Solutions Overview

noblis.org/runca

RunCyberAssurance®

with Noblis

Continuous Monitoring. Simplified.

A Premier Continuous Monitoring Application

noblis

For the best of reasons

Table of Contents

Technical Points of Contact

Abheek Sen

Solution Owner,
Solution Delivery Organization

abheek.sen@noblis.org

Andrew Lins

FedRAMP Program Manager

andrew.lins@noblis.org

Introduction

Maintaining the security of federal computing environments, whether on government networks or in the cloud, is an increasingly high-stakes challenge. Mandatory cybersecurity compliance standards and frameworks, such as those defined by the Federal Information Security Management Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP), include Continuous Monitoring (ConMon) as a key activity. To implement a successful ConMon program, agencies must typically define and implement an agency-specific process that satisfies the FISMA requirements in their unique environment, and then must capture, decipher, analyze and store a myriad of ConMon data, often with limited automation. As a result, many agencies struggle to manage their ConMon efforts.

Noblis' **Run***CyberAssurance* is a dynamic, robust network intelligence platform for ConMon. It significantly eases the burden faced by agencies in maintaining alignment with federal cybersecurity compliance standards. Its proven automation approach offers a fast, accurate view into the vulnerability and security posture of complex networked information systems, freeing cybersecurity professionals from mundane manual tasks and allowing them to focus on high-value threat assessment activities. Agencies can leverage **Run***CyberAssurance* as software-as-a-service (SaaS) or a customer-managed solution, and any agency that follows a Risk Management Framework such as FedRAMP can use it to improve its ConMon process.

***Run**CyberAssurance can improve the Continuous Monitoring workflow for federal agencies while maintaining alignment with cybersecurity compliance standards.*

Run*CyberAssurance* is a proven, powerful, secure tool that allows agencies to meet the most stringent ConMon cybersecurity compliance requirements. It gives agencies the ability to optimize, automate and streamline their ConMon efforts, minimizing the risk of human error and reducing the level of effort and cost needed to implement a successful ConMon program. Its automated dashboards and reports increase enterprise-wide visibility and facilitate effective threat detection. Because it accepts data feeds "as is" from over 45 industry standard vulnerability scanning tools and leverages existing personal identity verification (PIV) and common access card (CAC) for user authentication, it integrates easily into existing operations. **Run***CyberAssurance* also simplifies and speeds achievement of FedRAMP authorization and scales easily, without corresponding increases in staffing and cost. **Run***CyberAssurance* is a premier solution for low-risk, high-value automation of agency ConMon activities.

Government Challenge

Risk management programs that follow NIST 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, such as FedRAMP, require information systems to provide ConMon data for agency review on a monthly or more frequent basis. This includes vulnerability scan data, current system inventory and a POA&M. Agency experts must pull down the ConMon data and perform their own analyses, including:

- Comparing vulnerability scan data against FedRAMP, FISMA or agency-specific requirements
- Monitoring system architecture with the inventory
- Prioritize remediation based on severity and binding operating directives
- Tracking closure progress of outstanding open vulnerabilities in the POA&M

These analyses are typically performed manually. Manual data processing is slow and costly, with a higher chance of human error. With multiple systems and environments, agencies cannot easily correlate ConMon data between reporting periods or across different authorization boundaries to gain deeper insights into the data. Additionally, manual processing requires a greater level of effort as use of Cloud Service Providers (CSPs) scales up and becomes more complex. Our solution, **Run***CyberAssurance* was created to address these issues and provide a powerful, secure, automated tool that helps departments and agencies simplify and speed their ConMon analyses. Automation decreases processing time and increases the overall amount of ConMon data that can be managed with the same personnel, reducing the cost and level of effort required to manage the same amount of data.

The Noblis Solution

Run*CyberAssurance* automates the handling of structured data, minimizing the risk of human error, by using software "agents" to ingest and process monthly ConMon data from the vulnerability scanning tools associated with all information systems in all environments (on site and in data centers and the cloud). **Run***CyberAssurance* agents identify and process the structured ConMon data, ensuring that manual handling of that data is limited. By using agents that can be refreshed to process new data formats and collect data from new vulnerability scanning tools, **Run***CyberAssurance* can grow to accommodate various types of structured data, ensuring that as an organization's data requirements change, **Run***CyberAssurance* can accommodate those changes.

When used within the FedRAMP context, **Run***CyberAssurance* ensures continuous data monitoring, recording, measuring and tracking against FedRAMP requirements. Because **Run***CyberAssurance* leverages commonly used data formats, it easily ingests monthly ConMon deliverables, such as scan data from industry standard vulnerability scanning tools (e.g., Nessus, Retina, Qualys, etc.). Different types of alerts can be set to further track compliance and notify relevant stakeholders, resulting in their increased situational awareness. Additionally, **Run***CyberAssurance* can correlate ConMon data from different reporting periods, and across different authorization boundaries, with the results displayed on a single security dashboard. In addition to ConMon, **Run***CyberAssurance* also facilitates FedRAMP authorizations by extending the capability to ingest findings from assessments and non-technical sources. This allows for a complete, enterprise-wide picture of an organization's security posture, enabling early detection of and rapid reaction to trends and major events.

Run*CyberAssurance* is the only ConMon solution that supports over 45 vulnerability scans out of the box. Additionally, there is no other ConMon solution that fully meets FedRAMP's requirements for metric thresholds and reporting, nor is there another vendor with our unique FedRAMP positioning that enables multi-agency collaboration.

High-Level Architecture

Run*CyberAssurance* is deployed as a FedRAMP Moderate SaaS and can be deployed in a customer-managed environment in order to support an organization's unique requirements. The technical details discussed below pertain to configuration options. **Run***CyberAssurance* ingests scan data obtained both from automated sources (assessment and ConMon processes) as well as from manual sources (non-technical findings, zero-day vulnerabilities, etc.). All connections made to **Run***CyberAssurance* are secured via Transport Layer Security (TLS) version 1.2 or higher. Authentication security is bolstered by two-factor authentication, including PIV and CAC authentication, for which **Run***CyberAssurance* provides full support as specified by Homeland Security Presidential Directive 12 (HSPD-12).

As **Run***CyberAssurance* ingests and processes scan data, it notifies authorized users of any resulting configuration, compliance or vulnerability alerts. These authorized users can then access **Run***CyberAssurance* to view scan results and associated alerts, in order to determine the best course of action.

As RunCyberAssurance ingests and processes scan data, authorized users are notified of any resulting configuration, compliance or vulnerability alerts.

Run*CyberAssurance* also supports Role-Based Access Control (RBAC). With RBAC, permissions to perform certain operations, such as uploading scan data, are assigned to specific roles. Roles are defined as either advanced or basic. Advanced users can perform actions associated with a role, such as viewing data, uploading data within specific information system boundaries and creating new deviation requests. Similarly, administrators can perform advanced user actions, approve new users, set user privileges and create and assign groups and boundaries. Basic users, on the other hand, cannot perform these actions.

Run*CyberAssurance*'s reporting capability also provides summary views of an agency's portfolio of Cloud Service Offerings (CSOs), including detailed views of vulnerabilities, remediation activities, compliance issues and trends analyses. Report generation and agency collaboration capabilities ensure that deviation requests, significant changes and other risk management activities are effectively shared across all leveraging agencies for a given CSO.

Run*CyberAssurance* Key Features

Run*CyberAssurance* has several key features that provide stakeholders with insights into their security posture, helping them to make informed decisions. These include vulnerability management dashboards, consolidated continuous monitoring reports, performance management statuses and validated POA&Ms and inventories. The **Run***CyberAssurance* workflow is illustrated in Figure 1.

Figure 1: **Run***CyberAssurance Workflow*

Run*CyberAssurance* Vulnerability Management Dashboards

The **Run***CyberAssurance* Dashboard is a management-friendly, live dashboard that enables system administrators, information system security officers (ISSOs), information systems security managers (ISSMs), developers and other key stakeholders to view the most critical information in their computing environments.

- **Environment Six-Month Vulnerability Trends** – Tracks and measures changes in vulnerabilities
- **Top 10 Vulnerability Types (by frequency)** – Identifies the most common problems across the computing environment
- **Top 10 Vulnerabilities (by severity)** – Uses vulnerability risk and asset value/criticality to help determine which problems would have the greatest overall impact on the security posture of the computing environment
- **Top 10 Assets (by severity)** – Identifies which assets have the most serious vulnerabilities
- **New Hosts (last 15 days)** – Identifies any undocumented/unauthorized hosts on the network
- **Trending Authentication Tracking** – Tracks percentage of authentication success rates during scan
- **Scan Correlation with Compliance Documentation –** Correlates scan vulnerabilities with associated POA&Ms and inventory documentation, along with pending and active deviation requests

Consolidated Continuous Monitoring Report

The **Run***CyberAssurance* portfolio and single-system dashboards are illustrated in Figures 2 and 3, respectively. The **Run***CyberAssurance* portfolio dashboard provides a chief information officer view of an organization's risk posture by displaying metrics across the entire portfolio of systems that an organization uses. Additionally, this dashboard provides in-depth reporting of high-risk vulnerabilities, insecure assets and more across the entire portfolio. The single-system dashboard view displays meaningful analytics that capture metrics across each IT system, including performance management status, compliance with emerging security directives, the number of vulnerabilities (ranked by severity) that exceed a defined baseline and the number of vulnerabilities that remain un-remediated or un-mitigated within a required timeframe.

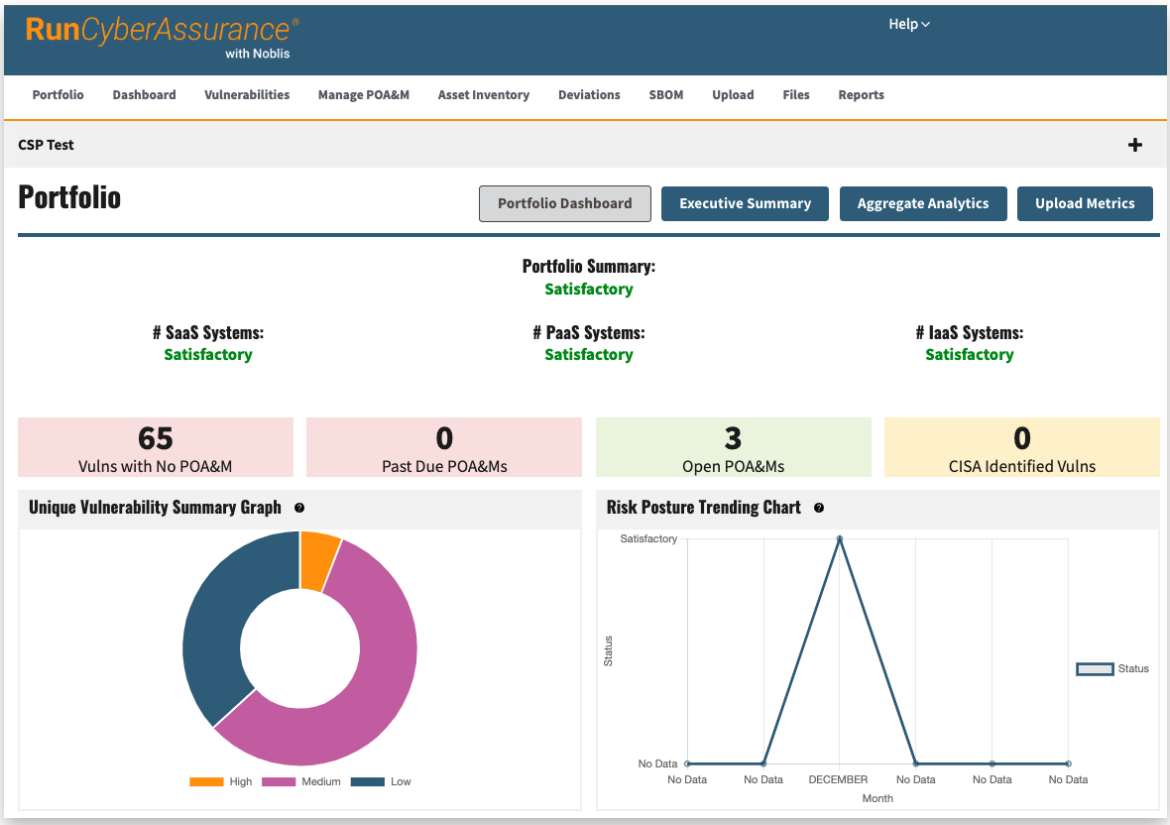


Figure 2: Portfolio Dashboard

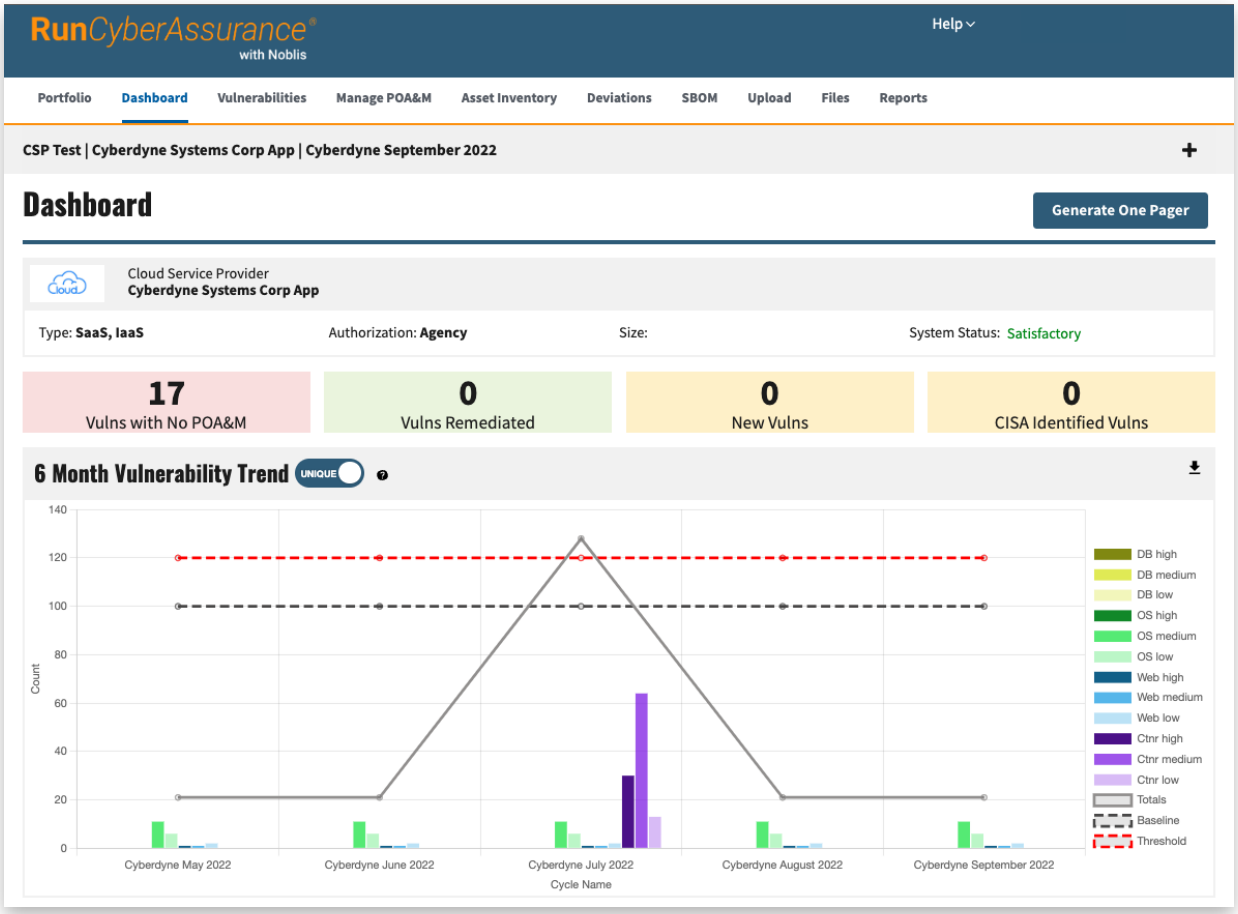


Figure 3: Single-System Dashboard

Performance Management Status

Run*CyberAssurance* automatically tracks security program metrics in near real time, promoting a high degree of accountability and transparency for compliance achievement. Customizable, automated reports can be tailored to capture information considered most relevant to analyst or decision-maker needs and can be scheduled for delivery to key staff on a daily, weekly, quarterly or other basis. Broad reporting highlights changes to the network, while demonstrating security program effectiveness. Monthly management statistic summaries enable more informed decision-making. Automated reporting supports platform and infrastructure scalability without proportionate staff and cost increases for ConMon activities.

Maintain Compliance with Emerging Security Directives

Run*CyberAssurance* facilitates compliance with emerging and developing security directives by:

- Enforcing security workflow
- Assisting compliance activities (FISMA, NIST SP 800-53, FedRAMP, etc.) by exporting required data into automated, usable tools, such as Microsoft Excel

- Fully supporting PIV/CAC authentication per HSPD-12
- Delivering alert messages to defined recipients in an encrypted and digitally signed format
- Reducing staff burden while preparing agencies for emerging, automated reporting compliance standards

Cloud-Based Software Optimizes Availability and Security

Run*CyberAssurance* provides a web-facing login portal that is accessible from anywhere. It offers secure, multi-factor authentication and a tiered user schema that enables privileged or standard access to data.

Validated Inventory and POA&M Tracking

Run*CyberAssurance* maintains a record of the approved security inventory baseline (Figure 4). After a vulnerability scan, algorithms compare scan results against the last approved security inventory baseline. This is known as a positive security model. Any deviation from the approved baseline configuration is treated as a configuration vulnerability. Owners of non-compliant assets are notified of the discrepancy via the use of the **Run***CyberAssurance* "Asset Inventory" Tab.

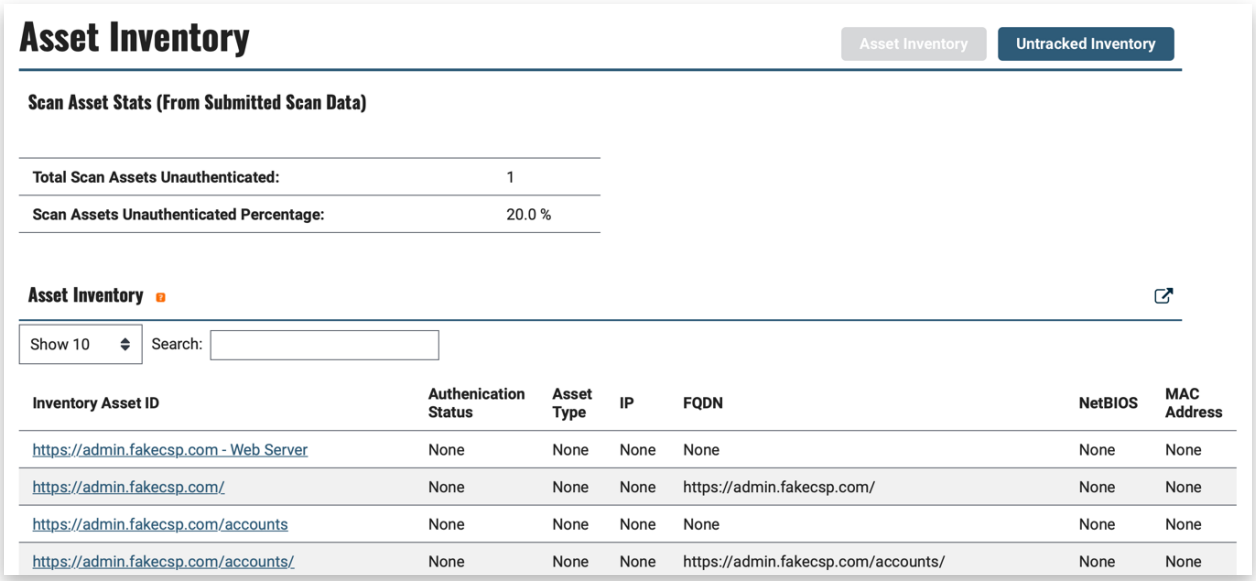
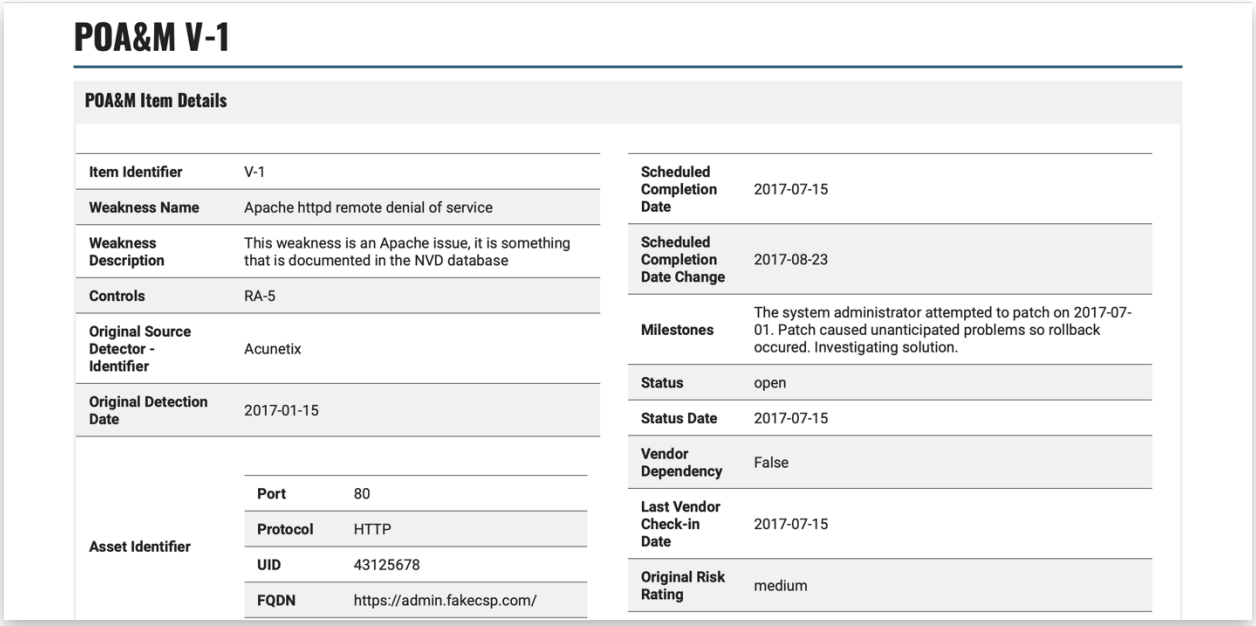


Figure 4: Asset Inventory

Run*CyberAssurance* also facilitates convenient tracking of progress against the POA&Ms, as shown in Figure 5. By correlating scan vulnerabilities with associated POA&Ms and Inventory documentation, along with pending and active deviation requests, **Run***CyberAssurance* enables managers to quickly and easily spot problems requiring attention.



POA&M V-1

POA&M Item Details

Item Identifier	V-1
Weakness Name	Apache httpd remote denial of service
Weakness Description	This weakness is an Apache issue, it is something that is documented in the NVD database
Controls	RA-5
Original Source Detector - Identifier	Acunetix
Original Detection Date	2017-01-15
Asset Identifier	**Port** 80 **Protocol** HTTP **UID** 43125678 **FQDN** https://admin.fakecsp.com/

Scheduled Completion Date	2017-07-15
Scheduled Completion Date Change	2017-08-23
Milestones	The system administrator attempted to patch on 2017-07-01. Patch caused unanticipated problems so rollback occured. Investigating solution.
Status	open
Status Date	2017-07-15
Vendor Dependency	False
Last Vendor Check-in Date	2017-07-15
Original Risk Rating	medium

Figure 5: POA&M Details

Summary of Run*CyberAssurance* Benefits

Run*CyberAssurance* is a robust solution for government ConMon efforts, with more than a decade of proven performance monitoring the security of government computing and web environments. Its benefits are summarized below.

Time and Cost Savings

Run*CyberAssurance* saves its users both time and money, allowing the same number of staff to manage more systems and data by:

- Streamlining data comparison analysis across various FedRAMP authorization documents to ensure consistency
- Reducing time from development to a FedRAMP Authorization for agencies, CSPs and third-party assessment organizations (3PAOs)
- Simplifying and speeding the process for managing thousands of information systems
- Automating reports to allow platform and infrastructure scalability without proportionate staff and cost increases
- Reducing cost by leveraging PIV and CAC card authentication

Integration with Popular Tools & Technology

Run*CyberAssurance* leverages existing investments in vulnerability scanning tools by automatically ingesting and processing data from 22 industry standard vulnerability scanning tools, the only product on the market with this capability. Additionally, **Run***CyberAssurance* software agents can be easily updated to consume data from updated and new scanning tools, keeping the platform evergreen.

Standardized Data Management

Run*CyberAssurance* works with standardized and fixed data sets, allowing automation to be used to improve the user experience. Automation capabilities include:

- Dashboard views of high-priority vulnerabilities that need attention or investigation
- Display of trend analyses of historical data gathered through ConMon
- Management of ConMon assessment and authorization documents, including POA&M and Security Assessment Report (SAR) artifacts
- Exportable table and graph data in common file formats, such as comma-separated values (CSV)

Deployment Flexibility

Because **Run***CyberAssurance* is deployed as a FedRAMP moderate SaaS client and can be deployed on a customer-managed environment, it optimizes availability and security using:

- A web-facing login portal that is accessible everywhere
- Multi-factor authentication
- A fixed user schema that enables privileged or normal access to data

These benefits make **Run***CyberAssurance* a unique and powerful platform for facilitating and increasing the value of the ConMon activities required by government standards and frameworks. It can be easily integrated into exisiting operations environments and reporting structures, and updated quickly to take advantage of evolving tools and data streams. It improves decision support and saves scarce resources, with less risk, greater speed and better confidence in results. **Run***CyberAssurance* is a premier ConMon solution for government users.

About Noblis

We exist to enrich lives and make our nation safer with our shared passion for excellence and innovation.

For more than 25 years, Noblis has been an innovator within the federal government, committed to solving the challenges of today and investing in the mission of tomorrow. As a nonprofit, Noblis works for the public good, bringing together the best possible capabilities, including science and technology expertise and solutions, in an environment of independence and objectivity to deliver enduring impact on federal missions.

Working with Us

Government agencies can access Noblis through a variety of contracting mechanisms. We have several contracts in place and available to Government agencies. We are also a GSA Schedule holder.

For a full list of vehicles, visit **noblis.org/contracting** or call us at 703.610.2000. Email us at **answers@noblis.org**.