓		
	Governance	✓		
	Risk Assessment	✓	✓	✓
	Risk Management	✓	✓	
	Supply Chain	✓		
PR	Access Control	✓	✓	✓
	Awareness Training	✓		✓
	Data Security	✓		✓
	Info Protection Process	✓		✓
	Maintenance	✓		✓
	Protective Technology	✓	✓	✓
DE	Anomalies and Events	✓	✓	✓
	Continuous Monitoring	✓	✓	✓
	Detection Process	✓		✓
RS	Response Planning	✓		✓
	Communications	✓		✓
	Analysis	✓	✓	✓
	Mitigation	✓	✓	✓
	Improvements	✓		✓
RC	Recovery Planning	✓		✓
	Improvements	✓		✓
	Communications	✓		✓

Cisco Advisory Services has the right people and process knowledge and best practices to help you understand, plan, and act on all areas of the NIST Cybersecurity Framework. Our Integration Services can help you make the most of your technology investments, and our Managed services can help you implement new controls even if you don't have the manpower in-house.

In the coming pages, we'll explore each of the NIST CSF core functions – Identify, Protect, Detect, Respond, and Recover – and we'll offer more detail around the green boxes we showed in Figure 2 (Cisco Products) and Figure 3 (Cisco Services).

Cisco Solutions for the Identify (ID) Function

Identify | Protect | Detect | Respond | Recover

According to NIST, the purpose of the Identify function is to "develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities." Part of that organizational understanding is visibility into what you have; that is, it's difficult to protect something if you don't know that you have it. That's why Cisco's delivers critical discovery capabilities; that is, identifying and categorizing systems, assets, and data on a continuous basis. Let's take a closer look at each category within the Identify function.

ID.AM: Asset Management. NIST defines the Asset Management category's goal as "the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy."

Subcategories include physical device inventories (ID.AM-1) and software application inventories (ID.AM-2).

How Cisco solutions map to the Asset Management category:

- Cisco ISE discovers and accurately identifies devices connected to wired, wireless, and virtual private networks. It gathers this information based on what's actually connecting to the network, a key step toward building and maintaining accurate physical device inventories (ID.AM-1).
- Cisco Firepower provides visibility into software applications running on your network, a key step toward building and maintaining accurate software application inventories (ID.AM-2).
- Cisco Meraki Systems Manager delivers cloud-based endpoint management and control for the provisioning, management and security of mobile and desktop devices.
- Cisco Cloudlock is a cloud-native CASB and Cloud Cybersecurity Platform that helps organizations securely leverage the cloud for apps they buy and build. Cloudlock delivers security for cloud applications and platforms, including SaaS (Google G Suite, Box, Dropbox, Salesforce, ServiceNow, Slack) IaaS (Amazon Web Services), and PaaS (Force.com). Cisco Umbrella, our leading Secure Internet Gateway, also integrates CASB features like discovery and control of SaaS apps.
- Duo's endpoint visibility allows you to see, track and report on all end user devices from a single dashboard.
- Cisco Advisory Services help you analyze your asset management capabilities today, and provides you with the information you need to improve tomorrow. We can not only advise on device inventory strategies (ID.AM-1 and ID.AM-2), but also help you map organizational communication and data flow (ID.AM-3), catalog external systems (ID.AM-4), prioritize and classify resources (ID.AM-5) and establish cybersecurity roles and responsibilities both inside and outside of your agency or organization. (ID.AM-6).
- Cisco Advanced Malware Protection identifies and blocks the malicious code that is so often the cause of data leaks today (PR.DS-5), while protecting data stored on systems (PR.DS-1) and traversing across networks (PR.DS-2).
- Cisco Stealthwatch analyzes NetFlow records and alerts on evidence of information loss – for example, when large amounts of data unexpected leave a database server directly for the internet. Stealthwatch is an essential data leak protection solution (PR.DS-5) with absolutely minimal network performance impact.

ID.BE: Business Environment. NIST defines the Business Environment category's goal as "the organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions." This category requires people and process controls, not technical controls.

Subcategories include the identification and communication of the organization's supply chain role (ID.BE-1) and its critical infrastructure role (ID.BE-2), and the establishment and communication of the organization's priority mission and objectives (ID.BE-3), service delivery dependencies (ID.BE-4), and resiliency requirements (ID.BE-5).

How Cisco solutions map to the Business Environment category:

- Cisco Advisory Services' Strategy & Risk Management services include assessments, planning and guidance to deliver a holistic view of IT risks from the perspective of your business environment. It helps you understand and communicate your role in the supply chain (ID.BE-1) and as a critical infrastructure provider, if applicable (ID.BE-2). It enables you to establish and communicate your organization's priorities (ID.BE-3), service delivery dependences (ID.BE-4), and contingency planning requirements including cyber incident response strategies (ID.BE-5).

ID.GV: Governance. NIST defines the Governance category's goal as "the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk." This category requires people and process controls, not technical controls.

Subcategories include cybersecurity policy establishment (ID.GV-1), roles and responsibilities coordination (ID.GV-2), legal and regulatory requirements understanding (ID.GV-3), and assurance that governance and risk management process address cybersecurity risks (ID.GV-4).

How Cisco solutions map to the Governance category:

- Cisco Advisory Services' Strategy & Risk Management services provide strategic planning and guidance that are essential for all four of these subcategories (ID.GV-1 through ID.GV-4). Our Security Design Assessment (SDA) services assess security business goals and help reduce regulatory compliance exposure (ID.GV-3).

ID.RA: Risk Assessment. NIST defines the Risk Assessment category's goal as "the organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals."

Subcategories include asset vulnerability identification and documentation (ID.RA-1), threat and vulnerability information collection from sharing forums (ID.RA-2), threat identification and documentation (ID.RA-3), identification of business impacts and likelihoods (ID.RA-4), risk determination using threat, vulnerability, likelihoods, and impacts (ID.RA-5) and risk response identification and prioritization ID.RA-6).

How Cisco solutions map to the Risk Assessment category:

- Cisco Firepower assists with the correlation of threats and actual asset vulnerability information to help identify and document threats (ID.RA-1 and ID.RA-3) and calculates the impact assessment based on likelihood of attack success (ID.RA-4 and ID.RA-5). This information is essential to identify and prioritize responses based on risk (ID.RA-6), but also for immediate corrective action in the Detect function.
- Cisco Advisory Services' Custom Threat Intelligence (CTI) service combines threat and networking intelligence to provide visibility into both internal and external Indicators of Compromise (ID.RA-2). Our Strategy & Risk Management services can help you understand all of these risks and put them into a cybersecurity context for appropriate risk assessment (ID.RA-6), and Security Design Assessment (SDA) services assess security business goals determine key cybersecurity risks (ID.RA-5). Finally, Cisco's Infrastructure Security Services include penetration tests, war dialing, and assessments that identify exploitable vulnerabilities in the network, whether it be externally, internally, or wireless (ID.RA-1). They identify weaknesses in network design and implementation across a variety of factors and provide recommendations and guidance to secure the infrastructure in alignment with business needs (ID.RA-5 and ID.RA-6).

ID.RM: Risk Management Strategy. NIST defines the Risk Management Strategy category's goal as "the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions." This category requires people and process controls, not technical controls.

Subcategories include the establishment, management and approval of risk management processes (ID.RM-1), determination of expression organizational risk tolerance (ID.RM-2), and organizational risk tolerance in context of its role in critical infrastructure or sector-specific risk analysis (ID.RM-3).

How Cisco solutions map to the Risk Management Strategy category:

- Cisco Advisory Services' Strategy & Risk Management services can help you develop and establish risk management processes (ID.RM-1), to understand and assess organizational risk tolerance (ID.RM-2), and to consider it in the context of your organization's role in the public sector (ID.RM-3).

Cisco Solutions for the Protect (PR) Function

Identify | **Protect** | Detect | Respond | Recover

The purpose of the Protect function is to "develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services," according to NIST. Recall that the Identify function inventoried systems, assets, and data – so Cisco supports the Protect function with the advanced capabilities that enforce and harden security controls before the inevitable cyberattack attack occurs. Let's take a closer look.

PR.AC: Access Control. NIST defines the Access Control category's goal as "limiting access to assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions."

Subcategories include identity and credential management (PR.AC-1), physical access control management (PR.AC-2), remote access management (PR.AC-3), permissions and user rights management according to least privilege and separation of duties principles (PR.AC-4), and network integrity protection including network segmentation (PR.AC-5).

How Cisco solutions map to the Access Control category:

- Cisco Firepower next-generation firewall delivers superior, multi-layered protection, improves visibility, and reduces security costs and complexity. It delivers network integrity protection (PR.AC-5) by combining next-generation firewall with next-generation intrusion prevention capabilities to enforce and harden your network before the cyberattack occurs.
- Cisco ISE provides advanced network access controls by connecting user identity with device profiling and access policy, ensuring that only authorized individuals with authorized devices can access only the systems and data that your access policy permits (PR.AC-1 and PR.AC-4). Cisco Stealthwatch protects network segmentation integrity.
- Duo delivers secure access to cloud and on-premises applications and servers from anywhere, on any device. Duo access controls allow you to make application access decisions based on the trust established in user identities and the trustworthiness of their devices. (PR.AC-3)
- Cisco TrustSec provides network integrity protection, enabling the network to function as an access policy enforcer (PR.AC-5). It delivers scalable network segmentation far more efficiently than costly internal firewalls, hard-to-manage access control lists (ACLs), or legacy virtual local area networks (VLANs). In addition, it works with Cisco ISE to ensure that only authorized individuals using authorized devices can complete their missions according to the principles of least privilege (PR.AC-4). Cisco MAC Security (MACsec), a TrustSec component provides secure communication between endpoints on wired LANs, encrypting each packet so that communication cannot be monitored or altered on the wire. It supports the IEEE 802.1X standard, providing port-based access control using authentication (PR.AC-1 and PR.AC-5).
- Cisco AnyConnect delivers scalable, secure remote access (PR-AC-3) through advanced virtual private networking. Cisco AnyConnect is the market-leading secure endpoint access solution that delivers enforcement that is context-aware, comprehensive and easy – from any location, on any device, and across any access medium.
- Cisco Cloudlock provides access controls for Software-As-A-Service (SaaS) and cloud-based applications like Box, Office 365, and Google G Suite. These cloud applications often offer only consumer-grade access controls, so sensitive information can be at greater risk for unauthorized access (PR.AC-5).
- Cisco Advisory Services Strategy & Risk Management services can help you understand and develop strategies for improved and efficient logical access control (for all subcategories except PR.AC-2).
- Cisco Connected Safety and Security is a portfolio of physical access control systems, IP cameras, video surveillance software, and incident response solutions (like radio dispatching) for comprehensive physical access control security (PR.AC-2), For more information on Cisco's solutions that protect people and property, please see www.cisco.com/go/physicalsecurity.

PR.AT: Awareness and Training. NIST defines Awareness and Training category's goal as "the organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements." This category requires people and process controls, not technical controls.

Subcategories ensure that all users are informed and trained (PR.AT-1), and that following groups understand their roles and responsibilities: privileged users (PR.AT-2), third-parties like suppliers and partners (PR.AT-3), senior executives (PR.AT-4), and both physical and information security personnel (PR.AT-5).

How Cisco solutions map to the Awareness and Training category:

- Cisco Advisory Services Strategy & Risk Management services can help you assess and improve your awareness and training initiatives to embed a role-based cybersecurity mindset in all personnel (PR.AT-1 through PR.AT-5).

PR.DS: Data Security. NIST defines the Data Security category's goal as "information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information."

The first two subcategories ensure that both data-at-rest (PR.DS-1) and data-in-transit (PR.DS-2) are protected. Others include formal asset management procedures (PR.DS-3), capacity planning to ensure availability (PR.DS-4), data leak protections (PR.DS-5), integrity checking on software, firmware, and information (PR.DS-6) and production environment separation from development and test environments (PR.DS-7).

How Cisco solutions map to the Data Security category:

- Cisco Firepower combines industry-leading next-generation firewall and next-generation intrusion prevention on a single platform – essential controls for protecting systems that store sensitive information (PR.DS-1) and recommends rules based on network activity to help prevent data leaks (PR.DS-5). Its advanced firewall capabilities can help ensure separation between development and test environments (PR.DS-7). Furthermore, its built-in virtual private network (VPN) technology encrypts and protects the confidentiality and integrity of data-in-transit (PR.DS-2).
- Cisco Advanced Malware Protection identifies and blocks the malicious code that is so often the cause of data leaks today (PR.DS-5), while protecting data stored on systems (PR.DS-1) and traversing across networks (PR.DS-2).
- Cisco Email and Web Security are important controls for data leak protections (PR.DS-5), eradicating spam that enables phishing schemes or tricks users to connect to high-risk sites. It also blocks untrustworthy email attachments that often contain viruses and malware designed to affect system integrity or exfiltrate data.
- Cisco ISE and TrustSec work together to ensure that only authorized individuals using authorized devices can access specific network resources – essential protections for both data in transit (PR. DS-2) and at rest (PR.DS-1). TrustSec enables the network itself to act as an enforcer – without the need for additional firewall devices -- and is a scalable and cost-effective solution for network segmentation between production and development environments (PR.DS-7). Cisco MACsec encrypts traffic on wired networks to ensure the confidentiality and integrity of data-in-transit (PR.DS-2).
- Cisco AnyConnect works with Cisco Firepower to enable secure remote access, combining strong two-factor authentication and encryption to protect data-in-transit for remote systems and mobile users (PR.DS-2).
- Cisco Cloudlock provides access controls for Software-As-A-Service (SaaS) and cloud-based applications like Box, Office365, and Google Drive. It can detect and respond to sensitive and classified information that is uploaded to these unauthorized cloud applications, and sensitive data that is exposed via oversharing, which are so prevalent today, and is therefore an essential data leak protection (PR.DS-5).
- Cisco Umbrella helps ensure the integrity of DNS requests – ensuring that the host to which you expect to connect is the one to which you actually connect. This helps prevent your uses from connecting to high-risk sites that can inject advanced malware, which protects both data in transit (PR.DS-2) and at rest (PR.DS-1).

- Cisco Stealthwatch analyzes NetFlow records and alerts on evidence of information loss – for example, when large amounts of data unexpected leave a database server directly for the internet. Stealthwatch is an essential data leak protection solution (PR.DS-5) with absolutely minimal network performance impact.
- Cisco Advisory Services Strategy & Risk Management services can help you assess and improve your data security strategies pursuant to all of the Data Security subcategories (PR.DS-1 through PR.DS-7)
- Meraki Systems Manager ensures data security/encryption is enabled on devices.
- Duo's endpoint visibility gives actionable data on operating systems, browsers and more to ensure the integrity of software on devices.

PR.IP: Information Protection Processes and Procedures. NIST defines the Information Protection Processes and Procedures category's goal as "security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets." This category requires people and process controls, not technical controls.

Twelve subcategories include the creation and maintenance of system configuration baselines (PR.IP-1), the management and implementation of a System Development Life Cycle (PR.IP-2), the establishment of change control processes (PR.IP-3), the creation of backup and restore processes (PR.IP-4), the establishment of physical operating environment policies and procedures (PR.IP-5), the destruction of data according to policy (PR.IP-6), the continuous improvement of protection processes (PR.IP-7), the sharing of protection technology effectiveness experiences with key stakeholders (PR.IP-8).

They also include response and recovery plan implementation and management (PR.IP-9) and testing (PR.IP-10) – both of which are later used in the Respond and Recover functions, respectively. Finally, they seek to ensure that cybersecurity is considered in human resources practices like de-provisioning and personnel screening (PR.IP-11) and that a vulnerability management plan is developed and implemented (PR.IP-12).

How Cisco solutions map to the Information Protection Processes and Procedures category:

- Cisco Advisory Services Strategy & Risk Management services can help you assess and improve your information protection processes and procedures pursuant to all of the subcategories (PR.IP-1 through PR.IP-8). Our Security Optimization Service (SOS) assesses, develops, and optimizes your security infrastructure on an ongoing basis – helping to establish and manage a System Development Life Cycle (PR.IP-2) and to continuously improve protection processes (PR.IP-7)

PR.MA: Maintenance. NIST defines the Maintenance category's goal as "maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures."

Two subcategories ensure that maintenance and repairs of organizational assets are performed in a timely manner and with approved/controlled tools (PR.MA-1), and that remote maintenance is approved, logged, and with methods that prevent unauthorized access (PR.MA-2).

How Cisco solutions map to the Maintenance category:

- Cisco AnyConnect can help ensure that remote maintenance is performed over secure virtual private network (VPN) sessions, which help to prevent against unauthorized access and tampering attempts (PR.MA-2).
- Cisco Advisory Services Strategy & Risk Management services can help you assess and improve your maintenance efforts pursuant to both subcategories (PR.MA-1 and PR.MA-2).

PR.PT: Protective Technology. NIST defines the Protective Technology category's goal as "technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements."

Subcategories include audit/log record policy and review (PR.PT-1), removable media protection and restricted use according to policy (PR.PT-2), controlled system access that incorporates the principle of least functionality (PR.PT-3), and the protection of communications and control networks (PR.PT-4).

According to NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, the principle of least functionality "helps to minimize the potential for introduction of security vulnerabilities and includes, but is not limited to, disabling or uninstalling unused/unnecessary operating system (OS) functionality, protocols, ports, and services, and limiting the software that can be installed and the functionality of that software."

How Cisco solutions map to the Protective Technology category:

- Cisco Firepower combines industry-leading next-generation firewall and next-generation intrusion prevention on a single platform – essential cybersecurity controls for the protection of communication and control networks (PR.PT-4). Cisco Firesight, its management component, can identify potentially unnecessary (or unauthorized) protocols or software running on your networks so that you can achieve the principle of least functionality (PR.PT-3). It also correlates vulnerability with threat information, delivering richer audit/log records for more efficient log review (PR.PT-1).
- Cisco AMP identifies and blocks the malicious code that can affect the availability and reliability of communications and control networks (PR.PT-4).
- Cisco ISE and TrustSec profiles devices and associates them with user identities for superior network access control, which can also help achieve the principle of least functionality (PR.PT-3).
- Duo application access controls extend access based on the trust established in user identities and the trustworthiness of their devices.
- Cisco AnyConnect controls and secures remote system access, supporting the principle of least functionality (PR.PT-3).
- Cisco Advisory Services Strategy & Risk Management services can help you assess and improve your protective technology pursuant to all subcategories (PR.PT-1 through PR.PT-4).
- Cisco Email and Web Security are important controls to protect communiations (PR.DS-4) via SMTP and HTTP.
- Cisco Meraki Systems Manager offers endpoint management to control the applicaitons and OSs running on mobile and desktop devices.

Cisco Solutions for the Detect (DE) Function

Identify | Protect | **Detect** | Respond | Recover

The Detect function helps organizations develop and implement the appropriate activities to quickly identify the occurrence of a cybersecurity event. Many cybersecurity incidents go unnoticed for months, allowing hackers ample time to explore your networks, locate sensitive information, and then slowly and carefully exfiltrate it.

Cisco defines Time-To-Detection (TTD) for malware analysis as the window of time between the first observation of a file and the detection of an actual threat. Cisco continually seeks to reduce the TTD so that our customers can detect cyber incidents faster than ever (and take corrective action before damage occurs). For more information on Time-To-Detection and many other cybersecurity insights, please see the latest Cisco Cybersecurity Report at www.cisco.com/go/securityreport.

Now let's take a closer look at the Detect function's categories:

DE.AE: Anomalies and Events. NIST defines the Anomalies and Events category's goal as "anomalous activity is detected in a timely manner and the potential impact of events is understood."

Five subcategories include the establishment and management of network baselines and expected data flows for both systems and users (DE.AE-1), the analysis of detected events to understand attack targets and methods, (DE.AE-2), the aggregation and correlation of event data (DE.AE-3), the determination of impact (DE.AE-4), and the establishment of incident alert thresholds (DE.AE-5).

How Cisco solutions map to the Anomalies and Events category:

- Cisco Firepower monitors, controls, and analyzes network traffic and application data to understand threats and attack methods (DE.AE-2). It pre-correlates threats with actual system vulnerability information to assess and rank the potential impact (DE.AE-4). Through out-of-box integration with many Security Information and Event Management (SIEM) products that collect event logs (DE.AE-3), ASA with Firepower services delivers richer and more meaningful incident data for aggregation and alerting (DE.AE-5).
- Cisco AMP is a lightweight solution that analyzes files for malware threats both at network entry time and continuously. Oftentimes malicious code enters the network as seemingly harmless files, like a simple PDF email attachment or a downloaded Flash file. But once inside the network, these files can begin behaving abnormally – an early sign of advanced malware. Therefore, Cisco AMP's continuously analyzes application data to understand threat and attack methods (DE.AE-2), assess the potential impact (DE.AE-4), and alerts and quarantines when files become actual malware (DE.AE-5).
- Cisco Email and Web Security scans and blocks malicious web and email traffic, offering understanding and insight into primary attack vectors that target end users (DEAE-2). It also helps prevent end users from leaking sensitive information through these methods as well.
- Cisco Umbrella provides up-to-the-minute view and analysis of Internet traffic to understand threats and attack methods, offering visibility into where attacks are being staged on the Internet (DE.AE-2).
- Cisco Stealthwatch learns normal network traffic (data flow) patterns and establishes baselines of expected behavior (DE.AE-1). It analyzes, detects and alerts on network traffic anomalies and suspicious traffic patterns (DE.AE-2 and DE.AE-5).
- Cisco Cloudlock monitors and controls cloud application data to help set baselines for expected data flows between users and cloud applications (DE.AE-1).
- Cisco Advisory Services Security Design Assessments can help you understand normal activity and baselines so that anomalous activity can be more readily detected (DE.AE-1). It offers a comprehensive view of security infrastructure, aligns security goals with business objectives, assesses security business goals directly, and reduces regulatory compliance exposure (DE.AE-1 through DE.AE-5).

DE.CM: Security Continuous Monitoring. NIST defines the Security Continuous Monitoring category's goal as "the information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures."

Subcategories include ongoing monitoring of networks (DE.CM1), physical environments (DE.CM-2), personnel activities (DE.CM-3), and external service provider activities (DE.CM-6) to detect potential cybersecurity events. They seek to detect malicious code, also known as malware (DE.CM-4) and unauthorized mobile code (DE.CM-5). They also include Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7) and vulnerability scanning (DE.CM-8).

How Cisco solutions map to the Security Continuous Monitoring category:

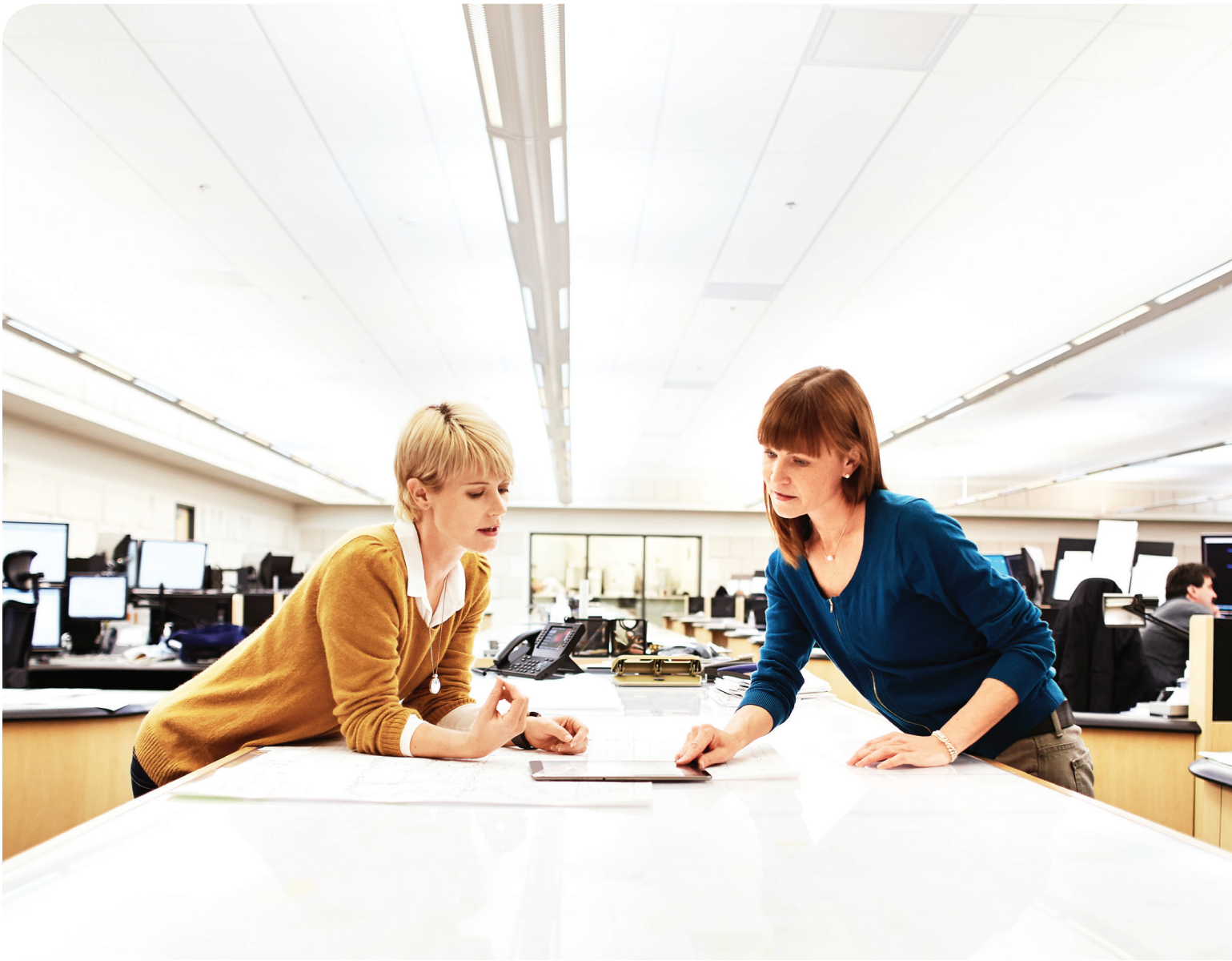
- Cisco Firepower monitors networks and personnel activities to detect potential cybersecurity events (DE.CM-1 and DE.CM-3). It offers insight into software applications actively communicating across your networks to help identify potentially unauthorized mobile code (DE.CM-5).
- Cisco Advanced Malware Protection (AMP) is the premier solution for malicious code detection on both networks and endpoints, including mobile devices (DE.CM-4 and DE.CM-5)
- Cisco AMP Threat Grid provides advanced malware analysis and threat intelligence, and identifies attacks with context-driven security analytics. It blocks attacks with prepackaged and custom threat feeds. Finally, it creates advanced indicators to respond rapidly and efficiently. (DE.CM-4 and DE.CM-5)
- Cisco Email and Web Security helps detect and deter cyber events that occur through the email and web attack vectors, including advanced malware that arrives through email attachments, through rogue websites, or through malvertising on legitimate sites (DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-6, and DE.CM-7).
- Cisco Stealthwatch continually analyzes network traffic for signs of unusual or suspicious activity, insider threat activity, the effects of spreading malware or propagation of malicious mobile core, and more (DE.CM-1, DE.CM-4, and DE.CM-7).
- Cisco Connected Safety and Security includes IP cameras and video surveillance software to continuously monitor physical environments, particularly Cisco Video Analytics that can classify objects, detect tampering, trigger alerts, and count people and vehicles to help identify physical events that could affect cybersecurity. (DE.CM-2). For more information on Cisco Video Analytics, please visit http://www.cisco.com/c/en/us/products/physical-security/video-analytics/index.html.
- Cisco Integration Services' Security Optimization Service (SOS) assesses, develops, and optimizes your security infrastructure on an ongoing basis to help you realize the goal of security continuous monitoring (DE.CM-1 through DE.CM-8).
- Cisco Cloudlock continuously monitors cloud environments to secure sensitive information and continuously detects compromised accounts and malicious insiders with User and Entity Behavior Analytics.
- Cisco Umbrella continuously monitors for and blocks attempted connections to malicious destinations before a connection is ever established.
- Duo's contextual access controls continuously monitor user activities and alers when access attempts seem abnormal.
- DE(CM): Anyconnect – AC personal activity monitored through IPFIX

DE.DP: Detection Processes. NIST defines the Detection Processes category's goal as "detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events." This category requires people and process controls, not technical controls.

Subcategories include well-defined roles and responsibilities for detection (DE.DP-1), and detection activity compliance with applicable requirements (DE.DP-2). They ensure that detection processes are tested (DE.DP-3), that detection information is communicated to appropriate parties (DE.DP-4), and that detection processes are continuously improved (DE.DP-5).

How Cisco solutions map to the Detection Processes category:

- Cisco Advisory Services Security and Risk Management services offer assessments, planning and guidance that deliver a holistic view of IT risks to be included in roles and responsibilities definition (DE.DP-1), detection process establishment (DE.DP-2), and detection process testing and evaluation (DE.DP-3), as well as continuous process improvement (DE.DP-5). It helps you ensure that your detection data is communicated to the right people at the right time (DE.DP-4).



Cisco Solutions for the Respond (RS) Function

Identify | Protect | Detect | **Respond** | Recover

The Respond function is a bit like an insurance policy: No one ever wants to use it, but you have to have it for when disaster strikes. And in today's world, the likelihood of a cyberattack affecting your organization is extremely high. You might already have been breached, but simply haven't discovered it yet. Therefore, the Respond helps organizations develop and implement the appropriate activities to take action regarding a detected cybersecurity event. We at Cisco have the capabilities and guidance you need to respond effectively to detected incidents.

RS.RP: Response Planning. NIST defines the Response Planning category's goal as "response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events." This category requires people and process controls, not technical controls.

Recall that the response plan itself was implemented, managed, and tested in the Protect function through its Information Protection Processes and Procedures (PR.IP) category. Here in the Respond function is where the response plan is actually used.

Therefore, Response Planning's sole subcategory ensures that the response plan is executed during or after an event (RS.RP-1).

How Cisco solutions map to the Response Planning category:

- Cisco Advisory Services' Incident Response (IR) service uses the latest intelligence and best practices to help build response plans and processes that engage all layers of defense. It provides a comprehensive range of readiness and response capabilities to help organizations prepare, manage, and recover from incidents quickly and effectively (RS.SP-1).

RS.CO: Communications. NIST defines the Communications category's goal as "response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies." This category requires people and process controls, not technical controls.

Subcategories ensure that personnel know their roles and plans when an event occurs (RS.CO-1), that events are reported appropriately (RS.CO-2), that information is shared according to the response plans (RS.CO-3), stakeholder coordination occurs according to the response plan (RS.CO-4), and that information is voluntarily shared externally to promote broader cybersecurity awareness (RS.CO-5).

How Cisco solutions map to the Communications category:

- Cisco Advisory Services' Incident Response (IR) service not only helps with response planning, but also with incident response roles and responsibilities definition (RS.CO-1), reporting processes (RS.CO-2), information sharing communication and coordination (RS.CO-3 and RS.CO-4). It can advise on when and how to share information externally for broader cybersecurity awareness (RS.CO-5).

RS.AN: Analysis. NIST defines the Analysis category's goal as "analysis is conducted to ensure adequate response and support recovery activities."

Subcategories include the investigation of detection systems' alerts (RS.AN-1), understanding of the incident's impact (RS.AN-2), and incident categorization commensurate with response plans (RS.AN-4). It also includes forensics analysis (RS.AN-3) during incident handling for audit reduction and reporting. Network flow (NetFlow) records play a critical role in incident understand and forensics analysis because they show what systems communicated with each other, when, and how much data was transmitted.

How Cisco solutions map to the Analysis category:

- Cisco Firepower provides indicators of compromise, impact assessment, and recommended rules capabilities in order to help analyze the potential effects of a cyber-incident (RS.AN-1 and (RS.AN-2). It integrates with log management and SIEM solutions to support forensics analysis across multiple technologies (RS.AN-3)
- Cisco AMP provides file- and network-trajectory capabilities to help analyze the effects and propagation of advanced malware for fast response (RS.AN-1). It shows which systems were affected, and how deep the malware went into each system to understand the malware's impact (RS.AN-2), to categorize the incident according to the response plan (RS.AN-3), and to perform the necessary forensics analysis to support response and recovery activities (RS.AN-4).
- Cisco Email and Web Security helps understand the attack vectors and impact for email or web-borne threats that become actual cyber-incidents (RS.AN-2).
- Cisco Stealthwatch plays a key role in analyzing NetFlow records for forensics analysis during and after a cyber-event (RS.AN-3). It shows traffic patterns, which systems communicated and when, and how much data passed among them – yielding critical clues for both understanding the incident's impact (RS.AN-2) and enacting the appropriate response and recovery plans (RS.AN-4).
- Cisco Cloudlock helps understand the attack vectors and impact for attacks that exploit software-as-a-service technologies like Box, Salesforce, Office365, and others (RS.AN-2).
- Cisco Advisory Services' Incident Response service provides the people, process, and technology necessary to help you investigate alerts (RS.AN-1), understand the impacts of a cyber-incident (RS.AN-1), and to act according to defined response plans (RS.AN-1).
- Cisco Umbrella Investigate provides threat intelligence for a complete view of the relationships and evolution of domains, IPs, autonomous systems (ASNs), and file hashes the security context needed to uncover and predict threats.

RS.MI: Mitigation. NIST defines the Mitigation category's goal as "activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident."

Subcategories include incident containment (RS.MI-1) and incident mitigation (RS.MI-2), as well as action taken on newly identified vulnerabilities whether they are actually mitigated or documented as accepted risks (RS.MI-3).

How Cisco solutions map to the Mitigation category:

- Cisco Firepower provides recommended rules based on actual network traffic to help mitigate threats and incidents in the future (RS.MI-2). It correlates network activity with vulnerability data to ensure that rule configuration is optimized to mitigate new threats, and to support the documentation of acceptable risks (RS.MI-3).
- Cisco AMP can quarantine malicious code to prevent its propagation and protect other systems from being affected (RS.MI-1). It provides the capabilities necessary to scope, contain, and remediate incidents that are so often tied to today's advanced malware (RS.MI-2).
- Cisco Email and Web Security can help contain incidents related to email or web security threats, including the containment of advanced malware that propagates through those attack vectors (RS.MI-1)
- Cisco Umbrella can prevent systems from contacting malicious sites by ensuring that DNS requests are valid and direct the requester to only appropriate hosts. This helps support incident mitigation efforts, as well as to contain command-and-control traffic that is initiated by breached systems (RS.MI-1).
- Cisco ISE helps contain security incidents by ensuring that only authorized devices with appropriate configurations are connected to the network (RS.MI-1). It works with Cisco TrustSec to change the access policies of individuals or systems during an incident to mitigate and contain the breach (RS-MI-2)
- Cisco TrustSec, working with Cisco ISE, dynamically enforces access policy at the network layer during a cyber-incident to limit its scope and mitigate its effects (RS.MI-1 and RS.MI-2)
- Cisco Cloudlock provides key insight into traffic bound to and from software-as-a-service applications to support response decisions during an incident (RS.MI-2)
- Cisco Advisory Services' Incident Response services provides a comprehensive range of readiness and response capabilities to help organizations prepare, mitigate, and recover from incidents quickly and effectively (RS.MI-1 through RS.MI-3).

RS.IM: Improvements. NIST defines the Improvements category's goal as "Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities." This category requires people and process controls, not technical controls.

Subcategories ensure that response plans incorporate lessons learned (RS.IM-1) and that response strategies are updated (RS.IM-2).

How Cisco solutions map to the Improvements category:

- Cisco Advisory Services' Incident Response service provides a comprehensive range of readiness and response capabilities to help organizations prepare, manage, recover, and learn from incidents quickly and effectively (RS.IM-1). It incorporates lessons learned not only from your own cyber-incidents, but also from the experience and best practices that we've learned by working with many customers – so that you can continually optimize and update your response strategies (RS.IM-2).

Cisco Solutions for the Recover (RC) Function

Identify | Protect | Detect | Respond | Recover

The Recover function maintains plans for resilience and restores any capabilities or services that were impaired due to a cybersecurity event. It supports timely recovery to normal operations to reduce the impact from a cybersecurity event, and helps you build lessons learned back into your cybersecurity operations. As you might expect, the Recover function is focused on people and process controls and not technical controls. The Recover function is just as important as the other four, but it can be easily overlooked.

RC.RP: Recovery Planning. NIST defines the Recovery Planning category's goal as "recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events." This category requires people and process controls, not technical controls.

Recall that the recovery plan itself was implemented, managed, and tested in the Protect function through its Information Protection Processes and Procedures (PR.IP) category. Here in the Recover function is where the recovery plan is actually used.

Therefore, its sole subcategory is recovery plan execution during or after an event (RC.RP-1).

How Cisco solutions map to the Recovery Planning category:

- Cisco Advisory Services' Incident Response (IR) services provide a comprehensive range of readiness and response capabilities to help organizations prepare, manage, and recover from incidents quickly and effectively, so that recovery plans can be developed and executed when an event occurs (RC.RP-1).

RC.IM: Improvements. NIST defines the Improvement category's goal as "recovery planning and processes are improved by incorporating lessons learned into future activities." This category requires people and process controls, not technical controls.

Subcategories include the incorporation of lessons learned into recovery plans (RC.IM-1) and ongoing updates of recovery strategies (RC.IM-2).

How Cisco solutions map to the Improvements category:

- Cisco Advisory Services' Incident Response (IR) services, as with the recovery planning category, can help ensure that lessons learned and ongoing improvements are incorporated into planning activities for continuous improvement (RC.IM-1). It incorporates lessons learned not only from your own recovery planning, but also from the experience and best practices that we've learned by working with many customers – so that you can continually optimize and update your recovery strategies (RC.IM-2).

Let us help you adopt the NIST Cybersecurity Framework.

For more information on Cisco Security, please visit www.cisco.com/go/security.

RC.CO: Communications. NIST defines the Communications category's goal as "restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams (CSIRTs), and vendors." This category requires people and process controls, not technical controls.

Subcategories include public relations management (RC.CO-1), post-incident reputation repair (RC.CO-2), and internal communication with stakeholders and executive management about recovery activities (RC.CO-3).

How Cisco solutions map to the Communications category:

- Cisco Advisory Services' Incident Response (IR) services can help ensure that your incident response communication plans are developed and executed effectively including public relations management (RC.CO-1), reputation repair (RC.CO-2), and internal communications (RC.CO-3).

Conclusion

Cisco provides one of the industry's most comprehensive advanced threat protection portfolios of cybersecurity products and solutions. Our approach reduces complexity, while providing superior visibility, continuous control, and advanced threat protection across the extended network. Our mission is truly effective security, which is exactly in line with the purpose of the NIST Cybersecurity Framework.

In this paper, we've shown how Cisco's capabilities align directly with the Framework. We discussed the motivation behind each discrete Framework component, and then explained exactly how Cisco products and services help you accomplish each specific goal. More importantly, we'll help you pull all of the components together to establish your continuous security life cycle program. With Cisco, you can adopt the Framework, and bolster cyber readiness and management efficiency and effectively.