Industry Spotlight: Media and Entertainment

Security teams are tasked with defending an increasingly fragmented digital ecosystem from cyber-attacks that are growing in speed, scale, and sophistication. Faced with this hostile cyber-threat landscape, organizations must look to uplift their security teams with autonomous systems that can detect and neutralize emerging threats before the damage is done.

At a Glance

- ✔ Protects hundreds of media and entertainment organizations globally
- ✔ Self-Learning AI technology that autonomously detects cyber-threats in real time
- ✔ Neutralizes attacks seconds after they emerge
- ✔ Autonomous investigations reduce time to triage by up to 92%

Security Challenges in a New Era of Cyber-Threats

The volume of sensitive data in use in the media and entertainment industry has exploded in recent years. More data is generated in one hour today than was created over the whole year of 2000, and the figures for streaming and virtual events only continue to rise.

With users sending and receiving data over a vast range of social platforms and devices in order to access media and entertainment services, safeguarding these digital systems with traditional security measures has become untenable. The high-profile nature of many entertainment events means that they continue to draw attention from some of the most dangerous cyber-attackers.

At the same time, organizations are increasingly transitioning to cloud infrastructure and SaaS collaboration platforms in the interest of supporting dynamic and sometimes disparate workforces. Human IT resources are being stretched to breaking point, and there is a greater need than ever for autonomous systems to expediate the more manual tasks of triage and investigation. Meanwhile, cyber-attacks are getting faster and more sophisticated, with several high-profile ransomware attacks targeting media and entertainment organizations reported in 2021. Security teams must balance the protection of sensitive data and valuable IP with ensuring business continuity and an optimized user experience.

Being able to interrupt attacks at machine speed is essential to safeguarding sensitive data and intellectual property, while allowing for seamless operations.

> "By using machine learning, Darktrace's self-learning technology gives us a real advantage in defending our organization."
>
> Marcello David, Head of IT Security, HBG Gaming

> "The increase in digital attacks globally means that cyber-threats are now our biggest business risk, and we can only mitigate this with AI."
>
> Farzin Najmi, VP of Technology, Network 18

Adapting to the Modern Threat Landscape

Proven to protect hundreds of media and entertainment corporations globally, Darktrace's Self-Learning AI is relied on by some of the world's most forward-thinking organizations to fight back against emerging threats in real time – no matter how novel or sophisticated.

Inspired by the principles of the human immune system, the AI works by learning what 'normal' looks like for every user and device in an organization's digital ecosystem. As a self-learning technology, its evolving understanding of 'normal' is unique for each organization and does not rely on prior knowledge – allowing it to spot the subtlest indicators of malicious activity as soon as they arise. These threats are then autonomously neutralized at machine speed and with surgical precision, allowing normal business operations to continue unimpeded.

Operative across cloud, SaaS, IoT, email, endpoint devices, industrial control systems, and the traditional network, Darktrace is able to autonomously defend organizations' data and digital systems wherever they are located. This capability is complemented by Cyber AI Analyst, which automates the investigation, triaging, and reporting of security incidents, reducing time to meaning by up to 92%.

In today's era of subtle and sophisticated attacks, media and entertainment organizations need AI defenses to stay one step ahead of the latest attacker innovations.

Case Study: Topical Phishing Attacks Neutralized

At US television production company Bunim/Murray, Darktrace's Self-Learning AI caught several novel phishing attacks in their earliest stages.

The attack started with several emails purporting to deliver corporate COVID-19 updates to the production studio's employees. These emails bore a spoofed corporate address, with the subject line 'COVID-19 Update' followed by the day's date. While the email appeared legitimate and could easily have persuaded a recipient to click on it, Darktrace recognized that this was a spoofed domain and that the emails contained an unusual and malicious link.

These subtle signals of attack were enough for Darktrace to prevent the emails from being delivered to recipients' inboxes - neutralizing the threat.

Darktrace's proven ability to stop threats in their tracks has led Bunim/Murray to turn off its legacy email security tools as the team feel safe in their email environment and in the knowledge that AI will autonomously detect and respond to all threat types – wherever they arise.

> "We were shocked by the things our traditional tools didn't catch that Antigena Email did."

Gabe Cortina, VP of Technology, Bunim-Murray

Threats by Numbers

$ $4.1 million is the average cost of a data breach on the entertainment sector.

800% increase in ransomware attacks from 2019 to 2021.

630% increase in cloud-based cyber-attacks between January and April 2020.

The Threat Visualizer displays Darktrace's findings in a clear interface