Secure remote working ready for takeoff

Lanseria International Airport started out as a grass strip airfield in 1974. Today, the privately owned airport is a bustling air hub and a crucial part of South Africa's transport infrastructure. Located north of Randburg and Sandton to the northwest of Johannesburg, Lanseria can accommodate aircraft up to the size of a Boeing 757 and is a favored airport for private jet operators. The airport hosts daily flights between Johannesburg, Durban, and Cape Town.

How can an airport operator ensure secure remote working for its employees?

Following the COVID-19 pandemic, Lanseria International Airport (Lanseria) supports more remote workers than ever. The airport's IT security team understood that to protect the business, they need to enhance its security, as well as enabling remote access.

Stewart Wapwanyika, Security Administrator at Lanseria, comments: "We wanted an always-on solution that employees can't bypass, and which delivers a good user experience. Our aim is to ensure employees can access our applications regardless of employees' location, and that working from home doesn't open us to threats like ransomware and data exfiltration."

Initially, the company used the virtual private network (VPN) feature that comes with its firewall, but it found this to be limited. "With limited visibility, we couldn't guarantee that users adhered to our policies," says Wapwanyika, "so we decided to look for something with more control. It was then that we started to have conversations around zero trust network access (ZTNA)."

Lanseria's project comes as the South African aviation industry is increasing cyber resilience more broadly. According to Wapwanyika: "Aviation's governing board is pushing zero trust as a component of airport security, so it was natural for us to want to pursue this path."

Having decided to take a ZTNA approach, Wapwanyika looked at the market options. "We quickly zeroed in on Netskope," he says. "This is because of a recommendation from a highly respected colleague in the security space, and great reports from Gartner."

Profile

Industry	Region	Established	Passengers
Aviation	South Africa	1974	4M Per Year

Click here to visit the Lanseria Airport website

Challenges
- Enable secure work from anywhere for growing remote workforce
- Leverage ZTNA to meet aviation industry expectations

Solutions
- Netskope NPA provides secure ZTNA to corporate apps
- Netskope Next Generation SWG to secure web access and spot data exfiltration

Results
- Enhanced remote working security
- Improved remote user experience of apps

"We wanted an always-on solution that employees can't bypass, and which delivers a good user experience. Our aim is to ensure employees can access our applications ...and that working from home doesn't open us to threats like ransomware and data exfiltration."

– Stewart Wapwanyika, Security Administrator, Lanseria International Airport

netskope

Security that's ready for anything

Cloud-based zero trust network access

Lanseria International Airport engaged Netskope to conduct a proof-of-concept (POC) of its proposed remote working security solution. The cutting-edge solution leverages several elements of the Netskope Intelligent Security Service Edge (SSE) including Netskope Private Access (NPA) to connect remote users to Lanseria's corporate applications that, as is common in the aviation industry, are hosted both on-premises and in the cloud. This ZTNA solution both helps reduce risk and optimize the user experience.

The POC also included the Netskope Next Gen Secure Web Gateway (SWG) for visibility and control across five lanes of user traffic, including web, managed SaaS, unmanaged SaaS, cloud service providers, and public facing custom apps.

Following the successful POC, Lanseria has now nearly completed rollout of NPA, which will protect the more than 50 private applications accessed by Lanseria's employees. Once complete, the company intends to start deployment of the Next Gen SWG to secure the business against data exfiltration and further protect users when they're accessing cloud applications as well as the public internet.

"The rollout is going really well," comments Wapwanyika. "We have now deployed NPA to around 95% of the user base and I am looking forward to starting on the Next Gen SWG deployment. My plan has always been to carry out a phased approach to ensure that every step is completed well before moving onto the next."

"Not only is our business inherently more secure, but our employees receive a great remote working experience. They can access the full range of applications they use in the office without experiencing any drop off in performance."

– Stewart Wapwanyika, Security Administrator,
  Lanseria International Airport

Enabling a high-performance remote workforce

With the rollout of NPA nearing completion, Lanseria International Airport and its employees are already experiencing benefits. "Not only is our business inherently more secure," says Wapwanyika, "but our employees receive a great remote working experience. They can access the full range of applications they use in the office without experiencing any drop off in performance. That's exactly the result we wanted when we set out on this project."

For Wapwanyika, one of the main benefits of working with Netskope is that its products are future proofed. As he puts it: "Netskope is laser focused on the cloud-first world that every business is moving to today. Partnering with a company that specializes in this space means that our security systems are ready for the future, and that we will be protected no matter how the enterprise IT environment evolves in the years ahead."

Lanseria also benefits from a strong working relationship with the Netskope team. "As with any deployment, there have been the odd technical issues," Wapwanyika explains. "But Netskope has resolved every ticket we've raised with them quickly and successfully. The Netskope team is very responsive, and they've been an immense help as we have gotten used to working with their systems."

The company anticipates further benefits once it has deployed the Next Gen SWG. These include better protection for users from web-borne threats such as ransomware, and an enhanced ability to detect and shut down data exfiltration to sites, applications, or cloud-based drives that do not belong to the airport.