2021 Industry Spotlight: Government and Defense

With state-sponsored attacks increasing in speed and scale, cyber security is a top priority for government and defense organizations. Darktrace uses AI to detect and respond to novel and sophisticated threats – from fast-moving ransomware to low-and-slow data exfiltration.

At a Glance

- ✔ Protects more than 270 government and defense organizations globally
- ✔ Detects in-progress attacks with Self-Learning AI technology
- ✔ Stops emerging cyber-threats in an average of 2 seconds
- ✔ Reduces time to meaning by up to 92%

Primary Security Challenges

The task of sustaining normal functionality amid a global pandemic has considerably strained governments on a local, state, and national level. Alongside ensuring that public services and infrastructure - such as utilities, healthcare, and transportation - remain operational, governmental bodies have had to contend with additional challenges: implementing national contact tracing programs, enabling research into vaccines and treatments, as well as providing financial assistance to citizens. Securing the systems that facilitate these services is of vital importance.

Additionally, like many organizations over the past year, government offices have had to transition to remote working. The usual cyber risks associated with working from home environments – such as rapid shifts in digital infastructure and workforce behavior, as well as cyber espionage over video conference and hacked smart home devices – are particularly concerning in the government and defense sector due to the sensitive nature of the data and information that it controls.

Ransomware also continues to wreak havoc. In 2020, local governments were the biggest target of ransomware attacks. This threat type has the potential to take down public services - even threaten the privacy of citizens' data and the strength of national security. Governmental organizations require a proactive approach to confronting these challenges and must leverage new solutions to fight back.

> "I'd spent over a year reviewing cyber security products from over two dozen vendors before seeing Darktrace and quickly discovered it had every feature I was looking for and some features I had not thought of."
>
> Director of Information Technology, Government

> "Using AI, Darktrace can detect and respond to email-borne threats, cloud-based attacks, and novel strains of malware that other tools miss."
>
> Michael Sherwood, Director of Innovation and Technology, City of Las Vegas

How Self-Learning AI Safeguards Government and Defense Organizations

Proven to protect hundreds of government and defense organizations, Darktrace's Self-Learning AI defends digital data and vital systems from threat - no matter how novel or sophisticated. As a self-learning technology, the AI is able to identify and respond to fast-moving ransomware at an early stage without relying on prior attack data, and operates across SaaS, cloud, IoT, email, endpoints, OT technology, and the traditional network.

Inspired by the principles of the human immune system, Darktrace works by learning what 'normal' looks like for every user, device, and virtual machine in an organization's dynamic workforce. This understanding of 'self' allows the AI to spot the subtlest indicators of malicious activity as they emerge, instantly flagging them to security teams, and autonomously responding to neutralize the threat at machine speed.

Darktrace Cyber AI Analyst augments teams during fast-moving attacks by autonomously investigating, triaging, and reporting on each security incident. This technology provides actionable intelligence via natural language reports that can be translated to various levels of technical detail - ultimately reducing time to meaning by up to 92%.

Autonomously Defending Against Eking Ransomware

At a governmental organization in APAC, Darktrace detected an example of Ransomware-as-a-Service (RaaS). With Darktrace, the defenders were able to recognize the anomalous behavior as soon as it occurred and stop the threat from advancing, while Cyber AI Analyst autonomously investigated and reported on every stage of the incident.

The attack started when a corporate device was infected with Eking. Darktrace's Self-Learning AI detected and alerted on this threat immediately, picking up on internal reconnaissance activity, SMB enumeration, and extensive scanning. Once the scanning was complete, files were encrypted on a second server, with the infected device transitioning from making just a few internal connections per day to making thousands in less than an hour.

While Darktrace's alerts and investigations empowered the team to take action straight away, this all this occurred late at night local time – when the security team were out of office. As it was, they were still able to act faster than they otherwise would have and limit the damage when they arrived in the morning. Had Darktrace Antigena been deployed, the AI would have autonomously taken action at the first stage of the attack and prevented encryption occurring.

Threats by Numbers

More than 4,000 ransomware attacks have occurred daily since 2016.

$1.1 million is the average cost of a data breach in the public sector.

"We uncovered several major issues our other security tools did not or were unable to."

CIO, Government

Darktrace's Threat Visualizer graphically displays events of interest