DARKTRACE

CASE STUDY

City of Las Vegas

Overview

Industry

- Government & Defense

Challenge

- Containing machine-speed attacks with strained security team
- Lack of visibility into insider traffic and email-borne threats
- Defending multi-cloud infrastructure from a unified view
- Imperative of securing IoT-powered smart city technology

Results

- Deployed Darktrace AI for real-time threat detection and autonomous response
- Achieved 100% visibility across hybrid cloud infrastructure and industrial network
- Able to autonomously neutralize cloud-based attacks in real time
- Protected critical infrastructure against never-before-seen threats

Background

In recent years, Las Vegas has become a prototypical smart city. As riders glide down the Strip aboard the first completely autonomous shuttle ever deployed on a public roadway, they are unlikely to notice much trash on the sidewalk — the city's surveillance cameras stream to an AI service that directs clean-up crews toward concentrations of litter. And when rush hour approaches, its passengers can rest assured that an array of connected sensors are helping officials anticipate gridlock at busy intersections.

But while smart infrastructure enables Las Vegas to achieve new heights of efficiency, conventional security tools are largely ill-equipped to defend the hybrid cloud and industrial networks that power this infrastructure. These diverse environments are increasingly attracting sophisticated cyber-criminals, who seek to disrupt public services or exfiltrate sensitive data. With a highly complex network to defend, the forward-thinking City of Las Vegas recognized the need for equally innovative cyber defenses.

> Using AI, Darktrace's Enterprise Immune System 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**

Challenge

When undertaking its smart city initiatives, the City of Las Vegas aimed to embrace innovation without compromising the security of its 650,000 residents and 42 million annual tourists. However, local governments know that internet-connected infrastructure is often vulnerable to targeted online assaults, which continue to blur the line between digital and physical threats. Today's automated malware often strikes at machine speed, rendering city officials justifiably concerned that an attack — even one that breached just a single smart device — could move laterally to encrypt or hijack its entire network in minutes.

In addition to the external attacks confronting Las Vegas' critical infrastructure, the city was also imperiled by insider threats to its private data and taxpayer information. Nearly three-quarters of global cyber security incidents are the product of either malicious or negligent employees, and with the city's security team relying on legacy tools that provided no visibility into internal network traffic, it had no way to detect these threats. Indeed, due to personnel limitations, the security team was ill-equipped to counter any kind of fast-acting cyber-attack in real time — before its damage was done.

Yet the greatest defensive challenge that Las Vegas faced was never-before-seen attacks, which cyber-criminals now launch on a daily basis. Traditional security tools work by using fixed rules and signatures to predefine what a threat looks like, preventing them from spotting threats that look unlike anything seen before. From spear phishing emails meant to deceive the city's employees by posing as trusted contacts, to novel attacks that attempt to infiltrate via the city's multi-cloud environment, Las Vegas sought a fundamentally unique security tool capable of keeping pace with an ever-evolving threat landscape.

Solution

The city's search for such an adaptive security solution led it to deploy Darktrace AI across its enterprise, cloud, and industrial networks. Powered by world-leading artificial intelligence, Darktrace immediately began to self-learn a unique 'pattern of life' for each Las Vegas employee and device. Crucially, Darktrace AI does not predefine what constitutes a threat to the city; rather, it detects the subtle behavioral anomalies associated with any attack — whether known or unknown. To fight back against automated attacks in real time, the city also deployed Darktrace Antigena, the first cyber AI response tool that autonomously neutralizes threats by taking intelligent, surgical actions.

Antigena works by confining infected devices to their typical 'pattern of life' within two seconds, containing significant threats without disrupting core municipal operations. These operations today rely heavily on Las Vegas' multi-cloud architecture, which includes Amazon Web Services, Microsoft Azure, and Office 365. Whereas the conventional, stove-pipe approach to securing these services lacks vital context, Darktrace analyzes data flows from across the city's entire digital infrastructure, enabling Antigena's cyber AI response to neutralize attacks wherever they originate.

> Darktrace represents a new frontier in AI-based cyber defense. Our team now has complete, real-coverage across our cloud, enterprise, and industrial infrastructure.
>
> **Michael Sherwood,**
> **Director of Innovation and Technology, City of Las Vegas**

Benefits

Darktrace has already detected and responded to numerous attacks against the City of Las Vegas, including a targeted spear phishing campaign that bypassed the city's native email controls. The sophisticated attackers, who had obtained the city's address book, were emailing recipients alphabetically, from "A" to "Z," with ostensibly harmless emails that contained a malicious payload. Despite the well-disguised nature of this attack, Antigena immediately flagged the domain linked in the emails as anomalous for Las Vegas' employees, an action only possible with the evolving understanding of 'self' that Darktrace AI learns.

Antigena was deployed in 'Passive Mode' at the time, a starter mode that restricts the AI to communicating what it would have done in response to the threat, without actually taking action. Interestingly enough, this served to demonstrate its ability to stop attacks that conventional tools miss. Whereas Darktrace detected the campaign at the letter "A," the city's array of legacy tools finally woke up to the threat at "R." In 'Active Mode', Antigena would have neutralized the attack before it reached a single user. Darktrace's AI has fundamentally transformed the city's defensive posture, affording its leaders the confidence to adopt smart technologies and cloud services alike.

Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com