Menlo Security

IT'S SAFE TO CLICK

ISOLATION BEST PRACTICES FOR HEALTHCARE ORGANIZATIONS

A Menlo Security Best Practices Guide

Executive Summary

The primary reasons for HCO vulnerabilities are older, unpatched software versions, outdated security architectures, and an overall lack of IT security experts.

Hospitals and other healthcare organizations (HCOs) are increasingly singled out by cyber criminals for ransomware and other attacks. Not only are patients' sensitive records being targeted, but also—as the U.S. Federal Bureau of Investigation (FBI) warns—an HCO's intellectual property or patient's credit card information. The primary reasons for HCO vulnerabilities are older, unpatched software versions, outdated security architectures, and an overall lack of IT security experts, constrained by tightening budgets. Making matters worse, doctors and other healthcare professionals often utilize external email systems (webmail) outside of the hospital's security controls, increasing the likelihood the organization will be impacted by phishing and spear-phishing attacks.

An isolation platform can prevent these attacks. By executing web sessions and opening attachments away from a user's endpoint and delivering only safely rendered information to their devices, users are protected from malware and phishing attacks. With a native user experience, administrators can open up more of the Internet and allow more flexible email policies for their users, while simultaneously eliminating the risk of attacks.

This document is intended to provide isolation best practices, consolidated from hundreds of customer environments in order to optimize the deployment of an isolation platform for web, email, and documents for HCOs.

Introduction

The majority of today's healthcare-targeted attacks, such as ransomware, are motivated by financial gain rather than simple notoriety. Cyber criminals will always target those organizations with the weakest defenses and the most valuable data. Few industries are as dependent on data and information more than healthcare; without patient records, and functional medical and network devices, a healthcare facility cannot operate.

Cyber criminals will always target those organizations with the weakest defenses and the most valuable data.

Hospitals and clinics pose a relatively easy target due to the high number of network ingress and egress points, and the fact that doctors and other healthcare workers routinely use multiple, often unsecured, email accounts, devices, and networks. Compounding the issue, medical institutions often lack sufficient budget and IT staff to keep ahead of cyber threats, and as a result, are playing a perpetual game of catch-up.

The result is an increasing number of healthcare facilities are falling victim to ransomware and phishing attacks, where critical systems and/or data are held hostage by cyber criminals until a hefty Bitcoin ransom is paid. Traditional security products are failing to prevent these attacks.

It's time to abandon the detection approach. A new approach is needed, and that new approach is isolation.

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 that ALL content could be bad. So, it completely contains and executes the content far away from a user's endpoint device, rendering only safe visual elements to the user and their endpoint. An isolation platform can ensure an HCO and their users—employees, contractors, and the like—are safe and protected from phishing, spear phishing, credential theft, malware, drive-by exploits, watering hole attacks, and more. But not all isolation platforms are built alike. This document is intended to provide best practices for hospitals and HCOs choosing isolation for web, email, and documents.

Isolation Best Practices

While there are many options when it comes to isolating web access, email, and documents, there are established and proven best practices that should be followed when implementing isolation in your security stack. As a best practice, a state-of-the-art, isolation solution for an HCO would:

- Eliminate web-based malware, 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 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, or network re-architecture, while working with existing and legacy network appliances.
- Integrate with existing security systems (e.g., secure web gateways and next generation firewalls) and email infrastructure, and support most single sign-on (SSO) and identity and access management (IAM) solutions.
- Reduce administrative burden of policy exceptions and lessen the workload for security professionals.
- Provide privacy, with controls for extensive visibility and forensics.

The following are the best practices an enterprise-ready isolation solution should enable and the capabilities it should provide HCOs.

An isolation platform must eliminate phishing attacks, particularly those targeting physicians and other healthcare workers using webmail accounts.

Eliminates Phishing Attacks

An isolation platform must eliminate phishing attacks, particularly those targeting physicians and other healthcare workers using webmail accounts. All email links should be opened in isolation, safely away from user endpoint devices. This eliminates 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.

While phishing itself is a dangerous intrusion that can lead to malware and ransomware, and ultimately data breaches for HCOs, there is another phishing danger that is a catalyst for even more serious attacks: Credential theft. An isolation platform should prevent sensitive user information, such as user credentials (usernames and passwords), credit card numbers, banking information, social security numbers, or other government identification numbers from being entered into malicious web forms on phony phishing web pages.

The ability for an HCO to assign this capability based on any number of factors, including by user or group, is a must. In this manner, the isolation solution eliminates credential theft that leads to a greater loss 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 HCO's administrators target specific users or groups of users that are more likely to click on potentially dangerous email and web links.

For HCOs, and many other organizations, anti-phishing training is vital to ensure that 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 successful. As a best practice, an isolation solution needs to provide time-of-click messages and warnings that are visible to users when they attempt to access potentially dangerous emails, web links, and web pages. The messages and warnings should be customizable by the HCO. In this way, the isolation solution extends phishing training and reinforces the messages from that training in real time.

Flexible Deployment Options

Public Cloud Deployment: Global and Always-on

Scale and adaptability are important factors when it comes to technology implementation for most healthcare organizations. A cloud-based isolation platform can support tens, if not hundreds of thousands of users. A cloud-based isolation platform scales quickly and effortlessly to address any increase in demand an HCO requires. As the number of users or traffic surges, an isolation platform must be able to scale and adapt. As a rule of thumb, any security platform an HCO—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, and 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 should not be necessary, since a cloud-based isolation platform should streamline integration with an HCO's existing network and security infrastructure.

Ideally, an on-premises isolation platform would eliminate installation, configuration, and maintenance costs associated with running complex stacks of software.

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

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 HCO 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 necessary, 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. As larger HCOs 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 vitally important for HCOs. It enables varying policies for access, isolation, and more to be applied to different groups. This, in many cases, is a 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 of the HCO, enabling local support for differentiated policies – a requirement for HCOs operating multiple facilities and clinics.

Consistent, Simple User Experience

A consistent, fundamentally unchanged user experience is paramount best practice for any HCO.

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 HCO. 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.

For example, if an isolation platform forces its users to change browsers or how they browse the web, it can significantly impact usability and user productivity. In a best-case scenario, there are minimal to no user experience and workflow impacts. 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 or 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, all invisibly to 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, and undetectable to a user. There should be no noticeable latency in serving an isolated web page. Pixelation, 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 endpoint devices. However, any Flash content must also be visible to a user. A best practice by an isolation platform would be to translate Adobe Flash entities into a new, encoded video format, such as HTML5. The new format must be provided to the user smoothly, just as it was intended to be, without flicker, hesitation or artifact.

An isolation solution must isolate documents launched by links embedded in web pages or emails. Support for most popular document types—such as Microsoft Word, Excel, and PowerPoint, Adobe Acrobat, Rich Text Format, and more—must be provided standard. Any document opened by a user must be isolated away from a user's endpoint device. However, an option for a safe, secure download must also be available, such as a clean and safe Adobe Acrobat (.pdf) version of a document, if the user requires a local copy. Or, if a user requires the original version of a document, and this is allowed by their organization and policy 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 then be available for the user to download.

Robust Endpoint Safety and Security

In addition to Flash and JavaScript mentioned in the previous section, many other web page components have, unfortunately, been leveraged by attackers to deliver malware to an endpoint device. 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 accessed "as is" by users and downloaded to their endpoint device. Instead, an isolation platform should stop CSS and web page fonts and images, and re-render them to appear just as they do on the web page a user selects, then send them to the endpoint device for viewing, again without latency, impairment, or visual impediment.

As is the case with any security solution, an isolation platform must also include several basic security mechanisms. For instance, an isolation platform should neutralize command-and-control (C2) communications that some malware might attempt unbeknownst to a user. By stopping malware C2, the isolation platform can prevent malware that was not distributed via the web or email from taking control of a user's device.

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 the web traffic is a threat. An isolation platform should enable an HCO 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 endpoint device. Also, while web browser plugins should be supported, an isolation platform should not allow those plugins to be executed on a user's endpoint device; instead, the plugins should be executed in the isolation platform, safely away from the endpoint.

An isolation platform must also block file uploads to websites that are isolated, ensuring no information or data from a user's endpoint device can be uploaded to an isolated website, protecting the user's and the HCO's sensitive data.

Healthcare-ready Deployment

HCOs should address security in a layered fashion, incorporating best available security solutions from a variety of vendors. An isolation platform must be deployment-ready within a diverse, varied network and security environment. An isolation platform should not force an HCO to purchase new equipment, abandon legacy solutions, or re-architect existing network infrastructure. It should work seamlessly and in concert with existing and legacy security solution deployments, with little or no change required.

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 HCO 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 should be certified to work with—and should have examples of active deployments with—industry leading, worldwide security solutions that most HCOs 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, management, and access control for an HCO.

An isolation solution should be certified to work with industry leading, worldwide security solutions that most HCOs have deployed.

An isolation solution needs to integrate with existing antivirus and antimalware products, to complete the layered security approach HCOs require today. By supporting an array of existing antivirus and antimalware offerings, the isolation solution ensures any documents or 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 component of security for HCOs today. An isolation platform should provide a centralized, comprehensive view of all policies and log entries, enabling fast, accurate decisions on endpoint security. For HCOs, time is a fleeting commodity, especially regarding security. An isolation platform needs to provide template-based management, saving 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 an 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 the existing system.

Ensure Your Isolation Solution Follows Best Practices

While there are best practices, there are also certain items to watch for when researching, comparing, and assessing isolation solutions. These items should be a warning that the isolation solution does not follow best practices:

- It does not support multi-tenancy, or does not provide a multi-tenant management portal.
- It requires a dramatic 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 cost an HCO more.
- The user experiences 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 is an important tool for HCOs to deploy in their fight against the onslaught of cyber crime. An isolation platform can greatly reduce the threat of ransomware, malware, and credential theft from web and email attacks and other exploit methods. It is important for HCOs to understand and relate the importance of security, user experience, and administration in isolation platforms. This guide should assist in the evaluation, selection, and deployment of best-in-class isolation platforms, which fit a healthcare organization's specific needs and requirements.

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. 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**

IT'S SAFE TO CLICK

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