Menlo Security

ISOLATION BEST PRACTICES FOR INSURANCE PROVIDERS

A Menlo Security Best Practices Guide

Introduction

Insurance providers are increasingly singled out by cybercriminals. These providers are an attractive target because they maintain a treasure trove of sensitive client information—such as Social Security numbers, employment history, and family contacts—that can be exploited for the purposes of healthcare and tax fraud.

Many providers are vulnerable to cyberattacks because they rely on older and unpatched server software versions, outdated security architectures, and a lack of IT security experts, and they are constrained by tightening budgets. Making matters worse, employees often utilize external email systems (webmail) outside of the organization's security controls, increasing the likelihood they 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 device, and delivering only safely rendered information to users' devices, an isolation platform protects users from malware and phishing attacks. And because the isolation platform provides a native user experience, administrators can open 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 help insurance providers optimize the deployment of an isolation platform for web, email, and documents.

Many insurance providers are vulnerable to cyberattacks because they rely on older and unpatched server software versions, outdated security architectures, and a lack of IT security experts.

Isolation Demystified

An isolation platform can address many of the gaps in security that are currently left open and assailable by cyberattacks. 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 away from a user's endpoint device, rendering only safe visual elements to the user and their endpoint. An isolation platform can ensure that an insurance provider 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. The best practices discussed in the following sections will assist insurance providers when investigating isolation platforms for web, email, and documents.

Isolation Best Practices

An isolation platform can ensure that an insurance provider and their users are safe and protected from phishing, spear-phishing, credential theft, malware, drive-by exploits, watering-hole attacks, and more.

While many options are available when it comes to isolating web access, email, and documents, insurance providers should follow established and proven best practices when considering which isolation solution to implement in their security stack. As a best practice, a state-of-the-art isolation solution for an insurance provider 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, without requiring 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 (such as 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 the administrative burden of policy exceptions and lessen the workload for security professionals.
- Provide privacy, with controls for extensive visibility and forensics.

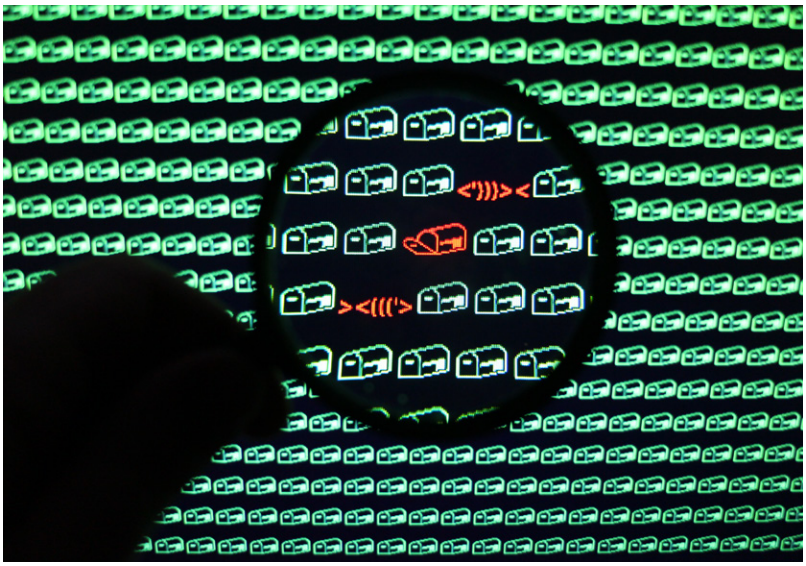
The following are best practices that an enterprise-ready isolation solution should enable and the capabilities it should offer to insurance providers.

Elimination of Phishing Attacks

An isolation platform must eliminate phishing attacks, particularly those targeting executives, adjusters, agents, and other insurance workers using webmail accounts. All email links should be opened in isolation, safely away from user endpoint devices. This strategy eliminates phishing, spear-phishing, and the threat of drive-by exploits. Any link in any email must be isolated in order to alleviate email-based malware threats, including ransomware.

An isolation platform must eliminate phishing attacks, particularly those targeting executives, adjusters, agents, and other insurance workers using webmail accounts.

While phishing itself is a dangerous intrusion that can lead to malware and ransomware cyberattacks—and ultimately data breaches for insurance providers—another phishing danger 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 a security administrator 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 can lead 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 administrators target specific users or groups of users who are more likely to click on potentially dangerous email and web links.

For many organizations, antiphishing training is vital to ensure that employees and contractors are aware of the dangers of phishing and know how to identify a phishing email. While phishing training and awareness is important, its teachings need to be constantly and 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 insurance provider. 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 insurance providers. A cloud-based isolation platform can support tens of thousands, if not hundreds of thousands, of users. A cloud-based isolation platform scales quickly and effortlessly to address any increase in demand that an insurance provider 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 insurance provider—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 insurance provider's existing network and security infrastructure.

As a rule of thumb, any security platform an insurance provider deploys should maintain a simple, consistent user experience; a cloud-based isolation platform is no exception.

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

An isolation platform must also be deployable as an on-premises solution. Ideally, an on-premises isolation platform would eliminate installation, configuration, and maintenance costs associated with running complex stacks of software. If an insurance provider decides to operate an isolation platform in a virtual appliance, the platform should be available as a preconfigured virtual machine (VM) 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, whether the deployment is 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 insurance providers 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 insurance providers. It enables varying policies for access, isolation, and more to be applied to different groups. This capability, in many cases, is a regulatory requirement. Tenant awareness also needs to be globally supported, regardless of user location. In addition, 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 insurance provider. This capability enables local support for differentiated policies—a requirement for insurance providers that operate multiple facilities and clinics.

A Consistent, Simple User Experience

If an isolation platform forces its users to change browsers or the way they browse the web, it can significantly impact usability and user productivity.

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 a paramount best practice for any insurance provider. 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 the way 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 when an isolation platform is deployed. 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, 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 by 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 a 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 email. Support for most popular document types—such as Microsoft Word, Excel, PowerPoint, Adobe Acrobat, Rich Text Format, and more—must

be provided as a standard capability. Any document opened by a user must be isolated from the 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 in a policy controlled by an administrator, the original document should be optionally scanned for viruses and possibly sandboxed for further testing. Only if or when the document is deemed safe would it 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, enable them to appear just as they do on the web page a user selects, then send the necessary code to the endpoint device for rendering in the user's web browser so they can be viewed again without latency, impairment, or visual impediment.

Another example of a security best practice is application traffic scanning and application traffic policy controls.

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 whether it matches a major URL category and whether the web traffic is a threat. An isolation platform should enable an insurance provider 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 plug-ins should be supported, an isolation platform should not allow those plug-ins to be executed on a user's endpoint device; instead, the plug-ins 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 that no information or data from a user's endpoint device can be uploaded to an isolated website, thus protecting both the user's and the insurance provider's sensitive data.

Provider-Ready Deployment

Insurance providers should address security in a layered fashion, incorporating the 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 insurance provider 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.

An isolation platform should not force an insurance provider to purchase new equipment, abandon legacy solutions, or re-architect existing network infrastructure.

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 insurance provider has an existing web proxy in place, the isolation platform must be flexible enough to support routing of web traffic through the existing proxy and to support proxy chaining, 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 insurance providers 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). It must also support Security Assertion Markup Language (SAML) 2.0, to simplify identity, management, and access control for an insurance provider.

An isolation solution needs to integrate with existing antivirus and antimalware products, to complete the layered security approach that insurance providers require today. By supporting an array of existing antivirus and antimalware offerings, the isolation solution ensures that any documents or files accessed over the web are scanned for viruses and malware. Postscan, if a file or document is deemed to be dangerous, the isolation solution must be able to alert the user to this danger.

Comprehensive Management Capabilities

The ability to view into, analyze, and manipulate collected data is a vital component of security for insurance providers today.

The ability to view into, analyze, and manipulate collected data is a vital component of security for insurance providers today. An isolation platform should provide a centralized, comprehensive view of all policies and log entries, enabling fast, accurate decisions on endpoint security. For insurance providers, 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 security information event and management (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.

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

For more information, visit **menlosecurity.com**

Make Sure Your Isolation Solution Follows Best Practices

When researching, comparing, and assessing isolation solutions, insurance providers should not only ensure that the solution they choose follows best practices, but also watch for items that are not desirable in an isolation solution. 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 insurance provider 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

An isolation solution is an important tool for insurance providers to deploy in their fight against the onslaught of cybercrime. An isolation platform can greatly reduce the threat of ransomware, malware, and credential theft from web and email attacks and other attack methods. It is important for insurance providers to understand best practices for security, user experience, and administration in isolation platforms. This guide should assist in the evaluation, selection, and deployment of a best-in-class isolation platform to fit an insurance provider's specific needs and requirements.

Menlo Security

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