Rancher Government Carbide

Secure the software supply chain.

RANCHER GOVERNMENT CARBIDE

Challenges

Securing the software supply chain is mission critical to the federal government, particularly after the 2020 SolarWinds breach and the increasing frequency of attacks. Given Cybersecurity Executive Order 14028, the ongoing risk of software supply chain attacks, and the criticality of software to daily operations, balancing security with innovation is essential to accelerating government missions. Furthermore, agencies must ensure software is free of vulnerabilities while identifying and tracking third-party components through software bills of materials (SBOMs).

Validating security and compliance within the Kubernetes ecosystem is often complex to navigate in the federal space. Infrastructure and clusters must be maintained at a certified level of security. While increasing agility and accelerating application development are key initiatives, limited tooling exists to help government agencies succeed in their DevSecOps missions.

For these reasons, RGS has developed Rancher Government Carbide, built to overcome:

- *Continuing attacks on the software supply chains*
- *The inability to link supply chain security with vulnerability assessments and software bills of materials*
- *Difficulty validating that Kubernetes infrastructure and clusters adhere to certified security levels*
- *Keeping pace with and meeting standards for federal-specific requirements*
- *Grappling with the lack of standardized tooling around software supply chain security*

Key benefits

Carbide

Secure the software supply chain by verifying provenance back to a specific entity.
Carbide further augments supply chain security through vulnerability assessments and generating SBOMs, both for Rancher software and its dependencies. This ensures the tools used and deployed within sensitive environments can be verified for compliance and security requirements.

Accelerate manual software security & validation processes.
Establishing and maintaining compliance with the security standards of the federal government is simplified, thanks to the ability to scan downstream clusters automatically. Plus, automating manual processes optimizes and refocuses staff.

RGS Support Subscription

Depend on a technology agnostic approach.
With a broad array of certified integrations, using additional software with Rancher Multi-Cluster Manager is easy. Customers can freely utilize all the leading-edge technologies that support government agency missions, create mission-specific environments, and use microservices to innovate.

Gain access to advanced Kubernetes expertise on demand.
The need to acquire expensive talent is eliminated, thanks to a team of specialized engineers with the highest-level security clearance. When it comes to large container environments with classified workloads, specialized talent is critical – which is why it is part of the package.

Solution

Rancher Carbide is an add-on support capability to the existing Rancher products suite. It is designed to assist supported customers with overcoming the challenges of application modernization, containers, and Kubernetes unique to the U.S. government and military. Carbide delivers cutting-edge capabilities to enable software supply chain security and support federal security and compliance requirements.

Carbide simplifies Kubernetes management by providing a better, more standardized way for users to verify and validate software. Its pipelines utilize tools for vulnerability scanning and generating SBOMs. Furthermore, it supports the first and only Kubernetes management platform and distribution with STIGs validated and published by DISA (Rancher MCM 2.6 & RKE2).

Capabilities

Software supply chain security

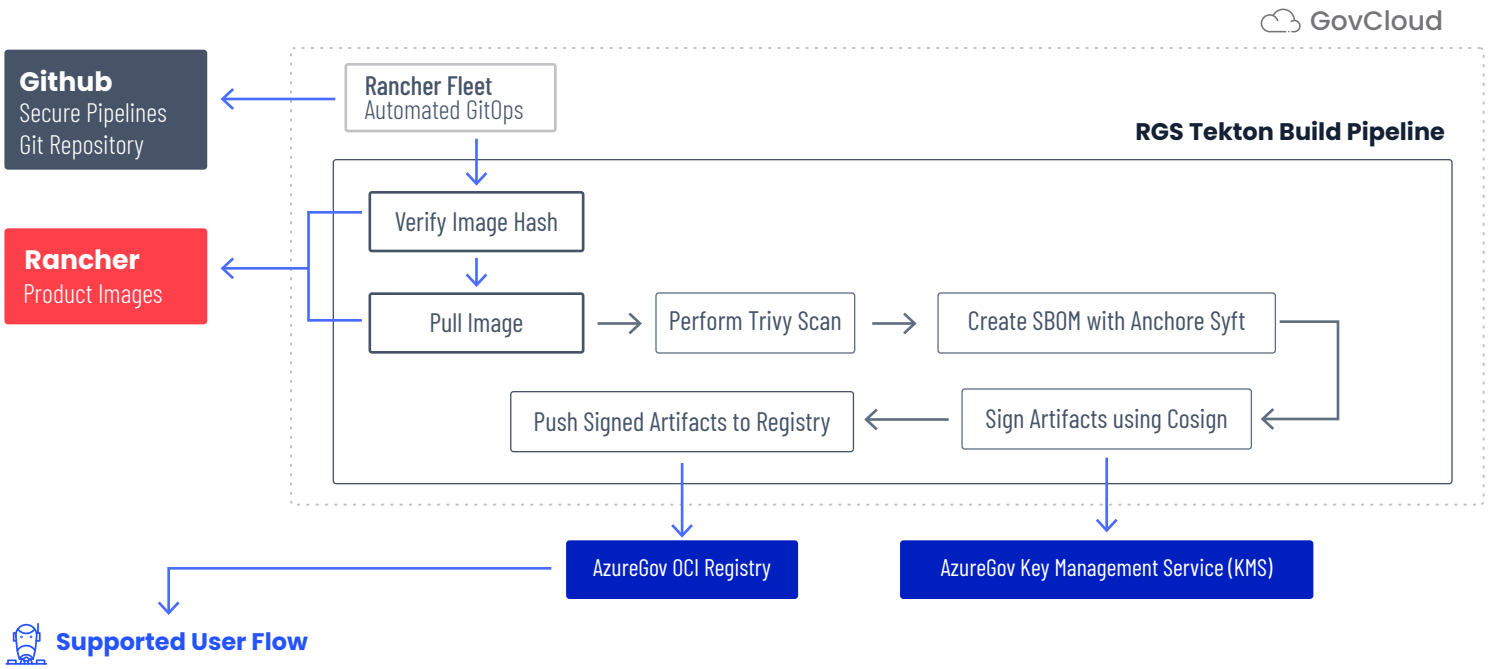
Enabled by Carbide Secured Registry (CSR)

CSR enables software supply chain security by providing a centralized secure container registry to end users, validated by a secured signing key.

Not only are users able to validate and verify the software itself, but also the vulnerability scan and SBOM in order to easily, reliably prove they are from Rancher.

- *SLSA (supply chain levels for software artifacts) level 3 compliant pipeline*
- *Software bill of materials (SBOM), vulnerability scans, attestations, and verifiable digital signatures for the entire Rancher portfolio*

Secure software pipeline flow



Supported User Flow

Verify Artifacts Using RGS Public Key → Pull/Package Images Locally Using Credentials → Take Images Over Airgap → Reverify Artifacts Using RGS Public Key → Push Artifacts to Airgap Registry → Deploy Rancher Using Carbide Images

Airgap documentation

Troubleshooting technical issues within an airgap environment is a difficult undertaking. To eliminate the headaches of working without external connectivity, Rancher provides airgap capable access to documentation for the entire Rancher product suite, including Carbide.

Customers can easily use Carbide over the airgap, deploy it into airgap environments, and access Rancher documentation which remains queryable, searchable, and indexable. Airgap documentation also extends out to the edge for customers working with small form factor devices in the field.

Capabilities

Edge capabilities

At Rancher Government Solutions, the edge is a first-class citizen. Rather than retrofitting tools to work in an edge environment, Rancher technologies are built for the edge from the start. DevSecOps teams are empowered to deploy full Kubernetes capabilities in resourced constrained environments.

DISA STIG certification

Rancher Government Solutions is the only company with approved Kubernetes management platform and distribution STIGs officially recognized and published by DISA (MCM 2.6 & RKE2).

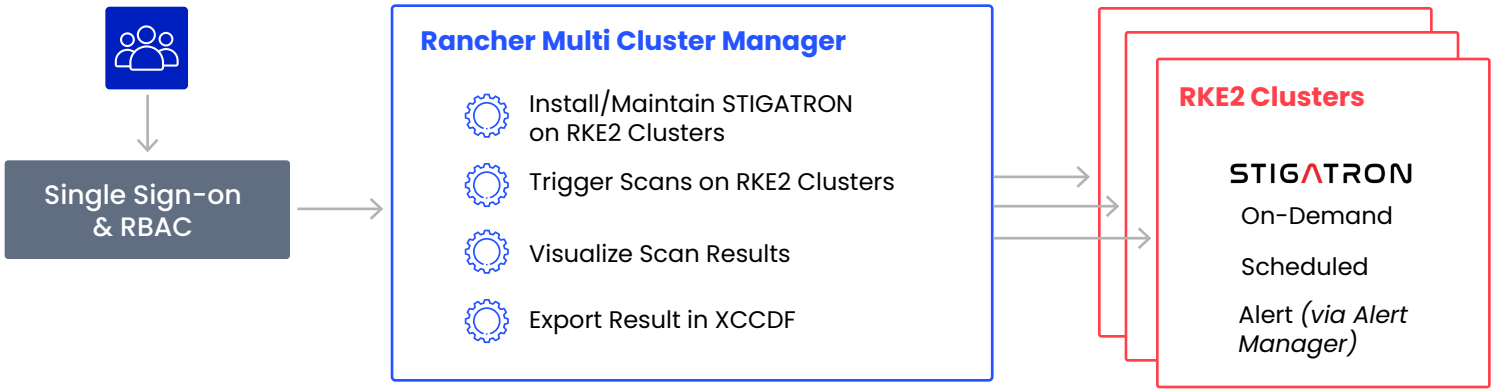
As opposed to retrofitting technologies to meet federal requirements, Rancher products are developed specifically for the federal government and its unique security needs. Furthermore, Rancher provides both the STIG itself and extensive tooling to support it. This allows customers to simplify the process of validating that clusters are in the correct state.

STIGATRON

Monitor and validate
the DISA STIG integrity of downstream RKE2 Kubernetes clusters

Empower
system administrators to refocus their time on more meaningful initiatives

Streamline
cyber auditing and compliance processes



STIGATRON is a tool within Carbide built to validate downstream clusters from the centralized Rancher Multi-cluster Manager. By automatically scanning downstream clusters and comparing them to the STIG cluster, STIGATRON alleviates the manual obstacles system administrators face in the validation process, enabling compliance with the security standards of the federal government.

STIGATRON also includes live compliance reporting, monitoring, and alerting. The need for a manual, checklist-oriented procedure is replaced with an automated process which performs scans and provides exportable artifacts in common cyber compliant formats (XCCDF). As a result, cyber assessors can easily ingest scan results without manual intervention to validate the state of processors in question.

Deployment

Rancher Government Solutions Support Subscription

Rancher Government Solutions is pleased to offer Carbide as part of a paid support subscription at no additional cost. RGS proudly offers multiple options to support customer needs, all of which include:

- *Assigned customer service representative to manage support requests and queries*
- *24/7/365 troubleshooting and break/fix for critical issues*
- *U.S. based support for non-critical issues during business hours*
- *One high-level architecture review session upon onboarding*
- *Full-stack support for Kubernetes, container runtime and Rancher products covered by purchased licensess*
- *Dedicated Slack or MS Teams for ad-hoc support*

Learn more: https://rancher government.com/support-and-maintenance-terms-of-service

Around-the-clock, cleared expert resources

No systems administrator wants to face a production cluster failure at 3:00 AM on a Saturday morning with no support resource in sight. Undertaking such an endeavor without an expert who is intimately familiar with the intricacies of Kubernetes is as good as swimming upriver without a paddle. When something goes wrong in a mission-critical production environment, having cleared experts available 24/7 is a must.

World-class support

RGS Support is dedicated to partnering with federal customers to extend IT teams and ensure the proper care and feeding of Kubernetes infrastructure.

RGS Support helps customers stay ahead of Kubernetes environments and allow internal technology professionals to focus on the projects that align with their talents and contribute to the agency mission.

Certified integrations

Authentication & Authorization
CERTIFIED INTEGRATIONS: Active Directory, GitHub, okta, OpenLDAP

App Management & CI/CD
CERTIFIED INTEGRATIONS: Bamboo, Drone, GitLab, Jenkins
RANCHER SLA: FLEET, HELM

Container Engine
RANCHER SLA: containerd, docker

Container Security & Secrets
CERTIFIED INTEGRATIONS: aqua, HashiCorp, PRISMA
RANCHER SLA: NeuVector *

Infrastructure Drivers
CERTIFIED INTEGRATIONS: aws, Azure, openstack, vmware
RANCHER SLA: HARVESTER *

Network & Service Mesh
CERTIFIED INTEGRATIONS: LINKERD, NGINX, Project Calico, træfik
RANCHER SLA: canal, flannel, Istio

Operating Systems
CERTIFIED INTEGRATIONS: Red Hat, SUSE, ubuntu, Windows

Persistent Storage
CERTIFIED INTEGRATIONS: OpenEBS, portworx, STORAGEOS
RANCHER SLA: LONGHORN *

Platforms & Orchestration
CERTIFIED INTEGRATIONS: AKS, Amazon EKS, GKE, Terraform
RANCHER SLA: K3S, RKE

Monitoring & Logging
CERTIFIED INTEGRATIONS: DATADOG, elasticsearch, splunk>, Sysdig
RANCHER SLA: fluentd, Grafana, Prometheus

Registry & Image Scanning
CERTIFIED INTEGRATIONS: Docker Registry, HARBOR, JFrog Artifactory
RANCHER SLA: NeuVector *

* *Additional support subscription required*

Setting the pace, not keeping the pace.

Rancher Government Solutions is working at the forefront of software supply chain security.

While the technology sector is making a collective effort to respond to the growing urgency, most software supply chain security technologies are in their infancy. On the contrary, RGS has established an early stake in the ground, having built and implemented best practices around Kubernetes which have yet to be established by other contributors to the industry; for example(s):

- *Verifying and validating SBOMs against existing clusters and compliance requirements*
- *Utilizing and building tooling & enforcement mechanisms around vulnerability scans*
- *Earning the distinction of a fully certified DISA STIG – and building extensive tooling to support it*
- *Building pipelines which incorporate elements like digital signatures to validate and verify providence back to a specific entity*

Customer Success:

+75%
increase in sysadmin productivity

100%
secure software supply chain

3x
security & validation process accelerated

"Rancher Carbide is so far beyond what we're able to do with Kubernetes internally and it's already made a tremendous impact."

-Federal Systems Integrator

Rancher Government: Security First

RKE2 is the only distribution of FIPS- 140-2 Kubernetes certified and hosted in the USAF IRONBANK container registry.

DISA STIG validated & published
Rancher MCM 2.6
RKE2 Kubernetes Distribution

RKE2 FIPS-140-2
The only vendor supporting FIPS in FOSS

CIS-benchmark tool
Enables automated security scans and validation

STIG'd AMI
Builder allowing customers to generate hardened OS images built for RKE2

Active Authorizations to Operate (ATOs)

RGS
Rancher Government Solutions

Cage Code: 8GLZ3
Duns Number: 11738783
Phone: 844.RGS.7779

Website: www.ranchergovernment.com
Address: Rancher Government Solutions
1900 Reston Metro Plaza Suite 600
Reston, VA 20190