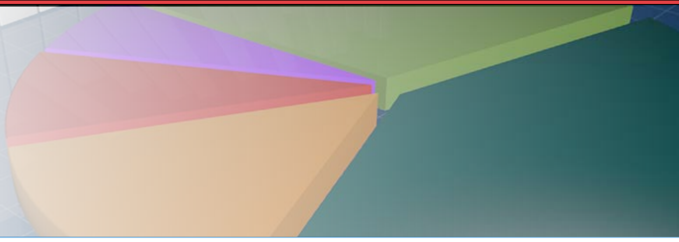
Continuous Monitoring

Integrated services, best practices, and automation tools from the leader in federal cybersecurity and information assurance.



Continuous monitoring of information systems has long been a policy goal for improving the security posture of federal networks. Achieving continuous monitoring requires a balanced combination of processes, people, and technologies to help agencies automatically detect and report vulnerabilities in the IT environment and maintain compliance with security controls and standards.

These factors make Telos Corporation a logical choice for emerging continuous monitoring programs. We tailor our services and solutions for cybersecurity and information assurance to our customers' specific technology and business environment – a key requirement for effective continuous monitoring.

Telos Cybersecurity Services

Telos has provided cybersecurity services to the DoD, the Intelligence Community, federal civilian agencies, and commercial marketplace for more than 20 years. Telos employs over 140 cybersecurity analysts and engineers, most holding major security certifications (CISSP, CISA, CISM, CCNA) with clearances up to TS-SCI, allowing us to work at the highest levels of security sensitivity.

Our staff's professional qualifications, combined with over two decades experience in providing security services, demonstrate our ability to provide world-class security services. For example:

> Telos cybersecurity engineers have ensured compliance of the Pentagon backbone networks with the governing DoD and NIST security guidelines, protecting thousands of users at dozens of locations in the National Capital Region.
>
> Telos supports diverse executive branch cybersecurity initiatives for GSA, including continuous monitoring via application and database vulnerability scanning, wireless network assessments, and secure configuration compliance.
>
> Telos supports the Intelligence Community with continuous monitoring policy and strategy development, engineering and tool deployment, and support and operation.

Our services in support of continuous monitoring include:

Security Policy and Operational Procedure Development. Telos consultants have broad experience developing, reviewing, and enforcing security policies for many types of government agencies. Because our engineers have worked in operational environments as both technicians and security engineers, they are ideally suited to develop continuous monitoring procedures that ensure network and system performance as well as security.

Security Engineering and Architecture Design. Continuous monitoring requires an understanding of a broad variety of information technologies, security requirements, and how they work together. Telos security engineers have experience with security information and event management systems (SIEMs), IDS/IPS and firewalls, enterprise operating systems as well as the application and database layers, and other resources that must be included in a continuous monitoring architectural framework.

Operational Security Management. Telos network security and operations personnel have experience monitoring network security 24/7/365 in some of the most security-conscious agencies of the federal government, the Intelligence Community and Department of Defense, including the Pentagon's Security Operations Center. Telos personnel function as a team to protect the network from failures, cyber attacks, network misconfigurations, viruses, and other vulnerabilities and threats.

Best-of-breed approaches and technologies for continuous monitoring.

Telos adheres to established IT security processes and frameworks to ensure the continuous monitoring and management of security postures. Our services and solutions reflect the recommendations of the NIST Risk Management Framework; the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) model; the emerging FedRAMP requirements for assessing and authorizing cloud services and products, and others.

NIST Risk Management Framework

The NIST Risk Management Framework (RMF) laid out in SP 800-37 provides a structured approach to managing risk throughout a system's life cycle. It identifies the elements essential to a successful organization-wide continuous monitoring program, including:

- Configuration management and change control
- Security impact analyses
- Ongoing assessment of system security controls
- Security status monitoring and reporting
- Active involvement of organizational officials

The sixth and final step of the RMF calls for the monitoring of security controls by determining the security impact of system changes, assessing a system's security controls in accordance with defined strategies, conducting remediation actions when indicated, updating security plans based on the results of continuous monitoring, and reporting and reviewing security status.

Telos works with agencies to establish, implement, and maintain a continuous monitoring program in accordance with guidance from NIST SP 800-137:

- Define continuous monitoring strategy;
- Establish measures and metrics;
- Establish monitoring and assessment frequencies;
- Implement a continuous monitoring program;
- Analyze data and report findings;
- Respond with mitigating strategies, or transfer or accept risks; and
- Review and update continuous monitoring strategy and program.

CAESARS: Risk Scoring Best Practices

The DHS Federal Network Security Branch issued the CAESARS detailed reference architecture that offers best-practices and an integrated approach with end-to-end processes for:

- Assessing the state of each IT asset under an organization's management
- Determining the gaps between the current state and accepted security baselines
- Expressing in quantitative measures the relative risk of each gap or deviation
- Providing letter grades that reflect the aggregate risk of sites and systems
- Ensuring that the responsibility for every system and site is assigned
- Providing targeted information for security and system managers to make changes needed to reduce risk
- Inspiring and encouraging competition among agency managers through measured and recognized improvement

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is designed to establish a unified risk management framework for cloud computing. This emerging standard set of controls and defined processes will result in cost savings and help to eliminate the discrepancies among agencies authorization processes by:

- Providing a framework that is compatible with FISMA security requirements and has been vetted by various government agencies and industry

- Offering effective and consistent assessment of cloud services
- Focusing continuous monitoring on near real time data feeds from cloud service providers
- Using the "approve once, use many" concept

Telos integrates new frameworks and standards into our work as they are available, tailoring each one to our customer's specific circumstances.

Xacta® IA Manager: automation tools to streamline processes for continuous monitoring.

Human judgment is essential in sound cybersecurity assessment and monitoring. But automation tools can also streamline processes and help eliminate errors and oversights. As NIST SP 800-137 suggests, "Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the security state of those controls."

Telos began automating security-related tasks through its Xacta IA Manager enterprise software offering over a decade ago and continues to support continuous monitoring and related activities with automation capabilities wherever they improve accuracy and efficiency.

Xacta IA Manager enables organizations to track the security state of a wide range of information systems on an ongoing basis and maintain the security authorization for the systems over time. Its elements work together to provide CISOs and other senior leaders as well as the practitioners with a dynamic view into the current status of security controls.

Its tightly integrated, complementary components include:

Xacta Continuum™: Organize your IT asset data and automate mapping of IT asset scans to the relevant controls. Xacta Continuum automatically detects changes to the IT environment so you always have situation awareness of potential risks and threats. Its automatic vulnerability update service delivers the right guidance at the right time about what actions to take in response to potential threats.

Xacta Continuum automatically imports asset data along with associated vulnerability and results information from systems and enterprise management platforms in addition to any third-party scanning/testing tools. It offers a central repository to organize your IT asset data as actionable information.

Telos: A Deep Legacy in Continuous Monitoring

Telos Corporation has been an advocate of continuous assessment, monitoring, and enforcement for more than a decade. We first conceived of continuous assessment in 1999 as part of our long-term strategy to make the C&A process more meaningful – less about documentation and paperwork drills, more about understanding risk posture on an ongoing, continuous basis.

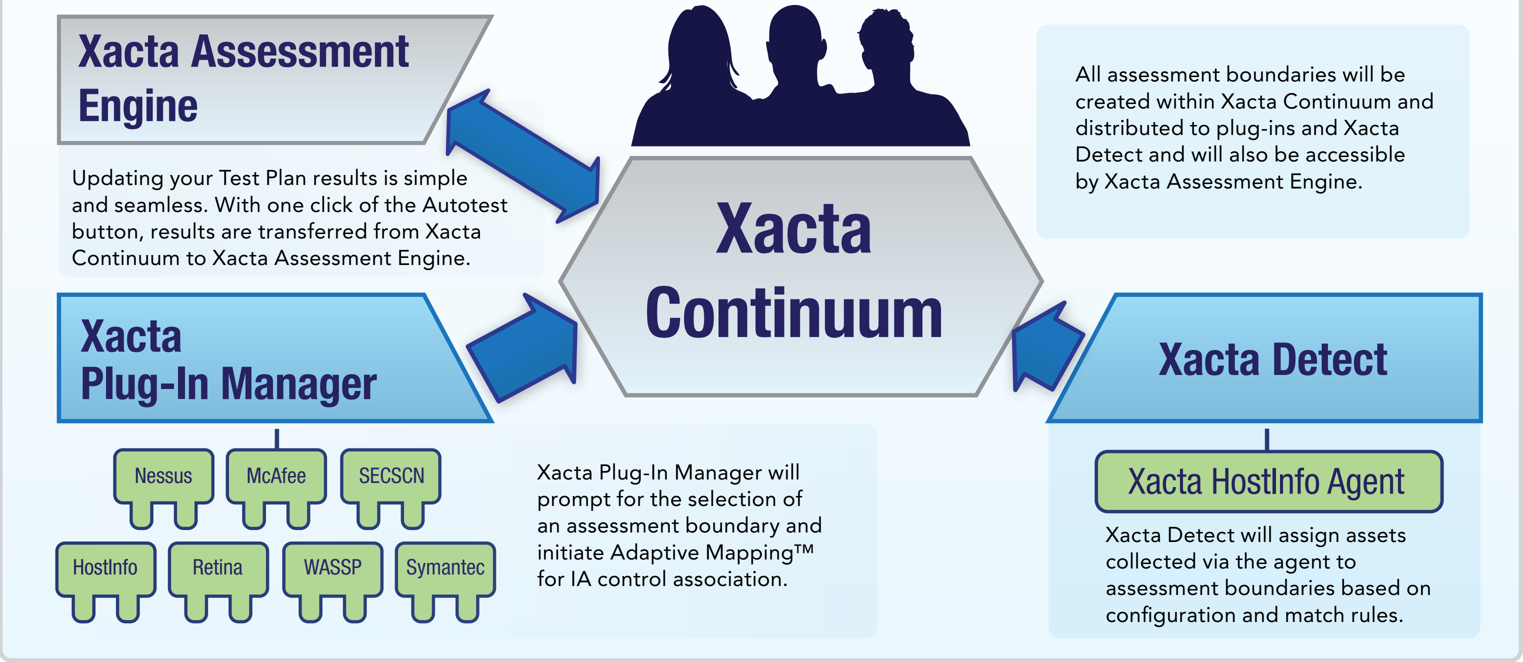
Telos introduced its patented continuous assessment functionality in Xacta IA Manager in February 2003. Today our cybersecurity personnel continue to monitor and protect some of the largest networks in the world and continually enhance the capabilities of Xacta IA Manager for today's continuous monitoring requirements.

Employing a patent-pending technology called Adaptive Mapping™, Xacta Continuum automates the complex task of mapping the results from IT asset scans to the associated IA controls such as NIST, DIACAP, ISO, and others. It takes scans from disparate sources, correlates the individual results on the fly, and allows the analyst to view the results in an aggregated manner so results for the same test from multiple sources can be analyzed side-by-side. You can then use these results to compare and determine if the ingested scanner results are valid.

Other key capabilities of Xacta Continuum include:

- **Vulnerability correlation** – Correlates vulnerability information from disparate scan sources so cybersecurity personnel can make more informed decisions and plan the appropriate next steps.
- **Remediation planning** – Facilitates the development of remediation plans of actions and milestones (POA&Ms) for individual issues and applies the POA&M to one or more assets based on assets-to-test relationships.
- **Security assessment result mapping** – enables consistent mapping of results from any security source across an organization or individual business unit.
- **Confidence scoring** – Association of results to IA controls are tracked, indicating to the security analyst how confident they can be in the Adaptive Mapping's analysis of control mapping.
- **Trending analysis** – Multiple testing cycles can be analyzed and compared to determine effectiveness of remediation efforts as well as rising areas for concern.

Xacta Continuum turns overwhelming streams of data into rich reports that you, your superiors, and your staff can immediately grasp.



Updating your Test Plan results is simple and seamless. With one click of the Autotest button, results are transferred from Xacta Continuum to Xacta Assessment Engine.

All assessment boundaries will be created within Xacta Continuum and distributed to plug-ins and Xacta Detect and will also be accessible by Xacta Assessment Engine.

Xacta Plug-In Manager will prompt for the selection of an assessment boundary and initiate Adaptive Mapping™ for IA control association.

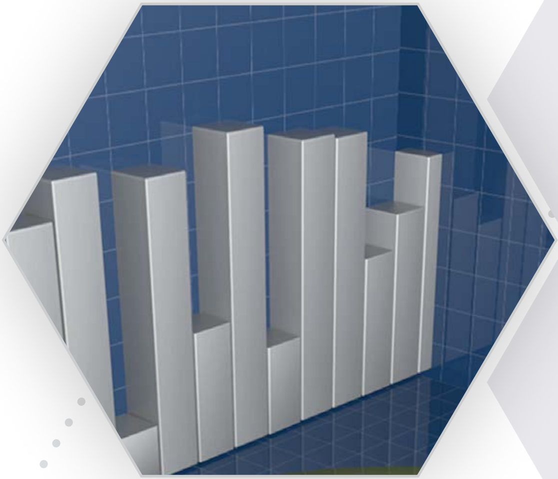
Xacta Detect will assign assets collected via the agent to assessment boundaries based on configuration and match rules.

Xacta HostInfo: Gather the information needed for security assurance. This family of platform-specific executables collects and provides security-relevant configuration information to the Xacta Detect server for assessment. Xacta HostInfo also supports NIST SCAP-validated testing capabilities to determine compliance with FDCC and other XCCDF checklists. HostInfo has the capability to communicate directly with Xacta Detect for fully automated collection of vulnerability and configuration results, which are then relayed to Xacta Continuum for compliance analysis and reporting. Xacta HostInfo is supported on Windows, OS X, and RedHat Linux.

Xacta Detect: Manages agent tasking and collects vulnerability and configuration data. Xacta Detect manages assets that have our Xacta HostInfo agent deployed on them. This allows our continuous monitoring suite to actively monitor those assets for security-relevant changes and passes that information to the Xacta Continuum console for further analysis to determine if the findings are associated and/or violate any security controls.

Contact Telos to begin planning your continuous monitoring program.

We look forward to applying our cybersecurity capabilities to your continuous monitoring requirements. Please contact us to begin a conversation about how we can help you keep your finger on the pulse of your cybersecurity posture.



Telos® Corporation
1-800-708-3567
sales@telos.com