Putting security front-and-center for remote areas of the Outback

Case Study +

Medical services that city dwellers take for granted can be difficult to deliver outside metro areas. The Royal Flying Doctor Service (RFDS) was formed nearly a century ago to provide health care to communities in the Australian bush. Using aviation, modern medicine, and communications technologies, the dedicated professionals of the RFDS serve as a lifeline for those who live, work, and travel in remote Queensland.

How can an organization with staff spread across Queensland effectively protect mission-critical data?

The RFDS provides aeromedical and primary health care services across regional, rural and remote Queensland. "The RFDS provides medical services across about 1.8 million square kilometers," says Adam Carey, the organization's Digital Infrastructure Program Manager. "Our clinicians look after patient health, our pilots provide aeromedical retrieval, and my role is to support patients' digital health."

Carey is responsible for digital transformation and cybersecurity programs at the RFDS. The organization recently transitioned core capabilities to software-as-a-service (SaaS) systems. This boosts productivity for workers in distant outposts. It also heightens risk across three dimensions.

First is the challenge of protecting remote and cloud-based systems. "The digital security of patient information is critical—privacy is part of the patient care we provide," Carey says.

In addition to the fundamental responsibility to protect patients, "the RFDS is absolutely iconic," he notes. "That puts a heavy responsibility on us, as technologists, to make sure the environment is safe. We have a reputation to protect and can't let a cyberattack erode trust with the public."

And third, a successful attack might undermine the availability of the digital services that RFDS staff need to do their jobs. "The stability, resiliency, and integrity of our systems have a major impact on our ability to provide medical care," Carey says.

> "We have nurses and clinicians in very remote communities, and they need to be able to work digitally from wherever they are. So, we have unique challenges in providing connectivity and security for their data."
>
> – Adam Carey, Digital Infrastructure Program Manager, Royal Flying Doctor Service (Queensland Section)

Royal Flying Doctor Service
QUEENSLAND SECTION

Profile

Industry	Region	Established	Impacts
Healthcare	Queensland	1928	>200 people/day

Click here to visit The Royal Flying Doctor Service (Queensland Section) website

Challenges

- Secure users and data deep in the Australian bush
- Protect traffic to and from myriad cloud-based apps

Solutions

- Netskope Next Generation SWG filters all web traffic
- SWG detects and mitigates threats, protecting RFDS staff and patient information
- SWG greatly enhances visibility into traffic and security events
- SWG integrates with RFDS SIEM

Results

- Better visibility leads to better decisions around security and risk
- Transparent to end users; their work is not interrupted by security incidents
- Improved agility for the RFDS in continuing the digital transformation journey

Boosting security and visibility, with transparency to end users

The RFDS leveraged the advanced security capabilities of the Netskope Next Gen Secure Web Gateway (SWG). It delivers anti-malware and intrusion prevention system (IPS) technologies, firewall and sandboxing, data loss prevention (DLP), threat-intelligence feeds, and other next-gen functionality, through the cloud.

Now, when RFDS users—on any device and in any location—connect to resources via the internet, they first connect to Netskope. The SWG inspects the traffic, then sends it on to the website, SaaS app, or other cloud-based destination. Not only does this improve security, but it also provides Carey's team with deep visibility into user activities.

"The Netskope platform does a lot of different things," Carey says. "We look at all parts of the network, and user and data flows. Netskope gives us visibility into the cloud services our staff use. It also gives us the ability to finetune which services and solutions are trusted, and which shouldn't be available. It's part of our DLP program to ensure we don't have data loss, and we use it to ring-fence critical data."

The SWG integrates directly with RFDS's security information and event management (SIEM) system. "That gives us another dimension of user activity, [so we can] ensure that activity on their account and on their data is normal," Carey says.

For end users, the solution is transparent. "We get no complaints from the field," he says. "Our clinicians and nurses don't have to think about security. They use the systems they need to interact with, while Netskope is in the background, protecting the data and ensuring it's not lost or leaked."

Building business agility without security risk

The SWG requires little effort from Carey and his team. "It's a very hands-off solution," he says. "We don't have to manage and monitor it day-to-day. We apply our data policies to endpoints, and data is then logged back in, to give us that 24x7 understanding of where our data is, at all times."

Ever since the RFDS implemented Netskope SWG, remote workers have been securely accessing the websites and cloud solutions they need, without interruption or incident.

"The Royal Flying Doctor Service now has much greater visibility into threats to our environment, allowing us to make more informed risk decisions."

He believes the enhanced security for all web traffic has made the RFDS stronger and more resilient. It has also improved his organization's flexibility.

"In our journey to 100 years," Carey concludes, "we have a strategy to continue to digitally innovate. Netskope allows us to be more agile in the technologies we provide to our clinicians and flight nurses. We know that they can safely use cloud-based services, and we can protect their data, regardless of the use case. We keep our users safe so they can deliver patient care."

> "We consider Netskope to be a trusted partner and part of the IT organization. Netskope understands the challenges we have out in the field, and helps us provide a solution that protects patient care and the security of the organization as a whole."
>
> – Adam Carey, Digital Infrastructure Program Manager, Royal Flying Doctor Service (Queensland Section)