Addressing NIST Security Controls with ForeScout

Make Your Risk Management Framework a Reality with CounterACT®

Common Agency Security Hurdles

Organizational Challenges

- Enable continuous monitoring and mitigation capabilities that leverage existing investments.
- Protect the security of federal organizations through **device and user** access controls.
- Improve network security through configuration management and auditing controls.
- Comply with the NIST 800-53 controls
- Facilitate streamlined network access and information sharing for trusted contractors, research organizations and customers.

Technical Challenges

- Discover personally owned and rogue devices as well as other endpoints connected to the network.
- Control access to confidential and sensitive data.
- Prevent infected or non-compliant devices from spreading malware or viruses across the network.
- Defend against targeted attacks that can steal data or force network downtime.
- Measure effectiveness of security controls and demonstrate compliance with regulations and federal standards.

Once a federal system has been categorized as *High, Medium or Low with Confidentiality, Integrity and Availability*, the next major milestone in most Risk Management Framework (RMF) processes is to identify all the security controls that will be required to support compliancy for the architecture. These controls will become the baseline for the architecture and drive the continuous monitoring and reporting of compliancy to governing entities. Oftentimes, the common controls are "those specific security controls that are inherited by one or more organizational information systems."[1] These controls are clearly understood by the agency and part of the core understanding of any organization's defense and/or architecture that helps to protect the systems that are organizationally defined or established. ForeScout CounterACT® can be leveraged for just this type of high-level, organization-wide control to track devices and their users connecting to agency networks.

The objective of the National Institute of Standards and Technology's (NIST) 800 Risk Management Framework is to provide federal organizations with a catalog of privacy and security controls to protect operational functions (Special Publication 800-53 Revision 4) and secure the confidentiality of unclassified information systems.

Securing Public Sector Networks with ForeScout

Many organizations today are unable to enforce cybersecurity policies across the enterprise. A key reason for this is the fact that devices that lack required security agents come and go from the network at will and are largely undetected by periodic, point-in-time vulnerability scans. This gap in security policy enforcement puts the entire network in jeopardy.

The ForeScout CounterACT security platform can address these deficiencies. CounterACT can operate within legacy, new and highly technical network infrastructure without reengineering the established network or disrupting services. The platform provides agency administrators with the critical ability to see and monitor devices on the network, from endpoints such as computers and printers to wireless devices accessing the system. CounterACT enforces network access policies across the network hierarchy, from switches to access and distribution layers.

An important objective of federal cybersecurity policies is to identify critical markers (CIA) within the network environment to help reduce possible attack vectors. CounterACT achieves this by supporting enterprise network security stacks. It can enforce a variety of actions and provide organizations with the options they need to support government security management regulations.

How ForeScout Addresses These Challenges:

- CounterACT maps directly to 10 of 18 Control Families and over 150 supporting controls.
- CounterACT supports these controls in real time for explicit Continuous Diagnostics and Mitigation requirements.
- CounterACT is already being used by several federal agencies today to help support their Continuous Diagnostics and Mitigation (CDM) programs.
- CounterACT is uniquely positioned to see what is on your network today without the use of agents, minimizing disturbance.

By helping enforce NIST fundamental controls, CounterACT also helps federal organizations keep in line with Federal Information Security Modernization Act (FISMA) requirements. Logically, ForeScout can support most federal, state and local security requirements by utilizing the base NIST security guidance for their network architectures.

In addition to playing a critical role in the response, the CounterACT platform also orchestrates and enables a variety of security tools to share information and work together. This orchestration allows agencies to integrate and automate their security responses while also helping them to support compliance and standardization goals and preserve their investments in existing security tools. The bottom line is that CounterACT sees IP-addressable endpoints, manages those endpoints through policies and rulesets and integrates with your current security tools to help meet requirements for continuous monitoring, enablement of security procedures and mitigation, and implementing automated responses to secure and protect the environment.

ForeScout in the NIST Risk Management Framework

CounterACT directly impacts and supports these specific control areas documented in 800-53 rev4:

- **Access Control.** Limits access to agency information systems to authorized users, processes administered on behalf of authorized users, or devices/ information systems, transactions and functions users are permitted to control.
- **Audit and Accountability.** Enforces appropriate use policy for network and information systems. This also allows agencies to audit information system use and validate standards compliance by producing documents and reports.
- **Continuous Monitoring.** Addresses management, operational and technical controls in information systems contained in the inventory of major information systems as required by NIST's Certification, Accreditation and Security Assessment control.
- **Configuration Management.** Focuses on policies and procedures, change control, monitoring and configuration changes, configuration settings and access restrictions for configurations changes.
- **Identification and Authentication.** Addresses device and host identification and authentication, authenticator management, feedback and cryptographic authentication.
- **Incident Response.** Covers policies and procedures, incident handling, reporting and response assistance—including forensic services and automated tools.
- **Risk Assessment.** Examines the creation of a Risk Assessment Policy and procedures to assess the potential impact of damage due to unauthorized access of information systems. Besides addressing potential risks, it focuses on software and hardware solutions that can mitigate risk by identifying and mitigating vulnerabilities.
- **System and Services Acquisition.** Emphasizes trustworthy information systems and supply chain security. Public sector organizations must clearly and specifically express their information security requirements when working with commercial industry to acquire vital systems, components and services.

- **System and Communications Protection.** Creates policies and procedures that reflect applicable federal laws, executive orders, directives, regulations, policies, standards and guidance that enforce monitoring and control communications at external and internal boundaries in the system.
- **System and Information Integrity.** Examines policies and procedures in remediation of security flaws, generating security alerts and advisories. CounterACT also provides intrusion protection capabilities and orchestrates interoperability with other cyber-prevention tools and techniques, including protection against spyware.

The CounterACT Security Platform

The ForeScout CounterACT security platform provides real-time monitoring control and policy-based remediation of managed, unmanaged and non-traditional devices to support your compliance efforts with NIST standards. Here's how:

See. Detects devices the instant they connect to the network without requiring agents. Profiles and classifies devices, users, applications and operating systems. Continuously monitors managed devices, Bring Your Own Devices (BYOD) and Internet of Things (IoT) endpoints.

Control. Allows, denies or limits network access based on device posture and security policies. Assesses and remediates malicious or high-risk endpoints. Assists with improving compliance with industry mandates and regulations, including NIST standards and beyond.

Orchestrate. Shares contextual insight and data with IT security and management systems. Automates common workflows, IT tasks and security processes across systems. Accelerates system-wide response to quickly mitigate risks and data breaches.

U.S. Government Certifications and Compliances

With its CounterACT platform, ForeScout Technologies offers a set of unique network security technologies that can help federal agencies successfully establish and implement policies that protect their technology infrastructure. CounterACT's granular policy structure can be easily implemented at the core of agency-wide RMF security architecture and common control platform. CounterACT has achieved the following U.S. Government certifications and compliances:

- **DISA UC APL** (Defense Information Systems Agency Unified Capabilities Approved Products List)
- **FIPS** (Federal Information Processing Standards) **140-2**
- Common Criteria Evaluation Certification **EAL4** (Evaluation Assurance Level 4)
- **USMC ATO** (Authority to Operate)
- **U.S. Army CoN** (Certificate of Networthiness)
- **Common Criteria Evaluation Assurance Level** (EAL) L4+

Want More Details?

For greater detail on how the ForeScout platform maps to NIST, download *Addressing NIST Risk Management Framework Controls with ForeScout CounterACT* at https://www.forescout.com/company/resources/nist-risk-management-framework-and-forescout-counteract-datasheet/

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] NIST 800-37 - http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Version 2_17