FireTower Guard & Live Forensic Console

Zero-day Attack Protection

FireTower Guard protects endpoint computers from Zero-day attacks

Situational Awareness Management

FireTower Console provides a bird's-eye view of FireTower Guard client PCs in the enterprise

Always-on Forensic Data for Incident Response

FireTower Console delivers an always-on incident triage platform for real-time forensic investigation

Enterprise Attacks in Progress Detection and Quarantine

FireTower Console detects attacks in progress and lateral movement in a multi-stage attack

Real-Time Alerts

FireTower Console displays all incoming software attempting to insert persistence mechanisms on FireTower Guard client PCs in real-time. All critical information is available either on-screen or one-click away from Faultwire.com®

FireTower Guard for enterprises is a purpose-built security application for protecting client PCs against all types of malware including Zero-day attacks. Included FireTower Console is an enterprise administration tool designed to monitor and control a network of FireTower Guard-protected client PCs while detecting attacks in progress and providing live enterprise forensic data for incident response when necessary.

FireTower Guard features automatic detection, quarantine of malware including Zero-day malware at endpoint computers by monitoring and authenticating critical system state change events through a cloud-based threat intelligence database called Autorun Setting repository. FireTower Guard monitors and aggregates all critical security forensics including persistence mechanisms from the networked endpoints to maintain a real-time enterprise threat database. FireTower Console employs a principle of Inter-Host Intrusion Prevention System to provide an always-on incident triage platform for real-time and postmortem forensic investigation. Windows support personnel can easily triage and identify which endpoint computers are at risk, if any, without requiring outside incident responders. FireTower Console also performs active and continuous monitoring to detect and alert attacks in progress or lateral movement of a multi-stage attack in the enterprise. FireTower Console is accessible through either a Windows based console or a browser-based console.

There are two service options available for FireTower Guard; one is based on FireTower Guard service installed at a customer-owned Windows or Linux machine, the other option is through a Security As a Service model with cloud-based FireTower service provided through Sampan Security, Inc.

FireTower Guard is designed specifically to deal with Zero-day attacks and can either function as a standalone solution or coexist with deployed security solutions. The design is scalable and modular for enterprise environments and is low cost with minimal maintenance, additional hardware, and personnel training.

SAMPAN security inc
info@SampanSecurity.com
www.SampanSecurity.com

FireTower Guard™

Zero-day Attack | Detection Containment Forensics

Malware is already inside your network!

Breaches are pervasive and businesses of all sizes have to deal with cyber security threats to avoid damage to their business operation, reputation, liability, and customer privacy issues. Large corporations throw money and resources into the fight and still fail to prevent breaches, but small and medium-sized enterprises (SMEs) with much smaller budgets are also fast becoming targets of opportunities. Stopping a targeted attack without properly trained incident responders and resources is an overwhelming task.

Since it is impossible to provide complete prevention at the endpoint perimeter, the question is not "If you will be breached?", but "When?". Enterprises need a cost-effective incident response plan ready to launch every time a cyber intrusion or attack is discovered. Once an incident response is initiated, the main goal is to quickly collect forensic data from hundreds or thousands of endpoint computers for triage analysis and identify at-risk systems for further incident investigation. According to one industry report, for a small business of 100 endpoint computers, one single incident response could cost at least 15K, but with instant forensic data as provided by FireTower Continuous Monitoring service the cost saved could already cover the software cost, not to mention the saving from future incidents.

Why Persistence Mechanisms?

Persistence mechanisms are used in modern operating systems to allow applications to start automatically after system reboots or according to a specified schedule. Microsoft Windows operating systems, for example, use "Autoruns" to accomplish this. 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.

As Zero-days are previously undiscovered and have no associated signature, traditional detection methods and perimeter-based defenses fall short of stopping them. An unconventional strategy is required to protect against Zero-days. FireTower Guard identifies unknown, potentially malicious Zero-day software by analyzing persistence mechanism change events in real-time. By starting at the endpoint and monitoring for persistence mechanism change events initiated by software, which could be legitimate or malicious, Zero-day attacks can be identified and tagged as potentially dangerous software.

This approach is validated by the fact that 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 and discovering breaches and malware. Most, if not all, recently reported cyber security Zero-day attack incidents involved persistence mechanisms.

A single Microsoft Windows PC contains hundreds of Autorun settings which makes identifying and verifying their validity a time-consuming process. In a corporate, intelligence, or military environment with hundreds or thousands of PCs, this process becomes impractical to accomplish through manual software tools. Automated tools are crucial for allowing support professionals and digital forensics investigators to perform their jobs more effectively and efficiently.

Inter-Host Intrusion Prevention System (IHIPS)

Gartner's report suggests that an effective security solutions should include continuous monitoring for patterns and behaviors indicative of malicious intent. Within an enterprise environment, continuous monitoring must be implemented with a measured approach. A key factor in a measured approach for continuous monitoring across the enterprise is the persistence mechanism change events. The detection of an unauthorized or malicious persistence mechanism change event could signal an intrusion to the target endpoint computer. The detection of multiple instances of unauthorized persistence mechanism change events across different hosts could signal targeted attacks in progress and lateral movement of malware within the enterprise network.

Inter-Host Intrusion Prevention System (IHIPS) continuously monitors enterprise critical forensics at endpoint computers and stacks the data in the enterprise threat database. FireTower Console with IHIPS technology is capable of detecting attacks in progress in the enterprise and identifying lateral movement of targeted or multi-stage attacks in progress.