For Discussion with Authorized Recipients Only

InZero Technologies

Patented TrustWall: the Mobile Device Firewall

Keeping the horse inside the barn, even if the door is open.

1. IN A NUTSHELL

Software security products remain vulnerable to malware, and can themselves become the conduit for spreading infection. This was recently brought home by the Clever "DoubleAgent," a malware that could exploit weaknesses found in 14 commonly used commercial security products. (*"The Clever "DoubleAgent" attack turns Antivirus into Malware,"* https://www.wired.com/2017/03/clever-doubleagent-attack-turns-antivirus-malware)

Consequently, more than ever, the need remains for an effective mobile firewall to prevent data exfiltration from an endpoint device in case of network or endpoint compromise. Existing software endpoint security provides no concrete assurance against

- ✓ zero-day attacks,
- ✓ the successful phishing scheme,
- ✓ exploitation of inadvertent OS code error,
- ✓ the malicious insider, or
- ✓ even the failure to heed network alerts (as occurred in the Target breach).

To advance security beyond "*Patch and Pray,*" InZero's TrustWall was created specifically to act as a hardware-enforced last line of defense "just in case" of infection. TrustWall is designed to eliminate data leak risks by creating a hardware-enforced firewall for mobile devices that prevents outgoing intranet data transmittal to an unauthorized recipient address. TrustWall creates a separate, isolated hardware-enforced firewall environment so that it is inaccessible to malware or code error that can compromise an operating OS/VM. While TrustWall cannot prevent internal data corruption from infection, it keeps the data away from the hacker.

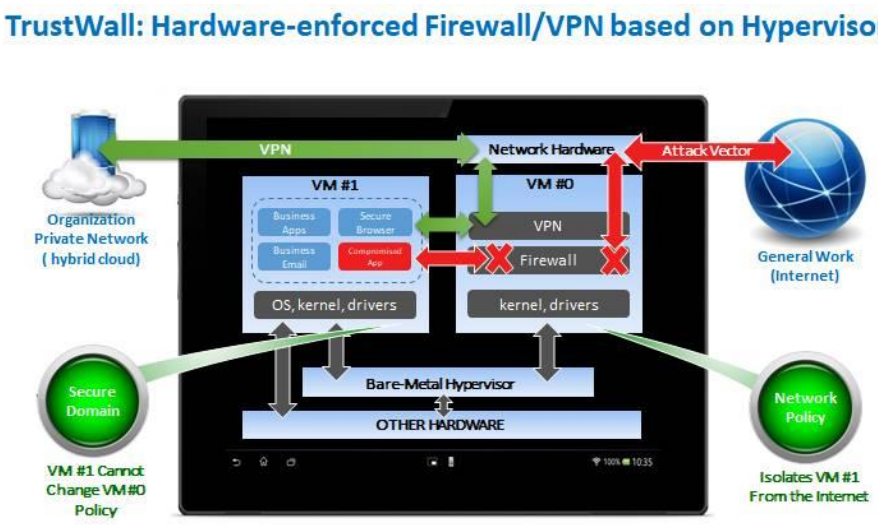
TrustWall can be implemented with either InZero's WorkPlay Technology (using ARM TrustZone) or Type-1 Mobile Virtualization (using Hypervisor Mode), or is a standalone technology available for any device containing ARM TrustZone or Hypervisor Mode.

2. INZERO'S TRUSTWALL: HOW IT WORKS

A hardware-enforced mini-OS/VM. TrustWall prevents organizational network data from being transmitted outside of authorized intranet recipients. TrustWall uses only minimal device resources for its function, and therefore, does not cause any appreciable consumption of device resources.

TrustWall for the locked-down mobile device. For the most critical security needs, a mobile device may be dedicated to a single trusted group – e.g., an enterprise intranet, government enclave, single-classification network (e.g., Top Secret, Classified), and the like. Still, this environment may be compromised by, for example, a participating malicious insider or group member who unwittingly sends a malicious attachment or clicks on a malicious link. TrustWall prevents the exfiltration in such circumstances because it will not permit outgoing traffic to an unauthorized addressee. When used, for example, for the single operating VM, TrustWall may be depicted as:

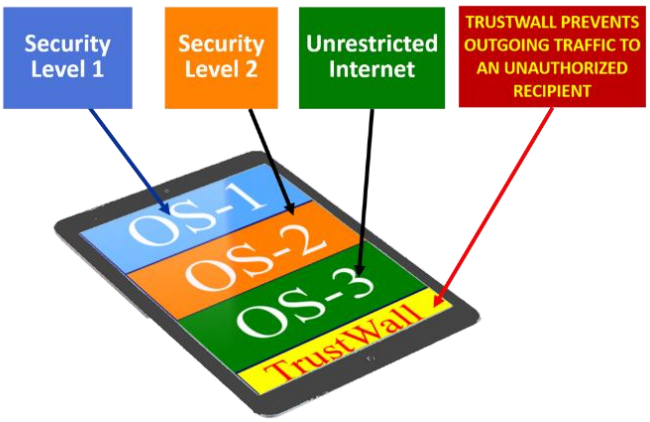
100 Carpenter Drive
Sterling, Virginia 20164
www.inzerosystems.com



TrustWall for multiple VM/OS use. More prevalent is mobile device use for multiple purposes. The most obvious scenario is the single device used for both business and personal needs. Today, business needs commonly include participation in an organization intranet, such as

- ✓ Healthcare system
- ✓ Retail product distribution
- ✓ Finance sector (investment, insurance, etc.)
- ✓ Different Government security-level groups
- ✓ Transportation and other infrastructure groups

In these scenarios, the user participates in multiple domains with differing degrees of security needs – an invitation for potential cross-domain contamination and with it, ultimately data loss. The multiple VM/OS scenario needs TrustWall to prevent intranet data from being sent to a non-participant. Our ability to provide even three hardware-separated domains in a single device allows a wide variety of different security level domains:



100 Carpenter Drive
Sterling, Virginia 20164
www.inzerosystems.com

We don't decide TrustWall security policy, the IT Admin does. Important to the practical and convenient deployment of TrustWall is determining the particular security policy it will enforce. TrustWall has been developed to enable organization IT Admin to implement outgoing traffic rules as desired – meaning, for example, limiting transmittals by:

- ✓ email address,
- ✓ IP address,
- ✓ MAC address
- ✓ Geographic locations, etc.

Moreover, the IT Admin policy cannot be overcome by user attempts to circumvent it. Thus, TrustWall advances common whitelisting by effectively employing hardware-level enforcement to keep both the hacker and the user away from the security policy it enforces.

3. THE GROWING NEED FOR TRUSTWALL

What the hacker doesn't know, won't hurt you. Prominent major data breaches in recent years not only originate in the endpoint device but required back-and-forth communication to the hacker to enable well-crafted exploits to proceed with the effort to extract a vast amount of data:

- ✓ the Target Store's data – over 40 million credit cards – entailed no less than 11 different steps by its well-organized hackers
- ✓ the Office of Personnel Management (OPM) breach – over 20 million records and 5 million fingerprints – entailed at least 5 separate exploitative steps
- ✓ likewise, the Anthem breach – over 70 million healthcare records – entailed at least 6 separate exploitative steps

Hackers cannot initiate the often–complex data exfiltration process if they do not know, in the first place, that the endpoint device has been successfully intruded. When the hacker is not a known and authorized group participant, TrustWall prevents him from knowing he succeeded.

Protecting against unknown device vulnerabilities. At any given time, security vulnerabilities exist in computers, and over the course of a given period, these are usually discovered, reported and patched, typically reported on cvedetails.com.

In its 2016 Threats Reports, McAfee concluded:

> *We analyzed survey data and detailed our findings. Among other things, we found that:*
>
> - *The gap between data loss and breach discovery is getting larger.*
> - *Healthcare providers and manufacturers are sitting ducks.*
> - *The typical data loss prevention approach is increasingly ineffective against new theft targets*

Digital Guardian (Oct. 2016) shares this view:

"Data is escaping from most organizations. It sometimes walks out with insiders, but mostly it is stolen by outside actors. It is leaving in multiple forms and channels."

In the article "**Critical Flaw Found in AVG, McAfee, Kaspersky Products"** (Dec 2015), the researchers reported:

> *"A serious vulnerability found in several security products could have been exploited by malicious actors to bypass Windows protection features, data exfiltration prevention firm enSilo reported."*

In the same time frame, BugSec Group and Cynet found "a severe vulnerability in several next generation and applications aware firewalls" that

100 Carpenter Drive
Sterling, Virginia 20164

"allows internal network hosts that have been infected with malware to "interact and extract data out of the organization, completely bypassing the firewall".

> *On a deeper level, a majority of the attackers behind this year's incidents were external actors motivated by financial gain. They went about their attacks by means of hacking, malware distribution, and phishing, with social engineering attacks considerably boosted by Dridex-based campaigns."*

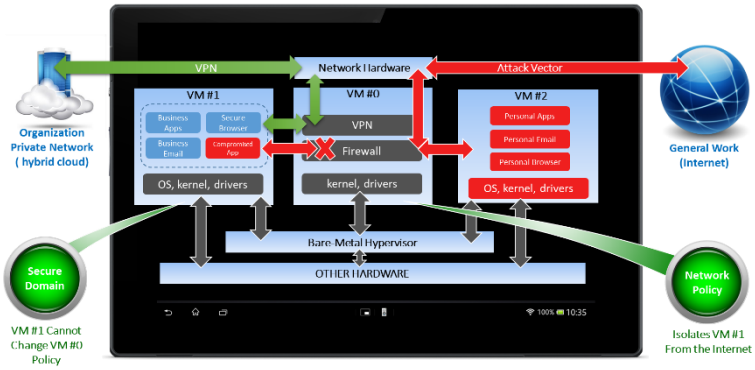
For another example, consider the McAfee Knowledge Center list of nine vulnerabilities for McAfee's "Endpoint DLP (Data Loss Prevention)" product. The list is described as having these four vulnerabilities (rated from CVE 3.5 to 6.9):

(1) Cross-Site Scripting
(2) Denial of Service
(3) Improper Access Control
(4) Cross-Site Request Forgery

At bottom, nothing's changed – DLP-type software solutions rely on both the integrity of their code and on the ability to recognize the enemy.

So, we decided to create a DLP solution at the hardware-level. Malware that can't touch it, can't overcome it.

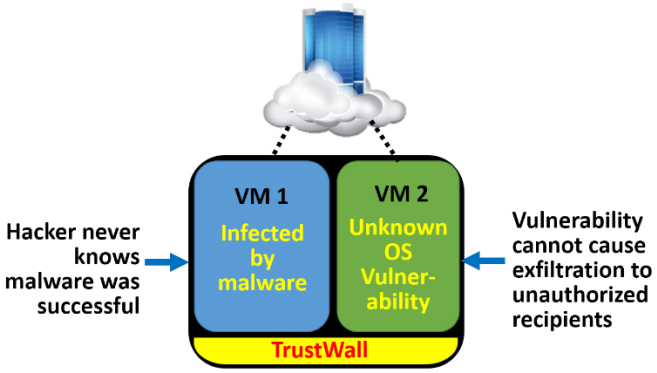
InZero Type-1 Virtualization with TrustWall



4. TRUSTWALL, A "PARTY KILLER": DISCOURAGING THE HACKER

The most damaging malware attacks are accomplished by phishing exploits. It's a profitable business when a single healthcare record fetches $25-50 on the Dark Web. It also only takes one or a few victims to bite, like the handful of OPM employees who succumbed to fake OPM web domains.

When an organization employs TrustWall to prevent the successful hacker from reaping the fruit of his labor, the organization makes itself an unattractive target.



TrustWall, the Just-in-Case Last Line of Defense

InZero Technologies, LLC

100 Carpenter Drive
Sterling, Virginia 20164

www.inzerosystems.com