

How Northern efficiently manages their onboard OT equipment without pulling trains out of service.

Introduction

Across Northern's fleet of trains and stations, Operational Technology (OT) devices are powering safety critical, network infrastructure and media systems, each provided and maintained by different 3rd parties, each with different access requirements & working practices. Managing access, credential distribution and network connectivity to these devices is a challenge that can require trains to be pulled from service, leading to delays and having a direct impact on rail passengers and staff.

Once a train arrives in the depot, an engineer either with safety training or an escort, can coordinate with other teams to gain access to the required cabinets, network and authentication credentials. Given time, access can be obtained, but it is especially difficult to revoke, as any change to a device configuration or password across the fleet presents significant cost. This scenario is the same across engine management, driver controls & diagnostics as well as network switches, CCTV and passenger information screens.

ABOUT NORTHERN

Northern is a train operating company (TOC) based in the north of England, UK. Operating over **500 trains** and managing **479 stations** across the country they are considered to be one of the UK's largest train operators. Their engineering teams play a massive part in ensuring the running over 2,500 services each day carrying at least 100 million passengers every year.

Northern can monitor every configuration change, every click and every command.

They have secured access to their onboard equipment and have added peace of mind with MFA, logging and secure credential storage

Northern enables modern security features across 1000's of OT & legacy devices.

The Solution

We worked alongside Northern to enroll their onboard devices into Silverhawk to enable privileged access management across device embedded web applications and network protocols including SSH, Remote Desktop and FTP.

This has allowed for indepth audit logging, user permissioning and multi-factor authentication across thousands of devices, whilst also providing rapid access into operational trains, helping to limit the requirement for physical access. This empowers Northern limit the number of devices third-party devices being plugged into the onboard networks and removes the requirement for hundreds of physical visits.

Silverhawk leverages existing network connectivity to automatically setup routes, connect & authenticate to operational technology running throughout the environment. Access to equipment through embedded web applications, SSH, RDP and other protocols can be tightly controlled and restricted to specific users and groups. Every user action is logged.

Individual device connections are assigned to teams, ensuring devices are only accessed by those with permission to find and access the device. This is further removing the requirement for engineers to plugin 3rd party laptops to maintain the onboard systems.

“Silverhawk allows us to quickly provide secure access for engineering teams. We’ve been able to keep trains in service and definitely saved hours of international travel.”

Marc Silverwood, Digital Trains, Northern

Results and Benefits

Northern initially chose to use Silverhawk improve logging & access management for legacy devices, web applications and OT equipment.

As well clearly improving the security of remote management, Silverhawk has really shown it's worth with the operational benefits, allowing for rapid collaboration across technical teams during fault diagnosis & change management actions.

Northern further have piece of mind that less devices are being connected directly into operational networks, helping to further ensure the integrity of running systems. Silverhawk has enabled them to have regain ownership over their network and device inventory so that access can be given and revoked on demand.

As engineers no longer have to drive or fly to diagnose faults, the company has saved on thousands of hours of travel from vendors working remotely.



Silverhawk

Operational
Technology
Gateway