2020 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 attacks – 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 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, and securing the systems that facilitate these services is of vital importance.

Additionally, like many organizations over the course of 2020, 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, accounting for approximately 44% of all observed attacks. Ransomware has the potential to take down public services and 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.

"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 Cyber AI Safeguards Government and Defense Organizations

Proven to protect hundreds of government and defense organizations, Darktrace Cyber AI defends digital data and vital systems from threat - no matter how novel or sophisticated the attack. As a self-learning technology, the AI is able to identify and respond to sophisticated attacks and 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 on-premise network.

Inspired by the principles of the human immune system, the AI 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's Cyber AI Analyst further augments this immune system approach by automating the investigation, triage, and reporting process of security incidents. In doing so, Cyber AI Analyst ultimately reduces the time to meaning by 92%, and also provides actionable intelligence via human readable reports that can be translated to various levels of technical detail.

Threats by Numbers

of global ransomware attacks were aimed at local governments in 2020

increase in the average number of attacks per site in US government on 2019.

Defending the City of Westland From Ransomware

An employee of the City of Westland fell victim to a phishing attack after they clicked on a malicious email link. Mere seconds later, Cryptolocker ransomware began to spread throughout the network. Soon after the attack, the City of Westland's CIO decided to deploy Darktrace Cyber AI. Darktrace's self-learning technology understands a unique 'pattern of life' for each user and device in the entire digital environment, empowering it to identify cyber-threats in real time.

Darktrace Cyber AI takes intelligent and informed actions to isolate attacks within seconds – all without disrupting the city's critical IT systems and public services. With only 5 full-time security staff protecting the sensitive data of over 84,000 residents, Darktrace Cyber AI has proven indispensable in safeguarding the city's infrastructure. The City of Westland is now confident that its infrastructure is protected, no matter how or when machine-speed threats strike.

[Discover how Darktrace detected Eking Ransomware in its earliest stages in a governmental organization]

For more information:

- Book a Free Trial Now
- Download Our Immune System White Paper
- Hear From Our Customers
- Read the Blog On Glupteba Malware
- Watch Our YouTube Video on RaaS

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,300 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.