Menlo Security

IT'S SAFE TO CLICK

ISOLATION BEST PRACTICES FOR THE ENTERTAINMENT INDUSTRY

A Menlo Security Best Practices Guide

Executive Summary

The entertainment industry has been inundated with ransomware and credential theft attacks

The entertainment industry—especially the major studios and production companies that create movies, broadcast television, streaming content, and even online and video games—is one of the industries most targeted for cyber attacks. A popular and repeated victim of attackers and hackers because of the industry's visibility and popularity, the attention and notoriety it garners attackers, its continued use of outsourced staff, contractors, and freelancers working project to project, and its use of small- to medium-sized offshore production and post-production facilities with limited IT and security staff and budgets, the entertainment industry has been inundated with ransomware and credential theft attacks. In recent years, there have been several high-profile cyber attacks, including the 2014 attack on Sony Pictures, and the 2017 attacks on Netflix and HBO, which have led to headlines, embarrassment, lost revenue, and in many cases, lost reputations and careers.

An isolation platform can prevent these cyber attacks by dramatically reducing the attack surface on user devices. Employees, contractors and freelancers—and studios, production houses, and post-production facilities—are protected from ransomware, phishing and spear-phishing, malware, credential theft, drive-by exploits, watering hole attacks, and more, when an isolation platform is deployed.

Consolidated from deployment to and feedback from hundreds of customer environments, this document is intended to provide studios, and production and post-production facilities with a guide to best practices for simplifying and optimizing their selection and deployment of a web, email, and document isolation platform to help end the siege of cyberattacks they have endured.

Introduction

Since the first films recorded onto celluloid photographic film, movie and television studios, production houses, and the vendors that provide them services have been prime targets for thieves looking to steal the latest movie or TV show. Those thieves would pirate the film or show, record it onto some form of media or load it onto a file-sharing site, releasing it to the public to make money or to frustrate studio and production executives, or both. It was a sort of crowning achievement for a pirate to steal and publicly show their stolen wares.

As movie- and show-making has moved from processing film to an all-digital process, the attack vectors and the thieves' approaches have changed

But, as movie- and show-making has moved from processing film to an all-digital process, the attack vectors and the thieves' approaches have changed drastically. Over the past several years, major studios and production companies around the world that make and release movies, shows for broadcast television and streaming content, and even online and video games have fallen victim to a new form of theft and attack: Debilitating, embarrassing, and costly cyberattacks and data breaches.

One of the first major, publicized cyberattacks was perpetrated on Sony Pictures in 2014 by the "Guardians of Peace" (GOP). Long thought to be a North Korean hacking team, the GOP hacked into Sony Pictures' network, installed malware, gathered information and user credentials, and in the end, stole—over the span of months—and published then-unreleased Sony productions, personal information of employees, movie stars, and their families, executive salary information, and—possibly worst of all—scads of private emails between employees, agents, and star talent. The fallout from this data breach and the subsequent private information release was paralyzing and devastating not only to Sony Pictures, but to the entire entertainment industry. It was at this point that everyone involved in movie and show production believed security would be increased, so instances such as this would never happen again.

If that were the only cyber attack against Hollywood and content creators worldwide, it would have been bad enough. Unfortunately, it hasn't been the only cyber attack on studios, production houses, and their vendors and suppliers.

While there were several, smaller attacks after the 2014 Sony Pictures attack, the next major cyber attack and data breach occurred in early 2017. This attack was perpetrated against Netflix, a major Hollywood studio and streaming content provider, and was initiated when one of their suppliers, Larson Studios, a family owned-and-operated post-production facility with limited security staff and

budget, was attacked. These attackers called themselves "The Dark Overlord," stole ten complete episodes of the Netflix hit show, "Orange is the New Black," and threatened to release the episodes if Netflix did not pay their demanded ransom. Netflix refused to pay, the episodes were released a month before the expected season premiere date, and, while there was some loss in viewership and advertising revenue, Netflix survived.

Another cyberattack happened in June 2017, and this time it was HBO's turn. An attacker calling himself the "Kind Mr. Smith" somehow infiltrated HBO's network and stole episodes of and scripts for their hit show, "Game of Thrones," in addition to episodes of other HBO shows, financial documents, cast and crew contact lists, an employee's emails, and credentials for social media accounts. (The attacker claimed the network attack was initiated via malicious emails; however, HBO, the U.S. Federal Bureau of Investigation (FBI) and other law enforcement authorities have never revealed how attackers breached HBO's network.) Like the Netflix cyberattack, the attacker demanded ransom; and, just like Netflix before it, HBO refused to pay. (In November 2017, an Iranian, with purported ties to a hacking group based in Iran, was indicted in absentia in U.S. federal court for the cyber attack and theft of 1.5 terabytes of data from HBO – seven times worse than the amount of data stolen during the 2014 Sony Pictures breach.)

But, why target studios, production houses, and post-product facilities for cyber attacks and breaches, and hold their films, shows and games for ransom? Initially, it was for the money: Attackers believed that they could demand and be paid a significant amount of money by studios, production houses, and possibly post-production facilities—even though most are small- to medium-sized businesses (SMBs)—not to publicly leak the films, shows, or games they had pilfered. They believed that those organizations, facing a potential revenue and reputational hit, would pay their lofty demands. However, when their ransom demands were not met or were ignored, their next tactic was to not only steal content, but private emails, internal memos, contracts, financial dealings or data, and any other information that could be used to embarrass studios, and production and post-production facilities and their executives, if it were made public. It turns out that the combination of revenue loss if attackers release a film, show, or game before its premiere and the adverse publicity and the reputation loss associated with public disclosure of private emails, dealings, contracts, and related information make for an even greater incentive for ransom to be paid.

Attackers will use any means possible to infiltrate, surveil, and then spring an attack on the network and production or post-production facilities

While it may seem that studios and production houses moving outsourced, off-shored post-production services back in-house may solve at least the supply chain infiltration by attackers, it is not an option, unfortunately, as studios and production companies face mounting budget constraints and increasing costs. However, working closely with vendors to ensure stringent cybersecurity methods are being put in place is doable and of vital importance.

The Motion Picture Association of America (MPAA) has compiled and published security recommendations for their members—studios and production houses—to enforce with their vendors. As a trade organization, the MPAA cannot mandate that vendors and suppliers adopt their guidelines; however, their members can, and many studios have begun to do that. The MPAA Content Security Best Practices Common Guidelines stipulate that vendors should air-gap production networks or systems that process or store digital content from Internet access, unless a business case is required. If there is a valid business case for the network or systems processing or storing digital content to be Internet connected, the guidelines from the MPAA state that the vendor must tightly control web browsing and limit access to prohibited websites, including webmail, for production environments and that non-production networks and systems must also block possible phishing emails and potentially dangerous attachments (MPAA Content Security Best Practices Common Guidelines DS-2.0, DS-2.1, DS-2.2 Internet).

But attackers will use any means possible to infiltrate, surveil, and then spring an attack on the network or specific devices on the network of studios, and production or post-production facilities. Attackers typically follow a path of least resistance to intrude on a network and devices connected to it. In most instances, that means taking advantage of employees, contractors, freelancers, and temporary workers at studios, production houses, and post-production facilities. Relying on social engineering, psychological tactics, and human nature to drive effective, malicious phishing, and spear-phishing email—or even social media—campaigns, attackers will deliver the keyloggers, spyware, droppers, worms, trojans, wipers, backdoors, and other malware they need to observe and usurp internal processes and user credentials, or to simply "phish-and-fool" employees into divulging credentials.

Once a user's credentials have been snatched, attackers can easily penetrate any network, steal a finished or near-finished movie, show, or game, delete it from the company's network, and hold it for ransom. Or, maybe even worse, the same attackers can download terabits of data—confidential salaries, sensitive financial information, even internal and external email communications—that

could prove to be embarrassing or damaging.

And all it takes is a single full-time employee, contractor, freelancer, or temporary employee to be fooled or panicked into opening an email from an unknown source, click a web link in an email leading to a phishing website and download a file from or input their credentials when asked onto a compromised website, or download a weaponized attachment or even open a calendar invitation, and they, their employer, and their employer's supply chain can fall victim to a cyber attack. Many of these attacks cannot be uncovered and stopped by perimeter and legacy security solutions; and, even if they could be stopped, given the frequency of attacks against the entertainment industry, it is clear that, while these solutions claim they can block up to 99.9 percent of cyber attacks, even that is woefully inadequate.

The old, standard detection approach needs to be discarded. The entertainment industry—the major studios and production companies that produce movies, broadcast television, streaming content, and even online and video games—and their services supply chain need a new approach to security, and that new approach is isolation.

An isolation platform ensures the entertainment industry's content, producers, their services supply chain, and their users are safe

Isolation Demystified

An isolation platform can address many of the gaps in security that are currently left open and assailable by cyber attacks. Isolation does not rely on detection. It does not make a "good vs. bad" or "allow vs. block" decision. Isolation simply assumes ALL content could be bad. It takes a zero-trust approach to emails, web access and content, and documents. It completely contains and executes the content far from a user's endpoint device and renders only safe visual elements to the user and their device.

An isolation platform ensures the entertainment industry's content, producers, their services supply chain, and their users—employees, contractors, freelancers, temporary workers, and the like—are safe and protected from web-borne malware, drive-by exploits, watering hole attacks, malvertising, phishing, spear-phishing, credential theft, and more.

However, not all isolation platforms are the same, which can make reviewing, selecting, and finally, deploying and employing an isolation platform confusing.

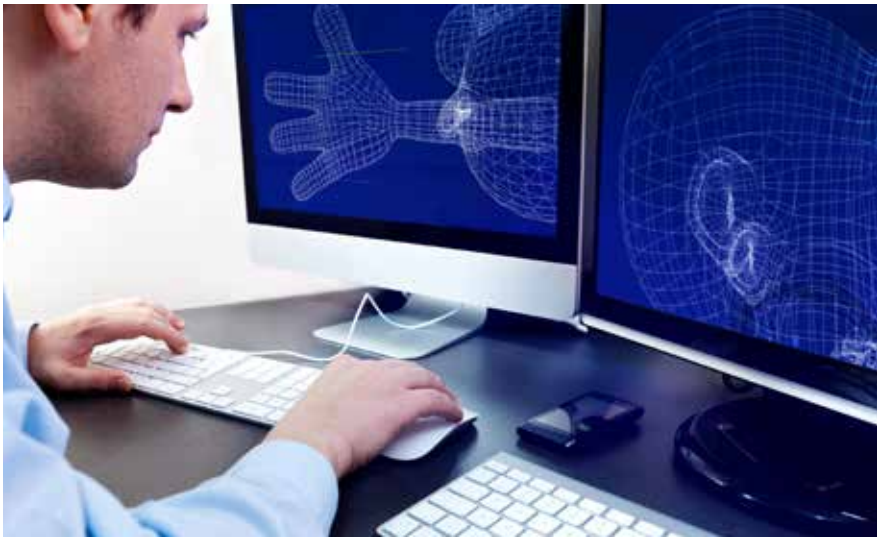
This document intends to provide entertainment industry content producers and, by default and enforcement, their services supply chain with selection and deployment best practice guidelines for web, email, and document isolation.

Isolation Best Practices

While there are several options when it comes to isolating web access, email, and documents, there are established and proven best practices that should be followed when it comes to implementing isolation in a security stack.

As a best practice, a state-of-the-art, enterprise-class isolation solution for an entertainment industry content producer would:

- Eliminate web-based malware (including drive-by downloads and watering hole attacks), weaponized documents, ransomware, and phishing attacks (including spear-phishing and whaling attacks).
- Generate zero "false positives" or "false negatives".
- Preserve the native user experience without discernible latency or browser impact.
- Work with any user endpoint device, operating system or web browser, and would not require the addition of a custom browser to the user's workflow.
- Offer a variety of deployment options, including global availability as a public cloud service, as an on-premises virtual appliance, or in a private cloud.



- Deploy quickly and simply, without requiring any endpoint software, web browser plug-ins, and network re-architecture, while working with existing and legacy network appliances.
- Integrate with existing security systems (e.g., secure web gateways), email infrastructure, and support most deployed single sign-on (SSO) and identity and access management (IAM) solutions.
- Reduce administrative burden of policy exceptions and lessen the workload for security operations centers (SOC).
- Provide privacy, with controls for extensive visibility and forensics.

The following are the best practices an enterprise-ready isolation solution should follow and the capabilities it should provide studios and production companies that produce movies, broadcast television, streaming content, and online and video games.

Flexible Deployment Options

Public Cloud Deployment: Global and Always-on

Global scale and adaptability are important factors when it comes to technology implementation for most entertainment industry content producers and their services supply chain. Since many studios and production houses outsource post-production services, oftentimes to offshore suppliers, global scale and accessibility are vital. A public cloud-based isolation platform supports tens, if not hundreds of thousands of users, worldwide. As a cloud-based platform, it scales quickly and effortlessly to address any increase in demand a studio or production facility requires. As the number of users or traffic surges, an isolation platform must be able to scale and adapt.

As rule of thumb, any security platform an entertainment industry content producer deploys should maintain a simple, consistent user experience

As rule of thumb, any security platform an entertainment industry content producer—or any organization, for that matter—deploys should maintain a simple, consistent user experience; a cloud-based isolation platform is no exception. Speed is always a factor when it comes to usability and productivity; as a best practice, a cloud-based isolation platform should route traffic based on the path of lowest latency to ensure a fast, reliable user experience, without latency, jiggle, or visual impediment. Network reconfiguration or increasing bandwidth shouldn't be required, as a cloud-based isolation platform should streamline integration with the existing network and security infrastructure of a studio, production house, or post-production facility.

On-premises Deployment: Flexible Physical, Virtual, or Private Cloud Deployment

An entertainment industry content producer or one of their services supply chain vendors may require or demand local network access due to mandates of industry or government security regulations. Or, a third-party hosting model cannot meet the security edicts of industry or government regulations. Therefore, as a best practice, an isolation platform must be deployable on-premises.

Ideally, an on-premises isolation platform would eliminate installation, configuration and maintenance costs associated with running complex stacks of software. Should an entertainment industry content producer decide to operate an isolation platform in a virtual appliance, the platform should be available as a pre-configured virtual machine image ready to run on leading hypervisors, including VMware vCenter Server, VMware ESXi, and Oracle VM Manager.

A virtual appliance deployment must also allow for rapid movement of instances between physical execution environments. Resource requirements must be reasonable, and not require extensive memory or storage space, regardless if physical or virtual. Processors and clock speeds must provide for effective processing and cost savings.

If a dedicated appliance is required, an isolation solution must be able to address this need, and if possible, provide a variety of options from which to choose. It must also address high availability needs to ensure reliability and constant protection from attacks. An entertainment industry content producer may require operations management capabilities either standalone or that integrate with existing management solutions; an isolation solution should be able to accommodate this request.

Multi-tenancy

Multi-tenant support in an isolation platform is vital for studios, production houses, post-production facilities, and other members of their services supply chain. It enables varying policies for access, isolation, and more to be applied against different groups. This, in many cases, may be a government or industry regulatory requirement. Tenant awareness also needs to be globally supported, regardless of user location. Additionally, if an on-premises deployment is required or desired, the isolation solution should support virtualization, enabling multiple versions of the virtualized image to be deployed in different locales or offices, enabling local support for differentiated policies – a requirement for studios, production houses, and post-production facilities with offices nationally or internationally.

Consistent, Simple User Experience

Even a minor change in user experience or workflow can have a negative, ripple effect on users' productivity. A consistent, fundamentally unchanged user experience is paramount best practice for any entertainment industry content producer. A user should experience the same workflow and be able to work with the same familiar software and services before and after deployment of an isolation solution. An isolation platform ensures that the creativity of content producers is not impeded by security. Isolation seamlessly enables content producers to be creative, secure, and productive.

For example, if an isolation platform forces users to use a new or different browser, or to change how they typically browse the web, it can significantly impact usability and user productivity. In a best-case scenario, minimal to no user experience and workflow impacts are best. Browser menus should remain unchanged. Users should be able to work with the tools made available to them in their native web browser, such as cut-and-paste, copy-and-paste, find in page, printing, and more, without limitation. Any browser extensions should be available and supported without requiring additional steps. Web pages in isolation

must appear as they would without isolation.

Dynamic content, such as JavaScript—which has been used as a conduit to deliver endpoint infecting malware—should be isolated and re-rendered, completely hidden from the user. Original web page images and fonts, and cascading style sheets (CSS)—all of which have been used to deliver malware payloads—should be isolated, all undetectable to a user. There should be no noticeable latency in serving an isolated web page. Pixelation, frozen images, choppy scrolling or other visual impediments, all common with "screen-scraping" technologies or with virtual desktop interface (VDI), must be eliminated with an isolation platform.

Embedded Adobe Flash must be isolated, as Flash sometimes camouflages malicious background tasks that may infect user devices

Embedded Adobe Flash must be isolated, as Flash sometimes camouflages malicious background tasks that may infect user devices. However, any Flash content must also be visible to a user. A best practice by an isolation platform is to convert Adobe Flash entities into a new encoded video format, such as HTML5. The new encoded video format must be provided to the user, as smooth and flowing just as it was intended to be, without flicker, hesitation, or artifact.

As a best practice, an isolation solution must isolate documents launched by links on webpages or embedded in emails. Support for most popular document types—such as Microsoft Office, Microsoft Office 365, Adobe Acrobat, Rich Text Format, and more—should be provided. Any document opened by a user must be isolated and opened in the isolation platform, away from a user's device. An option for a safe, secure download should also be made available, though, such as a clean and safe Adobe Acrobat (.pdf) version of a document, if a user requires a local copy. Or, if a user requires the original version of a document, and this is allowed by their organization as controlled by an administrator, the original document should be optionally scanned for viruses and possibly sandboxed for further testing, and only if deemed safe would it be available for the user to download.

Robust Endpoint Safety and Security

While dynamic content brings web pages to life and makes them entertaining and engaging, there is a dark side to dynamic content. Dynamic content, such as JavaScript, has oftentimes been used by attackers as a delivery mechanism for malware payloads when accessed by an unsuspecting user and their device. An isolation platform must isolate dynamic content, including JavaScript, and not allow it to reach a user's device. However, the accessed web page, even when isolated and re-rendered to the user on their device must continue to be as interactive and dynamic as intended, maintaining a satisfactory user experience. An isolation platform must deliver this, without latency, impairment

or visual artifact.

Many other web page components have, unfortunately, been leveraged by attackers to deliver malware to endpoint devices. For instance, cascading style sheets (CSS) have been used to conceal malware. Web page images and fonts have also served as a cover for malware. Cascading style sheets and web page images and fonts must not be allowed to be accessed "as is" by users and downloaded to their device. Instead, an isolation platform should stop CSS and web page fonts and images, re-render them, appearing just as they do on the web page a user selects, then send them to the user's device for viewing, yet again without latency, impairment, or visual impediment.

An isolation platform should also include several basic security mechanisms. For instance, an isolation platform should be able to neutralize any command-and-control (C2) communications any malware would attempt to launch unbeknownst to a user. By stopping malware C2, an isolation platform can prevent the malware not distributed via the web or email from taking control of a user's device or from exfiltrating sensitive data.

Another example of a security best practice is application traffic scanning and application traffic policy controls. An isolation platform should be able to analyze retrieved web traffic and determine if it matches a major URL category, and if that web traffic is a threat. An isolation platform should enable a studio, production house, post-production facility, and any organization in the services supply chain to define application traffic policy controls; that is, allow for the creation of policies that control traffic based on the application attempting to access a user's device. Also, while web browser plugins should be supported, an isolation platform should not allow those plugins to be executed on a user's device; instead, the plugins should be executed in the isolation platform, safely away from the device.

An isolation platform must also block file uploads to websites that are isolated, ensuring no information or data from a user's device can be uploaded to an isolated website, protecting the sensitive data of the user, the entertainment industry content producer, and their services supply chain.

Enterprise-ready Deployment

Studios and production houses, and their services supply chain, including post-production facilities should address security in a layered fashion, blending the best available security solutions from a variety of vendors. An isolation platform must be ready and available for deployment within a diverse, varied network and security environment. An isolation platform should never force a new equipment purchase, abandonment of legacy solutions, or re-architecture of existing

network infrastructure. It should work seamlessly and in concert with existing and legacy security solution deployments, with little or no change necessary.

The isolation solution should support flexible web traffic proxy. It should allow web traffic to be directed through the isolation platform simply by automatic configuration and provisioning, ideally via recognized device management systems, such as Microsoft Active Directory. If an entertainment industry content producer or one of their services supply chain vendors has an existing web proxy in place, the isolation platform must be flexible enough to support routing of web traffic through the existing proxy, while still performing isolation as required.

An isolation solution needs to integrate with existing anti-virus and anti-malware products, to complete the layered security approach

An isolation solution should be certified to work with—and should have examples of active deployments with—the industry leading, worldwide security solutions most organizations, including studios, production facilities, and their services supply chain vendors have deployed, such as firewalls, including next-generation firewalls (NGFWs), web proxy solutions, security information and event management (SIEM) offerings, and major threat detection vendor products. The isolation platform must integrate seamlessly with existing, recognized identity and access management (IAM) and single sign-on (SSO) products, including Microsoft Active Directory Federation Service (ADFS), as well as support Security Assertion Markup Language (SAML) 2.0, simplifying identity and management and access control for studios, production houses, their services supply chain providers, and their users.

An isolation solution needs to integrate with existing anti-virus and anti-malware products, to complete the layered security approach entertainment industry content producers and their suppliers need today. By supporting an array of existing anti-virus and anti-malware offerings, the isolation solution ensures any documents and files accessed over the web are scanned for viruses and malware. Post-scan, if a file or document is deemed as dangerous, the isolation solution must be able to alert the user to this danger.

Comprehensive Management Capabilities

A view into and the ability to analyze and manipulate collected data is a vital security component for studios, production facilities, and their supply chain. An isolation platform should provide a centralized, comprehensive view of all policies and log entries, enabling fast, accurate decisions on endpoint security. For studios and production facilities with worldwide locations, as well as their services supply chain vendors that are offshore, time is a fleeting commodity, especially regarding security. An isolation platform needs to provide template-based management for these organizations, saving them valuable time and human resources.

In addition, the ability to centrally view and manage policies and logs is a best practice for an isolation platform. Log data must be able to be extracted and exported into a studio or production company's deployed, existing SIEM or operations management system, for more intensive analysis and reporting capabilities. The exportation of log data is best supported via an application programming interface (API), simplifying the integration and information transfer process between an isolation platform and an existing system.

Eliminates Phishing Attacks

An isolation platform must eliminate phishing attacks. All email links should be opened in isolation, safely away from user devices. This would eliminate phishing, spear-phishing, and the threat of drive-by exploits. Any link, in any email, must be isolated, alleviating email-based malware threats, including ransomware.

Anti-phishing training is vital to ensuring employees and contractors are aware of the dangers of phishing, and how to identify a phishing email

While phishing itself is a dangerous intrusion that leads to malware infections and ultimately costly data breaches for studios, production companies, and their services supply chain, there is another phishing danger that is the springboard for even more serious attacks: Credential theft. An isolation platform should prevent sensitive user information, such as corporate user credentials (user names and passwords), credit card numbers, banking information, social security numbers or other government identification numbers, and more from being entered into malicious web forms on phony phishing web pages. It's a requirement that a studio, production company, or a member of their services supply chain be able to assign this capability based on any number of factors, including by user or group. This helps the isolation solution eliminate credential theft that leads to a greater loss or ransoming of critical information and data.

The monitoring of user behavior statistics, so that workflow policies may be defined and assigned, by group or individual, is also another best practice for an isolation platform. This capability helps an administrator target specific users or groups of users that are more likely to click on potentially dangerous email and web links, when access to those links is attempted, and how many times users or groups of users have attempted this risky behavior. Customizable workflow policies should include the ability for users or groups of users to input information into web forms, optional access to original documents, and more.

For many organizations, including studios, production facilities, and their services supply chain vendors, including post-production facilities, anti-phishing training is vital to ensuring employees and contractors are aware of the dangers of phishing, and how to identify a phishing email. While phishing training and awareness is important, its teachings need to be constantly, consistently reinforced to users for it to be most effective. As a best practice, an isolation solution needs to provide messages and warnings visible to users in real-time, as they attempt to access potentially dangerous emails, web links and web pages. The messages and warnings must be customizable for greatest impact. In this way, the isolation solution extends phishing training and reinforces the messages from that training constantly and consistently, extending the phishing training's benefit.

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 experts, 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**

Menlo Security
IT'S SAFE TO CLICK

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

Items of Which to be Aware

While there are best practices, there are also certain items to be aware of when researching, comparing, and assessing enterprise-level isolation solutions. These items should be a warning that the isolation solution may not be following best practices:

- It does not support multi-tenancy, or does not provide a mult-tenant management portal.
- It requires an increase in processor, storage, or other capacity.
- All web traffic is required to be routed to the same location or instance, increasing latency for users.
- It requires a bandwidth increase, which will increase costs.
- There is a limit on the number of users per deployment, requiring multiple deployments.
- The user experience delivers choppy, pixelated scrolling.
- The user's web browser experience is different and not consistent with their current practices.
- Videos are pixelated.

Conclusion

There is little argument that an isolation solution can serve as an important tool for studios, production houses, and their services supply chain vendors, including post-production facilities around the world in protecting against cyber attacks, and theft of movies, shows, or games, as well as sensitive communications and data. An isolation platform greatly reduces the threat of malware downloads leading to data hacks and breaches, and of credential theft from web and email attacks, phishing and hijacked websites, and other means. It is important for studios, production houses, and their services supply chain vendors to understand and believe in the importance of security, user experience, and administration in isolation platforms. This guide should assist in the selection, testing, and deployment of a best-in-class isolation platform that fits their specific security needs and requirements.