Forcepoint

Develop the CISA Zero Trust Maturity Model 2.0 with Forcepoint NGFW

Introduction

Implementing a Zero Trust architecture is essential for Federal Civilian Executive Branch Agencies seeking to strengthen their security posture. The United States Cybersecurity and Infrastructure Security Agency (CISA) has introduced the **Zero Trust Maturity Model Version 2.0**, which outlines key pillars for effective implementation. Forcepoint Next-Generation Firewall (NGFW) solutions are designed to support these pillars, facilitating a robust Zero Trust framework.

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 Federal agencies align with CISA's Zero Trust Maturity Model and enhance your cybersecurity posture, visit **Defense-Grade Security for the Public Sector for more information**.

Key Pillars of the Zero Trust Maturity Model Supported by NGFW

Identity

Forcepoint NGFW enforces identity management through granular access controls. By validating user identities based on roles and behaviors, it ensures only authenticated individuals can access sensitive resources. This strong identity verification aligns with Zero Trust principles, minimizing the risk of unauthorized access.

Devices

Effective device controls are critical for a Zero Trust approach. Forcepoint NGFW in combination with the Forcepoint Endpoint Context Agent allows agencies to reduce their attack surface and comply with secure posture before devices are authorized to access resources. This capability enables very high security efficacy with reduced risk to the mission.

Network

Forcepoint NGFW enforces strict network access policies, utilizing advanced threat detection to monitor network traffic for anomalies. By continuously analyzing user behavior and access patterns, agencies can rapidly identify and respond to potential threats, reinforcing the Zero Trust commitment to network security.

Applications and Workloads

The application layer is crucial for Zero Trust implementation. Forcepoint NGFW supports secure access to applications by enforcing strict security policies that govern user interactions. This ensures applications are only accessible to verified users, reducing the risk of data breaches.

Data

Protecting sensitive data is a core aspect of Zero Trust. Forcepoint NGFW integrates with Forcepoint's Data Loss Prevention (DLP) solutions to safeguard data from unauthorized access and exfiltration. This multi-layered, last line of defense strategy ensures critical information remains secure across all environments.