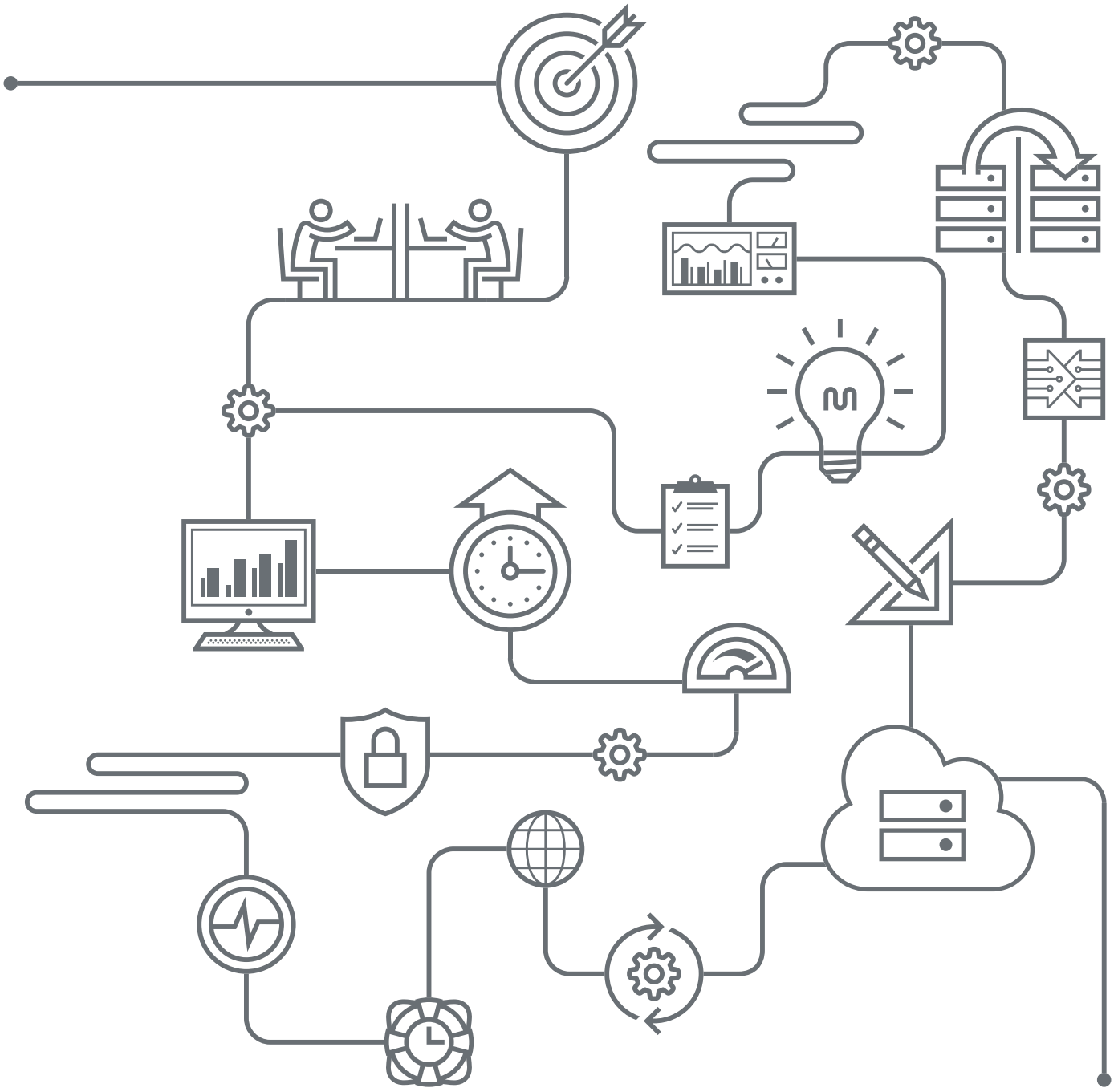
RMS AND COMPLIANCE ASSISTANCE

SERVICE OVERVIEW



OVERVIEW

Every day, your business is at risk for a security or data breach. The threat landscape has changed, with advanced persistent threats (APTs) continually challenging preventive security measures until they successfully breach an environment. These threats can come from anywhere in the world, without warning, and target any part of your business. And there's much at stake, from the sensitive data that gives you industry insights to the trust you've built with your customers — trust that can be hard to regain.

Rackspace Managed Security has been crafted to address the core challenges businesses face in keeping their cloud environments secure and compliant. Our experienced security professionals, using industry-leading technology, can help you effectively protect your business by proactively detecting and responding to security events.

OUR SERVICE OFFERINGS

We offer our customers two service offerings: Rackspace Managed Security and Rackspace Compliance Assistance.

Rackspace Managed Security — Get 24x7x365 host and network protection that's backed by a team of security experts with deep IT security experience. Using best-of-breed tools and analytics, our team of experts can rapidly detect security events and proactively respond to close them. Rackspace is your security force multiplier along your cloud journey.

Rackspace Compliance Assistance — Compliance Assistance is a separate offering that can be purchased as a stand-alone service or in conjunction with Managed Security services. Compliance Assistance helps ensure that you continue addressing your information security compliance requirements as your unique cloud journey unfolds. It offers configuration-hardening and file-integrity management, along with patch, user and configuration monitoring to help you confidently manage your compliance requirements. Our Compliance Assistance team is available during normal business hours in the U.S.

TOOLING

RACKSPACE MANAGED SECURITY

Rackspace Managed Security and Compliance Assistance utilize the following tooling to help actively counteract threat activity and ensure information security compliance, respectively.

RACKSPACE MANAGED SECURITY

HOST AND NETWORK PROTECTION

- Continuous endpoint protection guards against a variety of threat types, including known and unknown threats, as well as malware and malware-free attacks
- Blocks indicator of attack (IOA) behavior
- Prevents privilege escalation, ransomware, zero-day exploits and more
- Utilizes malware protection driven by machine learning
- Provides real-time and historical analysis of key endpoint activity, such as processes, threads and more
- Host-based monitoring requires Windows 2008 R2 and above, or RHEL/CentOS 6.2 and above
- Additional platform support (Debian/Ubuntu) is in development (anticipated release in Q2 2016)

THREAT INTELLIGENCE AND SECURITY ANALYTICS

- Ingestion of monitored environment activity and alert and event data, all logged into a single platform, enables a holistic view for event analysis
- "Single pane of glass" enables deeper investigation of alerts triggered by both security tools and anomalous raw data
- Rackspace currently consumes processed intelligence at the tactical, operational and strategic levels, including:
  - Tactical — IDS rules, IOCs and signatures
  - Operational and strategic — tactics, techniques and procedures (TTPs)

RACKSPACE COMPLIANCE ASSISTANCE

CONFIGURATION-HARDENING AND MONITORING

- Our team works with you to assign security-configuration profiles to hosts based on:
  - Your existing security information policy
  - Generally accepted standards, such as those from the Center for Internet Security (CIS)
  - Community best practices
- Rackspace detects and logs deviations from these profiles in real time to allow for remediation recommendations and reduced vulnerability windows

PATCH-MONITORING

- Provides an understanding of any threats that are relevant to an environment, including which common vulnerabilities and exposures (CVEs) are present in the environment
- Monitoring versions of all software on your hosts as defined by normal installation methods, such as apt on Debian/Ubuntu, Yum on RHEL/CentOS and Windows Add/Remove Programs
- Patch status reports are provided monthly
- Customer is responsible for managing the environment with patching vulnerabilities noted in referenced report

RACKSPACE MANAGED SECURITY	RACKSPACE COMPLIANCE ASSISTANCE

LOG MANAGEMENT
• Initially, Rackspace Managed Security collects standard operating system logs based on your platform (e.g., syslog, Windows events)
• During onboarding, Rackspace works with you to identify additional logs for us to collect, which may include applications-related logs
• All logs are captured and ingested into our analytics platform, where they are used to:
  • Correlate log events with other environmental activities and alerts
  • Add context to event triage and investigation
  • Provide situational awareness of the customer environment
	USER MONITORING
	• Monitors and documents user-host access, authentication level and logon activity to ensure that customers can prove compliance with access controls (available only for Linux-based instances at this time)
	• Provides a report showing user name, root privileges, UID and GUID of the customer accounts
	• Shows the shell used to log in with date, time and IP address used
	• Assigns security configuration profiles to hosts based on your existing security information policy or generally accepted standards, such as those from the Center for Internet Security (CIS), as well as community best practices
	• Detects and logs deviations from these profiles in real time to allow for remediation recommendations and reduced vulnerability windows

VULNERABILITY MANAGEMENT • Scanning and agent technologies are utilized by our Customer Security Operations Center (CSOC) to respond to threats • Internal scans are conducted on individual customer networks, and external scans are conducted on shared infrastructure • Customize the number of scans, with limitations based on impact to systems and time for scans to complete • No limitations on number of hosts • PCI-scanning standard with Attestation of Compliance (AOC) provided • Other scan options available	**FILE-INTEGRITY MANAGEMENT** • Detects, reports and documents changes to files on a host, based on customers' security and compliance requirements • Detects unexpected changes to content/ ownership/permissions of system binaries, configuration files, source code and critical files • Includes registry keys and Windows servers but does not scan source code

HUMAN EXPERTISE

FANATICAL SUPPORT® FOR MANAGED SECURITY

Rackspace Managed Security maintains a 24x7x365 Customer Security Operations Center (CSOC) located at Rackspace headquarters in San Antonio, Texas. CSOC is the basis of how we deliver the Managed Security offering and is included in the price. All CSOC hosts and systems are safeguarded by two-factor authentication (badge and fingerprint scan). Access is granted only to CSOC members and appropriate Rackspace personnel.

CSOC is staffed by trained and experienced security analysts whose credentials exceed industry standards. They are "best in breed" security professionals. CSOC analysts are GCIA- and GCIH-certified and hold many other industry standard certifications:

- Level 1 analysts monitor lower-level events and escalate to Levels 2 and, 3 if event severity increases through the triage process.
- Level 2 analysts are responsible for monitoring all medium-level to high-level events and escalate to Level 3 analysts if event severity increases through the triage process.
- Level 3 analysts are responsible for all critical-level event handling and triage and are also responsible for conducting hunting missions in our customers' environments to identify anomalies indicative of attacker activity.

HOW TO CONTACT SUPPORT

Service requests can be made in one of three ways:

- Contacting your account team directly
- Submitting a trouble ticket through the MyRackspace® Customer Portal (http://my.rackspace.com)
- Calling our toll-free support number: 800-961-4454

All service requests will be assigned a ticket, regardless of the method chosen to contact Rackspace. All tickets associated with the account will be available for review through our customer portal, providing you a complete history of changes performed by Rackspace support personnel.

SERVICE OPERATIONS

With Rackspace Managed Security or Rackspace Compliance Assistance, Rackspace will actively detect and respond to security or compliance events. Once we successfully complete onboarding, the day-to-day support of your Rackspace Managed Security supported environments, incident and change management, and day-to-day management will be delivered according to a customer runbook.

CUSTOMER RUNBOOKS

During the implementation process, Rackspace will work with you to create a customized monitoring-response runbook. This runbook defines the Rackspace Support team's standard operating procedures for working with you on monitoring alerts and includes custom escalation procedures in accordance with best practices and your business needs. These customer runbooks are designed to present the right information, at the right time, to our Security Operations team. It's important to respond quickly and effectively to security events.

MONITORING

As part of Rackspace Managed Security and Rackspace Compliance Assistance, Rackspace provides 24x7x365 monitoring by our staff of security professionals. During the onboarding process, Rackspace will confirm any monitoring requirements in addition to our default configuration. Your technical account manager (TAM) will provide guidance and consultation around best practices.

INCIDENT MANAGEMENT

Incident management refers to managing incidents when restoration of services is the primary objective. Rackspace will work on restoring normal service as quickly as possible when a security problem or incident occurs. Rackspace will apply a consistent approach to all incidents, except where a specific approach is agreed upon with you in accordance with your account's custom runbook.

Rackspace is responsible for remediating issues with the customer's approval. Sometimes approval is completed during the onboarding process (preapproved actions). If remediation falls outside the preapproved actions list, we will seek approval from the customer before leveraging CSOC system administrators or additional Rackspace support teams in order to execute the remediation plan.

Notification logistics will be outlined in service-level agreements (SLAs) and will depend on the applicable severity level of the security event. For more information, see **https://www.rackspace.com/information/legal/rackspace-managed-security.**

We make every effort to reduce false positive incidents. CSOC ingests and correlates all events and logging for all Rackspace Managed Security customers into a big data analytics solution that acts as the "single pane of glass" for CSOC analysts and for rule and correlation generation. This allows CSOC analysts to quickly query, identify inefficiencies in rules and to execute rule-tuning from a central location across all customers to reduce false positives and monitor rules more efficiently.

REPORTING

We employ three standard reporting processes:

- Flash report – issued within two hours of a critical event being identified or within four hours of a category-high event
- Weekly report – a metric-driven summary of events observed within the environment over the previous week
- Monthly report – a technical summary of activity over the previous month that includes a summary of observed threats in the environment, specific to the customer and in the context of the broader threat landscape

APPENDIX

SUPPORTED OPERATING SYSTEMS

MANAGED SECURITY	COMPLIANCE ASSISTANCE
• Windows Server 2008 R2 or later • RHEL/CentOS 6.2 or later • Ubuntu 14.04	• CentOS (5, 6, 7) • Fedora (21–25) • RHEL (5, 6, 7) • Oracle Linux (5 & 6) • Amazon Linux AMI (current supported releases) • Debian (7) and Ubuntu (12.04.5 and newer) • Windows 2008 R2 and newer (64bit OS versions only)

rackspace®

Learn more at www.**rackspace**.com/**managed-security**