INDUSTRY SPOTLIGHT

Cyber Defense for Media & Entertainment

With the safeguarding of intellectual property at the heart of its business model, the media and entertainment sector has learned through experience the necessity of fortifying its cyber defenses. Devastating breaches of industry giants such as Sony, Netflix, and HBO have shown that even the sector's leading companies cannot defend against cyber threats without a fundamental shift in their security practices.

The Sony breach, for instance, was set in motion when cyber-criminals stole the login credentials of a system administrator, an increasingly common threat which evades most traditional security tools. These stolen credential enabled an attack that cost the company several hundred million dollars in direct and indirect losses, including diminished revenues from leaked films as well as negative publicity from the revelation that Sony disparaged its actors behind closed doors.

Indeed, experts assess production companies to be especially susceptible to cyber-crime due to the vast number of employees required to create a movie or TV show. Such massive teams compound security risks posed by human error and insider threat, while many team members are BYOD users whose devices can infect company networks with malware. This expansive attack surface has recently been extended exponentially by the industry's move to the cloud, with threat actors exploiting vulnerabilities in third-party systems to either exfiltrate sensitive data or pivot to the enterprise.

Similar concerns also imperil entertainment companies ranging from gaming operators to sports teams, whose strategic evaluations of players would put them at a major competitive disadvantage if leaked to rival clubs. Intellectual property and private data pervade the media and entertainment space, meaning that the long-term reputation of every organization therein depends upon protecting its hard-earned products and ideas.

In addition to stealing sensitive information, today's advanced threat actors also seek to halt digital operations and hold physical systems for ransom. Major amusement parks earn millions per day while large film studios spend millions per shoot, emblematic of an industry that can ill-afford these business interruptions. It is therefore imperative that industry leaders are not only able to spot attacks on their network, but also respond to such attacks at machine speed, before they have time to escalate into a crisis.

> “Darktrace's ability to inform us about emerging threats is unique and has given us much more confidence in our ability to stop attacks, before any damage is done.”
>
> **Raffaello Ghilardi, Chief Information Officer, Giunti Editore**

Threats By Numbers

More data was lost or stolen from media and entertainment firms in just the first half of 2017 than throughout the whole of 2016.

Experts only expect this trend to continue as ready-to-deploy exploit kits become more accessible to less skilled attackers.

IP theft costs U.S. companies **$600 million** a year.

Media and entertainment companies rely on their ability to monopolize revenues from their own IP.

CASE STUDY

Bunim/Murray Productions

Bunim/Murray Productions
We are Banijay

Background

Founded in 1987, Bunim/Murray Productions is a leading entertainment production company responsible for shows such as 'Project Runway', 'The Real World', and 'Keeping up with the Kardashians.' The company has been a pioneer in reality TV for over 30 years, and its programs have been recognized by Emmy, Peabody, and People's Choice Awards.

Challenge

With hundreds of BYOD users and critical data to protect, Bunim/Murray Productions faces the constant challenge of monitoring network activity to detect and respond to emerging threats, whether from malware or malicious insiders. As these threats develop and become more advanced, Bunim/Murray's security team required a technology that could provide real-time visibility across its digital estate, and defend against cyber-attacks targeting sensitive data and IP.

> Within one week of installing Darktrace, the Enterprise Immune System notified us to threats and vulnerabilities we had been totally unaware of.
>
> **Gabe Cortina, VP of Technology, Bunim/Murray Productions**

Solution

To secure its network and award-winning content against advanced attacks, Bunim/Murray Productions deployed Darktrace's Enterprise Immune System in its data center for a four-week Proof of Value. After a swift installation, Darktrace's self-learning technology immediately began learning the normal 'pattern of life' for every user and device, providing complete visibility and detecting threats at an early stage.

"Within one week of installing Darktrace, the Enterprise Immune System notified us to threats and vulnerabilities we had been totally unaware of," said Gabe Cortina, VP of Technology, Bunim/Murray Productions. "Darktrace's ability to learn what 'normal' looks like for every device and user enables us to detect and stop threats before they can do damage."

Bunim/Murray's security team was also struck by the simplicity of Darktrace's Threat Visualizer interface, which displays all network activity in a single pane of glass and prioritizes the most serious threats for investigation. According to Cortina, "The user interface is so intuitive that anyone on my team can log on and find out what they need right away."