

Security

Network security threats – from Internet-born worms and viruses to DDoS attacks, internal data losses, natural disasters and terror-related risks – pose a multi-billion dollar threat to corporations. That’s why Rackspace Managed Hosting takes a comprehensive approach by providing you the industry’s most potent security tools and techniques that are designed, built and maintained specifically for managed hosting.



From secure server builds and security-tested OS installations to a physically secure data center and monitored network, we take a multi-layered approach to keeping your hosting operations reliable and secure.

Security Components & Technologies:

Infrastructure	Rackspace Web security starts at the data center itself, and includes traditional locks and access controls, motion detection, video and biometric surveillance systems. Robust fire suppression, HVAC, power feeds and generator backups protect the physical plant, and hot-swappable servers and routers are available in the event of an outage. Rackspace uses background checks and certifications to ensure the integrity of all data center personnel.
Network	Rackspace Managed Hosting provides 24x7x365 staffed security and the monitoring of both internal devices and external threats. Our 100% Cisco Powered Network, built on hardened routers and regularly audited by Cisco, ensures maximum security protection for every customer. Our network incorporates patented Rackspace Intrusion Detection Systems and we welcome 3rd party security oversight. Firewalls are implemented, configured and managed by experienced Web security specialists and deployed in a “private IP” space, while customer servers and routers are segregated Virtual Local Area Network (VLAN) configurations. Other Rackspace network security features include multi-level privileges, OS lockdowns, centralized authentication and device change logs.
Hardware	All server Operating Systems are loaded, hardened and managed to ensure maximum web security. Many hacking and DDoS attacks can be prevented by consistent patching and by the disabling non-essential OS services. By maintaining on-site inventories and close relationships with key hardware vendors, as well as Web laboratories and automated deployment systems, Rackspace Managed Hosting can guarantee hardware availability. When any Web device is removed from service, Rackspace fully cleans all mission-critical data before that device is routed for disposal.
Applications	The Rackspace security regimen also addresses the inherent vulnerabilities of Internet-oriented applications, including enterprise databases, Microsoft IIS, Apache, Linux, mail services, FTP servers, DNS and streaming media. Rackspace implements well-configured firewalls and deactivates non-essential features to further protect business applications.
Business Processes	The specialists at Rackspace work with customers to address internal policies and processes that might affect Web security. This might include consultations or referrals to 3rd party business security firms.
Security Patching	Rackspace constantly updates its Web security systems to ensure optimum protection for our customers. We maintain close relationships with key technology vendors, the ability to monitor and address emerging threats and the ability to quickly process and apply new security patches.

Rev 091604-1

Security Components & Technologies: (Cont.)

Threat Analysis	Rackspace employs advanced technologies such as Microsoft Operations Manager to identify and address security weaknesses in Web-oriented servers, applications and activities. We constantly examine all firewalls, load-balancers, SSL accelerators and switches, as well as external developments, for any potential security events.
Forensics	Should a security event occur, Rackspace can conduct a comprehensive post-incident examination designed to reduce the risk of future threats. By documenting dollar losses, if any, Rackspace can help justify the involvement of the FBI or other law enforcement agencies.
Security Testing Laboratory	Rackspace subjects all devices to full security testing before they are deployed in the Web infrastructure. Our security testing includes the installation, configuration and patching of the Operating System, the disabling of vulnerable or unneeded services and the use of advanced vulnerability tests.
Certified Engineers & Security Teams	To ensure a fast and appropriate response to any security event, qualified Rackspace personnel are available on a 24x7x365 basis. Our Web security specialists have earned Cisco Certified Security Professional, Certified Information System Security Professional and other security certifications.
Scanning	Rackspace offers scanning of software and network elements for detection of viruses and other security vulnerabilities.
Security Portal	Rackspace has created an innovative Web-based information portal to give every customer precise, up-to-the-minute information on every aspect of their web infrastructure. MyRackspace provides information on emerging Internet threats and vendor responses, as well as specific information on each customer's infrastructure performance, security status, trouble tickets and any current alerts.