ForeScout: Foundational for CDM Ongoing Assessment

ForeScout's CDM Phase 1 CDM deployments in Federal Civilian departments and agencies (DAs) are a foundational data source for Phase 3 capabilities, including Ongoing Assessment (OA). An OA solution requires a complete, continuous and rich stream of information about the devices on a network and their behavior in real time to assess the status of implemented NIST SP800-53 controls and the ability to implement countermeasures to ensure that an agency maintains an acceptable level of risk and authorization of key systems.

The CDM Ongoing Assessment Request for Service (RFS) details six steps to operationalize OA that are consistent with the NIST Risk Management Framework. ForeScout CounterACT® is central to this process as a crucial source of data to assess whether an agency is in compliance with the controls and when risk is unacceptable. When changes to the controls must be made, the ForeScout platform can automate adjustments and implement new controls to reduce risk to the enterprise on a continuous basis. ***The ability to SEE devices in real time and take actions to CONTROL the endpoint to enforce ongoing assessment compliance is a critical step forward for automating the assessment and authorization process.***

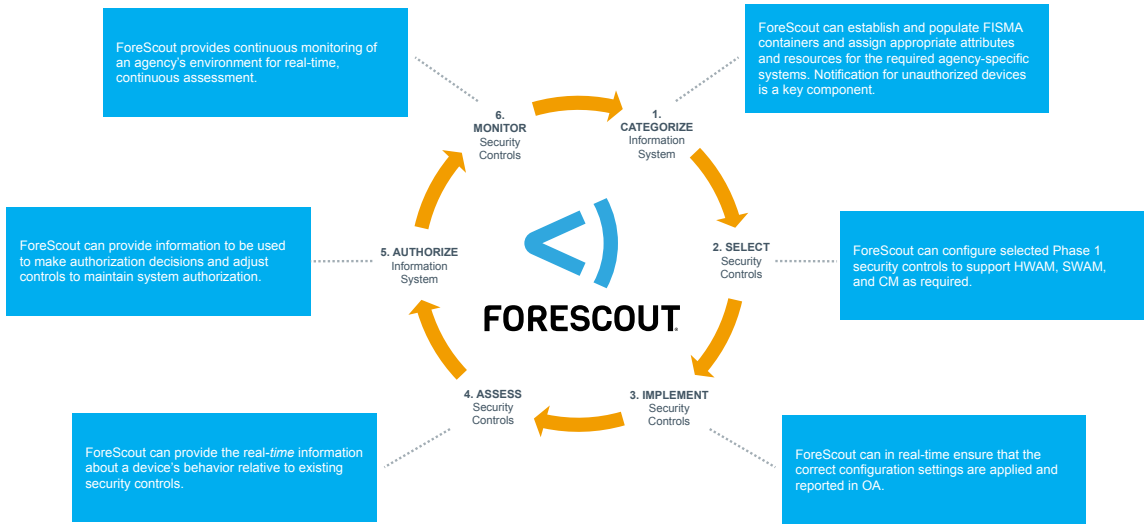

Figure 1: ForeScout CounterACT is central to the CDM Ongoing Assessment process.

The OA RFS notes, "Agencies are expected for the initial scope of this RFS to have Phase 1 Master Device Records (MDR) established that will support initial Ongoing Assessment activities." For an agency to effectively assess its security controls it must have a comprehensive view of the IP-connected devices in its environment. **A full and complete ForeScout CounterACT Phase 1 deployment is crucial to assess and authorize information systems because *you can't assess what you can't see.***

The ForeScout platform offers several key benefits that align directly with the RFS's stated objectives:

- To enable an Agency to make authorization decisions relative to their stated risk tolerance in a timely manner that is consistent with the processes established within the NIST Risk Management Framework (RMF), ForeScout CounterACT provides data in real time that provides the basis for assessing whether changes to a control will impact a system's authorization.
- To shorten the RMF cycle and provide a near real-time view of Agency-defined security and privacy policies as captured within the attributes of FISMA container objects, ForeScout CounterACT can identify devices and changes in their behavior in real time to enable OA and ongoing authorization of security controls. *The ForeScout platform integrates with the network at the switch level so it can detect admission and authentication requests from new devices and identify changes in behavior for devices on the network within the FISMA container.*
- To orchestrate the automation of security controls, ***ForeScout enables bi-directional integrations with other common CDM tools to unify system-wide security management as shown in figure 2.*** This unique set of network, security and management interoperability technologies extends the power of ForeScout CounterACT to more than 70 third-party solutions, allowing the combined system to accelerate response, achieve major operational efficiencies and provide superior security. (https://www.forescout.com/products/extended-modules/orchestrate/) For example, the ForeScout Extended Module for Splunk® enables ForeScout and Splunk to share information and enable a user to take action in the environment using ForeScout CounterACT if a security control is degraded or no longer in place. (for example, if, a device is missing a security software patch, has a newly reported flaw, or is suspected of contributing to a malware outbreak).

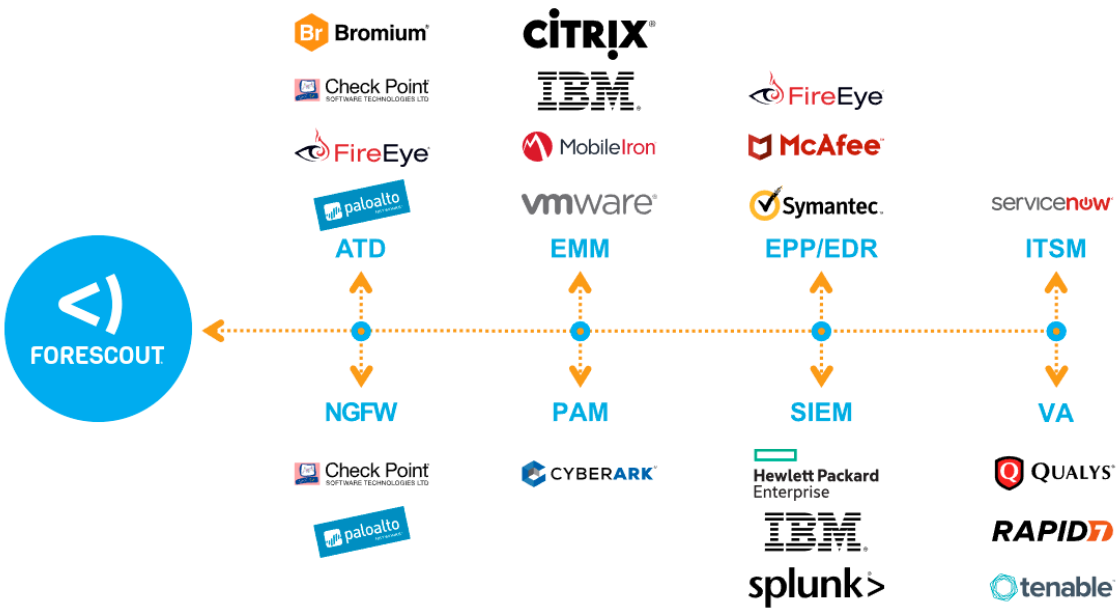

Figure 2: ForeScout orchestrates incident response and cyber-hygiene for OA from formerly siloed security products.

Objective: Establish and populate FISMA Containers. All containers established and contain system attributes — 100% reported accurately.	**ForeScout CounterACT can populate devices within the enterprise into the appropriate FISMA containers for all the assets in HWAM seen and reported to the dashboard.** Using a 'ForeScout Groups' defined policy, a device can be added to the corresponding FISMA container. This can be done statically or dynamically via IP space or connected locations for any asset seen by CounterACT.
Objective: Security Controls Automation/Implementation. Controls identified are configured to automate on deployed CDM capabilities — controls establish 95% success rate of applying configuration settings.	The ForeScout platform can automate implementation of security controls in real time as devices connect to the network or change behavior and/or configuration. **CounterACT can take a variety of actions that include the ability to change registry or endpoint settings, run scripts, and start and stop services on any managed host** to quickly automate the process of compliance for devices accessing the network.
OA Operational Requirements:	
OR-1: Shall provide ongoing assessment data consolidation and assessment frequencies to deliver an effective continuous collection, analysis and impact assessment of security policies in order to maximize automation and reduce human interaction.	ForeScout CounterACT is the real-time eyes and ears of the OA data. The ability to provide a continuous collection of data on endpoints connecting and disconnecting is critical to the OA process. The ForeScout platform's policy-based decisions are scalable and can be updated to map directly back to the controls required to both assess and then automate to reduce human interaction for the quick positive cyber hygiene that is required to "stay green" in the OA process.
OR-2: Shall complete the ongoing assessment activities so that mitigation responses and operational recovery can be completed to reduce threat propagation to other agency information and information systems.	ForeScout CounterACT's real-time visibility can be combined with the real world actions required to mitigate threats and reduce or even prevent the exposure of others to the newly assessed threat found in the information systems. Orchestration via CounterACT with other tools plays an important role here. The ability to drive both the detection and the remediation/control process makes ForeScout CounterACT a powerful tool in the OA process. Tools must be able to keep pace and provide scalability to hundreds of thousands of devices quickly based on ever-evolving criteria.
Ongoing Assessment Monitoring Functional Requirements: This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers. Ongoing assessment will require information about the attributes associated with the MUR, MDR and MSR. This capability supports the Detection Process CSF Category under the Detect CSF Function.	
FR-1: Shall monitor for changes to the data elements/attributes for all CDM capabilities and report changes to CDM Operate, Monitor and Improve (OMI) capabilities in order to support ongoing assessment.	ForeScout CounterACT evaluates the endpoint to detect changes to the data elements/attributes in real time. The OA process requires that tools be able to provide timely notification of changes and give the ability to automate responses based on the security policy as it relates to the FISMA container controls. OA will require a level of review and oversight such that tools will need to have dedicated communication paths in place to optimize the CDM capabilities.

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