Menlo Security

IT'S SAFE TO CLICK

ENTERTAINMENT INDUSTRY SOLUTION BRIEF

The Problem

Studios and production companies producing movies, broadcast television and streaming shows, and even online and video games generally employ a three-step workflow—pre-production, production, and post-production—to create their final product.

Post-production refers to processes required after filming or shooting ends, with services divided into two areas: Audio, which includes dialogue, automatic dialogue replacement (ADR), Foley, sound effects (SFX), music, and more; and video, including editing, telecine, film transfer, visual effects (VFX) including animation, 3D upscaling, motion video including titles, color grading, and more. A studio or production company provides raw, digital output from filming or shooting to one or even several different post-production facilities, leading to the creation of a digital master.

A standard practice for studios today is to outsource and even offshore time-consuming, labor-intensive, and costly post-production services to facilities located around the world, at a significant cost savings. Many post-production facilities are small- and medium-sized businesses (SMBs), though, and have limited budgets and staff dedicated to cybersecurity. In addition, many post-production employees are contractors or temporary employees, working project to project. Combining the lack of strong cybersecurity and a temporary workforce, the opportunity for attackers to steal and hold hostage a complete or near-complete movie, show or game, demanding ransom from the studio or production company, the post-production facility, or both, is very real. But, the revenue lost by a studio or production company if attackers release a film, show, or game before its general availability, the adverse publicity, and the reputation loss can be greater than the ransom.

Moving post-production services back in-house is not an option for studios and production companies due to budget constraints and increasing costs, but working closely with vendors to ensure stringent cybersecurity methods are in place is. The Motion Picture Association of America (MPAA) has produced security recommendations for studios to enforce with their vendors, and many studios have begun to do that, requiring vendors to air-gap production networks or systems that process or store digital content from Internet access, unless a business case requires it. And, if one does, the vendor must tightly control web browsing and limit access to prohibited websites—including webmail—for production environments, and non-production networks and systems must also block possible phishing emails and potentially dangerous attachments.

However, attackers can and will use nearly any means possible to infiltrate a post-production facility's network. Phishing and spear-phishing—relying on social engineering—are two methods attackers use to deliver keyloggers and malware to observe internal processes and steal user credentials, or "phish-and-fool" employees into divulging their credentials. Once that occurs, attackers can then penetrate the network, and ultimately steal a finished or near-finished movie, show or game, delete it from the network, and hold it—and the studio or its vendors—for ransom.

About Menlo Security

Menlo Security is making it safe to click via isolation, protecting organizations from cyber attack by eliminating the threat of malware from web and email. Menlo Security's Isolation Platform (MSIP) isolates all active content in the cloud, enabling users to safely interact with websites, links and documents online without compromising security.

Menlo Security is trusted by some of the world's largest enterprises, including Fortune 500 companies and financial services institutions (FSIs). The company was founded by security industry veterans, in collaboration with acclaimed researchers from the University of California, Berkeley, and backed by General Catalyst, Sutter Hill Ventures and Osage University Partners.

For more information,
visit menlosecurity.com

The Solution: Menlo Security Isolation

Detection-based security tools require up-to-date intelligence on malicious websites and methods to make their necessary "good" versus "bad", "allow" versus "block" decisions. But, web and email security based on isolation technology avoids the problems of distinguishing between legitimate and malicious web content and emails. Isolation inserts a secure, trusted execution environment, or isolation platform, between a user's email and web access, and potential sources of attack. By executing user web sessions away from their endpoint and delivering only safe rendering information to their devices, users are protected and their endpoints insulated from malware and malicious activity, and so is the studio, production company or post-production facility.

Menlo Security's Isolation solution eliminates web malware typically delivered by drive-by downloads, watering hole attacks, malvertising, and more, as well as the credential theft and ransomware email attacks typically deliver. By integrating Phishing Isolation with a studio, production company or post-production vendor's existing mail server infrastructure—such as Microsoft Exchange, Gmail, or Office 365—all email links can be directed to pass through the Menlo Security Isolation Platform. Deployment requires no changes to existing email platforms and, more importantly, to the user's experience. When users click on any web link, known or unknown, when they access the web or in an email they receive, they are 100% isolated from all malware threats, including ransomware. Menlo Security ensures that zero-day and emerging malware and phishing techniques are stopped before they can start. To further prevent users from entering critical credentials or sensitive information into malicious web forms or fraudulent web pages, leading to credential theft and even more insidious attacks, websites opened from links within emails can be rendered in read-only mode.

Menlo Security's Isolation Platform enables production companies and post-production vendors to address the requirements of many studios, as well as MPAA's Content Security Best Practices, Digital Security 2.0 guidelines for securing network and systems that process or store digital content from Internet access, including email, by tightly controlling web access, eliminating potential phishing emails, and prohibiting certain file attachments (e.g., Visual Basic scripts, executables, etc.) from being downloaded and accessed by users. Menlo Security also ensures that even non-production networks can block potential phishing emails and secure user access to certain file attachments by opening them in the isolation platform, far away from the user's device.

Administrators can monitor behavior statistics and customize time-of-click messages to reinforce, in real time, anti-phishing awareness training. With zero dependency on error-prone threat detection methods, Menlo Security Isolation Platform is the only security solution that protects web and email access of every studio, production company or post-production house user immediately upon deployment.

Menlo Security
IT'S SAFE TO CLICK

2300 Geng Rd, Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1795
info@menlosecurity.com