DARKTRACE

Quickplay

QUICKPLAY™

Industry

- Media & Entertainment

Challenge

- Protect content data, customer information and brand reputation
- Monitor technical workforce in a data-rich and fast-moving environment
- Optimize customer experience while balancing business risk
- Monitor internal network 24/7
- Intelligently pinpoint and target security resources

Benefits

- Gained an understanding of how its users, devices and network operates
- Total visibility of all network activity in real time
- Resilient defense of data and brand, while leveraging interconnectivity and human creativity
- Alerting of real anomalies that may indicate threats
- Proactive cyber intelligence capability

Business Background

Our internet-reliant age has created a demand for content anytime, anywhere, making premium video management delivery more complex and costly. The ability to deliver real-time, high-definition content for media companies, managed broadcast operations and telecommunications companies allows premium video service providers to focus on growing their businesses. This company delivers premium video to any device on any network and has powered major events such as the Olympics and the World Cup.

Challenge

Reputation, data protection and relationships with the telecommunications companies that serve their video content is taken very seriously by media companies. The complexity and sophistication of today's threat landscape has exposed the limitations of legacy solutions and how they are ill-equipped to deal with threats that they now face. This company was looking for a new and proactive approach to cyber security to stay ahead of the curve. Faced with the challenge of defending against advanced cyber-threats, the company realized that it required a next-generation security solution that would take into account its highly-connected environment and the large volumes of data that its employees handle on a day-to-day basis. The company wanted to improve its ability to preempt potential security problems quickly and stop suspicious activities from escalating.

Solution

When the company evaluated its cyber security investments, it chose to deploy Darktrace's mathematics-driven Enterprise Immune System technology, due to its unique ability to detect real threats that bypass other legacy security controls, and do this in real time, as they emerge on the network.

Based on machine learning and Bayesian mathematics developed at the University of Cambridge, the Enterprise Immune System is a self-learning, cyber threat defense platform, which forms an adaptive, probabilistic understanding of 'self' within a network. With Darktrace, the company is capable of detecting very subtle deviations from the organization's normal 'pattern of life' as they happen, and respond proactively to any anomalous behaviors that are uncovered.

In addition, Darktrace's proprietary Threat Visualizer, a 3D graphical visualization interface, allows the company's analysts to investigate any detected anomalies in great detail and address potential issues proactively. This enables the analysts to better understand what is happening within their information systems and focus on tangibly mitigating the most important risks to the business in real time.

Benefits

Since choosing to deploy Darktrace's Enterprise Immune System, this media content leader has successfully enhanced its security stack in order to continue to deliver world-class content, while protecting its information and brand with confidence. With early visibility and continuous monitoring of network activity, the company can effectively safeguard its data and interconnected systems, without hindering its employees' freedom to experiment, explore the internet and remain a dynamic enterprise.

With Darktrace's adaptive, self-learning platform, the company now has an unprecedented understanding of how its users, devices and network operate. Its security team have found Darktrace to be extremely time-efficient, as the technology passively monitors the network on a 24/7 basis and only alerts the security team to real potential threats, rather than flooding them with false positives. The company is now able to rapidly resolve any developing issues, before they result in a crisis, and considerably reduce the risk of undergoing a debilitating cyber-attack or compromise.