

## The Scottish Government



### Overview

#### Industry

- Government

#### Challenge

- Safeguard its reputation and critical data
- Varied and evolving threat landscape
- Protect against potential insider threats

#### Results

- Real-time threat detection and risk mitigation
- Vastly improved understanding of user and device behavior
- Full network visibility

### Business Background

The Scottish Government, established in 1999, is a devolved government whose responsibilities include health, education, transport, justice, rural affairs, economic development, housing and the environment for Scotland. The governing Scottish National Party, led by the First Minister, Nicola Sturgeon, is composed of cabinet secretaries and ministers who collectively manage an annual budget of £28.6 billion across the various sectors they individually supervise.

“

Darktrace's Enterprise Immune System has transformed our cyber defense strategy and given us the confidence that we can handle potential incidents quickly.

**Mark McKenny, Cyber Defense Manager,  
The Scottish Government**

”

### Challenge

The Scottish Government is responsible for a vast amount of sensitive data and, as such, recognized the need to defend its systems from potential cyber-threats as paramount, particularly in the face of modern cyber attackers.

The reality of the modern cyber landscape is one of sophisticated and rapidly-evolving threats and insiders who aim to exploit their position to gain an advantage. Indeed, even a non-malicious insider's activity could potentially compromise an online network, a pressing concern when sensitive information is digitized. The Scottish Government was realistic about these risks and recognized the need to employ a new-generation cyber security technology able to tackle the challenge of modern cyber-threats.

## Solution

After reviewing and trialling a number of technologies, the Scottish Government decided to embark on a four-week Proof of Value (POV) trial period with Darktrace. During the POV, the efficacy of Darktrace's Enterprise Immune System was clearly evidenced.

The technology, which is developed by mathematicians from the University of Cambridge, detected a number of points of interest: malware actively attempting to contact an attacker, unusual and insecure data transferrals, and employees using prohibited sites and software.

Darktrace's unique Enterprise Immune System is inspired by the biological principles of the human immune system, and is powered by machine learning technology. Unlike legacy approaches, it does not use pre-set rules or signatures in order to detect threats. It models the behaviors of each device and user within an entire network to build a 'pattern of life' specific to that system.

Any deviation from 'normal' activity, however subtle, is identified in real time, so that action can be taken. Additionally, the Scottish Government's security team receive a Threat Intelligence Report (TIR) with further analysis and explanation. Anomalous behavior is analyzed and classified according to threat level, so the Scottish Government can handle and respond to issues immediately and efficiently.

## Benefits

Thanks to Darktrace's self-learning technology, the Scottish Government is now fully equipped to detect novel cyber-threats and mitigate the risk they pose. Darktrace's Threat Visualizer Interface provides it with a comprehensive, graphical overview of its network and potential threats as they occur, in real time. The classification system enables it to prioritize issues according to importance and employ human resources efficiently.

The most advanced 'immune system' cyber defense technology provides the Scottish Government with complete network visibility, an overview of their user and device behaviors, and the confidence that potentially damaging cyber attacks will not go unnoticed.

"Darktrace's Enterprise Immune System has transformed our cyber defense strategy and given us the confidence that we can handle potential incidents quickly," said Mark McKenny, Cyber Defense Manager, The Scottish Government. "We are proud to be using the latest technology and innovation, to help protect our systems and citizens' data."

### 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)