DARKTRACE

CASE STUDY

Aqua-Leisure Industries

Overview

Industry

- Sporting Goods and Aquatic Leisure Products

Challenge

- Needed a proactive approach to protect customer data and intellectual property
- Concerned about increasingly sophisticated malware
- Limited by legacy defenses based on rules and signatures
- Incomplete visibility of all network devices, including IoT

Results

- Detects all forms of threats, including insider
- Prioritizes genuine threats and cuts through the noise
- Continuous monitoring of every user and device on the network
- Autonomous response capability

Business Background

Aqua-Leisure Industries, founded in 1970, has nearly 50 years of experience in design, manufacture and global distribution of; swim & dive products, leisure time floats & lounges, games & toys, SwimSchool educational products and general sporting goods. With headquarters near Boston, Massachusetts and satellite offices in Hong Kong and Shanghai China, the company sells directly to a broad and constantly evolving spectrum of global retailers. Trading partners include sporting goods retailers, mass merchant retailers, toy retailers, grocery, drug, club, super & hyper markets, web based on-line retailers as well as independent retail stores and a broad supply network. With its global reach, Aqua-Leisure's network oversees sensitive intellectual property and the private information of its customers, employees and trading partners.

> We were immediately able to see the return on our investment.
>
> **Leonard Galinsky, Director of IT, Aqua-Leisure**

Challenge

As manufacturers expand their digital networks to keep pace with a dynamic global market, new and obscure attack vectors are emerging at an alarming rate. Aqua-Leisure was realistic about its changing risk profile, and saw the protection of its sensitive customer data and intellectual property as a top business priority. In particular, the company was concerned about its new BYOD policies and increased adoption of IoT devices.

Against this background, Aqua-Leisure wanted to evaluate and revamp its existing security stack to include a self-learning technology capable of identifying sophisticated attacks at their earliest stages. The organization's main line of defense had always been its firewalls, which, like most legacy tools, used rules and signatures based on previous attacks to detect and block

known threats. Yet today's threat landscape – characterized by customized and bespoke cyber-attacks that have yet to be seen – called for a more proactive and nuanced approach.

Above all, Aqua-Leisure's security team wanted an intelligent platform that could provide visibility of all network traffic, and detect fast-moving cyber-attacks within minutes. Additionally, as threats were becoming faster and more automated, Aqua-Leisure saw the need for a technology that could respond autonomously to in-progress attacks.

Solution

To meet these challenges, Aqua-Leisure deployed Darktrace into the core of its network. After a swift installation, the security team was immediately impressed by the Enterprise Immune System's ability to detect and respond to never-before-seen threats that had easily bypassed its perimeter defenses. Within just a couple of weeks, the platform was identifying novel threats that Aqua-Leisure's legacy tools had missed.

Powered by unsupervised machine learning and AI algorithms developed at the University of Cambridge, Darktrace uniquely develops a 'pattern of life' for every user and device on the network. As the technology develops an evolving understanding of network activity, it can detect subtle anomalies and sophisticated threats that depart from this normal sense of 'self'.

Darktrace also maps Aqua-Leisure's network onto an interactive and intuitive 3D Threat Visualizer. The interface allows Aqua-Leisure's security team to view its complex network infrastructure in a single pane of glass, providing complete visibility of IoT and rogue devices. Additionally, each anomaly is classified by its level of deviation from 'normal' network activity, allowing the security team to focus on the most important threats without worrying about false positives.

"Once we plugged in Darktrace's self-learning technology, we were immediately able to see the return on our investment," commented Leonard Galinsky, Director of IT, Aqua-Leisure. "Darktrace's AI not only identified threats that had bypassed our perimeter defenses, but also gave us unprecedented awareness of our network. We saw over 300 devices on a network of only 55 users – about 40% more devices than we expected."

> Darktrace has allowed us to gain unprecedented insight into our network – we now feel confident in our security stack's ability to detect any emerging cyber-attacks, regardless of their entry point into the network.
>
> **Leonard Galinsky, Director of IT, Aqua-Leisure**

Benefits

Thanks to Darktrace's Enterprise Immune System, Aqua-Leisure's team now enjoys greater confidence in its security stack's ability to fight back against potential cyber-threats in real time. Darktrace's innovative approach spots anomalies as they emerge, ranking each according to its threat potential so the team can cut through the noise and focus on genuine threats. Because Darktrace's technology is constantly evolving its understanding of 'normal', it grows and adapts as the company expands. With Darktrace, Aqua-Leisure can remain proactive in the face of a threat landscape characterized by machine-speed, sophisticated attacks.

Equipped with the graphical 3D Threat Visualizer, Aqua-Leisure now has unprecedented visibility of its internal and external traffic, and continues to leverage these insights to shore up any residual blind spots. As pernicious threats continue to compromise IoT and third-party devices in corporate networks around the world, Aqua-Leisure appreciates the importance of gaining complete visibility of its entire network.

"When it comes to cyber defense, Darktrace's AI technology is setting the bar for technological innovation," commented Leonard Galinsky. "The Enterprise Immune System's unique ability to identify threats in real time has allowed us to remain proactive in the face of an increasingly sophisticated cyber climate. Further, Darktrace has allowed us to gain unprecedented insight into our network – we now feel confident in our security stack's ability to detect any emerging cyber-attacks, regardless of their entry point into the network."

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