

# Безопасность

## Безопасность платформы

### Организация РэкКорп

Штаб-квартира RackCorp находится в Австралии, а ее представительства расположены в 16 странах мира. Мы уделяем большое внимание безопасности из-за того, что наши клиенты имеют конфиденциальные данные в государственных, банковских и других важных секторах экономики, таких как горнодобывающая промышленность.

**RackCorp ежегодно сертифицируется независимыми сторонними аудиторами по стандарту ISO27001, PCI-DSS.** Мы уделяем большое внимание защите наших клиентов и уделяем **большое внимание защите себя** как цепочки поставок для наших чувствительных клиентов.

RackCorp сертифицированы по стандарту ISO27001, что означает, что наши процессы и отслеживание изменений строго контролируются и подлежат внешнему аудиту.

### Целостность программного обеспечения/кода

Большое внимание было уделено выбору надежного программного обеспечения для нашего решения UMP с использованием закаленных в боях приложений, которые, как мы уверены, проверяют вносимые изменения кода и могут быстро обновлять и защищать наших клиентов от атак.

### Защита системы и ведение журнала

В платформы встроены надежные средства защиты с использованием selinux и функций оповещения для обнаружения ненормального поведения системы и сообщения о нем.

Возможности защиты SIEM доступны с использованием собственных систем обнаружения RackCorp.

Все системы основаны на Linux и имеют строгие политики для предотвращения вирусов. Антивирус Sophos доступен для клиентов, у которых есть требования соответствия для развертывания антивируса на каждом сервере, где это возможно (виртуальные маршрутизаторы исключаются).

## Доступ администратора

Все действия администратора, предпринятые через административный портал, регистрируются и о них можно сообщить. Нет общих учетных записей пользователей, поэтому все действия можно отследить до конкретных пользователей.

## Защита пользователей

Варианты антивируса доступны с использованием ClamAV или Sophos для сканирования электронной почты и пользовательских облачных загрузок. Они обеспечивают хороший уровень защиты на месте без необходимости использования сторонних сканирующих шлюзов, которые могут быть удалены, в иностранных юрисдикциях.

RackCorp не одобряет использование сторонних шлюзов для сканирования почты, поскольку это справедливо вызывает серьезную обеспокоенность у правительства и крупных корпораций как суверенный риск, так и риск для безопасности правительства/угрозы. Обнаружение на месте может иметь более низкую скорость обнаружения, чем сторонние шлюзы, но соответствующие наборы правил для блокировки или изоляции вложений компенсируют эту разницу в безопасности и дают преимущество в том, что не все ваши внутренние и внешние электронные письма ретранслируются через третью сторону..

## Спам / Антивирусная защита и администрирование

RackCorp использует защиту SpamAssassin с нашими собственными базами данных, наборами правил и политиками, которые ежедневно обновляются нашей командой безопасности для устранения последних угроз.

Администраторы почты имеют разрешение на просмотр задержанного спама/вирусов, просмотр журналов их получения и, при необходимости, выпуск этих электронных писем, чтобы они могли быть доставлены конечному пользователю. Существуют разрешения, которые позволяют заблокировать определенных почтовых администраторов от чтения электронной почты.

EMAIL						
VIEW ADD NEW SPAM QUEUE						
SPAM SCORE	FROM	TO	SUBJECT	TIME RECEIVED	ACTIONS	
20	luciano@rackcorp.com	cto@fordmotors.com	Production Materials Cost	02/10/2022 08:35	ALLOW	DELETE
10	robert.murry@basf.com	susy.silva@fujitsu.com	Production Meeting	08/10/2022 16:28	ALLOW	DELETE
85	info@globalcloud.com	lary.flyn@dell.com	Sales Meeting	04/10/2022 05:43	ALLOW	DELETE
95	deeewcm-ewfewf@clearscore.com	it.security@jbl.com.au	Law Enforcement Action	05/10/2022 00:02	ALLOW	DELETE
40	info@tinyhouses.com	douglas@gmail.com	House Development Cost	09/10/2022 11:25	ALLOW	DELETE
35	info@vectorconsulting.com	patricia@gmail.com	Finantial Report	03/10/2022 09:00	ALLOW	DELETE
20	maria@techdivision.com	matt@hotmail.com	Quotation	08/10/2022 10:55	ALLOW	DELETE
5	sales@dhl.com.au	accounting@importingfactory.com	Invoice #5458252	02/10/2022 23:04	ALLOW	DELETE

Несколько пользователей-администраторов могут одновременно работать с очередями спама.

Удержание / освобождение электронной почты, управляемое с помощью вышеуказанного, также доступно через службу JSON API:

```
./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" }
```

Вся функциональность административного портала RackCorp UMS управляется с помощью JSON API

## Интеграция аутентификации (SAML)

RackCorp UMS предоставляет несколько подключаемых модулей сторонних производителей для поставщиков, поддерживающих аутентификацию SAML. Несколько поставщиков 2FA уже изначально поддерживают эту платформу (любой, у кого есть плагин Roundcube).

Revision #3

Created 12 October 2022 02:16:24 by KonS

Updated 12 October 2022 10:19:54 by KonS