Security (EN)

Platform Security

RackCorp Organisation

RackCorp is headquartered in Australia with operations based in 16 countries around the world. We have a strong focus on security due to the nature of our customers with sensitive data in government, banking, and high-value sectors such as mining.

RackCorp is ISO27001, PCI-DSS certified by independent third party auditors yearly. We have a significant focus on protecting our customers, and **take great care around protecting ourselves as a supply-chain** to our sensitive customers.

> RackCorp is ISO27001 certified, meaning our processes and change tracking is tightly controlled and externally auditable.

Software / Code Integrity

Great care was taken to choose trusted software for our UMP solution, using battle-hardened applications that we are confident in auditing the code changes that are made, and are able to quickly update and protect our customers from attacks.

System Protection and Logging

Strong protections using selinux and alerting functions have been built into the platforms to detect and report on abnormal system behavior.

> SIEM Protection capabilities are available utilising RackCorp's proprietary detection systems.

All systems are Linux-based, and have strong policies in place to prevent Viruses. Sophos Anti-virus is available for customers who have compliance requirements to deploy Anti-Virus on every server where possible (virtual routers are excluded)

Administrator Access

All Administrator actions taken through the administrative portal is logged and is reportable. There are no shared user accounts, so all activity can be traced back to specific users.

User Protection

Anti-Virus options are available using ClamAV or Sophos for scanning of emails and user cloud uploads. These provide a good level of on-site protection without the need for third-party scanning gateways that may be off-site, in foreign jurisdictions.

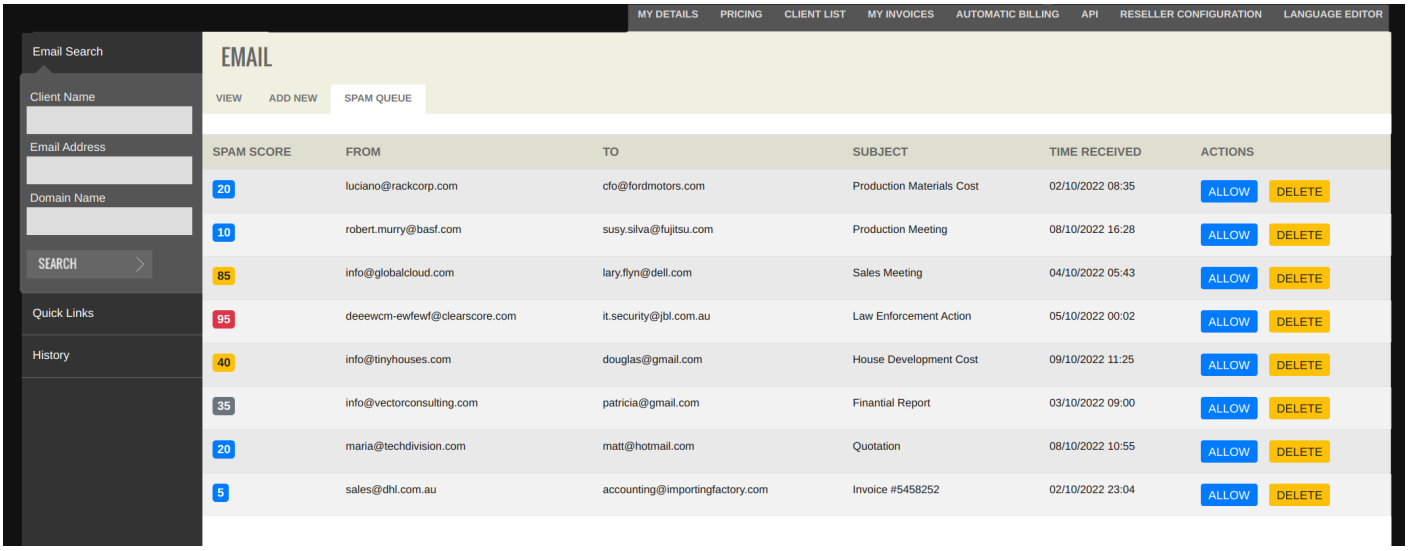
> RackCorp discourages the use of third party mail scanning gateways as this is rightly a large cause of concern for government and large corporations as both a sovereign risk, and government / threat actor security risk. On-site detection may have lower detection rates than third-party gateways, but appropriate rulesets to block or isolate attachments make up for this security difference, and come with the benefit of not having all of your internal and external emails relayed via a third party.

Spam / Anti-Virus Protection and Administration

RackCorp utilises SpamAssassin protection with our own custom databases, rulesets, and policies which are updated daily by our security team to address the latest threats.

Mail Administrators have permission to view held spam / viruses, and view logs of their receipt and optionally release these emails to allow them to progress through to the end customer. Permissions exist that allow specific mail administrators to be locked from reading emails.

EMAIL SPAM MARSHALLING MODULE



> Multiple admin users can operate simultaneously on spam queues.

Email holds / releases controllable via the above are also available via the JSON API service:

```
./rc_acpi.sh '{ "startTime":0 , "endTime":2147483647 ,"fromDomain":"gmail.com",
"status":"ONHOLD"  }'

Return:
{ "timestamp":1665516666.609 , "status":"ONHOLD", "expiry":1665519800,
"fromDomain":"gmail.com", "fromEmail":"rackcorptest345@gmail.com",
"toEmail":"salestest@rackcorp.com", "subject":"This is a test email"  }
```

> All functionality of the RackCorp UMS administrative portal is controllable by way of JSON API

Authentication Integration (SAML)

The RackCorp UMS provides several third party plugin capabilities for vendors who support SAML authentication. Several 2FA vendors natively support this platform already (anyone with a Roundcube plugin)

Revision #8
Created 11 October 2022 15:06:39 by Stephen D
Updated 12 October 2022 05:57:37 by RackCorp