



# DARKTRACE

## CASE STUDY

## The FirstGroup



### Overview

#### Industry

- Transportation

#### Challenge

- Connected, integrated transportation systems
- Complex threat environment
- Sensitive information to be protected

#### Benefits

- Proactive identification of emerging threats
- No longer limited to seeing events at ingress/egress points
- Real-time visualization of 100% network activity
- Enhanced ability to prevent negative impact and cyber-attacks
- Quick installation

### Business Background

The First Group is a British transport group, registered and operating in the UK. The company also operates transportation services in Ireland, Canada, and the United States. Founded in 1986, the group is Britain's large bus operator, running more than 20% of all local bus services with a fleet of almost 9,000 buses across over 40 major towns and cities. The First Group is listed on the London Stock Exchange.

### Challenge

Transport systems are becoming increasingly interconnected via digital applications, making them more susceptible to cyber-attacks. The First Group was aware that new attack vectors meant that its critical systems and networks were vulnerable to the new, evolving cyber-threats, from all over the world.

These vulnerabilities had become a matter of great concern to the company, which was anxious to maintain its market-leading position as the UK's most prominent transportation company and a growing global provider of transport services. As its systems become more complex over time, and breaches spread across these integrated systems, it wanted to get better visibility into network activity and proactively monitor for threats.

Ultimately, it wanted to ensure it had early warning of emerging cyber threats within its own systems, irrespective of how or where those threats might occur, and better protect its company and services in today's landscape.

## Solution

Following a thorough review of the market, First Group decided to deploy Darktrace's Enterprise Immune System technology into the core of its network, in order to enhance its ability to defend itself against potential damaging cyber incidents. Delivered as an appliance, the technology was installed within one hour.

The Enterprise Immune System is powered by new machine learning and probabilistic mathematics developed at the University of Cambridge, and is uniquely capable of learning a sense of 'self' within an organization, in order to detect genuine anomalies in real time. By modeling user, device and network behaviors on a continual basis, Darktrace's self-learning software is capable of constantly adapting with the First Group's evolving and busy network, without requiring manual input, rules or signatures.

In addition to this next-generation threat detection capability, Darktrace also provides a 3D graphical overview of all network activity, via its unique Threat Visualizer interface. The Visualizer enables users to see, investigate and mitigate emerging threats, and gives them an overall understanding of how its devices and users are interacting, at any one time.

## Benefits

Thanks to Darktrace's 'immune system' technology, the First Group can better defend against new and novel cyber-threats that may infiltrate the network, as well as identify unusual, internal activities (including insider threat) early.

The company is no longer constrained by partial visibility and traditional detection methodologies. Without any rules or signatures, the security team at First Group today receives early warning of genuinely anomalous activities that merit its attention – enabling them to focus on what really matters.

The First Group uses the Threat Visualizer on a daily basis to understand the state of the network. They also do this to pre-empt emerging problems that can be addressed quickly, before they escalate, from sophisticated threats through to network misconfigurations that might turn into vulnerabilities. Thanks to the classification function within the Visualizer, analysts can also prioritize its resources and ensure that high-level incidents are dealt with first.

Today, the Enterprise Immune System is relied upon to keep the First Group ahead of emerging threats, and to continually learn more about its environment in order to adaptively protect against tomorrow's 'unknown unknowns'.

### Contact Us

North America: +1 415 229 9100

Europe: +44 (0) 1223 394 100

Asia Pacific: +65 6804 5010

[info@darktrace.com](mailto:info@darktrace.com)

[darktrace.com](https://darktrace.com)