SAMPAN security inc

STAY PROTECTED FROM LIVE PC INTRUSION

# FireTower Security Solution Overview

SAMPAN security inc

July 2017

# Sampan Security, Inc.

# FireTower Security Solution Overview

This document was last updated on: June, 2017

license is required (NLR) and there is no Commodity Classification Automated Tracking System (CCATS) number required. The Software may not be exported or re-exported to entities within, or residents or citizens of, embargoed countries or countries subject to applicable trade sanctions, nor to prohibited or denied persons or entities without proper government licenses. Information about such restrictions can be found at the following websites:
http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm and
http://www.treas.gov/offices/enforcement/ofac/.
You are responsible for any violation of the US export control laws related to your copy of Sampan Security product. By accepting this Agreement, you confirm that you are not a resident or citizen of any country currently embargoed by the U.S. and that you are not otherwise prohibited from receiving the Software.

Sampan Security, Inc. Nashua, New Hampshire, U.S.A.
http://www.sampansecurity.com and http://firetower.net

# CONTENTS

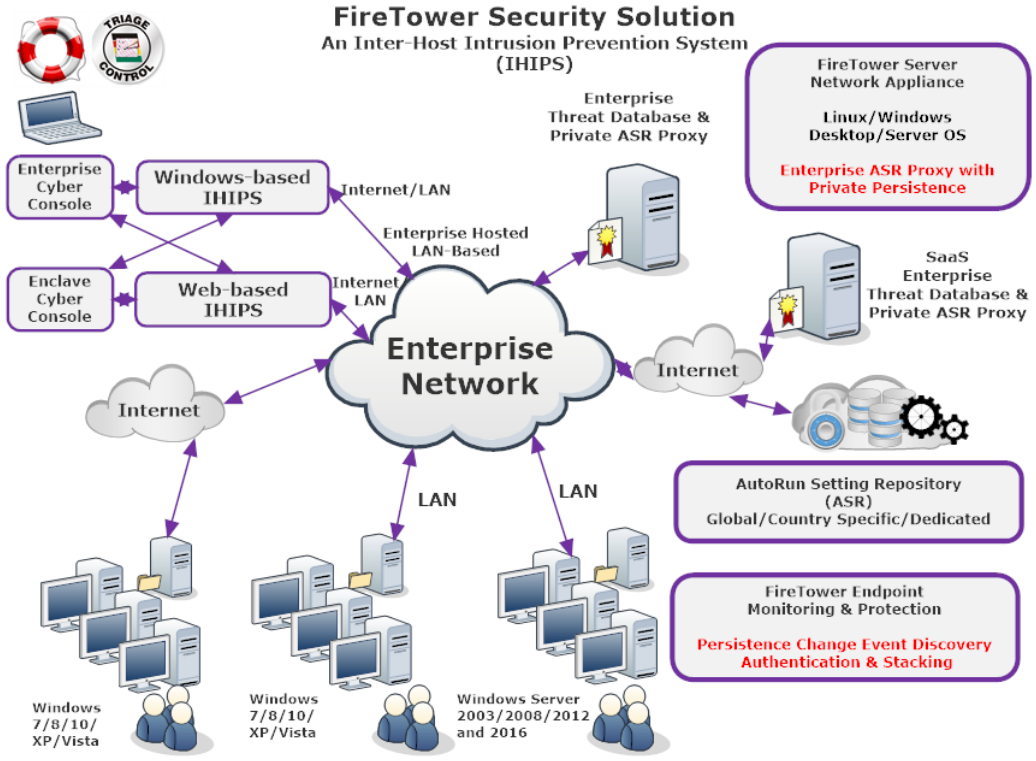
# 1. Introduction

FireTower, an endpoint detection and response (EDR) security solution, offers automatic, real-time protection against zero-day attack malware and live forensics for incident response investigation.

FireTower discovers and authenticates critical change events at endpoint computers and synthesizes discoveries to a centralized enterprise threat database maintained by the FireTower Server service. Through this threat database, FireTower provides an interactive threat exploration interface with built-in analytics to hunt for indicators of compromise, to deliver comprehensive endpoint visibility and to enhance the detection and containment of malicious activities.

The FireTower Security Solution can be deployed to perform continuous monitoring for security operations center and to provide live forensics for hunting indicators of compromise and ongoing attacks.

# 2. FireTower Architecture and Component



# 3. FireTower Security Solution Components

FireTower Security Solution consists of the following subsystems:

1. FireTower Autorun Setting Repository (ASR) (cloud based)
2. FireTower Server
3. FireTower Client
4. FireTower Cyber Console Access
    a. Cyber Console in Windows
    b. Cyber Console in Browser

# 4. FireTower Autorun Setting Repository (ASR)

A cloud-based Autorun Setting Repository (ASR) is used for persistence mechanism authentication. ASR provides detection scheme with ratings for Autorun entries and identifies them as known good, known bad, or unknown (zero-day)

ASR allows support professionals and digital forensics investigators to quickly disregard the majority of good Autorun entries and focus on a smaller list of questionable or possibly malicious entries.

ASR is maintained by a security threat investigation team at Sampan Security, Inc. All enterprise persistence mechanism change events are authenticated by an enterprise-specific on-premises FireTower ASR Proxy service at FireTower Server. All updates to public ASR are imported and synced up automatically and regularly with the enterprise ASR proxy service. All the enterprise threat data are contained in the FireTower server database on-premises and never exposed to outside.

# 5. FireTower Server

FireTower Server maintains an enterprise threat database collected from all endpoint computers within the enterprise and provides an interactive threat exploration interface for enterprise security situational awareness with continuous threat monitoring and real-time incident response investigation capabilities. The full exploration interface, Cyber Console or CyCon, is available through a Windows based program called WinCyCon.exe (x86 and x64). A backup exploration interface is also available through a browser interface.

FireTower Server software can be hosted in the cloud as a Security as a Service from Sampan Security, Inc., a customer on-premises non-dedicated/dedicated Windows desktop or server, or a customer on-premises non-dedicated/dedicated Linux desktop or server.

# 6. FireTower Client

FireTower client software needs is installed at all protected enterprise endpoint computers. FireTower client software identifies malicious software by monitoring the behavior of current and incoming applications on each endpoint computer. This allows FireTower to detect and stop malware even if it has not previously been catalogued and identified as malicious.

The FireTower Security Solution offers adjustable levels of endpoint security to accommodate varying levels of security vulnerability acceptable as defined by your enterprise security's posture. FireTower client profile settings are dynamically adjustable from the Cyber Console.

# 7. FireTower Cyber Console in Windows

Cyber Console is an interactive threat exploration interface with built-in analytics to hunt for indicators of compromise, to deliver comprehensive endpoint visibility and to enhance the detection and containment of malicious activities. The FireTower threat database can be accessed through CyCon with administration login and password credentials. From there, it can be used to access information for all connected FireTower protected client computers. CyCon displays essential client PC information, Autorun entries, alerts and other critical system information. CyCon also enables administrators to perform advanced functions such as quarantining and removing suspicious Autorun entries and conducting inter–host forensic analysis.

Cyber Console provides deployment and client software update functions through enterprise domain controller to any and all client computers. For security reasons these deployment and update functions are available only if CyCon is running from the FireTower Server.

Cyber Console for Windows can be copied to and executed from any Windows PC. This includes the FireTower Windows Server, any Windows client resided in the enterprise network, or any Windows PC from outside of the enterprise network with access to the enterprise FireTower Server (a routable IP address or via DNS is needed for external access).

# 8. FireTower Security Technologies

## Endpoint Protection Platform (EPP)

According to a Gartner report, Endpoint protection platforms form the basis of the enterprise's toolset to provide anti-malware scanning along with many other endpoint security features. An EPP is primary a preventative tool that performs endpoint anti-malware scanning and relies heavily on signature-based detection methods – also known as Anti-Virus (AV) software. However EPP endpoint security solutions fail to offer any level of protection against Zero-day attacks.

## Endpoint Perimeter Defense and Prevention:

Traditional AV security solutions setup an imaginary perimeter on the PC for protection. Its main function is to scan and prevent malware from entering through this "perimeter" to execute using the signature-based detection method. It performs flawlessly for malware with a known signature, just like a security guard at the entrances of a protected establishment with a list of "unwelcomed guests". If a Zero-day exploit is attempted to enter this perimeter, it will not be stopped. The malware can successfully download malicious payloads since it does not have a signature (not on the unwelcomed guest list).

Enterprise security protection has been dominated by EPP solutions with signature-based detection methods and prevention. With ever-increasing Zero-day attacks, EPP solutions have been enhanced with reputation and whitelist databases, scanning, sandboxing, and other technologies. However, these solutions are still based on perimeter detection and prevention. Furthermore, they provide no visibility and exploration capabilities into the endpoint computer once Zero-day malware penetrates inside the perimeter.

## Endpoint Detection and Response (EDR):

To meet the challenge of increased threats to major enterprises, small businesses, and personal computer devices alike, modern security architecture now includes a new and important component: Endpoint Detection and Response (EDR) tools to deal with Zero-day threats. EDR is not a replacement for other endpoint security solutions such as EPP, but is a vital component to a comprehensive cyber defense system.

EDR Tools perform proactive continuous monitoring and recording of relevant activity on endpoint computers (desktops and servers). To cope with Zero-day attacks that always penetrate the perimeter defense offered by EPP solutions, EDR tools enable an enterprise to achieve comprehensive endpoint visibility, improve its ability to detect malicious activities and simplify security incident response.

The EDR tools add to the AV software prevention mindset to a more pragmatic and realistic tactic of detection and incident response at the endpoint computers. The EDR tools should perform the following tasks:

1. Collect endpoint data
2. Centralize the data
3. Post-process (data mining) the data

These EDR requirements are very generic on what kind of endpoint data that has to be collected, centralized, and analyzed. The FireTower Security Solution accomplishes these tasks.

The endpoint data needed by EDR tools have to take into consideration that each typical modern day breach/incident involving multiple computers in the enterprise, each computers with multiple malicious actors and with multiple attack stages.

Gartner's report suggests that security solutions should include continuous monitoring for patterns and behaviors indicative of malicious intent. However in an enterprise, continuous monitoring can only be implemented with a measured approach so as not to overwhelm the CPU and incident response investigation. The FireTower Security Solution takes such a measured approach using persistence mechanisms to detect and contain Zero-day attacks.

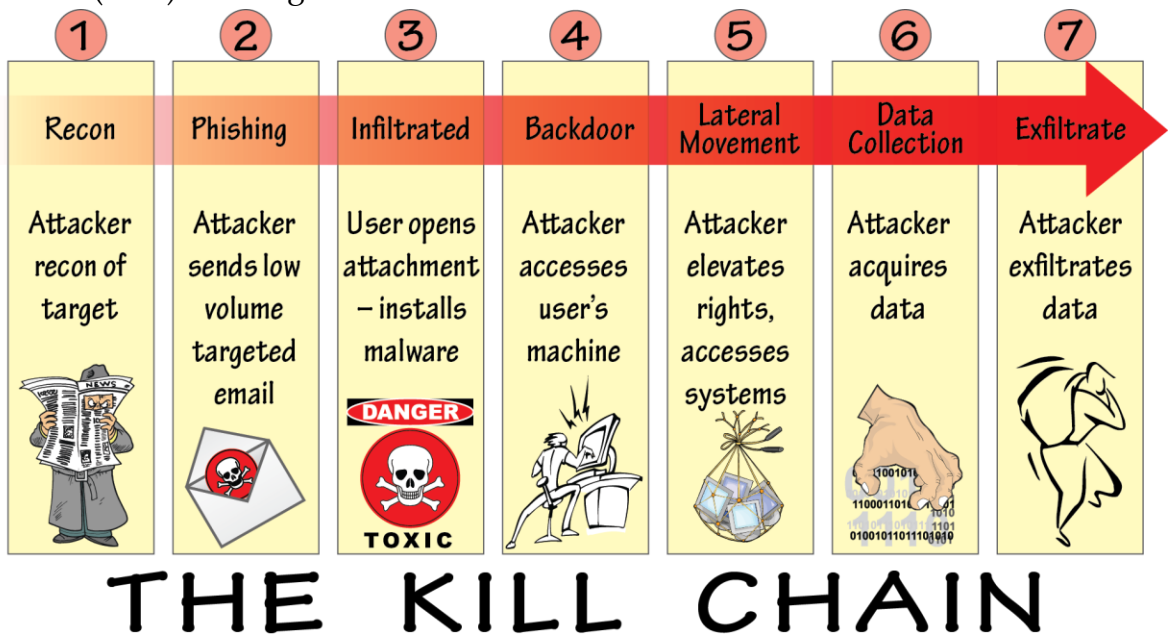
## Zero-day Attacks: Exploits and Payloads

Although EDR can also detect known malware intrusions, but we will be concentrate on the Zero-day attack detection and response capabilities.

A cyber attack incident is typically started with a software (exploit) taking the advantage of a software vulnerability and delivering and executing malicious software (payloads) against a target system. A Zero-day attack happens once the software vulnerability is exploited and attackers release payloads before software vendors have an opportunity to create a patch to fix the vulnerability or security vendors have an opportunity to create a signature for this exploit. A Zero-day exploit leaves no opportunity for detection and therefore EDR tools have to discover, detect, and contain the malware execution beyond perimeter.

## Cyber Attack Life Cycle and Characteristics:

The following diagram depicting the life cycle staged attacks of an Advanced Persistent Threat (APT) and targeted attacks.




Credit: Advanced Persistent Threats, SP Guard APT/Spearphishing Defense from Iconix.com

Each cyber breach incident consists of multiple attack stages (infection, lateral movement, data source, exfiltration point) and at different computers, each attack stage consist of multiple actors (payloads). Unlike known malware with a signature for detection (before execution) and remediation (malware removal), there is no signature for Zero-day attacks and hence EDR tools have to detect and contain the intrusion and identify all payloads during remediation phase.

## The Design Goal of EDR Tools:

The design goal of EDR tools is to be able to detect and contain malicious payload executions and optionally with automatic remediation while minimizing the requirements of computing resource usage and IT support staffing and training.

## Persistence Mechanisms as the Missing Link for Zero-Day Attack Detection and Response:

FireTower Security Solution delivers a unique methodology for defending against Zero-day attacks through analyzing persistence mechanisms, such as Autoruns in Windows PCs, to help identify unknown (Zero-day), possibly malicious, software insertions. This methodology relies on software running on endpoint PCs working in tandem with applications and database components in the cloud. This EDR tool will use persistence mechanism change events to discover, authenticate, and optionally contain malicious persistence mechanisms and then roll up all the associated payloads during remediation phase. Persistence mechanisms have long been used by support professionals to diagnose and resolve crashes, instability, degraded performance, unwanted programs, and virus incidents in Windows. The persistence mechanism based EDR tool can be operated by existing corporate Windows IT personnel with minimal additional training.

## Persistence Mechanisms:

Persistence mechanisms are used in modern operating systems to allow applications to start automatically after system reboots or based on a specified schedule. Microsoft Windows operating systems, for example, use "Autoruns" to accomplish this. A typical Autorun settings consist of 300-500 entries per Windows computer system. Please note that Autorun setting is only one of the persistence mechanisms and FireTower client software monitors other relevant persistence mechanisms for Zero-day attack detection. Malware and Zero-day attacks alike commonly abuse persistence mechanisms built into operating systems in order to gain a foothold and dwell on a PC after it has successfully infiltrated the PC's perimeter defense.

## Malware is Virtually Always Persistent:

Persistence mechanisms are a key marker event in the malware kill chain and have been used as Indicators of Compromise (IOCs) to hunt down the Advanced Persistent Threats. Malware is virtually always persistent as postmortem analysis indicated that the majority of recent zero-day cyber security attacks made use of injected or altered persistence mechanisms. The persistence mechanism based detection scheme only needs to detect one malicious actor deploying persistence mechanisms among all the actors of a security incident and at only one stage of a multi-stage targeted attack scenario.

Malicious persistence mechanisms are usually deployed by Zero-day attack payload early in the kill chain and can therefore be discovered and authenticated early in the security breach incident timelines. Once a malicious persistence mechanism is detected it can be contained easily by killing off both the persistence mechanism as well as the dropper software.

# 9. FireTower Security Operations

## Coexistence with Anti-Virus software if deployed

If any AV software is deployed in the enterprise, most likely all the known malware and exploits will be stopped by the installed AV software assuming your AV malware signature database is up-to-date. FireTower will be in a normal operational state as the incoming known malware already stopped and quarantined by the AV software.

## FireTower Persistence Mechanism Discovery and Authentication

A persistence mechanism (or Autorun setting in the Windows operating system context) is a program that is automatically started by Windows when the operating system starts, a user logs in, or an application starts. The Discovery task logs all existing "persistence mechanisms" including associated metadata, digital certificate and hash values (MD5, SHA-1, and SHA-256) of target binary files. For a real-time protection scenario, it continues to monitor the persistence mechanisms and triggers automatic authentication on the changes.

## Autorun Setting Repository (ASR)

A cloud-based Autorun Setting Repository (ASR) is used for persistence mechanism authentication in real-time. ASR provides detection schema with ratings for Autorun entries and identifies them as known good, known bad, or unknown (zero-day):

Green: Autorun whitelist database kept at ASR
Red: Autorun blacklist from cloud-based 60+ Anti-virus engines
Orange: Zero-day entry with suspicious behavior observed by FireTower
Yellow: Zero-day entry without suspicious behaviors,

## Sources of Persistence Mechanisms

1. Windows Update (digitally signed by Microsoft)
2. Application software installed by users.
3. Results from malware payload execution

## FireTower Enterprise Protection Profile

Endpoint protection profile settings:

A. OFF: monitoring only
B. NORMAL protection: Only allow Yellow and Green rated persistence mechanism change events (e.g. home office small business computers)
C. ESCALATED protection: Only allow Green rated persistence mechanisms change events (e.g. small and medium business computers)
D. LOCKDOWN protection: Only allow Green rated Windows system persistence mechanisms change events (e.g. Government, defense industry, or enterprise computers)

| Profile/Rating | Green | Yellow | Orange | Red |
|---|---|---|---|---|
| Monitoring | Pass | Pass | Pass | Pass |
| Normal | Pass | Pass | Stop | Stop |
| Escalated | Pass<br>System/Applications | Stop | Stop | Stop |
| Lockdown | Pass<br>System only and signed by Microsoft | Stop | Stop | Stop |

## Enterprise Proprietary Persistence Mechanisms:

FireTower Security Solution integrates a real-time authentication module for system critical change events at endpoint computers through Autorun Setting Repository with a proxy option to keep all enterprise proprietary information private. All updates to cloud based ASR are synced up automatically and regularly with the enterprise ASR proxy service. All enterprise threat data are contained in the FireTower server database on-premises and never exposed to outside.

FireTower Server Proxy Service allows the enterprise to determine the authentication rating for persistence mechanism within the enterprise, and these enterprise proprietary rating will take precedence over public rating. Case in point, the enterprise can change

the rating of a benign social media persistence mechanism to Red which will prohibit the client computer endpoints to run this enterprise unauthorized application.

## Enterprise client (desktop/server) security management

FireTower Security Solution enables the enterprise to organize their client computers based on grouping: location, building, department, computer type, and network environment. Each client computer can be associated with more than one group. FireTower Security Solution also enables the root administrator to assign group administrators to monitor and management for their designated groups. The visibility and privileges of these group administrators only apply to the group they are assigned to.

# 10. FireTower Enterprise Protection Tasks

The following protection tasks provided through FireTower Security Solution cover the full spectrum of enterprise security requirements.

## 1. Zero-day attack Detection and Containment

Setting endpoint protection profile to Normal, Escalated, or Lockdown enables FireTower Client software to detect and contain incoming Zero-day malicious software in real-time based on the group specific security posture.

## 2. Continuous Monitoring for Security Operations Center

FireTower delivers the continuous monitoring capabilities using Cyber Console (CyCon) Dashboard for the enterprise security situational awareness and Inter-Host Intrusion Prevention System (IHIPS) Activity Tab for attack in progress detection.

IHIPS continuously searches the enterprise threat database to identify the threats and provide early identification of ongoing attacks or malware lateral movements within enterprise endpoints.

Following the Observe, Orient, Decide and Act (OODA) Loop decision cycle, continuous monitoring using the interactive threat exploration interface provided by FireTower Cyber Console can be achieved the OODA Loop.

**Observe**: to enterprise threat situational awareness using FireTower Cyber Console Dashboard and IHIPS Activity

**Orient**: to suspicious threat events through sorting and filtering using FireTower Cyber Console IHIPS Activity

**Decide**: if suspicious or malicious threat events have been validated based on ASR Authentication Rating using FireTower Cyber Console IHIPS Activity

**Act**: to issue command of quarantine to all at-risk systems using FireTower Cyber Console IHIPS Quarantine All command

The IHIPS Activity View displays all of the endpoint persistence mechanism change events in chronological order. It displays which endpoint just registered a persistence mechanism change event while the lower pane displays all endpoints with the same persistence mechanism across the enterprise. Temporal Analysis for inter-host consecutive persistence mechanism change events are carried out by sorting change events in chronological order to determine whether the events from different endpoints have the same persistence mechanism change event which could signal potential malware lateral movements across the enterprise.

## 3. Incident Response and Forensic Investigation

Focusing on persistence mechanisms is already the industry standard practice for incident response and forensic investigation. Most forensic investigations initiate the incident response process by examining persistence mechanisms as it is a fast and effective method for assessing malware incidents, discovering breaches and malware.

FireTower delivers live forensic support by continuously monitoring persistence mechanism change events. Incident response can then be conducted instantly when a breach is suspected thus eliminating the delay and extra cost of using external professional investigators.