RGS
Rancher Government Solutions

Technical Brief

Rancher Government Carbide™

Unmatched Kubernetes Supply Chain Security and STIG Compliance for the Federal Government

Rancher Government Carbide™ (RGS Carbide™) is layered on top of Rancher Kubernetes to provide government IT teams with two additional layers of security as well as documentation for air-gapped environments.

CARBIDE

Securing the Supply Chain

With software supply chain hacking on the rise, proving provenance in its software components is critical to the Federal Government. RGS Carbide™ addresses this issue with its Secure Software Pipeline. The Secure Software Pipeline built into RGS Carbide™ provides government IT teams the following:

Provenance Assurance. Proof that images acquired by government IT teams are those provided by RGS. This provenance will be secured and maintained via signed keys.

Vulnerability Scans. Every RGS Carbide™ provided image will be subject to a series of security analyses and gate-checks to ensure security compliance.

Software Bill of Materials (SBOM). A docker-registry with a detailed and verifiable list of all software components that provides end-to-end supply chain integrity for a clear path to compliance.

Automating the STIG Compliance Assessment Process

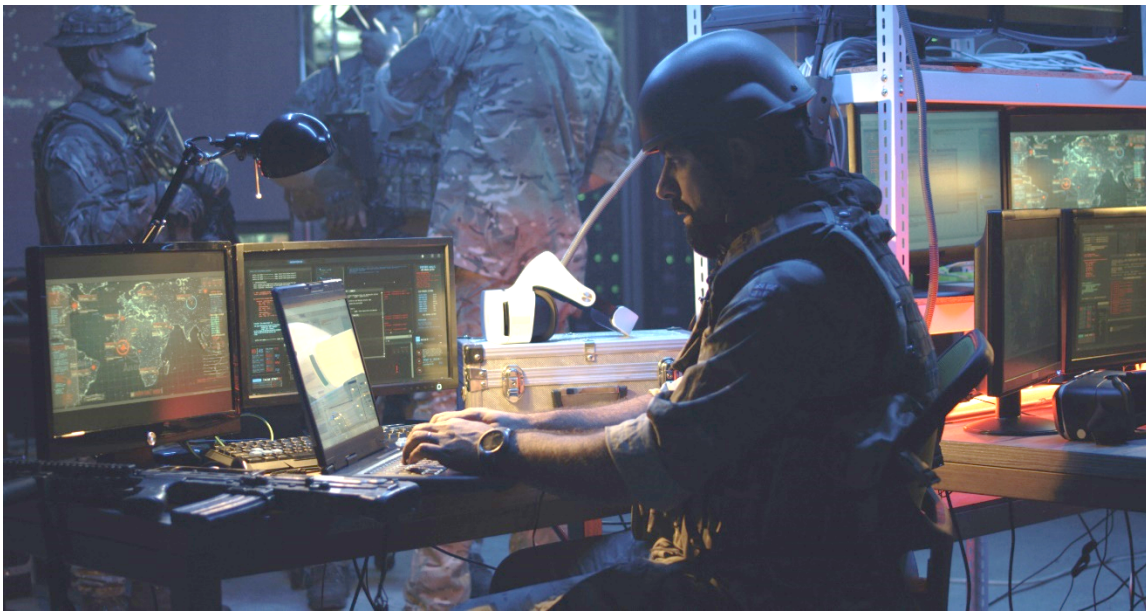
Proving security compliance in the Federal Government is very difficult and often time-consuming. The RGS team built Stigatron™ into RGS Carbide™ to make the process of proving STIG compliance easier. Stigatron™ provides STIG compliance validation for your current cluster and downstream RKE2 and Rancher Multi-cluster Manager (MCM), both of which have been validated by the Defense Information Systems Agency (DISA).

STIGATRON

With Stigatron™, RGS has essentially replaced the traditional manual process where a government cyber auditor comes and sits behind an IT team member while he or she walks through the system clicking buttons and looking for what the auditor needs. Stigatron™ automates most of this process, essentially giving the technical person the ability to quickly provide the cyber auditor exactly what he or she needs to prove STIG compliance.

Providing Robust Documentation to Better Support Air Gap Environments

Air gap environments restrict computers or computer networks from connecting to unsecured networks, making accessing Kubernetes documentation on the internet impossible. Anyone who has worked in an air gapped environment knows how painful it can be to troubleshoot issues without internet or documentation access. To resolve this issue, Carbide packages all existing Rancher documentation and makes it consumable to those working in air gap environments. In addition, RGS is streamlining the packaging of the documentation back into the Rancher product as a bolt-on.



RGS Carbide Subscription Details

Every Rancher Government Carbide™ subscription includes the following RGS products and services:

- **Best in Class Enterprise Support** – A team of mission-experienced open source, Kubernetes engineers who provide technical support to civilian, DoD, and intelligence communities. Because RGS understands how sensitive the US Federal Government is to foreign influence, our development and support teams are all US-born and US-based, and many hold security clearances, up to top-secret.

- **Secure Software Pipeline** – A secure pipeline modeled after the DoD Iron Bank registry strategy that provides provenance back to RGS, vulnerability scans, and a Software Bill of Materials (SBOM).

- **Stigatron™** – A 365-day security compliance monitoring tool that looks for vulnerabilities in your downrange clusters and alerts you to anomalies, while also allowing you to export those scan results in industry-standard formats. Stigatron™ can be used in two ways:

    - **On-demand** – At the beginning of a new project or any time throughout its lifecycle, you can trigger a Stigatron™ scan and export the results to be read by a tool your cyber auditor will understand.

    - **Scheduled Scans** – You can also set up scheduled scans in Stigatron™ that will run automatically.

- **Offline Documentation for Air Gap Environments** – All existing Rancher documentation will be packaged and sent with the RGS Carbide™ launch.

- **Improved, Tailored Rancher MCM Dashboard** – An updated Rancher MCM user dashboard that lets you manage all Rancher products from within one interface. When you install RGS Carbide™ several additional icons will pop up in the dashboard display. These additional items include:

    - **Secure Software Pipeline** – Items relevant to the Secure Software Pipeline that deploys with RGS Carbide™.

    - **Stigatron™** — Items pertaining to Stigatron™ setup, scan, and export.

    - **Offline Documentation** – Access to offline Rancher documents.

- **World-class Training & Certifications** – A robust training portfolio for self-paced cloud-native learning with certifications in CKA, CKD, CKS and others — offered in partnership with The Linux Foundation. Each RGS Carbide™ license comes with a 1-seat training license as well as a certification program for one designee with The Linux Foundation.

RGS Carbide
A Deeper Dive

The Benefits of RGS Carbide™ as a "Bolt-on"

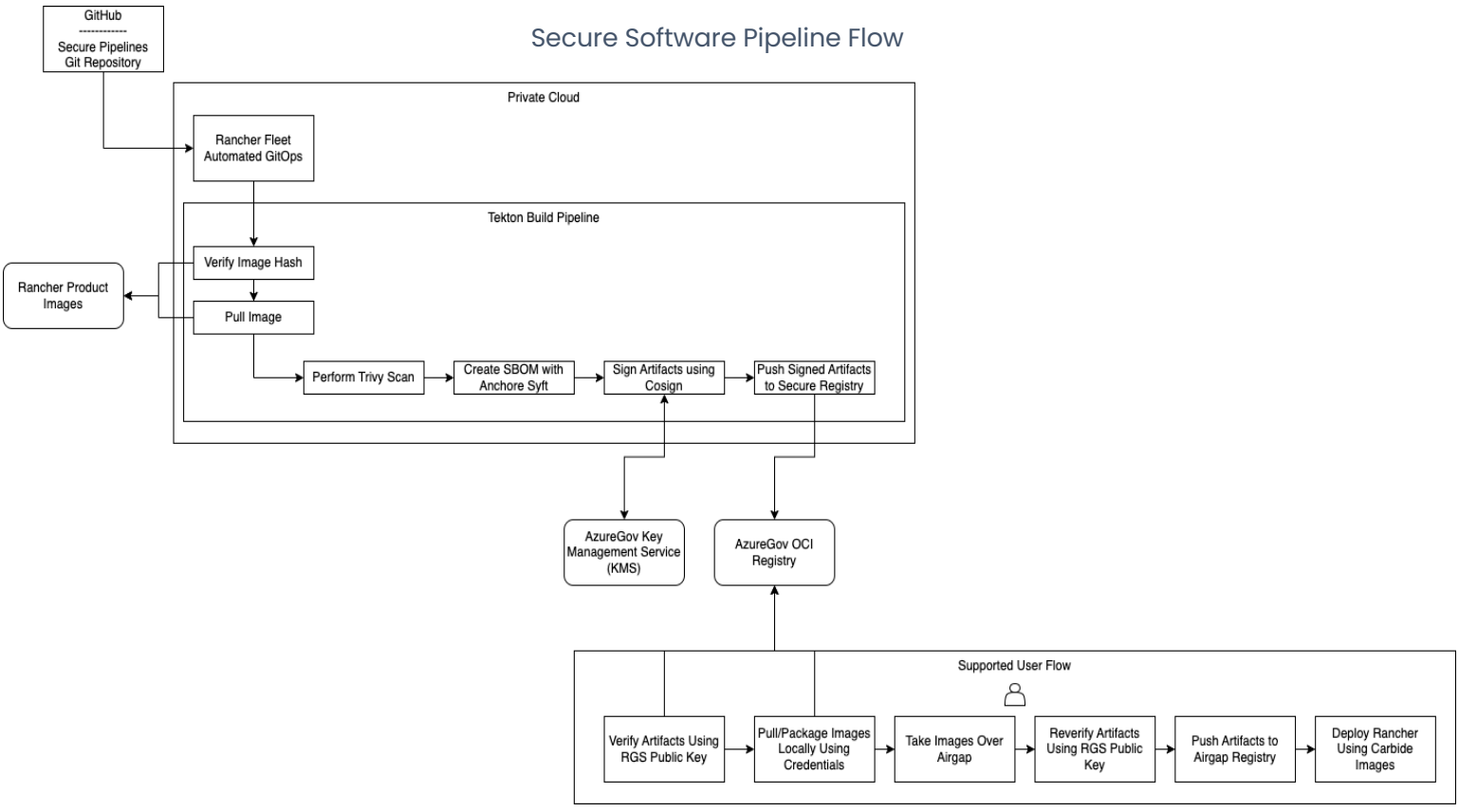
In creating Rancher Government Carbide™, we wanted to ensure that its release would not affect existing deployments, so we built it without forking or changing any upline Rancher products. This means that existing clients can install and deploy RGS Carbide™ without making any changes to their existing architecture.

The Power of a Secure Software Pipeline

RGS Carbide™ provides government customers with the most secure and transparent Kubernetes supply chain on the market through its Secure Software Pipeline which ensures containers and assets are SLSA Level 3 compliant. The RGS Carbide™ Secure Software Pipeline is built using Microsoft Azure Government and performs the following tasks:

- **Build.** All Rancher-owned images are recompiled by RGS.
- **Scan.** Every image will be subject to a series of security analyses and gate checks to ensure compliance.
- **Notarize.** All assets built by RGS Carbide™ will be digitally signed to validate the integrity and provenance of all software.
- **Host.** By leveraging the DoD Iron Bank registry strategy, RGS Carbide™ customers will get their containers and assets from RGS directly, **not** the FOSS public endpoints.

Secure Software Pipeline Flow



Accelerate Security Compliance with Stigatron™

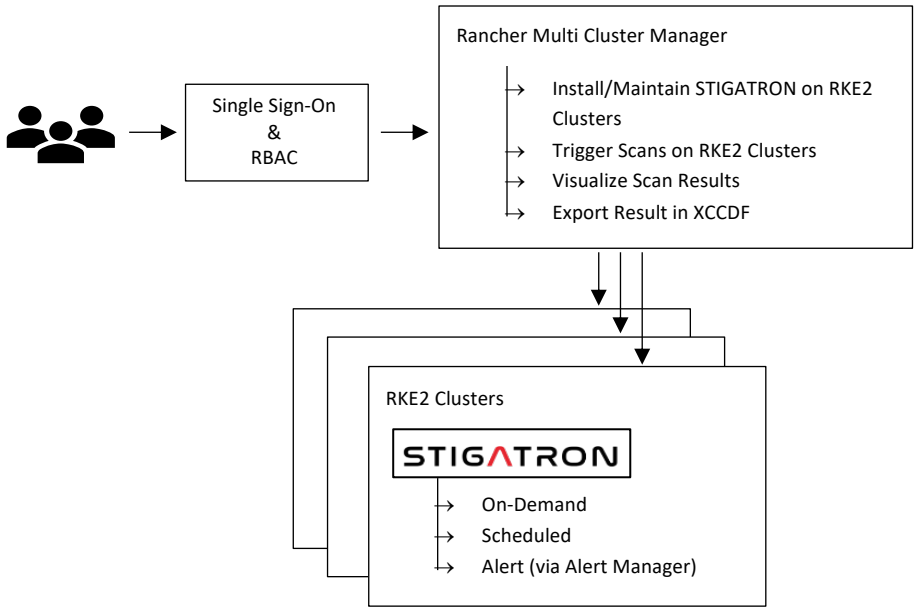
US Federal Government customers typically rely on their internal IT operations teams to ensure their Rancher Kubernetes clusters are STIG compliant at install and whenever a CISA cyber auditor requires proof. Obtaining proof of compliance is time-consuming because most operations teams wait until a request is made to certify their clusters. This "wait until they ask" approach also potentially introduces risk since STIG compliance is not re-evaluated on an ongoing basis as things change in software components. RGS Carbide™ minimizes this time-intensive process and the inherent risk it brings with Stigatron™.

Stigatron™ is a cluster monitoring and notification tool designed to provide on-demand and scheduled transparency into software vulnerabilities. Stigatron™ helps you keep watch over your downrange Rancher Kubernetes clusters, alerting you when they are not STIG compliant and freeing up your IT operations team to focus on higher value tasks.

Stigatron™: How it Works

Stigatron™ is deployed in Rancher Multi-cluster Manager. When initiated, either via an on-demand scan request or a scheduled scan, Stigatron™ will start a Kubernetes job and has access rights to scan your downrange clusters. It will evaluate all clusters against the STIG controls established in RKE2 and MCM. Once the scan is complete, Stigatron™ will create a map in Kubernetes and will spin up a visualizer cloud to provide an access point for your team to view the results. All this backend processing is made transparent through the Rancher MCM user dashboard, which has been upgraded to include Stigatron™ with the release of RGS Carbide™.

It is important to note that because Stigatron™ works through Rancher Multi-cluster Manager, it will inherit all the security settings established within the manager via your role-based access controls.



Integrate Stigatron™ Notifications with Other Security Monitoring Tools and Dashboards

Stigatron™ works with your existing security infrastructure. Using our export function, Stigatron™ scan results can be exported and read into most security monitoring tools. After a scan is complete, not only will you be able to view the results within the enhanced Rancher MCM dashboard that will deploy with RGS Carbide™, but also, you'll be able to quickly export the scan results into all the traditional federal systems that the cyber auditors use. This helps ensure cyber auditors review the scan results in tools they understand, thereby making the audit process faster and easier.

RGS Carbide™ is Compliant with SLSA Level 3

While there is no SLSA Level 3 certification, RGS has ensured that RGS Carbide™ was built to be SLSA Level 3 compliant.

Planned Future Releases

While future releases of RGS Carbide™ are continuously evolving, some of the items we have on our radar include:

- **Custom STIG Compliance Assessment.** In the future, the RGS Carbide™ team would like to allow government customers to upload their own STIGs and have Stigatron™ assess compliance against these customer-specific STIGs.
- **Secure Software Pipeline Improvements.** RGS Engineers are also working to continually harden the images they provide, including upstream images.
- **Air Gapped Rancher Multi-Cluster Manager.** Additionally, RGS has plans to deploy an air gapped Kubernetes cluster with a minimized feature set offered in the Rancher MCM dashboard, so that edge-deployed military and intelligence personnel can complete basic tasks like restarting workloads without having to be Kubernetes experts.

About Rancher Government Solutions

Rancher Government Solutions (RGS) is specifically designed to address the unique security and operational needs of the U.S. Government and military as it relates to application modernization, containers, and Kubernetes.

Rancher is a complete open source software stack for teams adopting containers. It addresses the operational and security challenges of managing multiple Kubernetes clusters at scale, while providing DevOps teams with integrated tools for running containerized workloads.

RGS supports all Rancher products with US based American citizens with the highest security clearances who are currently supporting programs across the Department of Defense, Intelligence Community, and civilian agencies.

To learn more contact us at info@ranchergovernment.com or 844-RGS-7779.