

Cyber AI for Municipalities

Hundreds of municipalities and cities around the world rely on Cyber AI to protect against the most advanced and fast-moving cyber-attacks, including ransomware. When security teams are outpaced, the machine fights back.

At a Glance

- ✓ Protects over 130 public sector organizations and 60 US municipalities
- ✓ Responds to an emerging threat every 3 seconds worldwide
- ✓ Installs in just 1 hour



Held to Ransom

Some of the most significant ransomware attacks of the past year were waged against US cities and local governments, resulting in critical data being encrypted and vital services crippled.

These recent spates of ransomware have brought to the fore the vulnerabilities that connected infrastructure and public services face in the wake of increasingly sophisticated and fast-moving threats. Ransomware campaigns are designed to specifically identify and exploit the weaknesses of their targets and spread across networks in a matter of seconds. Their speed and sophistication give security teams almost no time to react before the damage is done.

Governments and policy-makers are recognizing the importance of advanced solutions for the entirety of their digital environments and are relying on Cyber AI and Autonomous Response technology to safeguard the services and critical infrastructure of cities and municipalities.

“Darktrace Antigena is the only automated cyber defense technology on the market that is capable of fighting the most important battles for us.”

Michael Sherwood, CIO, City of Las Vegas

The Machine Fights Back

Darktrace’s award-winning Cyber AI is trusted by hundreds of cities, municipalities, and providers of critical national infrastructure in the United States and around the globe, including the smart city of Las Vegas.

Darktrace’s technology is able to not only identify but also respond to cyber-attacks such as ransomware – before they encrypt files, interrupt municipal operations, and disable public services.

Modeled on the human immune system, Darktrace AI learns what is normal for each digital environment without relying on rules or signatures. Darktrace’s self-learning Cyber AI forms an ever-evolving understanding of an organization’s unique digital ecosystem, allowing it to autonomously identify and respond to malicious activity the moment it transpires – even novel threats previously unknown to the security community.

Using a unique technology known as ‘Autonomous Response’, recognized by Gartner as the future of cyber defense, Darktrace Antigena fights back in real time – neutralizing ransomware in its tracks within seconds.

Stopping Ransomware Before Encryption Begins

Traditional security tools that use rules and signatures to stop cyber-threats at the border are now ill-equipped to defend against automated ransomware attacks and zero-day threats. As more sophisticated malware strains have emerged, human teams are now outpaced in their ability to neutralize threats.

However, with the detection and Autonomous Response capabilities of Darktrace's self-learning AI, identifying and stopping novel ransomware attacks and zero-day threats is now routine. Due to ransomware's highly anomalous behavior that deviates from organizations' 'pattern of life', Darktrace's Cyber AI will detect attacks within seconds of threatening behavior emerging.

As soon as anomalous connections are made to external servers, Darktrace Antigena is activated and interrupts SMB encryption attempts - instantaneously preventing attacks spreading beyond patient zero.

“For us, deploying Darktrace wasn’t an option; it was a necessity in staying ahead of today’s advanced and unpredictable threats.”

Paul Haugan, Director of Innovation and Technology, City of Auburn

Case Study: City of Westland

In February 2017, 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 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 AI takes intelligent and informed actions to isolate the attack 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.

Darktrace Proof of Value

Discover how Autonomous Response can supercharge 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 visualization interface, the Threat Visualizer.

- Installs in 1 hour
- Access to the Threat Visualizer
- Threats and findings reported within a week
- 100% visibility of your environment

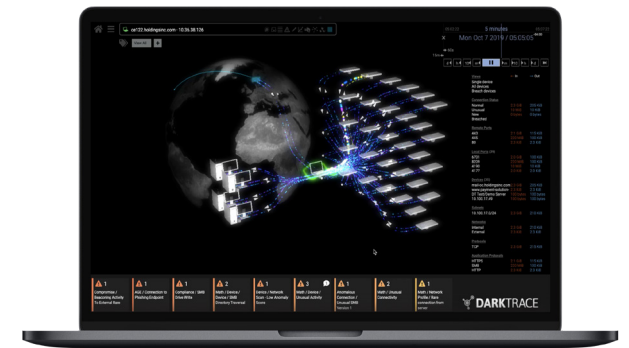


Figure 1: Cyber AI identifies a ransomware attack