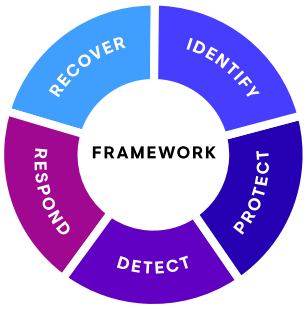
SOLUTION BRIEF

Secureworks

NIST Cybersecurity Compliance

How Secureworks Aligns with NIST-CSF and NIST SP 800-171



NIST-CSF Functional Area	Secureworks Capabilities
IDENTIFY	✓
PROTECT	✓
DETECT	✓
RESPOND	✓
RECOVER	✓

What is the NIST Cybersecurity Framework? (NIST-CSF)

In February 2013, Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, mandated NIST work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. NIST's cyber standards-setting role was further reinforced by the Cybersecurity Enhancement Act of 2014.

The voluntary NIST-CSF Framework was created via an industry-government collaboration and consists of cybersecurity standards, guidelines and practices to promote the protection of critical infrastructure. The Framework provides a flexible, repeatable and cost-effective approach that helps owners and operators of critical infrastructure to identify and prioritize their cyber-risk.

What is NIST Special Publication 800-171?

NIST SP 800-171 combines requirements of FIPS 200 and NIST SP 800-53 into 110 discrete security controls across 14 administrative and technical categories. Specific compliance requirements are enumerated within each category.

How does Secureworks further NIST cybersecurity compliance?

Compliance is a journey, not a discrete one-time event. Achieving regulatory compliance requires ongoing attention and continuous improvement. Secureworks helps organizations advance their compliance programs with an extensive portfolio of cybersecurity products and services:

- Taegis™ XDR – Extended Detection and Response
- Taegis™ ManagedXDR – Managed Detection and Response
- Taegis™ ManagedXDR Elite -- Continuous Managed Threat Hunting
- Taegis™ NGAV Add-On for XDR and ManagedXDR
- Taegis™ VDR – Vulnerability Detection and Response
- Security Advisory Services
- Governance Risk and Compliance Services
- Adversarial Security Testing Services

The Challenge

Organizations of all sizes who wish to conform to NIST cybersecurity regulations need a trusted partner to help them navigate the complexities of the various regulations and interpretations surrounding the requirements and compliance aspects of their security programs.

The Solution

Secureworks helps organizations advance their compliance programs through a comprehensive portfolio of cybersecurity products and services that help businesses move forward from any starting point on the cybersecurity maturity continuum.

Why Secureworks

The Secureworks portfolio of products, services and expertise combine to support you on your journey to regulatory compliance with the NIST guidelines. Secureworks' capabilities span the complete range of NIST-CSF general functional areas and NIST SP 800-171 specific information security categories.

We help you navigate the complexities of new data security and privacy risk in our digitally connected world, enabling your unique business objectives and needs, strengthening your security posture, and implementing effective data breach, remediation and recovery capabilities.

#	NIST SP 800-171 Category	Secureworks Capabilities
3.1	Access Control	✓
3.2	Awareness and Training	✓
3.3	Audit and Accountability	✓
3.4	Configuration Management	✓
3.5	Identification and Authentication	✓
3.6	Incident Response	✓
3.7	Maintenance	✓
3.8	Media Protection	✓
3.9	Personnel Security	✓
3.10	Physical Protection	✓
3.11	Risk Assessment	✓
3.12	Security Assessment	✓
3.13	System and Communications Protection	✓
3.14	System and Information Integrity	✓

The Secureworks Approach

Secureworks has developed a four-step approach to help organizations identify gaps and r remediate deficiencies to meet NIST cybersecurity requirements:

- **Know Your Data:** Understand and identify the scope of NIST-CSF and NIST SP 800-171 data security requirements specific to your operation
- **Assess Current State:** Assess the current state and identify gaps in your current operations and practices
- **Build the Program**: Build the right people, process and control strategies to meet the NIST data security guidelines
- **Test, Operate and Manage:** Test, operate and manage in line with NIST data security requirements, and remove the workload from the security function, allowing security and privacy to become business enablers

Mapping Legend

Secureworks Services

✓ Services fully address the requirement area

Secureworks Products

● Product maps to the requirement

◐ Product helps address the requirement

○ Product has no impact on the requirement

NIST-CSF

- Voluntary Framework created by Presidential Executive Order 13636
- Consists of standards, guidelines and best practices to manage cybersecurity risk
- Framework guidance is customized by sectors and organizations to best suit their risks, situations, and needs

NIST-800-171

- Specifies protection of Controlled Unclassified Information (CUI) residing in non-federal systems
- Combines FIPS 200 and NIST SP 800-53
- Includes 110 security controls spanning 14 administrative and technical categories

Secureworks

3.1 Access Control

#	NIST-800-171 Requirement	Products	Services
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (incl. other systems)	◐	✓
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute	◐	✓
3.1.3	Control the flow of CUI in accordance w/ approved authorizations	◐	✓
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion	◐	✓
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts	◐	✓
3.1.6	Use non-privileged accounts or roles when accessing non-security functions	◐	✓
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions	◐	✓
3.1.8	Limit unsuccessful logon attempts	◐	✓
3.1.9	Provide privacy and security notices consistent with applicable CUI rules	○	✓
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity	◐	✓
3.1.11	Terminate automatically a user session after a defined condition	◐	✓
3.1.12	Monitor and control remote access sessions	●	✓
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions	●	✓
3.1.14	Route remote access via managed access control points	◐	✓
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information	◐	✓
3.1.16	Authorize wireless access prior to allowing such connections	○	✓
3.1.17	Protect wireless access using authentication and encryption	◐	✓
3.1.18	Control connection of mobile devices	◐	✓
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms	○	✓
3.1.20	Verify & control/limit connections to and use of external systems	◐	✓

Secureworks Value

- Taegis XDR monitors network traffic as it crosses internal boundaries or external perimeter, for threat detection. Log retention aid investigations and reporting
- Taegis VDR creates an inventory of external systems as part of discovery activities
- Security Advisory Services services help establish an asset inventory and define secure network architecture for protection, detection and response capabilities
- Network security devices like Secureworks iSensor™ and third-party network security tools implement network segregation and segmentation
- Via orchestration and automation, Taegis XDR, which monitors network security systems, is designed to implement network response actions

3.2 Awareness and Training

#	NIST-800-171 Requirement	Products	Services
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards & procedures related to the security of those systems	●	✓
3.2.2	Ensure that organizational personnel are adequately trained carry out their assigned information security-related duties and responsibilities	○	✓
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat	◐	✓

Secureworks Value

- Security Advisory Services evaluate and assess current security controls, policies and processes
- Incident Response Tabletop Exercises are designed to ensure security staff, privileged users, 3rd-party stakeholders and senior executives know their roles and responsibilities when dealing with a major cyber security incident

Secureworks®

3.3 Audit and Accountability

#	NIST-800-171 Requirement	Products	Services
3.3.1	Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity	●	✓
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions	●	✓
3.3.3	Review and update audited events	◐	✓
3.3.4	Alert in the event of an audit process failure	◐	✓
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity	●	✓
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting	●	✓
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records	◐	✓
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion	◐	✓
3.3.9	Limit management of audit functionality to a subset of privileged users	◐	✓

Secureworks Value

- Taegis XDR continuously monitors and logs network security, servers, IAM systems, endpoint solutions including antimalware and EDR, and cloud environments
- Taegis ManagedXDR has 24x7 analysts performing deeper analysis, triage and investigations of identified alerts for confirmation, escalation and response and containment actions
- Security Advisory Services evaluate and assess current security controls, policies and processes
- Adversarial Testing verifies the effectiveness of the existing controls and identifies missing controls

3.4 Configuration Management

#	NIST-800-171 Requirement	Products	Services
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles	●	✓
3.4.2	Establish and enforce security configuration settings for info technology products employed in organizational systems	◐	✓
3.4.3	Track, review, approve or disapprove, and audit changes to organizational systems	◐	✓
3.4.4	Analyze the security impact of changes prior to implementation	●	✓
3.4.5	Define, document, approve, enforce physical & logical access restrictions associated with changes to organizational systems	○	✓
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities	○	✓
3.4.7	Restrict, disable, and prevent the use of nonessential, functions, ports, protocols, or services	●	✓
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny- all, permit-by-exception (whitelisting) policy to allow execution of authorized software	●	✓
3.4.9	Control and monitor user-installed software	◐	✓

Secureworks Value

- Taegis XDR monitors network security solutions for threats and anomalies, and via orchestration and automation, implements network response actions
- Network security devices like Secureworks iSensor & 3rd-party network security tools implement network segregation / segmentation
- Taegis VDR creates an inventory of systems as part of discovery activities
- Security Advisory Services services define a robust security architecture for Operational Technology environments and establish an asset inventory
- Adversarial Testing verifies the effectiveness of the existing controls and identifies missing controls

Secureworks®

3.5 Identification and Authentication

#	NIST-800-171 Requirement	Products	Services
3.5.1	Identify system users, processes acting on behalf of users, and devices	●	✓
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems	◐	✓
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts	◐	✓
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts	◐	✓
3.5.5	Prevent reuse of identifiers for a defined period	◐	✓
3.5.6	Disable identifiers after a defined period of inactivity	◐	✓
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created	○	✓
3.5.8	Prohibit password reuse for a specified number of generations	○	✓
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password	○	✓
3.5.10	Store and transmit only cryptographically protected passwords	○	✓
3.5.11	Obscure feedback of authentication information	○	✓

Secureworks Value

- Security Advisory Services evaluate and assess current security controls, policies and processes
- Adversarial Testing verifies the effectiveness of the existing controls and identifies missing controls

3.6 Incident Response

#	NIST-800-171 Requirement	Products	Services
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities	●	✓
3.6.2	Track, document, and report incidents to appropriate organizational officials and/or authorities	●	✓
3.6.3	Test the organizational incident response capability	●	✓

Secureworks Value

- Taegis XDR is built for collaborative investigation
- Taegis ManagedXDR has a standard Analyst workflow and a Threat Engagement Manager who reviews the roles and responsibilities with the customer team
- Secureworks Incident Management Retainer provides organizations with the support and expertise they need to prepare, respond and recover from a variety of incident types

3.7 Maintenance

#	NIST-800-171 Requirement	Products	Services
3.7.1	Perform maintenance on organizational systems	◐	✓
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance	◐	✓
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI	○	✓
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in org. systems	○	✓
3.7.5	Require multifactor auth. to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete	○	✓
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization	○	✓

Secureworks Value

- Taegis VDR detects and prioritizes vulnerabilities on systems needing maintenance with role-based access controls
- Comprehensive Security Advisory Services help inform the processes and procedures governing the maintenance of sensitive information systems

Secureworks®

3.8 Media Protection

#	NIST-800-171 Requirement	Products	Services
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital	○	✓
3.8.2	Limit access to CUI on system media to authorized users	○	✓
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse	○	✓
3.8.4	Mark media with necessary CUI markings & distribution limitations	○	✓
3.8.5	Control access to media containing CUI, maintain accountability for media during transport outside of controlled areas	○	✓
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards	○	✓
3.8.7	Control the use of removable media on system components	○	✓
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner	○	✓
3.8.9	Protect the confidentiality of backup CUI at storage locations	○	✓

Secureworks Value

- Security Controls Assessment informs the processes and procedures governing media protection
- Security Advisory Services evaluate and assess current security controls, policies and processes
- Adversarial Testing verifies the effectiveness of the existing controls and identifies missing controls

3.9 Personnel Security

#	NIST-800-171 Requirement	Products	Services
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI	○	✓
3.9.2	Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	○	✓

Secureworks Value

- Security Controls Assessment informs the processes and procedures governing personnel security

3.10 Physical Protection

#	NIST-800-171 Requirement	Products	Services
3.10.1	Limit physical access to organizational systems, equipment & respective operating environments to authorized individuals	○	✓
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems	◐	✓
3.10.3	Escort visitors and monitor visitor activity	○	✓
3.10.4	Maintain audit logs of physical access	◐	✓
3.10.5	Control and manage physical access devices	○	✓

Secureworks Value

- Security Controls Assessment informs the processes and procedures governing the physical protection of sensitive information systems

3.11 Risk Assessment

#	NIST-800-171 Requirement	Products	Services
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI	●	✓
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically & when new vulnerabilities affecting the system are identified	●	✓
3.11.3	Remediate vulnerabilities in accordance with assessments of risk	●	✓

Secureworks Value

- Taegis VDR continuously scans, identifies, assesses, prioritizes, alerts and reports on asset vulnerabilities
- Taegis ManagedXDR 24x7 analysts perform deeper analysis, triage and investigations of identified alerts for confirmation, escalation, response and containment actions

Secureworks®

3.12 Security Assessment

#	NIST-800-171 Requirement	Products	Services
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application	●	✓
3.12.2	Develop and implement plans of action designed to correct deficiencies & reduce or eliminate vulnerabilities in org. systems	●	✓
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls	●	✓
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems	●	✓

3.13 System and Communications Protection

#	NIST-800-171 Requirement	Products	Services
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at external boundaries and key internal boundaries of org. systems	●	✓
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems	○	✓
3.13.3	Separate user functionality from system management functionality	○	✓
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources	●	✓
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks	●	✓
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)	●	✓
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks. (i.e., split tunneling)	○	✓
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards	○	✓
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or a defined inactivity period	○	✓
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems	○	✓
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI	○	✓
3.13.12	Prohibit remote activation of collaborative computing devices & provide indication of devices in use to users present at the device	○	✓
3.13.13	Control and monitor the use of mobile code	○	✓
3.3.15	Protect the authenticity of communications sessions	◐	✓
3.13.16	Protect the confidentiality of CUI at rest	◐	✓

Secureworks Value

- Taegis ManagedXDR Threat Engagement Manager reviews detection activity for requirement compliance and drives continuous process improvement
- Security Controls Assessment informs the processes and procedures, and Adversarial Security Testing verifies the controls
- Secureworks Incident Management Retainer provides organizations with the support and expertise they need to prepare, respond and recover from a variety of incident types

Secureworks Value

- Network security devices like Secureworks iSensor & 3rd-party network security tools implement network segregation / segmentation
- Taegis XDR monitors network security solutions for threats and anomalies, and via orchestration and automation, can implement network response actions
- Security Advisory Services define a secure network architecture for protection, detection and response

3.14 System and Information Integrity

#	NIST-800-171 Requirement	Products	Services
3.14.1	Identify, report, and correct system flaws in a timely manner	●	✓
3.14.2	Provide protection from malicious code at appropriate locations within organizational systems	●	✓
3.14.3	Monitor system security alerts and advisories and take actions in response	●	✓
3.14.4	Update malicious code protection mechanisms when new releases are available	●	✓
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed	●	✓
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks	●	✓
3.14.7	Identify unauthorized use of organizational systems	●	✓

Getting Started with NIST Compliance

Security Controls Assessment

An experienced security expert assesses how current security controls align with the top security frameworks and compliance mandates to identify critical gaps and drive prioritized corrective actions.

- Key Objective: Assess and Map Existing Security Controls Against Regulatory Requirements and Industry Best Practice

Deliverables:

- An Executive Summary: Engagement overview, a summary of the findings and identification of high-level risk areas
- Detailed Findings and Recommendations for each control, prioritized in a matrix with severity ratings where controls are not fully implemented
- Optional presentation to key stakeholders

Security Maturity Assessment

Assess your current cybersecurity program maturity, define your target state and develop a customized plan of action with expert-led analysis and guidance based on an understanding of your unique business priorities, security expertise and knowledge of industry leading standards.

- Key Objective: Identify and prioritize areas of improvement across your security program to drive security maturity

Deliverables:

- Report: Executive summary, detailed methodology, findings, narratives and prioritized recommendations and opportunities for improvement
- Current and target profiles and scores for each aspect of the Security Maturity Assessment

The information contained within this document represents Secureworks' internal assessment and estimation of the NIST compliance framework mappings across Secureworks' commercial portfolio as of the publication date. Although Secureworks' products and services may assist in meeting certain compliance and regulatory use cases, Secureworks products and services are not designed for compliance and regulatory use. In addition, any written summaries or reports produced by Secureworks or generated by the Secureworks' products and services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

Sample Responses

- CTU™ threat intelligence is used throughout Secureworks product and service offerings
- SAS/GRC - Risk Assessment can help identify all of the critical risk areas along with their respective impact and likelihood within a client's environment

Take the First Step

Secureworks comprehensive portfolio of security services can help you start your NIST compliance journey today!

- Security Advisory Services
- Governance, Risk and Compliance Services
- Adversarial Security Testing Services

Explore Taegis

Secureworks Taegis offers a flexible, extensible platform for Extended Detection and Response and Vulnerability Detection and Response to help you meet your NIST compliance needs.

- Taegis XDR
- Taegis ManagedXDR
- Taegis ManagedXDR Elite
- Taegis NGAV Add-On
- Taegis VDR

About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.