Zero Trust and Rackspace Government Cloud

Leverage an integrated, standard security model and system management strategy to reduce risk.

Zero Trust and Rackspace Government Cloud

Leverage an integrated, standard security model and system management strategy to reduce risk.

Zero Trust is an overarching security framework for today's highly diverse and distributed environments based on:

- Perimeterless IT security across the entire organization
- Verification and authentication of devices and user identity, regardless of network location
- Access to network applications, services and workflows based on continuous authentication and verification

Zero Trust security enables government agencies to reduce the attack surface and lateral threat movement once a network is infiltrated. With Zero Trust, you'll also benefit from consistency in authenticating and verifying devices, systems and users before allowing access to data and network resources.

Get There Faster with Rackspace Government Solutions

Rackspace Technology embedded automated security and compliance is standard on Rackspace Government Cloud on both private or public cloud infrastructures. Private and public cloud platforms automate reinforcement of security standards and policies.

Rackspace Government Cloud Solutions consistently automates security standards established by recognized security authorities including, the National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) General Services Administration (GSA) and Federal Risk and Authorization Management Program (FedRAMP).

Zero Trust and Rackspace Government Cloud Benefits

Benefit from an integrated, standard security model and system management strategy that eliminates implicit trust at every level and incorporates the following capabilities:

- System design principles to address threats both inside and outside traditional network boundaries.
- Segmented identity and access management under the principle of least privilege.
- Multi-zone security architecture requiring continuous verification via real-time information from multiple sources to determine access and other system responses so that authorized users receive the access they need, when they need it for functions they are authorized to perform.
- Incident detection and response
- Business continuity enablement

About Rackspace Technology®

Rackspace Technology is your trusted partner across cloud, applications, security, data and infrastructure.

- A leader in the 2020 Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide
- Leader in the 2020 Forrester Wave™ report for managed multicloud services
- Founder, alongside NASA, of OpenStack® and operator of the largest OpenStack Cloud
- 2,500+ cloud engineers
- Servicing more than half of the U.S. federal government agencies
- 20+ years of hosting experience

Security and Compliance

- JAB authorized FedRAMP ATO
- FISMA authorized
- NIST 800-53
- NIST 800-171 DFARS ready
- CJIS, ITAR and FIPS 140 compliant
- 24x7x365 SOC, staffed by a U.S. team
- Always-available, secure business continuity capabilities

AWS and VMware® Expertise

- AWS 500 Certified Partner Network
- AWS Public Sector Partner
- 2,700+ AWS accreditations
- 1,600+ AWS technical certifications
- 85+ AWS professional certifications
- 15 AWS competencies, including DevOps, SaaS, IoT, machine learning, data and analytics, storage, workloads, Oracle®, healthcare and financial services
- AWS-certified experts directly supporting your team
- VMware and Dell® accredited partner

rackspace technology.

Zero Trust and Rackspace Government Cloud

Leverage an integrated, standard security model and system management strategy to reduce risk.

Zero Trust is an overarching security framework for today's highly diverse and distributed environments based on:

- Perimeterless IT security across the entire organization
- Verification and authentication of devices and user identity, regardless of network location
- Access to network applications, services and workflows based on continuous authentication and verification

Zero Trust security enables government agencies to reduce the attack surface and lateral threat movement once a network is infiltrated. With Zero Trust, you'll also benefit from consistency in authenticating and verifying devices, systems and users before allowing access to data and network resources.

Get There Faster with Rackspace Government Solutions

Rackspace Technology embedded automated security and compliance is standard on Rackspace Government Cloud on both private or public cloud infrastructures. Private and public cloud platforms automate reinforcement of security standards and policies.

Rackspace Government Cloud Solutions consistently automates security standards established by recognized security authorities including, the National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) General Services Administration (GSA) and Federal Risk and Authorization Management Program (FedRAMP).

Zero Trust and Rackspace Government Cloud Benefits

Benefit from an integrated, standard security model and system management strategy that eliminates implicit trust at every level and incorporates the following capabilities:

- System design principles to address threats both inside and outside traditional network boundaries.
- Segmented identity and access management under the principle of least privilege.
- Multi-zone security architecture requiring continuous verification via real-time information from multiple sources to determine access and other system responses so that authorized users receive the access they need, when they need it for functions they are authorized to perform.
- Incident detection and response
- Business continuity enablement

About Rackspace Technology®

Rackspace Technology is your trusted partner across cloud, applications, security, data and infrastructure.

- A leader in the 2020 Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide
- Leader in the 2020 Forrester Wave™ report for managed multicloud services
- Founder, alongside NASA, of OpenStack® and operator of the largest OpenStack Cloud
- 2,500+ cloud engineers
- Servicing more than half of the U.S. federal government agencies
- 20+ years of hosting experience

Security and Compliance

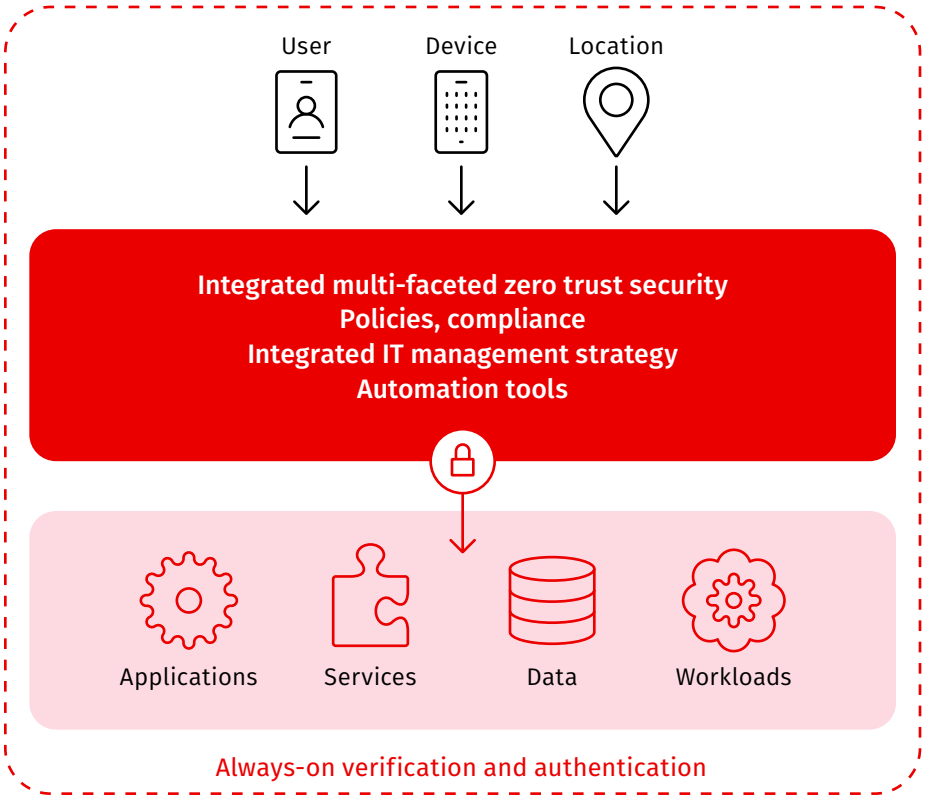
- JAB authorized FedRAMP ATO
- FISMA authorized
- NIST 800-53
- NIST 800-171 DFARS ready
- CJIS, ITAR and FIPS 140 compliant
- 24x7x365 SOC, staffed by a U.S. team
- Always-available, secure business continuity capabilities

AWS and VMware® Expertise

- AWS 500 Certified Partner Network
- AWS Public Sector Partner
- 2,700+ AWS accreditations
- 1,600+ AWS technical certifications
- 85+ AWS professional certifications
- 15 AWS competencies, including DevOps, SaaS, IoT, machine learning, data and analytics, storage, workloads, Oracle®, healthcare and financial services
- AWS-certified experts directly supporting your team
- VMware and Dell® accredited partner

rackspace technology®

Zero Trust Framework on Rackspace Government Cloud



Certified Rackspace Technology security and cloud experts continuously update the Zero Trust architecture to ensure your organization is always compliant with the latest security guidelines, protecting your organization and your supply chain (CMMC, executive orders, federal CIO, FAR, DFARS, FedRAMP, Section 889, NIST, HIPAA, FISMA and other relevant security requirements).

The operations team at Rackspace Technology manages all provisioning, hardening, encryption, backups, monitoring and alerting. A U.S. only team is available to you for around-the-clock support.

Getting Started

Are you planning your migration strategy to ensure you incorporate Zero Trust security across your organization and your supply chain? Rackspace Technology works side-by-side with your team to help you move to a Zero Trust security model in three steps, at any stage of your cloud journey, including:

Step 1: Evaluate your workloads.

Step 2: Determine where your security authentication and verification gaps exist.

Step 3: Plan and implement the security strategy that is right for your organization, from policy adoption to implementation.

Take the Next Step

Let's talk about how Zero Trust on Rackspace Government Cloud helps you achieve your security and compliance goals.

Learn more: **www.rackspace.com/cloud/rackspace-government-cloud**
Call: **1-800-961-2888**

aws partner network

Premier
Consulting Partner

- SaaS Competency
- DevOps Competency
- Data & Analytics Competency
- Migration Competency
- Storage Competency
- Public Sector Partner
- Public Sector Solution Provider

vmware PARTNER
PREMIER SERVICE PROVIDER

vmware PARTNER
SOLUTION COMPETENCY
VMWARE CLOUD ON AWS

vmware CLOUD VERIFIED

rackspace technology

Thank you for downloading this Rackspace data sheet! Carahsoft is the Public Sector Distributor and Aggregator for Rackspace Government solutions whose Managed Service offerings are available via GSA, NASA SEWP, NASPO, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring Rackspace's solutions, please check out the following resources and information:

For additional resources:
carah.io/rackspaceresources

For upcoming events:
carah.io/rackspaceevents

For additional Rackspace solutions:
carah.io/rackspacesolutions

For additional solutions:
carah.io/rackspacesolutions

To set up a meeting:
RGS@carahsoft.com
703-871-8587

To purchase, check out the contract vehicles available for procurement:
carah.io/rackspacecontracts