# Research Center Improves Visibility and Cyber Threat Mitigation

MARS Suite empowers a paradigm shift in how a government propulsion research center manages cyber threats.

## The Challenge

The Government Propulsion Research Center in this customer story has a complex network configuration comprised of over 10,000 workstations, over 3,000 servers, and thousands of other networking related devices divided into the private research center domain, private data center domain, and the public data center domain. This environment also includes air-gaped labs and extended environments like an operations and support center, a space science and technology center, and a test area network, each of which pose unique cybersecurity challenges.

The Center encountered several issues with identifying and managing threats due to the size and complexity of this environment. Vulnerability and threat data were not being utilized properly due to incompatible toolsets. The inability to assign findings quickly and accurately to the correct organization allowed threats to remain unmitigated for extended periods of time.

Cybersecurity personnel, systems owners, and administrators became overwhelmed with trying to identify and manage the many thousands of vulnerabilities against the Center, then mitigate those that posed the highest risk. Those responsible for managing vulnerabilities found themselves in a constant battle of trying to manage threat surfaces with spreadsheets while manually tracking vulnerabilities from week to week.

Vulnerabilities with approved Plan of Actions and Milestones (POAMs) and Risk Based Decisions (RBDs) became burdensome to manage due to the incompatibility of the disparate tools housing the data. Furthermore, all assets were being treated with the same criticality due to limitations within the toolsets. This frequently hindered management and administrators from being able to recognize and understand the true, comprehensive risk picture.

## The Solution

Personnel from both All Points and Mission Multiplier, the driving forces behind the development of MARS Suite, were already integrated into the Center's IT security team. These personnel had an intimate understanding of the challenges presented by the Center's network, and turned to MARS Suite to address these challenges.

MARS Suite is a DoD-approved and NIAP tested cybersecurity product that provides the continuous cyber monitoring and enterprise risk management capabilities that the Center needed. MARS Suite enables increased operational efficiencies by simplifying cyber risk management decisions. Its integrated platform delivers a comprehensive view of an organization's real-time cyber risk posture. It capitalizes on this increased visibility by simplifying protective task prioritization and assignment with letter-grade scoring of enterprise cybersecurity risk elements.

Through these functionalities, MARS Suite was poised to provide the Center with comprehensive real-time situational awareness, detailed asset visibility, and a simpler way to dynamically combat cyber threats and mitigate vulnerabilities. It would also provide an opportunity for the Center to leverage legacy infrastructure into a single comprehensive solution, a functionality that was imperative given the Center's complex environment.

### The Challenge

- Account for complex network configuration
- Identify and manage threats in a timely manner
- Reduce workload for cybersecurity personnel
- Aggregate data from disparate, incompatible security tools
- Simplify management of vulnerabilities with POA&Ms and RBDs

### The Solution

- MARS Suite dynamic risk scoring dashboard with Asset, Threat, and Vulnerability Management capabilities

### The Results

- Significant labor and time savings
- Enabled a paradigm shift away from volume-based threat mitigation
- Provided real-time insights into the Center's cyber posture
- Created a constantly maintained list of actionable items concentrated on unaddressed threats

# Research Center Improves Visibility and Cyber Threat Mitigation

MARS SUITE

## The Results

MARS Suite has been in use at the Propulsion Research Center since 2019, demonstrating seamless integration with legacy systems, scaling dynamically to fit the Center's needs, and significantly simplifying resource allocation.

After integration into the Center's network, MARS Suite provided a Common Operating Picture for Center management, cybersecurity personnel, and administrators. Immediately after the integration of MARS Suite, Center personnel were able to associate vulnerability findings with asset criticality, risk levels, and exposures, and integrate RBD and POAM information. These new abilities made it possible to reduce strain on both system administrators and cybersecurity personnel.

MARS Suite is assisting the Propulsion Research Center monitor its cybersecurity posture by:

- Presenting cybersecurity data in three key cyber domains: Asset, Threat, and Vulnerability Management

  ***Note:*** *The Incident Management domain has also been included in the base product since the original installation at the Center.*

- Populating dynamic dashboards with real-time insights into the Center's cyber posture
- Aggregating data from the National Vulnerability Database to provide the Center with up-to-date threat data based upon near real-time exploitation trends relevant to its systems and network
- Quickly identifying all systems related to a specific threat
- Associating risks across all organizational units with the related vulnerabilities, threats, or assets
- Maintaining a list of actionable items concentrated on threats that have not yet been addressed
- Categorizing assets in terms of value and scan status

> *MARS Suite does exactly what we need it to do. We've seen significant labor and time savings.  MARS meets our requirements, from the analysts all the way up to the C-suite. We are much more effective at working on the data, managing vulnerabilities, and reporting status to leadership.*
>
> CISO of the Propulsion Research Center

MARS Suite positively influenced the way the Center identifies and responds to threats. By helping give system administrators and cybersecurity professionals the ability to easily identify, prioritize, and focus on the Center's most critical cyber risks, MARS Suite has enabled a paradigm shift away from volume-based threat mitigation, helping the Propulsion Research Center to keep the nation's space program on track and its systems safe and secure.

### About MARS Suite

The MARS Suite solution is NSA NIAP tested and DoD JTIC approved. It was developed by a team that brings together organizations and industry experts with a depth of pertinent cyber knowledge, a breadth of diverse skillsets, and years of relevant domain expertise. This unique combination enables the team to develop, deploy, and operate cyber solutions in some of the most challenging and sensitive government, defense, civilian, critical infrastructure, and commercial environments. MARS Suite leverages Human Centered Design (HCD) Methodology to deliver solutions that not only leverage an organization's existing investments in infrastructure, but also the personnel, depth of organizational knowledge, and inimitable understanding of unique institutional workflows that they possess. More information is available at marssuite.com.

**Contact the MARS Suite team:**

missioncontrol@marssuite.com | (256) 298-9124