The NIST Cybersecurity Framework (CSF): Mapping Ivanti's Solutions to CSF Controls

ivanti.com

The most common techniques used by cybercriminals have remained constant over the past several years, with phishing and ransomware continuing to occupy two of the top three spots every year. These attacks continue to evolve and now include the use of:

- Machine learning artificial intelligence (AI)
- Automation
- Chaining exploits against known and zero-day vulnerabilities
- Zero-click exploit kits developed by the NSO Group
- Fileless malware
- The "cybercrime-as-a-service" business model

These evolutions help cybercriminals stay one step ahead of their targets and defeat most cyberdefenses that an organization stands up.

The Everywhere Workplace shift accelerated by the global pandemic extended the cyberrisk and threat landscape, especially surrounding data privacy and its protection.

To combat today's threats, Ivanti recommends a defense-in-depth cybersecurity strategy that employs one or more of the three cybersecurity frameworks:

- NIST Cybersecurity Framework (CSF)
- Center for Internet Security (CIS) Critical Security Controls version 8
- Zero Trust Security Architecture

Simply, the solution is to place as many impediments as possible in front of cybercriminals, thereby increasing the chance that they will give up and seek out other targets which lack the proper security controls.

In this white paper, we seek to better explain the NIST Cybersecurity Framework, as well as show how Ivanti's own products correspond with the recommendations within.

What is the NIST Cybersecurity Framework?

The National Institute of Standards and Technology (NIST) was founded in 1901 and is part of the U.S. Department of Commerce. NIST's Information Technology Laboratory has developed several cybersecurity frameworks, but we will focus on the three most common:

- The NIST Cybersecurity Framework (CSF) – the gold-standard of all cybersecurity frameworks
- NIST Special Publication 800-53
- NIST Special Publication 800-171

Released in February 2014, the NIST Cybersecurity Framework version 1.0 was developed in response to Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity.

This framework was initially intended to be used to protect critical infrastructure like electrical power generation and distributions plants, nuclear facilities, transportation and communications infrastructures, water treatment, public health, food, and agriculture, etc.

With input and collaboration from private sector industries, version 1.1 was released in April 2018. This version not only provides standards and guidelines for computer and information technology for the public sector, but also is widely used in the private sector; its principles can be implemented by any organization that seeks to start or improve their cybersecurity program.

Most lately in September 2021, NIST released Draft NISTIR 8374, which provides basic preventive guidelines for organizations to protect themselves from ransomware attacks within context of the broader NIST Cybersecurity Framework.

The framework presents cybersecurity best practices in an organized manner for identifying risks and assets that require protection. It then lists the security controls that an organization must follow to protect these assets, including detecting risks, responding to threats and recovering assets in the event of a cybersecurity incident. Each function contains a category underneath and, digging deeper, more subcategories as guidelines to follow and implement.

NIST Cybersecurity Framework Function Details

The Cybersecurity Framework Core lists the functions that follow the common structure of cyberdefense strategies:

NIST Cybersecurity Framework 1.1

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assesment	Information Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

Identity

Identifying and maintaining a comprehensive inventory of assets and solutions are the first steps of an effective cybersecurity program. This function requires an accurate inventory of enterprise software and hardware systems that access corporate data.

Enterprise Software Inventory	Hardware System Inventory
Software components	Networks
Libraries	Servers
Operating systems and versions	Desktops
Applications	Mobile Devices
Software Bill of Materials (SBOM)	

Then, the organization must:

- Identify threats, vulnerabilities and weaknesses within and between all systems.
- Identify and document the data collected, used and stored, as well as network flows.
- Create and maintain a comprehensive risk management strategy that includes establishing cybersecurity policies, access controls, and roles and responsibilities for all employees.

Protect

Protect involves creating internal processes and implementing technology controls to ensure the adequate protection of sensitive data. These controls include but are not limited to:

- Enforcing strong multi-factor authentication (MFA).
- Employing protective technologies such as encrypting data at rest, in use and in transit.
- Performing regular data backups, including offline storage.
- Enabling policy enforcement points such as next-generation firewalls and cloud access security brokers (CASB).
- Deploying and regularly updating endpoint security products such as intelligent patch management, threat defense for mobile devices, and antivirus for servers, laptops and desktops.
- Leveraging robust contextual conditional access controls that employ robust authentication and authorization methods for not only the trusted user, but also the trusted device, applications, network source (location), and time.
- Providing employees with comprehensive, updated security awareness training.

Detect

Detecting cybersecurity incidents that can potentially lead to data breaches, ransomware, business disruption and advanced persistent threats (APT) is critical to any organization. The Detect function involves implementing and developing control processes and procedures that are regularly tested to ensure your organization can detect risks and threats when they occur.

This process includes leveraging automation and machine intelligence for:

- Network instrumentation
- Monitoring system logs
- Data flows between endpoints
- Storage (on-premises or cloud)
- Databases
- Networks

Part of a comprehensive threat detection strategy includes establishing communications channels and operational protocols with cybersecurity teams, partners and governing bodies.

Respond

The Respond function focuses on your organization's preparedness to respond to risk and threat incidents rapidly and effectively. This process includes both documentation and regular testing of response processes and procedures, along with coordination with both internal and external stakeholders.

Automated response controls can also be implemented with technological innovations including:

- Outbound traffic detection.
- Network segmentation.
- Software defined perimeter.
- Vulnerability and risk-based patch management.
- Dynamic attribute-based access control policies that can change authorization and security policies based on environmental, network, and Internet conditions and risk status.

Recover

The Recover function involves business continuity preparation and planning, recovery and resiliency testing before an incident, as well as root cause analysis with documentation updates with lessons learned after an incident.

This function also includes communications with internal and external stakeholders, along with managing public relations and company reputation.

A significant technical component of the recover best practices is the successful integration of the following processes, all conforming to the appropriate level of Information Technology Infrastructure Library (ITIL) processes:

- Service management
- Configuration and change management
- Release automation
- Testing
- Validation

Ultimately, Ivanti always recommends a multilayered defense-in-depth cybersecurity strategy to combat today's threats. The more impediments an organization places in front of cybercriminals, the better the chance that they will give up and seek out other targets which lack the proper security controls.

Function	Category	Ivanti Product Mapping
Identify	**Asset Management** 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 organizational objectives and the organization's risk strategy.	**Ivanti Neurons for Discovery** provides accurate real-time visibility of all your IT assets, including hardware systems, software, data, services, personnel inventory and their management using active and passive scanning to identify and track assets. (ID.AM-1, ID.AM-2, and ID.AM-5) **Ivanti Neurons for Spend Intelligence** delivers insights into your software landscape and application asset inventory with instant visibility into software usage, software configuration drift, and software end of life. (ID-AM-2) **Ivanti IT Asset Management (ITAM)** maintains accurate inventory and actionable insights of hardware, server, client, virtual, cloud or software assets throughout their entire lifecycle. (ID.AM-1 and ID.AM-2) For on-premises solutions, **Ivanti Endpoint Manager (EPM)** also provides accurate real-time visibility of your IT assets, including hardware systems, software, data, services, personnel inventory and their management using active and passive scanning to identify and track assets. (ID.AM-1, ID.AM-2, and ID.AM-5) Furthermore, **Ivanti Neurons for Unified Endpoint Management (UEM)** and **Ivanti Endpoint Manager Mobile (EPMM)** manage an inventory of enrolled mobile devices, desktop clients, and all installed software applications. It also ensures mobile devices and clients are always under management and enforces compliance with your company's security and privacy policies. These managed devices and their content are classified by criticality and business value. (ID.AM-1 and ID.AM-2) Additional Ivanti products: **Neurons for Secure Access (NSA)** (ID.AM-1) **Ivanti Network Access Control (NAC)** (ID.AM-1) **Ivanti Security Controls (ISEC)** (ID.AM-2) **Ivanti Patch for MEM (Microsoft Endpoint Manager)** (ID.AM-2) **Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** (ID.AM-1 and ID.AM-5) **Ivanti Neurons for App Security Orchestration & Correlation (ASOC)** (ID.AM-2 and ID.AM-5)
	Business Environment 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.	
	Governance 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 cybersecurity risk.	

Function	Category	Ivanti Product Mapping
Identify	**Risk Assessment** The organization understands the cybersecurity risk to organizational operations – including mission, functions, image or reputation –organizational assets and individuals.	**Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** delivers automated insights into your risk exposure by providing remediation prioritization based on adversarial risk. The solution identifies and documents asset weaknesses and vulnerabilities. Threat and vulnerability information are received from information sharing forums and sources. Potential business impacts and trends are also identified, whereby threats, vulnerabilities, trends and impacts are used to determine risk and appropriate response are identified and prioritized for automated patching. (ID.RA-1, ID.RA-2, ID.RA-4, ID-RA-5, and ID-RA-6.) **Ivanti Neurons for Patch Management** scans endpoints for weaknesses and vulnerabilities by identifying missing patches in every endpoint, with the ability to filter and import Common Vulnerabilities and Exposures (CVE) data for use with an intelligent patching strategy. (ID.RA-1) **Ivanti Neurons for GRC (Governance Risk and Compliance)** identifies and documents internal and external threats, and potential business impacts and likelihoods are identified. (ID.RA-3 and ID.RA-4)
	Risk Management Strategy The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.	
	Supply Chain Risk Management The organization's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** identifies cyber risks for real world exploits in your IT and cloud infrastructure, including applications and web services. It also enables you to prioritize the vulnerabilities and weaknesses that pose the most risk using our patented Vulnerability Risk Rating (VRR) engine. VRR represents the risk posed by a given vulnerability, provided as a numerical score between 0 and 10. The higher the risk, the higher the VRR. Cyber supply chain risk management processes are identified, established, assessed, managed and agreed to by organizational stakeholders. (ID.SC-1) **Ivanti Neurons for IT Asset Management (ITAM)** consolidates your IT asset data and lets you identify, prioritize, and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process. It can track, configure, optimize and strategically manage your internal supply chain assets through their full lifecycle. (ID.SC-2)

Function	Category	Ivanti Product Mapping
Protect	**Identity Management & Access Control** Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**Ivanti Neurons for Unified Endpoint Management (UEM) with Ivanti Access** integrates with your existing Identity Provider, and can enforce conditional access based on trusted user, device, application, network and context rules, while Ivanti **Zero Sign-On** manages the issuance, verification, revocation and auditing of identities and credentials for authorized devices, users and processes. (PR.AC-1) **Ivanti Neurons for Zero Trust Access, Ivanti Connect Secure and Ivanti Tunnel** manage and provide secure remote access to on-premises, data center and cloud (SaaS-based) resources. Users, devices, applications, networks, time and location are authenticated implementing multi-factor authentication (MFA) using the stronger and adaptive factors. (PR.AC-3 and PR.AC-7) Also, **Ivanti Network Access Control (NAC)** can enforce micro segmentation ensuring network integrity for not only north-south but also east-west network data traffic. (PR.AC-5 and PR.AC-7) **Ivanti Application Control with Privilege Management** manages access permissions, while incorporating the principles of least privileges and separation of duties. It controls access to protected assets with Role-Based Access Control (RBAC). (PR.AC-4)
	Awareness & Training The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	Data Security Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity and availability of information.	**Ivanti Neurons for Unified Endpoint Management (UEM)** can check, enable and enforce file-based encryption on iOS, iPadOS and Android mobile devices, as well as full-disk encryption using BitLocker for Windows and FileVault for macOS clients to protect data-at-rest. Also, WPA3-Personal (Secure Authentication of Equals) and Enterprise for wireless networks can be enabled. (PR.DS-1, PR.DS-2, PR.DS-4, and PR-DS-6) For on-premises deployments, **Ivanti Endpoint Manager Mobile (EPMM)** can also check, enable, and enforce file-based encryption on iOS, iPadOS, and Android mobile devices, as well as full-disk encryption using BitLocker for Windows and FileVault for macOS clients to protect data-at-rest. Also, WPA3-Personal (Secure Authentication of Equals) and Enterprise for wireless networks can be enabled. (PR.DS-1, PR.DS-2, PR.DS-4, and PR-DS-6) **Ivanti Neurons for Zero Trust Access and Ivanti Connect Secure** implements the stronger cryptographic cipher suites with Transport Layer Security version 1.3 to protect data-in-transit, along with enforcing user behavior, analytics and risk; multi-factor and adaptive authentication (MFA) and authorization; device posture; trusted application; and access context (location and time) controls. The integration with Lookout Cloud Access Security Broker (CASB) and SWG (Secure Web Gateway) solutions, specifically the API controls deployment helps with insider threats and data leakage. (PR.DS-2 and PR.DS-5)

Function	Category	Ivanti Product Mapping
Protect		**Ivanti Neurons for ITAM (IT Asset Management)** and **Ivanti Neurons for ITSM (IT Service Management)** formally manage digital assets throughout its lifecycle from removal, transfers and disposition and track system with sensitive data. (PR.DS-3) **Ivanti Neurons for Unified Endpoint Management (UEM)**, **Ivanti Neurons for Healing** and **Ivanti Neurons Workspace with Digital Experience Score** (DEX Score) ensures and maintains that adequate capacity is available to managed systems. (PR.DS-4) **Ivanti RBVM for Applications** implements integrity checking mechanisms used to verify software, firmware and information integrity. (PR.DS-6) Also, **Ivanti Neurons for Zero Trust Access** arbitrates micro segmentation of the customer's development and testing environments separate from the production environment by enforcing user and application least privileges. (PR-DS-7)
	Information Protection Processes & Procedures 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.	**Ivanti Endpoint Security (EPS) for Endpoint Manager (EPM), Neurons for Unified Endpoint Management (UEM)** and **Ivanti Neurons for Healing** incorporates baseline configurations along with configuration changes to create and maintain information technology and industrial control systems. (PR.IP-1) Also, **Ivanti Neurons for ITSM (IT Service Management)** facilitates documentation and ticketing of configuration change control processes. (PR. IP-3) **Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** provides the tools to manage and implement a vulnerability response plan. (IP-12)
	Maintenance Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**Ivanti IT Service Management (ITSM)** and **Ivanti Neurons for Healing** deliver approved and controlled tools to service and maintain organizational assets and are performed and logged in a timely manner. (PR. MA-1) Additionally, **Ivanti Endpoint Manager (EPM), Ivanti Neurons Workspace** and **Ivanti Neurons for Healing** supplies the tools for remote maintenance of organizational assets that is approved, logged and performed in a timely manner to prevent unauthorized access. (PR.MA-2)
	Protective Technology Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.	**Endpoint Security (EPS) for Manager (EPM)** and **Ivanti Application Control and Ivanti Neurons for Unified Endpoint Management (UEM)** protects removeable media and ensures that its use is restricted according to the company's security and privacy policies. (PR.PT-2) Also, **Endpoint Security (EPS) for Endpoint Manager (EPM), Ivanti User Workspace Manager, Ivanti Security Controls, Ivanti Neurons for Zero Trust Access, Ivanti Connect Secure** and **Ivanti Application Control** with privilege management incorporates the principle of least functionality by configuring systems to provide only essential capabilities for end users. (PR.PT-3)

Function	Category	Ivanti Product Mapping
Protect		**Ivanti Network Access Control (NAC), Ivanti Connect Secure (ICS), Ivanti Virtual Application Delivery Controller (vADC), Endpoint Security (EPS) for Endpoint Manager (EPM)** and **Neurons for Unified Endpoint Management (UEM)** can protect communications and control networks. (PR.PT-4) And **Ivanti Virtual Application Delivery Controller (vADC)** provides network failsafe mechanisms for load balancing and hot swapping to achieve resilience requirements in normal and adverse situations. (PR. PT-5)
Detect	**Anomalies & Events** Anomalous activity is detected, and the potential impact of events is understood.	**Ivanti Neurons for Discovery with Service Mapping** provides visibility into your cloud or data-center network topology, enabling you to view infrastructure relationships, app dependencies, communication flows and service mappings related to both ITSM and ITOM processes. The solution establishes and manages a baseline of network operations and expected data flows for users and systems. (DE.AE-1)
	Security Continuous Monitoring The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**Ivanti Neurons for Zero Trust Access** uses the web to create a secure connection from the device to an application through gateways while constantly verifying the user, their device, applications, time of day and source geolocation based on granular constraints to detect and record authorized access events. (DE.CM-3) **Ivanti Mobile Threat Defense (MTD)** defends and remediates threats targeting mobile devices. It can monitor and detect end user activity for potential cybersecurity events and unauthorized mobile code and exploit kits. (DE.CM-3, and DE.CM-5) For on-premises deployments, **Ivanti Endpoint Manager (EPM)** can be integrated with SIEM solutions to monitor unauthorized personnel, connections, devices and software. (DE.CM-7)
	Detection Processes Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
Respond	**Response Planning** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity incidents.	Ivanti IT Service Management (ITSM) with the Security Operations Content keeps track of response plans and approvals executed during or after an event. (RS.RP-1)
	Communications Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	
	Analysis Analysis is conducted to ensure effective response and support recovery activities.	

Function	Category	Ivanti Product Mapping
Respond	**Mitigation** Activities are performed to prevent expansion of an event, mitigate its effects and resolve the incident.	**Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)** are adaptive risk-based vulnerability management solutions. Organizations need only minutes to know and manage the actions that will shut down exposure across their attack surface. The administrator will know what actions to take in seconds and accelerate remediation activities for the most important vulnerability exposure points across your attack surface, infrastructure, applications and development frameworks. Its capabilities include containing and mitigating security incidents and identifying new vulnerabilities or documented as accepted risks. (RS.MI-1, RS.MI-2, and RS.MI-3) And for on-premises deployments, **Ivanti Endpoint Security (EPS) for Endpoint Manager (EPM)** with **Application Control** is capable of isolating infected devices and containing and mitigating cybersecurity incidents. It is also capable of identifying new vulnerabilities or can be documented as accepted risks. (RS.MI-1, RS.MI-2, and RS.MI-3). **Ivanti Neurons for Secure Access, Ivanti Neurons for Zero Trust Access (NZTA), Ivanti Connect Secure (ICS)** and **Ivanti Network Access Control (NAC) Profiler** – along with **Ivanti Sentry** and **Ivanti Access** integrated with **Ivanti Mobile Threat Defense** – all have the capability to contain cybersecurity incidents. (RS.MI-1)
	Improvements Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
Recover	**Recovery Planning** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	Improvements Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Communications Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs and vendors).	

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com