WHITE PAPER

SPIKES SECURITY

AirGap™

The Technology That Makes Isla® a Powerful Web Malware Isolation System

Introduction

Web browsers have become a primary target for cyber attacks on the enterprise. If you think about it, it makes perfect sense. The ubiquitous web browser is the only application on your desktop that regularly downloads and executes code from trusted and untrusted networks. And because ports 80 and 443 on corporate firewalls are always open, there is pretty much a direct connection between internal users and external web sites, even if it first passes through a web proxy. It's not surprising then, that hackers are able to develop and launch complex APTs, drive-by malware, polymorphic threats, and various zero-day attacks to exploit the inherent vulnerabilities associated with browser code and plug-ins.

The traditional response to this never-ending security problem has been to augment the firewall with a multi-layer, defense-in-depth (DID) security architecture to protect the network perimeter and endpoint devices. The assumption is that if the first layer does not detect the attack, the second layer will, and so on. This DID architecture is typically based on various forms of detection technologies (signatures, heuristics, content analysis, etc.).

Unfortunately, the headlines we see each week of new cyber attacks provide strong evidence that detection technology is no longer effective in protecting corporate networks. In fact, this was verified in research of more than 1,000 organizations published in 2015 by FireEye, which showed that 96% of these organizations had been breached even though all of them employed a DID security strategy[1]. Clearly, detection technologies are failing miserably.

> ***96% of the 1,000 organizations had been breached even though all of them employed a DID security strategy.***

Isolation Technology

More recently, some vendors have begun to offer endpoint security products focused on software-based isolation through sandboxing. While this strategy represents a step forward, it also has inherent risks. For example, software sandbox technologies can be breached through targeted attacks, giving hackers full access to all files and resources on the endpoint and possibly inside the corporate network. Other vendors have tried hardware-assisted endpoint isolation, which also represents a step forward. However, it faces similar risks of vulnerabilities, plus the complexity of deployment, configuration, and updates on a broad scale makes it less attractive to enterprise customers.

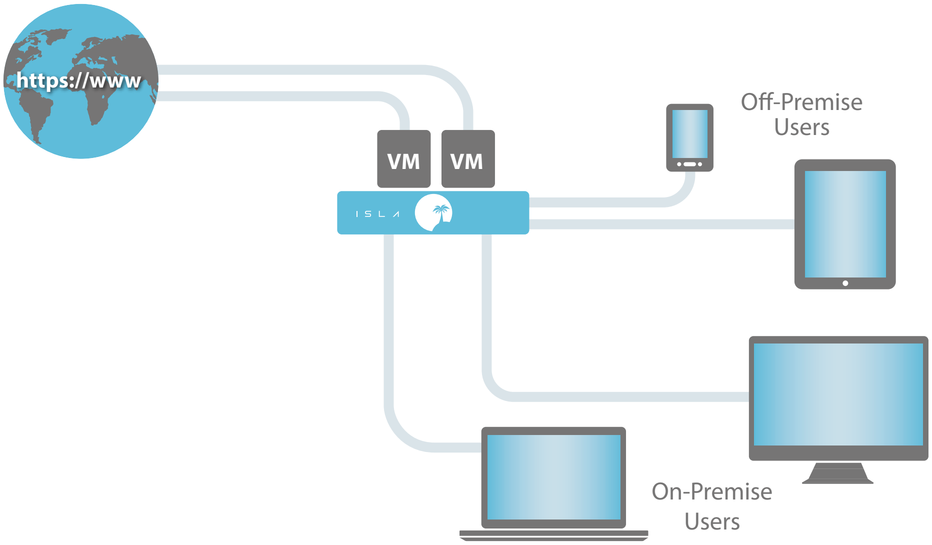
The safest, most effective solution to this problem is to apply isolation technology to the entire network, rather than individual endpoints. More specifically, what this means is that all external web content – whether it is from trusted or untrusted web sites – should be isolated and

[1] FireEye, (2015) Maginot Revisited: More Real-World Results from Real-World Tests. Retrieved from: https://www2.fireeye.com/WEB-2015RPTMaginotRevisited.html

rendered outside the network, and never be allowed to access endpoint devices. This network isolation strategy effectively eliminates the web browser as the primary vector for cyber attacks on businesses.

AirGap Isolation Technology

Spikes Security provides network-level, browser malware isolation through its patent-pending AirGap isolation technology. This breakthrough technology has been integrated into the Isla® family of security appliances, which are deployed in the DMZ outside the corporate firewall. The appliances prevent all browser malware from entering the corporate network and infecting endpoint devices, while providing end users with a safe and secure browsing experience. This paper summarizes the underlying architecture and components of the AirGap technology.



Physical Isolation

The value of the AirGap technology and architecture begins with its ability to create literal physical separation and isolation between untrusted content and a secure network. Specifically, what this means is that while end users are located inside the network, the active web browser is located on the Isla appliance outside the network. End users inside the network can continue to use their favorite web browser (or a lightweight Isla client viewer), but they no longer have direct access to the web. Instead, desktop browsers connect directly to Isla, which processes all web requests from end users, then fully renders the original web content on the appliance – never on the endpoint inside the secure network. Isla then actively and continuously transforms all audio, video, text, and graphics and delivers that to the browser on the desktop (which essentially becomes a "viewer"). From a security perspective, this isolation ensures that any malware-infested web content stays on the appliance outside the network.

Resource Isolation

One of the obvious benefits of isolating the browser outside the network is the resulting isolation of the endpoint (OS, applications, and files) from all browser-borne malware. As a result, cyber criminals can no longer exploit vulnerabilities of the internal browser to gain access to the operating system or any other internal resources on endpoint devices. Instead, malware-infected web sessions are terminated outside the firewall on the Isla appliance. The appliance is designed for maximum security, and only runs SE-Linux®, a Type 1 hypervisor, and a specialized browser – there are no other sensitive files or personally identifiable information stored on the appliance. Essentially, the Isla appliance is an empty room with no doors, no windows, no information, and no opportunity for malware to access the network and infect the organization. It is where malware goes to die.

Session Isolation

When end users inside the network initiate an external web session (via a web content request using their normal browser), the AirGap technology on Isla automatically creates and launches each user web session within its own isolated VM, administered using a fast, efficient, and secure Type 1 hypervisor. The software VM – combined with hardware-assisted isolation enforced with the Intel® Virtualization Technology (VT) processor extensions – ensure that each user session is completely isolated from all other user sessions. Memory, disk, and CPU resources are not shared between users, thus preventing any form of malicious activity or cross-contamination between user sessions. When a user completes a session, each VM is completely destroyed – along with malware that may have been downloaded into that VM. The Isla appliance also destroys any stored data, session cookies, and residual data. This ensures that each user always enjoys a clean, secure, high performance browsing session.

> ***Each user always enjoys a clean, secure, high performance browsing session.***

Content Isolation

As noted above, when original web content is rendered within the Isla VM, it is possible that it could contain malware, and thus should not be delivered to the endpoint in that state. For that reason, the AirGap technology actively and continuously transforms all web content – audio, video, text, and graphics – to benign multimedia streams. Think of it as a "digital distillation" process where all content is purified. In this process, all data streams carrying requested content are automatically cleansed of potentially malicious payloads, making it impossible for cyber criminals to inject malformed activity commands within the content. In terms of content delivery to the internal network, all data streams are isolated and kept private with strong AES-256 encryption, which uses 256-bit symmetric key pairs that are generated when a client registers (or re-registers) with the Isla appliance. These keys are used to establish a uniquely encrypted communication path for each individual client to provide complete privacy for each user session. This strategy is far more secure than traditional SSL connectivity.

Isolating Attackers

Even with the AirGap's complete, end-to-end focus on security through isolation, it is important to be prepared to isolate any suspicious traffic that may target the Isla appliance. To isolate potential intruders, AirGap technology includes active monitoring with trip wires that instantly identify and isolate any malicious traffic. This is actually fairly easy to do on Isla because, remember, the system is purpose-built for specific functions. So if any unauthorized activity, non-standard system states, or blocked processes are found, AirGap technology automatically isolates the out-of-bounds activity and can immediately destroy the VM session (and all malware it may contain).

Summary

The only effective way to prevent all browser-borne malware attacks – known or unknown – is to shift the focus from detection to isolation. Specifically, web browser isolation deployed at the gateway outside the firewall is the most secure, most scalable, and least complex way to eliminate the primary threat vector for cyber attacks on the enterprise. And the best solution available is the Isla browser isolation system based on patent-pending AirGap technology from Spikes Security. Learn more or request a demo at www.spikes.com.