White Paper

Menlo Security Isolation Platform

Technology Overview

Menlo Security

The prevailing security model is rooted in the assumption that security systems can reliably distinguish between what's "good" and what's "bad"

Introduction

The Menlo Security Isolation Platform (MSIP) eliminates malware from key attack vectors including Web and Email. The MSIP uses patent-pending, cloud-based isolation and Adaptive Clientless Rendering™ (ACR) technology that obviates the need for endpoint software or plug-ins and delivers a transparent user experience. As a result, organizations can now deploy isolation technology at scale to open up more of the Web to users while simultaneously eliminating the risk of infection by Web-borne malware.

This paper provides an overview of the key technology innovations underlying the Menlo Security Isolation Platform and also presents several applications supported by the Platform.

Pervasive Threats from Web and Email

The Web and email are the two main vectors by which users and their organizations are compromised today. The scope of risk from Web and Email are enormous. Per a recently published study[1] :

- 1/3 of the Alexa top 1 million Web sites are either malicious (e.g. serving malware) or vulnerable to compromise by attackers.
- 1/5 of the top 1 million Web sites are running software with known vulnerabilities (published CVEs) and are vulnerable to compromise.

It's therefore no wonder why attackers find it relatively easy to find sites that can be used to launch attacks. The situation with email is equally challenging: In a recent study, Verizon reported that 23 percent of recipients open phishing emails, and 11 percent click on attachments.

Despite enormous investments in the current crop of security technologies (and user training), organizations continue to be compromised at alarming rates. Clearly, conventional threat prevention systems are proving inadequate in the face of today's threat environment.

Threat Prevention Today: "Good" vs. "Bad"

Conventional threat prevention products attempt to distinguish between "good" content and "bad" content, and then implement policies intended to allow the good content and block the bad. This approach to threat prevention is ineffective. Signature-based technologies like anti-virus and intrusion prevention cannot stop modern malware. Advanced detection techniques using big data analysis and behavioral modeling are equally ineffective. And technologies like network sandboxing that temporarily contain and execute content to look for malicious behaviors ultimately come down to a policy decision to allow or block the original content from reaching it's target. In every case, the good vs bad determination is never perfect, and thus the policy choice involves high levels of risk and high costs for mistakes:

- False positives block users from accessing legitimate content, which compromises productivity, generates requests for re-classification of blocked content and creates security alerts that have to be analyzed by the IT security team. In a recent study[2], organizations reported wasting $1.3M annually investigating malware alerts.
- False negatives allow malware and phishing attacks to reach users and their devices, which can lead to significant losses via data theft and fraud.

[1] *State of the Web 2015: Vulnerability Report, Menlo Security, March 24, 2015*

[2] *"The Cost of Malware Containment", Ponemon Institute, January, 2015*

Menlo Security

Every generation of detection-based prevention technology sparks a new generation of attacks that evade defenses

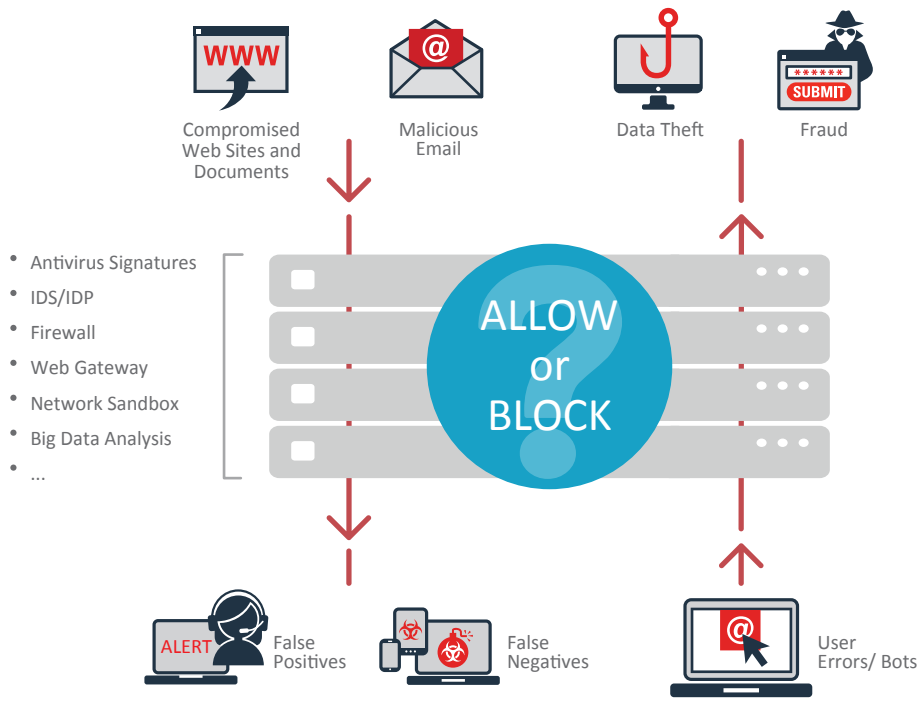

Figure1: Legacy threat prevention solutions are failing

Security professionals are locked in a cat-and-mouse struggle with smart, motivated, well-financed attackers, and every generation of detection-based prevention technology sparks a new generation of attacks that evade defenses. It's time for a new approach.

The Promise and Challenge of Isolation

Isolation enables administrators to open up more of the Internet to their users while simultaneously eliminating the risk of attacks

A new model for security is emerging that avoids the problems of trying to distinguish between legitimate content and malware, between good and bad. This model, based on isolation technology, inserts a secure, trusted execution environment, or Isolation Platform, between the user and potential sources of attacks. By executing user sessions away from the endpoint and delivering only safe rendering information to user devices, users are protected from malware and malicious activity.

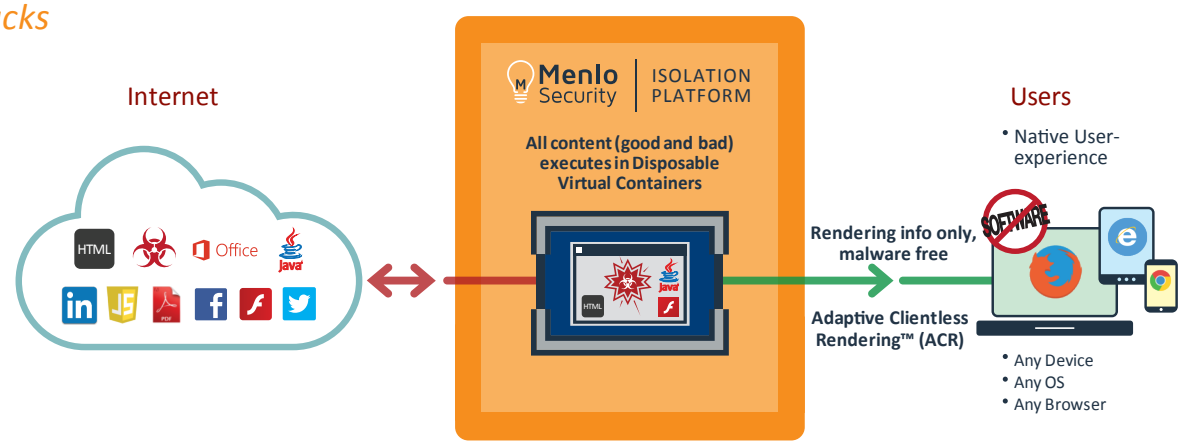

Figure 2: Isolation eliminates malware with no false positives or false negatives

Menlo Security

Isolation eliminates the possibility of malware reaching user devices via compromised or malicious Web sites or documents. The user's session and all active content (e.g. Java, Flash, etc.), whether good or bad, is fully executed and contained in the isolation platform. Only safe, malware-free rendering information is delivered to the user's endpoint. No active content - including any potential malware - leaves the platform. As a result, malware has no path to reach an endpoint, and legitimate content needn't be blocked in the interest of security. Isolation thus enables administrators to open up more of the Internet to their users while simultaneously eliminating the risk of attacks.

Prior attempts to use isolation technology to prevent malware have suffered from several key limitations, chief among these the need to deploy and manage endpoint software and interference with the user's native experience. These issues have limited the widespread adoption of isolation technology.

The Menlo Security Isolation Platform

In order to be accepted by users and scale across an enterprise, an isolation solution must be:

- Transparent – no impact on the user experience
- Easy to deploy and manage – no requirement for endpoint software

The Menlo Security Isolation Platform (MSIP) delivers on the promise of isolation security without compromising the user experience or placing a significant burden on IT staff. By leveraging patent-pending virtualization and Adaptive Clientless Rendering (ACR) technologies, the MSIP enables enterprise-wide deployment of isolation security, dramatically reducing risks while opening up more of the Internet.

MSIP Architecture

The MSIP is available as a public cloud service and can also be delivered as a virtual appliance for deployment in an organization's data center.

The MSIP is deployed between a user's device (e.g. desktop, laptop, tablet or smartphone) and the Internet. User Web requests are proxied via the MSIP, which accesses the Web on the user's behalf and executes the user's session completely. Only safe, malware-free rendering information is sent to the user's endpoint, eliminating the possibility of malware reaching the user's device. The Platform, which provides isolation for both clear-text (HTTP) and SSL-encrypted (HTTPS) Web content, is available as a public cloud service and can also be delivered as a virtual appliance for deployment in an organization's data center.

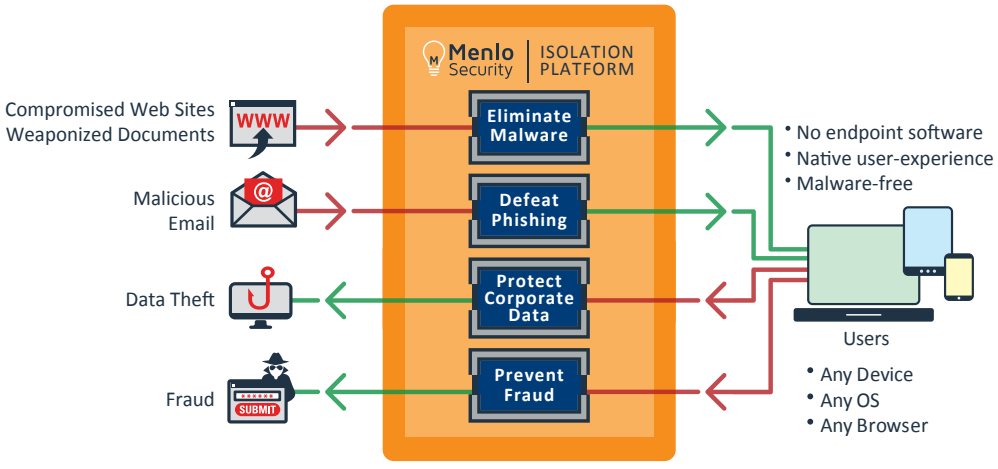

Figure 3: Available as a public cloud service or for deployment in an organization's data center, the MSIP eliminates malware and its effects across the most critical threat vectors

Menlo Security

In addition to preventing malware from reaching endpoints, the MSIP can also perform other functions, such as blocking user input to designated Web sites, effectively making them "read only"

The MSIP architecture is based on two key elements: Disposable Virtual Containers (DVCs) and Adaptive Clientless Rendering (ACR) technology, which are described below:

Disposable Virtual Containers (DVCs)

DVCs are dedicated containers within the MSIP. Execution of all active content in the user's session takes place entirely within the DVCs. The Platform allocates a new DVC any time a user opens a new tab on their browser. The MSIP maintains a pool of idle DVCs so that there's no latency associated with "starting up" a user's session. Whenever a browser tab closes (or unauthorized activity occurs) the associated DVC is disposed along with all content, preventing the ability of malware to persist or spread.

The DVC provides complete control over the execution of the user's session in both directions, i.e. from Web server to endpoint and vice-versa. So in addition to preventing malware from reaching endpoints, a DVC can also be used to perform additional security functions, such as blocking user input to designated Web sites, or specific sub-sections within these sites, effectively making them "read only". This capability can be used to prevent users from entering information into social media sites, or from mistakenly uploading private data into phishing or other malicious Web sites.

Adaptive Clientless Rendering Technology

Menlo Security's patent-pending Adaptive Clientless Rendering (ACR) technology provides the connection from the user's session running in the MSIP to the user's native browser. ACR technology requires no endpoint software or plug-ins and delivers a completely native user experience essentially indistinguishable from direct interaction with a Web site.

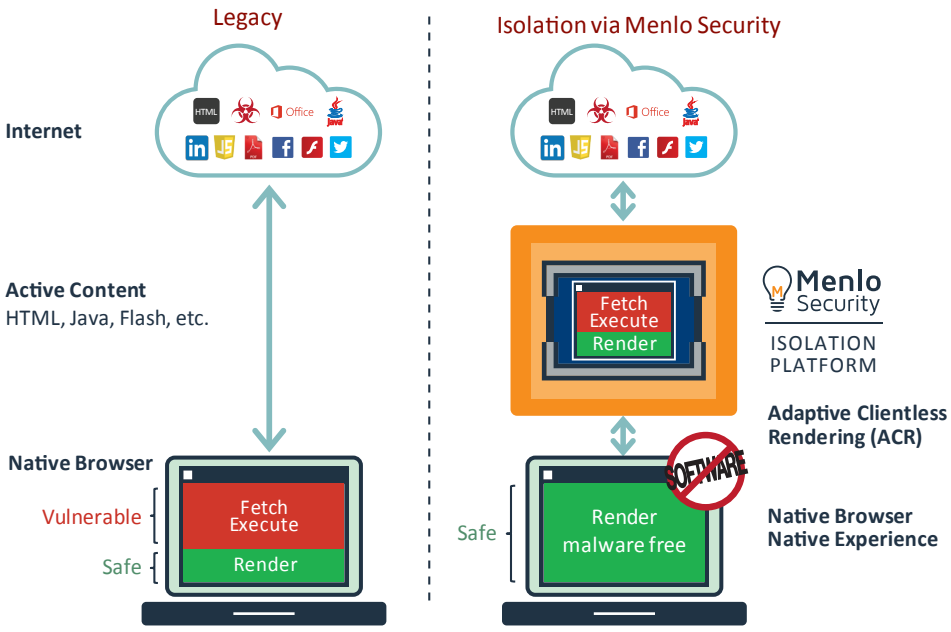

Figure 4: Menlo Security's Adaptive Clientless Rendering technology delivers a malware free, transparent user experience to the user's native browser

ACR technology leverages the fact that all modern browsers use a common framework for describing the elements on a Web page, including text, graphics, video, etc. When Web content executes normally in a user's browser it generates document object model (DOM) elements and an associated rendering tree that tells the browser how to create the user's display. When a user's session is executed in the MSIP it also generates DOM and rendering tree information which is then optimized

Menlo Security

ACR technology delivers a user experience essentially indistinguishable from direct interaction with a Web site

and synchronized via the ACR protocol to the user's browser. The user's browser takes the information delivered via the protocol and generates the user's view as if the content were executing in the local browser.

A trusted JavaScript delivered to the user's browser from the MSIP at the beginning of each session establishes and maintains the ACR channel using SSL. For each type of Web content the ACR engine selects the optimal encoding and transport mechanism for delivery to the user's browser. For example, dangerous content such as Java or Flash is executed in the MSIP and then delivered as a hi-fidelity, interactive experience in the user's browser. In all cases, the user's browser receives non-executable, malware-free content that renders naturally and preserves the user's native experience. The ACR protocol carries user activity (keystrokes and mouse clicks) to the MSIP and prevents malicious activity from flowing in the upstream direction.

By optimizing the processing and delivery of each content type, ACR technology provides a better experience than other approaches to remote rendering in several respects:

- Works with the user's native browser (IE, Chrome, Safari, Firefox), meaning no requirement for any software on the end user device i.e. no thin client, replacement browser, plug-in, etc.;
- No pixelation, choppy scrolling or other visual artifacts common with "screen-scraping" technologies like VDI;
- Preservation of native browser functionality such as cut and paste, printing, etc.;
- Native support for browser extensions.

Key Architectural Advantages of the MSIP

The Menlo Security Isolation Platform delivers a secure, scalable and transparent isolation solution with unique characteristics, including:

Imperceptible Latency

The MSIP and ACR technology eliminate any discernible latency from the user's experience.

Easy Deployment and integration

The MSIP is available as a public cloud service as well as on-premises via virtual appliances. Configuring endpoints to use the service is a simple proxy setting that can be provisioned automatically. The service integrates easily with Web security gateways and other infrastructure including single sign-on systems.

Comprehensive Security and Privacy Controls

MSIP technology is based on a comprehensive security architecture that addresses all aspects of the infrastructure. User logs are viewable only by the customer.

Extensive Visibility and Forensics

The MSIP provides robust data for forensics, including:

- Browsing activity by user and Web category
- Browsing activity to sites with known vulnerabilities
- Malware activity (e.g. attempts to access or execute unauthorized files or processes)
- Threats averted

Log data can also be sent to an organization's SIEM system.

Menlo Security

Common Use Cases

The MSIP can be deployed stand-alone or in conjunction with existing security systems to address a range of critical needs, including:

Safe Access to Uncategorized Web Sites
Isolating uncategorized Web sites via the Menlo Security Platform enables users to safely access more of the Web while reducing the risk of malware.

Safe Viewing of Web Documents
The MSIP can eliminate the risks from weaponized documents (.pdf, .doc, .xls, .ppt) by isolating them in the Platform. Administrators can optionally allow users to download "safe" PDF versions of rendered documents (with all active content removed) and can also allow download of original documents for designated users.

Eliminate Java and Flash from Endpoints
Potentially harmful content such as Java and Flash is executed within the Platform, delivering a high-fidelity experience to the user without allowing any active content to reach and infect the endpoint. Administrators can remove Java and Flash from user's browsers but still allow access to Java and Flash content without the risk of malware.

Safe Email and Anti Phishing
The MSIP isolates and eliminates malware from sites accessed by clicking on links in emails. Additionally, the Email Isolation Service blocks user inputs to unknown Web sites and thus prevents users from revealing their personal information to phishing sites.

Protect Online Applications Against Bots
Operated as a "reverse proxy," the MSIP can protect Web applications against fraud perpetrated by bots and other malware on infected endpoints. It defeats man-in-the browser, credential stealing and other exploits. Deployed in the data center between the Web server tier and the Internet, the MSIP is transparent to the user's Web experience and requires no modification of the Web application.

Summary

The Menlo Security Isolation Platform delivers a unique and compelling set of benefits:

- Zero malware – No harmful content leaves the MSIP
- Zero false positives or false negatives
- Zero impact on user experience - No noticeable latency, native experience
- Zero software to install
- Zero compatibility issues – Works with any hardware, OS or browser
- Prevents attacks via Web content, documents, phishing, and infected endpoints
- Integrates with existing security systems (e.g. Web security gateways), mail systems, single sign-on and other infrastructure

Menlo Security

For More Information
www.menlosecurity.com