Self-Learning AI for Canadian Municipalities

As cyber-attacks like ransomware become more sophisticated and severe, more than 20 Canadian municipalities have already turned to Darktrace's Self-Learning AI to detect and respond to threats in their organizations.

At a Glance

- Protects over 350 public sector organizations worldwide
- Autonomous Response stops ransomware in seconds
- Covers the entire digital estate – including OT, email, cloud, SaaS, and endpoints

COUNTY OF LAMBTON
The Corporation of the County of Wellington
CITY OF Leduc
Cornwall ONTARIO CANADA
PORT COLBORNE
Hastings County
St. Catharines
Dufferin county
Greater Grand Sudbury
TOWN OF MONO
MAPLE RIDGE British Columbia

A Rising Threat

In recent years, around 44% of global ransomware attacks have targeted municipalities, with attackers exploiting the fact that these organizations – many of which operate or manage critical infrastructure – cannot afford to remain offline in the event of an attack.

At the same time, security teams at these organizations are stretched too thin, lacking the time or resources to chase down possible attacks. Security defenses reliant on Threat Intelligence require constant updating to keep up with modern threats, while rules-based approaches tend to be either too lenient – missing more nuanced attacks – or too strict, generating hundreds of false positives and creating alert fatigue.

Cyber-attacks can result not only in physical disruption but also heavy financial costs from ransom payments, fines for PII breaches, and PR setbacks. As the average total cost of a data breach in Canada rises to C$6.35M, many Canadian municipalities are now recognizing the need for advanced, AI-driven solutions which can detect the most sophisticated attacks and stop them autonomously at machine-speed, without the need for human intervention.

A Self-Learning Approach

Darktrace's Self-Learning AI learns a municipality's unique digital environment, using an evolving understanding of what 'normal' looks like for an organization to spot malicious activity which doesn't belong.

Darktrace brings its AI to your data, wherever it resides – whether that's in cloud infrastructure and applications, email systems, on-premise networks, endpoints or industrial systems. Not only does this provide greater visibility for security teams, but it allows the AI to draw out subtle, malicious patterns from across the entire digital environment.

Securing Critical Infrastructure with AI

For municipalities, the security of critical OT environments is often left to IT staff lacking the time or resources to adequately protect them from attacks. These systems can support critical infrastructure, including water treatment and utilities, and make lucrative targets for attackers, so their security is paramount. But with Self-Learning AI and Autonomous Response, even small teams can monitor their OT and IT systems together effectively and with ease.

Machine-Speed Action with Autonomous Response

As both the speed and cost of ransomware attacks rise, cyber security solutions are needed which not only detect attacks but stop them autonomously, even when human security teams are unavailable.

Autonomous Response uses Darktrace's evolving knowledge of 'self' to deliver precise actions in response to sophisticated threats, wherever and whenever they emerge. These proportionate actions avoid business disruption; as potentially devastating attacks are neutralized by Autonomous Response, the organization's work continues uninterrupted.

Autonomous Response is also entirely configurable and can be set up to only take autonomous action with human confirmation, or for specified devices, times of day, or forms of attack.

Case Study: City of Maple Ridge

MAPLE RIDGE
British Columbia

City of Maple Ridge was one of many organizations which adopted a hybrid workforce in 2020, complexifying a network which was already managed by a very small security team. The team became increasingly concerned by the lack of visibility they had over their own traffic.

Maple Ridge implemented Darktrace's AI, which provided total visibility across the digital estate, detecting novel cyber-threats that had previously gone unnoticed. Now, the team are looking to employ Autonomous Response to respond to future threats around the clock. "It's a really big problem having just a few people doing a lot of the security," says Sean Serediuk, Infrastructure and Security Services Manager, "We're now hoping to implement Autonomous Response to deal with threats when they pop up as it sees fit."

Case Study: Dufferin County

Dufferin county

The security team at Dufferin County lacked visibility over their digital environment, and previously had a reactive approach to security. Implementing Self-Learning AI has revealed previously unknown cyber-threats and alleviated the team's workload.

"There's so much data out there, parsing through it isn't humanly possible," says their IT Manager, Peter Routledge, "AI helps us to identify in a smarter way where we need to direct our resources." With AI working around the clock, Dufferin County have been able to shine a light on employee behavior and potential insider threats which had previously passed unnoticed. Darktrace AI has helped the team mitigate the effects of the SolarWinds compromise and other high-profile supply chain breaches.

> "AI brings us from a reactive state to a proactive one. It helps us identify in a smart way where we need to direct our resources."
>
> **Peter Routledge, IT Manager, Dufferin County**

Darktrace Proof of Value

Discover how Autonomous Response can enhance your cyber defense by starting your 30-day free trial. As part of a Darktrace Proof of Value (POV), you will benefit from a dedicated Darktrace Cyber Technologist and access to our award-winning Threat Visualizer.

○ Installs in 1 hour

○ Threats and findings reported within a week

○ 100% visibility of your environment