Business white paper

Security-first, AI-powered networking for NIST compliance

Accelerating NIST compliance with
HPE Aruba Networking

Table of contents

NIST frameworks for cybersecurity and risk management

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, publishes recommended technology standards and guidelines—often referred to in groups as frameworks—that may be adopted by regulatory agencies and enterprises.

NIST frameworks form the foundation of a variety of U.S., international, and industry-specific cybersecurity and privacy mandates, making NIST compliance a requirement for some public and private organizations. NIST guidelines are incorporated in legislation like FedRAMP, the Federal Information Security Management Act (FISMA), and Health Insurance Portability and Accountability Act (HIPAA), as well as programs like Comply to Connect (C2C). NIST standards can also be mapped to requirements in ISO standards, as well as laws and regulations like the California Consumer Privacy Act (CCPA) and EU General Data Protection Regulation (GDPR). Even if they are not subject to specific regulations, many organizations tend to voluntarily adopt NIST frameworks as best practices[1].

Some of the most common NIST publications provide:

- **NIST Cybersecurity Framework (CSF)—**standards, guidelines, and practices that organizations can use to manage cybersecurity risk based on business drivers[2].
- **NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations—**guidelines for security and privacy controls for IT systems designed to protect operations, assets, and people from a variety of threats and risks[3].
- **NIST 800-207: Zero Trust Architecture—**definitions and general deployment models for cybersecurity strategies focused on users, assets, and resources, rather than static network perimeter defenses[4]. Note that, in May 2021, the US government issued an executive order directing United States federal agencies to comply with NIST SP 800-207 as a fundamental step for Zero Trust implementation[5].

Challenges of NIST compliance

Whether implementing Zero Trust technology and practices for the first time or adding capabilities to meet expanded industry or regulatory requirements, compliance with NIST best practices can often be challenging for organizations.

Cross-domain requirements—Compliance frameworks based on NIST standards commonly span technology domains within an organization, impacting practices and infrastructure from edge to cloud.

Fragmented capabilities—Capabilities required to comply with NIST frameworks often evolve over time and span multiple technology solutions, which can lead to piecemeal adoption of point products. This patchwork approach to security not only increases architectural and operational complexity, it also exposes the organization to security gaps, inconsistencies in policies and enforcement, and potential cyber security risk.

Team collaboration—Delivering successful innovation that meets compliance requirements often requires network and security teams to work together to pursue common goals and objectives—providing superior experiences while keeping the organization safe from increasingly prevalent and sophisticated attacks.

[1] General Perspectives. National Institute of Standards and Technology. https://www.nist.gov/cyberframework/general-perspectives. December 2021.

[2] Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. April 2018.

[3] Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5. September 2020.

[4] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207. August 2020.

[5] Biden, Jr., J. Executive Order on Improving the Nation's Cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. May 2021.

Failure to comply with regional and industry cybersecurity and data privacy requirements can result in fines and other penalties.

Security-first, AI-powered networking for adoption of NIST best practices

Accelerate your path to compliance with security-first, AI-powered networking from HPE Aruba Networking. Built on a foundation of Zero Trust, HPE Aruba Networking security-first, AI-powered networking solutions provide a common foundation for networking and security teams to power distinctive experiences and innovative business results without sacrificing cybersecurity protection.

A security-first, AI-powered network from HPE Aruba Networking eases compliance with cybersecurity standards and regulations by allowing organizations to use the network as a security solution. The network can now provide more advanced visibility, insights, centralized policy management, data protection, threat defense, and access control in a single platform. With these built-in Zero Trust Security capabilities, the network itself becomes a critical line of defense that can help satisfy security, data privacy, and risk management requirements without the added complexity that comes from multiple disparate tools, or the costly and disruptive requirement of a rip-and-replace of existing infrastructure.

AI-powered networking also multiplies an organization's human power—a crucial factor as regulatory frameworks expand, talent gaps widen, and cyber threats increase. With HPE Aruba Networking security-first, AI-powered networking, teams can benefit from intelligent automation that reduces manual effort, improves visibility and anomaly detection, and enhances monitoring and diagnostics, all of which ensure the organization is not exposed to unnecessary risk.

Achieving key NIST requirements with HPE Aruba Networking

NIST guidelines span a variety of capabilities and requirements aimed at bolstering cybersecurity and business resilience. Guidelines include requirements for cybersecurity strategy and governance, incident detection and response, and infrastructure and application security.

Cybersecurity

NIST's cybersecurity framework provides a structured approach to managing and mitigating cybersecurity risk. NIST guidance includes functional outcomes that can be operationalized to address evolving cybersecurity risk[6].

HPE Aruba Networking solutions support NIST cybersecurity framework capabilities, including:

- Identification
- Protection
- Detection
- Response
- Recovery

Zero Trust principles

Zero Trust Security principles are a key consideration for modern security architectures. NIST Special Publication 800-207 outlines a variety of requirements for implementing a Zero Trust architecture[7]. In a paradigm shift from perimeter-based security models, Zero Trust assumes there is no implicit trust granted to subjects (users and devices) based solely on their physical or network location. Instead, subjects are granted least-privilege access to just the resources needed to do their job or fulfill their function.

[6] Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. April 2018.

[7] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207. August 2020.

While no single vendor or solution can deliver all the cyber protection an organization needs, starting with a network that provides a built-in foundation for Zero Trust Security can help reduce the number of disparate tools needed to achieve NIST guidelines while adding protection at critical digital entry points.

HPE Aruba Networking Edge Services Platform (ESP) is built on Zero Trust Security principles from edge to cloud, enhancing protection while simplifying operations. HPE Aruba Networking delivers key Zero Trust capabilities—comprehensive visibility, authentication and authorization, and least-privilege access controls, as well as continuous monitoring and policy enforcement—in concert with the broader security ecosystem, on and off the corporate network.

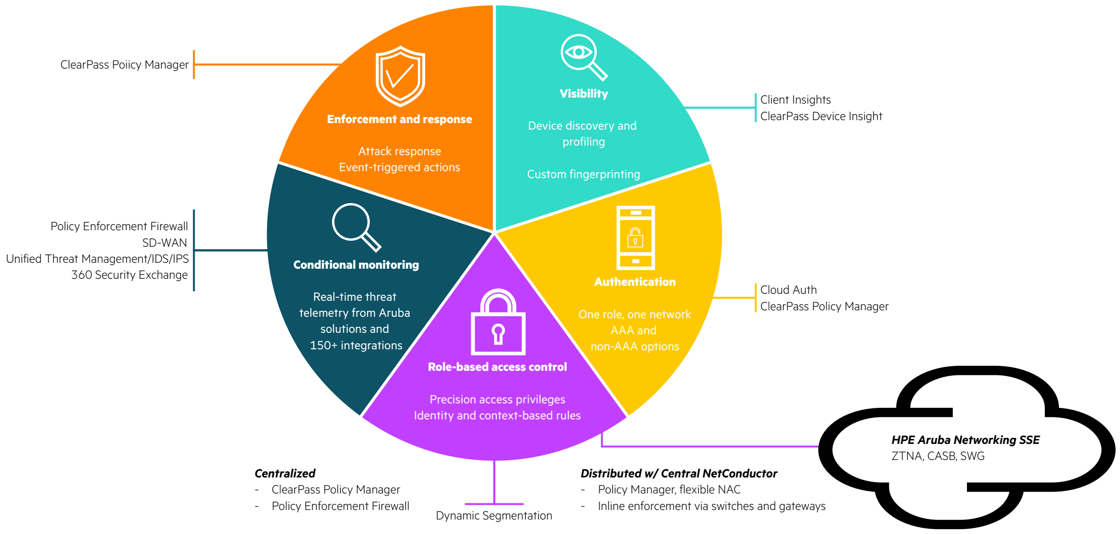
ClearPass Poiicy Manager
Enforcement and response
Attack response
Event-triggered actions
Visibility
Device discovery and profiling
Custom fingerprinting
Client Insights
ClearPass Device Insight
Policy Enforcement Firewall
SD-WAN
Unified Threat Management/IDS/IPS
360 Security Exchange
Conditional monitoring
Real-time threat telemetry from Aruba solutions and 150+ integrations
Authentication
One role, one network
AAA and non-AAA options
Cloud Auth
ClearPass Policy Manager
Role-based access control
Precision access privileges
Identity and context-based rules
HPE Aruba Networking SSE
ZTNA, CASB, SWG
Centralized
- ClearPass Policy Manager
- Policy Enforcement Firewall
Dynamic Segmentation
Distributed w/ Central NetConductor
- Policy Manager, flexible NAC
- Inline enforcement via switches and gateways

Figure 1. HPE Aruba Networking Zero Trust Security foundation

Visibility: Users, devices, applications

Zero Trust Security starts with visibility of connected users and devices. Cloud-based network management solution **HPE Aruba Networking Central** includes AI-powered visibility and profiling with **Client Insights**. Client Insights analyzes native infrastructure telemetry directly from access points, switches, gateways, and clients, without requiring installation of physical collectors or agents. Client Insights provides accurate AI/ML device profiling with up to 99% profiling accuracy of known clients with <5% rate of unknowns across a wide variety of endpoints connecting to the network, including a diverse set of IoT devices across the entire wired and wireless infrastructure[8]. For environments not managed by cloud-based HPE Aruba Networking Central or with third-party network devices, **HPE Aruba Networking ClearPass Device Insight** provides ML-based identification and profiling of clients.

Gain up to 99% profiling accuracy for network-connected devices, including IoT

Application identification and classification capabilities within HPE Aruba Networking Central give organizations visibility into applications in use within the organization, as well as the ability to define and categorize applications according to custom-defined risk profiles. Gateways can selectively inspect traffic at the gateway based on risk profile, giving network and security teams a shared approach to optimizing network performance and protection.

[8] Aruba Helps Network Teams Overcome Scarce Staff Resources with First AIOps Solution that Combines Network and Security Insights for Improved IT Efficiency. https://www.businesswire.com/news/home/20220726005426/en/Aruba-Helps-Network-Teams-Overcome-Scarce-Staff-Resources-with-First-AIOps-Solution-that-Combines-Network-and-Security-Insights-for-Improved-IT-Efficiency; AI-powered Network Infrastructure: The answer to IT Efficiency. https://www.arubanetworks.com/resource/ai-powered-network-infrastructure-the-answer-to-it-efficiency/

Authentication and authorization

After a user or device is known and profiled, the next step is to authenticate its identity each time it connects to the network. With **HPE Aruba Networking ClearPass**, users and devices can be authenticated against a wide variety of identity sources, such as Active Directory. Using a rich policy engine that enables precision access privileges, ClearPass controls what users and what devices can access what resources. Policies follow the user and device seamlessly across wired, wireless, and wide area networks—even within multi-vendor environments. **ClearPass OnGuard** can also provide and support endpoint posture assessments, ensuring that configuration and compliance guidelines are followed, and non-compliant devices stay off the network.

For networks managed by HPE Aruba Networking Central, cloud-native network access control (NAC) solution **Cloud Auth** enables frictionless on-boarding of end users and client devices either through MAC address-based authentication or integrations with common cloud identity stores such as Google Workspace^{TM} or Azure Active Directory to automatically assign the right level of network access.

Identity-based access

HPE Aruba Networking's **Dynamic Segmentation** separates network traffic based on identity and associated access permissions, enforcing least-privilege access to applications and data from edge to cloud. Dynamic Segmentation supports multiple enforcement models—centralized and distributed—allowing IT to use one or both models based on the needs of their environment. Centralized enforcement is provided by **Policy Enforcement Firewall**, a full application firewall embedded in HPE Aruba Networking network infrastructure.

For distributed enforcement inline within gateway and switching infrastructure, **HPE Aruba Networking Central NetConductor** uses widely adopted technology, such as EVPN/VXLAN, to produce a distributed network overlay. This full-stack solution includes cloud-native security services for global policy management and network configuration with a simple business-logic interface and intuitive workflows that network and security teams can use to deliver optimal network performance while defining and enforcing granular security policies that are the foundation of Zero Trust architectures.

HPE Aruba Networking Central NetConductor provides network and security teams a shared toolset for simply defining and easily propagating granular L2-L7 access policies throughout the network. Stateful application-aware firewall capabilities within **HPE Aruba Networking CX 6300 and 6400 switches** enforce policies based on business intent, without the manual effort, inconsistencies, and potential risks associated with VLANs and ACLs.

Organizations can also use **HPE Aruba Networking EdgeConnect SD-WAN** to enforce consistent security policies spanning the WAN and the LAN with built-in end-to-end, next-generation firewall capabilities including IDS/IPS, DDoS protection, and enterprise-wide micro-segmentation. Built-in next-generation firewall services enable organizations to consolidate branch network and security functions by eliminating legacy firewalls and routers in branches.

Within the data center, **HPE Aruba Networking Fabric Composer** eases implementation of Zero Trust Security by simplifying and automating the micro-segmentation process with an easy-to-use, point-and-click user interface. The **HPE Aruba Networking CX 10000 switch** delivers distributed micro-segmentation, east-west firewalling, encryption, and telemetry services inline, across every port, closer to critical enterprise applications, eliminating the need for additional firewalls.

For hybrid and remote users, as well as third parties such as contractors and temporary workers, **HPE Aruba Networking SSE Zero Trust Network Access (ZTNA)** limits access, via a trust broker, to only specific applications or microsegments that have been approved for the user as defined via a single global policy interface. Continuous monitoring ensures that policies automatically adapt based on changes in identity, location, and device health—making it easier to ensure Zero Trust for every access event.

Continuous monitoring, enforcement, and response

Ongoing monitoring of users and devices on the network is another Zero Trust Security best practice. HPE Aruba Networking solutions integrate with over 150 best-of-breed security solutions within the **Aruba 360 Security Exchange** to supply and act on real-time threat telemetry coming from multiple sources. Bi-directional communication between the network and the broader security ecosystem enables organizations to leverage network data to not only gain visibility into and control over user and device activity, but also increase the value of their investments.

Risk management framework

NIST's risk management guidance includes NIST Special Publication 800-53, which establishes system and organizational controls for organizations or systems that process, store, or transmit information[9]. Controls are designed to guide organizations in implementing appropriate security and privacy risk management policies[10]. Requirements span technical, operational, and organizational measures to both manage risks posed to the security of infrastructure as well as protect the privacy of individuals[11].

HPE Aruba Networking can help satisfy NIST guidelines for risk management, including:

- Awareness and training
- Access and authorization
- Business continuity
- Configuration management
- Incident handling
- Secure software development
- Supply chain security
- System and services acquisition
- Vulnerability reporting and resolution

Secure software development

HPE Aruba Networking uses secure development processes to reduce vulnerabilities while optimizing solution costs and availability. Developing products according to **software development lifecycle and secure software development framework** best practices helps protect organizations from unnecessary exposure to risk.

- **Requirement analysis—**Analyze security risks and set high-level security requirements.
- **Definition—**Perform security threat modeling and analysis.
- **Design—**Design to mitigate security risks per requirements. Identify open source and third-party components.
- **Coding—**Reuse secured components. Implement secure coding practices. Review code and use static code analysis tools.
- **Testing—**Test security features by performing security scans, input validation, and penetration testing to achieve a secure configuration.
- **Deployment—**Digitally sign software (code signing) to verify code integrity. Scan for malware and conduct review of open-source code. Deliver software bill of materials (SBOM).
- **Maintenance—**Post to HPE Aruba Networking Support Portal. Patch and maintain releases as needed.

[9] Joint Task Force. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication 800-53. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5. September 2020.

[10] Joint Task Force. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication 800-53. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5. September 2020.

[11] Joint Task Force. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication 800-53. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5. September 2020.

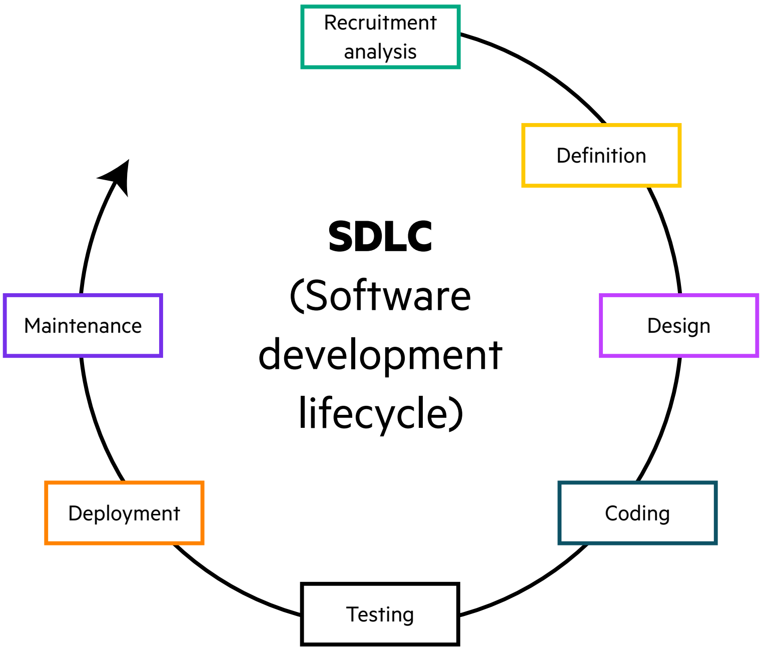

Figure 2. Software Development Lifecycle (SDLC)

Supply chain security

HPE is a leader in the ICT industry for supply chain cybersecurity. HPE Aruba Networking solutions are built using only certified **TAA-compliant** SKUs, reducing the likelihood that hardware and software components in the product have been manipulated by anyone in a hostile country. To be TAA-compliant, products must be manufactured or "substantially transformed" in the United States or a TAA "designated country[12]."

Solutions are delivered with a **software bill of materials** for risk management of software components. As cybersecurity threats evolve, HPE Aruba Networking continues to identify and mitigate cybersecurity risks within its supply chain and provide secure products so organizations can concentrate on their business goals.

Building on a secure foundation

Approved by the U.S. National Security Agency (NSA), the Commercial National Security Algorithm (CNSA) Suite is a set of publicly available algorithms that serve as the cryptographic base for unclassified information and most classified information. The NSA has authorized the use of CNSA to facilitate the sharing of sensitive and classified information among multiple departments as well as to bring secure mobility to commercial laptops, tablets, and smartphones. The **HPE Aruba Networking Advanced Cryptography (ACR) module** delivers CNSA cryptography, enabling user mobility and secure access to networks that handle controlled unclassified, confidential, and classified information.

HPE Aruba Networking solutions have been evaluated and authorized for use in compliance with U.S. cybersecurity mandates and programs such as such as Common Criteria, FIPS-140, DoDIN-APL, and USGv6—signifying that solutions have met stringent security requirements.

[12] Federal Acquisition Regulation: 52.225-5 Trade Agreements. https://www.acquisition.gov/far/52.225-5. United States Government.

HPE Aruba Networking infrastructure was selected for classified and unclassified networks within the Pentagon, headquarters of the United States Department of Defense, supporting over tens of thousands of devices daily. The Pentagon also expanded its deployment of ClearPass Policy Manager for secure network access control across its networks[13].

To safeguard against malicious boot code and device impersonation attacks, HPE Aruba Networking wired and wireless networking solutions use **Trusted Platform Module (TPM) technology**, an international standard for a secure, tamper-resistant crypto-processor designed to secure hardware by integrating cryptographic keys into devices. Installed during manufacturing, TPM chip technology can provide a secure root of trust upon which to build additional layers of Zero Trust and Secure Access Service Edge (SASE) security.

To prevent unauthorized rogue access points from gaining backdoor access to the network and intercepting user data, HPE Aruba Networking Central offers advanced **wireless intrusion prevention**. Network and security teams can set custom rules for rogue AP detection according to their own risk thresholds.

Software updates and device configurations

HPE Aruba Networking Central simplifies the configuration workflow for managed devices by allowing administrators to combine a set of devices into groups. Groups enable administrators to manage devices efficiently using either a UI-based configuration workflow or CLI-based configuration template.

HPE Aruba Networking makes software performance and security updates available via its award-winning **Support Portal**.

2023 WINNER tsia STAR Awards

2023 TSIA STAR Award for Innovation in Customer Portals that improve the Digital Customer Experience

Vulnerability reporting and resolution

HPE Aruba Networking Threat Labs manages and mitigates security vulnerabilities within HPE Aruba Networking products. Vulnerabilities can be reported by independent security researchers, customers, or even HPE Aruba Networking employees. HPE Aruba Networking also operates a public bug bounty program, which can uncover vulnerabilities faster.

Business continuity

HPE Aruba Networking network and management platforms offers a variety of resilience capabilities designed to support minimally uninterrupted operations and improved network uptime, including such hitless failover, in-service software upgrades, VSF enhanced software upgrades, Live Upgrades, and high-availability design.

[13] The Pentagon Modernizes Wired and Wireless Connectivity, Across All Classification Levels, with Aruba Infrastructure. https://www.businesswire.com/news/home/20201026005079/en/The-Pentagon-Modernizes-Wired-and-Wireless-Connectivity-Across-All-Classification-Levels-with-Aruba-Infrastructure. Oct. 2020.

Complement HPE Aruba Networking solutions with HPE GreenLake Disaster Recovery and Backup as a Service, which uses encrypted backups to protect on-premises and cloud native workloads against ransomware attacks, and HPE Services, which can help you set up policies for information system security and risk management tailored to your organization.

Conclusion

Without a strategic approach to simplification and collaboration, comprehensive NIST guidelines for cybersecurity, Zero Trust and risk management controls can be difficult to implement. With HPE Aruba Networking security-first, AI-powered networking, the network can become an asset for your organization that helps teams achieve shared objectives for security, privacy, and compliance.

For more information, visit arubanetworks.com/products/security/

Additional resources

HPE supply chain security innovation: Enhancing trust and resilience from edge to cloud

Product Security Incident Response Policy | HPE Aruba Networking

Cybersecurity training and certification | HPE Services - Education

Make the right purchase decision.
Contact our presales specialists.

✉ **Contact us**

Visit **ArubaNetworks.com**

Hewlett Packard
Enterprise