FORTINET

SOLUTION BRIEF

Raising the Cyber Grade: How Policy and Innovation Combine for Better FITARA Scorecards

Federal agency efforts to improve IT operations are graded each year via the FITARA Scorecard,[1] which measures progress against the objectives laid out in the Federal Information Technology Acquisition Reform Act (FITARA)[2], a comprehensive piece of legislation designed to create greater transparency and improve risk management in Federal IT. The legislation is a roadmap for CIO procurement and management of technology solutions.

The FITARA Scorecard, which is released every June and December, currently grades 24 Federal agencies on a scale of A to F in eight categories.[3] It is highly anticipated by members of Congress, agency leadership, and industry stakeholders.

Scorecard Measures Progress – and Opportunity for Improvement

The ultimate goal for CIOs is to score – and maintain – high marks in each category of the scorecard while delivering on agency missions. The scorecard is one way that CIOs can measure progress and identify areas that need the most improvement.

The December 2020 scorecard, for example, marked just the second time that every agency received a passing score since the House Oversight and Reform Committee started measuring agency progress against FITARA and other key metrics.[4]

That said, agencies are struggling to improve their scores in the cyber category of the scorecard. Only one agency scored an A in the category. More than half of the agencies received a grade of C or below, and two received an F.

With the recent increase in large-scale cyberattacks, including attacks against the Federal government,[5] the Biden administration is proposing unprecedented levels of investment in cybersecurity, and members of Congress will be closely watching for improvements across the Federal government – and improvements in the FITARA Scorecard cyber category score.

Rapidly Evolving Threats Can Stymie Cybersecurity Progress

The cyber score measures an agency's compliance with FISMA guidelines and security standards,[6] which are laid out in NIST Special Publication 800-53v5.[7] Many of the FISMA guidelines address basic cyber hygiene, which is critically important to establishing a baseline cybersecurity posture that helps protect critical systems and data. However, rapidly proliferating and evolving cyber threats present severe, ongoing challenges to IT teams working to maintain their agency's security posture, let alone improve it – and raise their cyber score.

Innovation Meets Policy to Help Agencies Improve Cyber Scores

Fortinet's flagship FortiGate Next Generation Firewall helps agencies bring policy and innovation together for better cybersecurity. FortiGate is a high-performance network security appliance that enforces security policies, identifies and stops threats, and provides technology teams with real-time views into their networks. It protects against all types of cyberattacks, regardless of threat vector or motivation behind the attack.

In a recent FortiGate review, the SANS Institute mapped FortiGate to NIST 800-53v5 standards,[8] demonstrating how the appliance helps agencies meet their FISMA obligations. SANS concluded, "the FortiGate product does a remarkable job of providing compliance, covering a large cross section of control families. It is all the more impressive that it does so in a way that is manageable from a single, easy-to-navigate interface."

It can be easy to fall into the trap of responding to the latest cyber threat with the shiniest new technology tool, which can bring about greater technology and management complexity with marginal security benefit.

To truly secure Federal infrastructure, agencies need a methodical, integrated approach that emphasizes continual improvement and mission delivery. This approach can bring policy and innovation together to meet NIST standards, achieve FISMA compliance, and most importantly, secure networks and protect the American people. An added bonus: incremental improvement in cyber scores from one FITARA Scorecard to the next.

FortiGate Addresses Compliance With NIST 800 – 53v5 Control Families

The SANS Institute review identified many features that help achieve compliance with NIST 800-53v5 control families, including:

Access Control

A secure network starts with strong user and device security that offers access control and enforcement, letting the good guys into the areas where they are allowed to go and keeping the bad actors out. Access control is a key tenet of a zero trust architecture, and can be achieved with FortiGate through:

- Account management features
- Logging features
- Customizable HTML pages
- Session management features

Audit and Accountability

The FortiGate appliance includes multiple logging and auditing controls. Logs can be stored and viewed locally, and they can also be forwarded to other assigned locations, such as the Department of Homeland Security's EINSTEIN data hubs.

Assessment, Authorization, and Monitoring

The FortiGate appliance supports the continuous monitoring control family with its logging feature and FortiView, a comprehensive monitoring system that integrates real-time and historical data into a single view on FortiGate. If while on the network a user's dynamic "reputation score" is determined to be too risky, they can be immediately removed from the network.

Configuration Management

The configuration management control family focuses on the secure configuration of devices. The FortiGate appliance offers configuration backup and an application control feature, which detects and inspects application traffic on the network. It also provides user compliance through FortiClient, an endpoint detection agent that provides information, visibility, and control of the endpoint and supports secure remote connectivity. FortiClient features zero trust capabilities through application segmentation, offering an alternative connection method to traditional VPNs.

Contingency Planning

FortiGate features help ensure agencies can continue to operate during and after an unexpected event. These include:

- Application control
- Multiple protocols for administration
- Configuration backup and recovery

Identification and Authentication

The FortiGate appliance positively identifies and securely authenticates permanent users, temporary employees, and contractors. Different access rights are assigned to different user roles on the network.

Program Management

The program management control family requires the implementation of an insider threat program. An early indicator of insider threats is the use of unsanctioned applications. FortiView, application control, and FortiClient compliance (application whitelisting) are all features on the FortiGate appliance that support detection of unsanctioned applications.

System and Information Integrity

To prevent threats to the integrity of data and the systems processing data, FortiGate offers:

- Malicious code protection
- System monitoring
- Security alerts, advisories, and directives
- Software, firmware, and information integrity
- Spam protection
- Information input validation
- Error handling
- Non-persistence
- Memory protection

Fortinet Helps Agencies Take a Holistic Approach to Cybersecurity

As a partner to Federal technology teams, Fortinet can take a holistic view of each agency's security landscape and implement the security solutions that meet the agency's unique mission requirements. And, with FortiGate mapped to NIST standards, FITARA cyber scores can improve in a single scorecard cycle.

Learn more at https://www.fortinet.com/federal

[1] A Look Back: How the FITARA Scorecards Have Evolved
[2] The Federal Information Technology Acquisition Reform Act (FITARA) Frequently Asked Questions
[3] FITARA Dashboard
[4] Want a Good FITARA Scorecard Grade? A Couple of CIOs Tell How….
[5] US Government and Cyber Crime
[6] Securing Federal Networks
[7] Security and Privacy Controls for Information Systems and Organizations
[8] Achieving NIST 800-53v5 Compliance with FortiGate

June 23, 2021 9:38 AM

16TB-Seagate:Dropbox (300Brand Creative):Creative:Clients: MeriTalk:ISSUE BRIEF:IB-MT-immixGroup-Fortinet-Issue-Brief-41316:Layout:MT-immixGroup-Fortinet-Issue-Brief-41316-r2

123456-0-0-EN