Network Malware Isolation

The Technology That Makes Isla® a Powerful Tool for Defeating Malware

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 both 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 can 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 strategy1. Clearly, detection technologies are failing to counter modern threats.

Isolation Technology

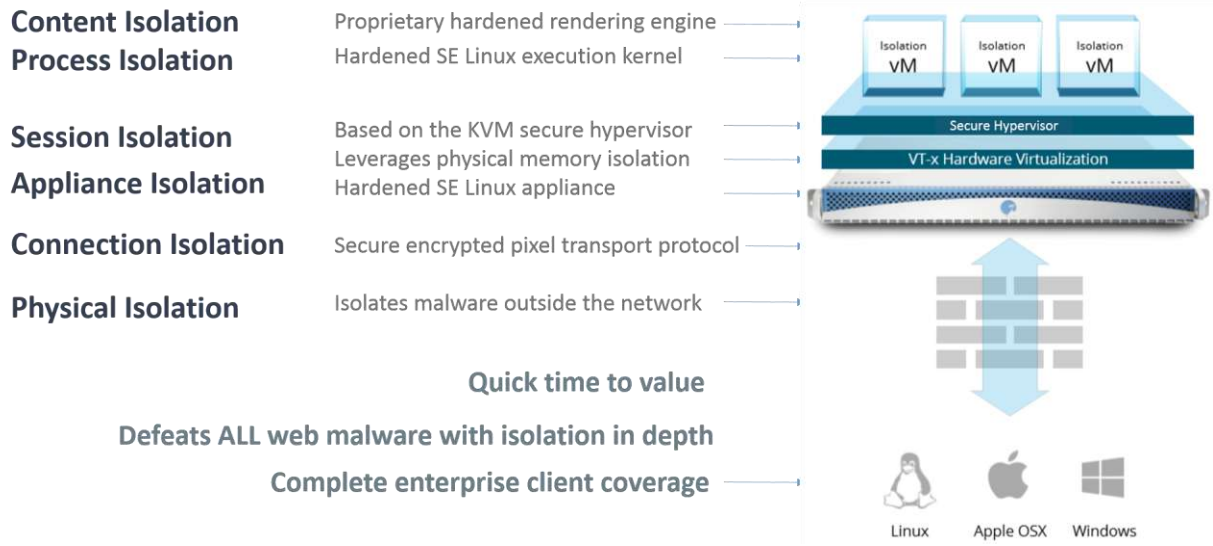
For many years vendors have been offering endpoint security products focused on software-based isolation through sandboxing. While this strategy represents a step forward, it also has inherent risks. For example, software sandbox technologies can be breached through targeted attacks, giving hackers full 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, hardware and software dependencies coupled with the complexity of deployment, configuration, and updates on a broad scale makes it less practical for enterprises to deploy and maintain.

There has been an emerging consensus in the industry that Isolation will be a key part of an organizations defenses in the future. 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 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.

Isla Web Malware Isolation Technology

Cyberincs Isla provides network-level, browser malware isolation. This breakthrough technology has been implemented in the Isla® family of security appliances, which are deployed in the DMZ outside the corporate firewall, or hosted in a private cloud datacenter. 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.

Isla applies the concept of “defense in depth” by implementing “isolation in depth” to the problem of malware exploits. The diagram below summarizes the underlying architecture and components of the Isla Network Malware Isolation solution.



Isolation in depth:

Content Isolation- Isla isolates all web content in a hardened rendering engine with no access to the endpoint or other processes executing within the **R**emote **A**pplication **C**ontainer or RAC.
Process Isolation- The Isla RAC uses a hardened SE Linux operating system kernel which applies mandatory access controls to isolate each running process from each other.
Session Isolation- Each Isla session is contained within its own RAC which is isolated from all other sessions using Intel’s VT-X technology. This delivers hardware based separation of the execution environment of each RAC ensuring that attackers have no access to other sessions.
Appliance Isolation- The Isla appliance uses a hardened SE Linux kernel with mandatory access controls to ensure the appliance is isolated from attack be external threat actors.
Connection Isolation- Isla utilizes a secure, proprietary transport protocol between the user and the appliance ensuring complete isolation of each connection.
Physical Isolation- Deploying Isla outside the perimeter of the protected network ensures that no malware can attack the endpoint or be used for covert surveillance of the network.

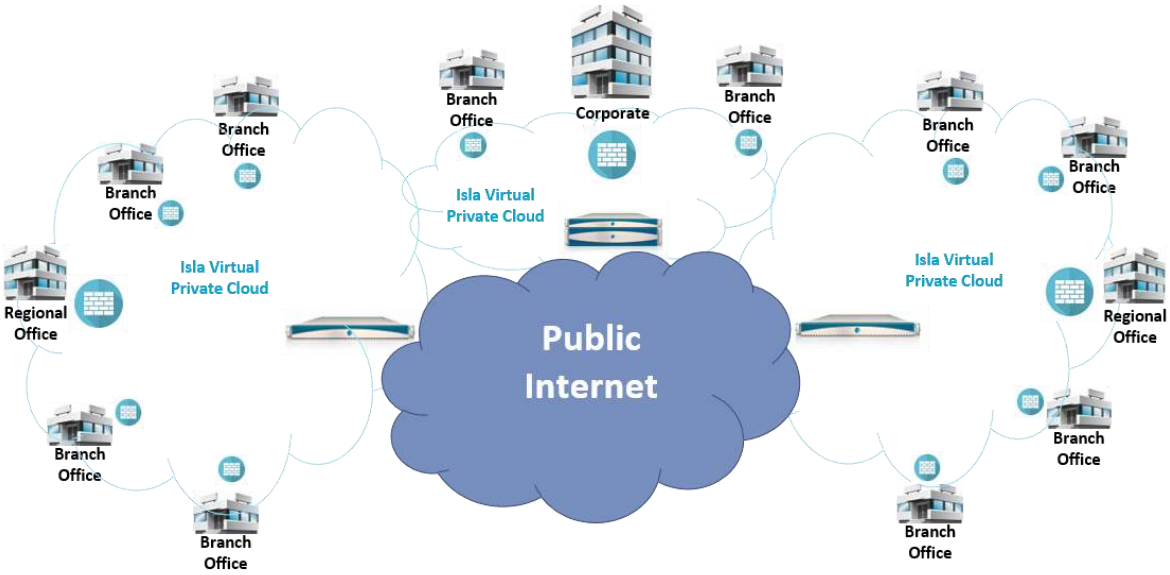
Isolating Attackers

Even with the Isla’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, Isla includes active monitoring with trip wires that instantly identify and isolate any malicious traffic. So, if any unauthorized activity, non-standard system states, or blocked processes are found, Isla automatically isolates the out-of-bounds activity and can immediately destroy the VM session (and all malware it may contain).

Flexible Deployment

Isolating potentially dangerous web content at the network layer rather than the individual endpoint provides the security architect with many options to optimize their defenses. Isla appliances, deployed outside the firewall in a “DMZ” segment of the corporate firewall provide the flexibility of a cloud deployment while ensuring ownership and control of the end to end solution. We refer to this type of deployment as a “Virtual

Private Cloud" enabling protection of multiple corporate locations from a regionally centralized location which lowers the costs of deployment and maintenance.



Isla Private Cloud Architecture

Isla Cloud Service

For those organizations that are looking to move their infrastructure to the "cloud" Isla is offered as a "turn key" service by Cyberincs' Isla Cloud Service partners. Isla Cloud service offers all the benefits of a cloud delivered service, no upfront capital investments, lower operational costs and a professionally managed service.

Isla Cloud Service Partners deliver the highest levels of service and security directly from their data centers and enjoy the benefits of a full partnership with Cyberinc to ensure that the highest levels of browser security are available around the clock and around the world.

ISLA
Isla Cloud Service

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 or in the cloud , 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 network malware isolation system. Learn more or request a demo at www.cyberinc.com.