Forcepoint

Solution Brief

Implement NIST Cybersecurity Framework 2.0

with Forcepoint NGFW

Challenge

› Federal Civilian Executive Branch Agencies face increasing cyber threats and regulatory pressures, requiring effective cybersecurity strategies that align with established frameworks like NIST Cybersecurity Framework 2.0.

Solution

› Forcepoint NGFW solutions provide advanced threat protection, access control and centralized management, supporting all six core functions of the NIST framework for a comprehensive security posture.

Outcome

› By implementing Forcepoint NGFW, agencies enhance their cybersecurity resilience, improve incident response and ensure compliance with NIST guidelines, ultimately protecting critical assets.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 provides a comprehensive approach to managing cybersecurity risks. Forcepoint's Next-Generation Firewall (NGFW) solutions are specifically designed to support these frameworks, enabling agencies to boost their cybersecurity posture.

Overview of NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework 2.0 establishes six core functions:

1. **Govern:** Establish policies and governance to manage cybersecurity risks.
2. **Identify:** Understand the agencies' environment, assets, and risks.
3. **Protect:** Implement safeguards to ensure critical services are delivered.
4. **Detect:** Develop and implement activities to identify cybersecurity events.
5. **Respond:** Take action regarding detected cybersecurity events.
6. **Recover:** Restore services impaired by cybersecurity events.

These functions work together to create a comprehensive cybersecurity strategy that can be adapted to an agencies' unique needs.

Forcepoint NGFW Overview

Forcepoint NGFW provides industry-leading network security protection with intelligent traffic management, delivering secure connectivity across sites while reducing operational complexity and costs.

Forcepoint NGFW solutions combine traditional firewall capabilities with advanced threat detection and prevention features. Key capabilities include:

→ Deep packet inspection

→ Access and Application control

→ Intrusion prevention

→ Advanced threat protection

→ Centralized management and reporting

Forcepoint NGFW enhances visibility into network traffic, supports policy enforcement to thousands of engines and provides rapid response capabilities to mitigate potential threats.

Alignment with NIST Cybersecurity Framework 2.0

Govern

- **Policy Enforcement:** Forcepoint NGFW assists in the development and enforcement of security policies, ensuring compliance with regulatory requirements and best practices as specified in the NIST framework.
- **Risk Management:** The product's robust reporting capabilities allow agencies to maintain visibility over risk management processes, enabling informed decision-making and continuous governance.

Identify

- **Asset Management:** Forcepoint NGFW provides detailed visibility into all engines and users on the network, helping agencies effectively understand their cybersecurity landscape.
- **Risk Assessment:** The advanced analytics capabilities enable agencies to continuously assess vulnerabilities and threats in real-time, allowing agencies to prioritize security measures based on identified risks.
- **Governance:** Forcepoint solutions support the establishment of cybersecurity policies and procedures by enabling agencies to define and enforce security controls effectively.

Protect

- **Access Control:** Forcepoint NGFW goes beyond traditional methods by leveraging contextual information to enforce policies. Administrators can define policies based on the user's identity, the device being used, the location from which the connection is made, the application being accessed and other contextual factors. Policies can be applied globally or to specific sites, providing granular control over access to sensitive applications and data.
- **Data Security:** Integration with Forcepoint Data Loss Prevention (DLP) solution helps protect sensitive information from unauthorized access and exfiltration as a last line of defense, aligning with the "Protect" function.
- **Awareness and Training:** Forcepoint's security solutions include user education components that promote cybersecurity awareness, a critical aspect of organizational protection.

Detect

- **Anomalous Activity Detection:** The NGFW's advanced threat detection capabilities identify unusual patterns in network traffic, enabling early detection of potential threats.
- **Continuous Monitoring:** Forcepoint NGFW provides real-time monitoring, facilitating prompt identification of cybersecurity events, which is essential for effective detection.

Respond

- **Incident Response Capabilities:** Forcepoint NGFW allows for automated responses to detected threats, such as blocking malicious traffic or isolating affected systems, enabling a proactive incident management approach.
- **Reporting and Analysis:** The centralized management console provides comprehensive reporting on security incidents, allowing agencies to analyze events and refine response strategies.

Recovery

- **Backup and Recovery Plans:** Forcepoint NGFW aids in the development of effective recovery plans by ensuring that access controls are quickly restored post-incident.
- **Continuous Improvement:** By evaluating incident response activities through detailed reporting and analytics, agencies can enhance their recovery strategies and adapt to evolving threats.

Key Features of Forcepoint NGFW Supporting NIST Compliance

- **Advanced Threat Protection**
  Forcepoint NGFW integrates advanced threat protection capabilities, including intrusion detection and prevention systems (IDPS), to help identify and mitigate threats in real-time, supporting both detection and response functions. Additionally, Forcepoint NGFW integrates with Forcepoint Remote Browser Isolation (RBI) and Advanced Malware Detection and Protection (AMDP) services to provide multiple layers of security, ensuring safe access to web applications and sites, even in remote locations.
- **Centralized Management**
  The centralized management console streamlines security operations, enabling agencies to manage policies, monitor threats, and generate compliance reports efficiently.

Forcepoint's Public Sector Focus

Forcepoint is the industry-leading user and data security cybersecurity company, entrusted to safeguard agencies and public sector entities while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

By leveraging Forcepoint NGFW, agencies can implement a zero-trust security strategy that protects critical assets and fosters a culture of cybersecurity resilience.

Discover how Forcepoint NGFW can help your agencies align with NIST Cybersecurity Framework 2.0 and enhance your cybersecurity posture, visit **Defense-Grade Security for the Public Sector** for more information.

- **User and Device Analytics**
  Forcepoint NGFW leverages statistical anomaly detection based on traffic patterns observed from users and devices. This adds an additional layer of security and aligns with the framework's emphasis on continuous monitoring.
- **Endpoint Context Agent (ECA)**
  Provides additional visibility and context into endpoint devices, allowing administrators to better understand the devices and users that are accessing the network. ECA can be deployed on endpoint devices, such as laptops and desktops, and integrates with other Forcepoint security solutions to provide a comprehensive security framework. It provides granular visibility into network traffic at the endpoint level, including information about the user, device and application being used, to enable more effective policy enforcement and threat detection.
- **Integration with Existing Security Tools**
  Forcepoint NGFW can seamlessly integrate ith other security solutions, such as Security Information and Event Management (SIEM) systems, enhancing overall security posture and aligning with NIST's recommendations for a holistic cybersecurity strategy.

forcepoint.com/contact