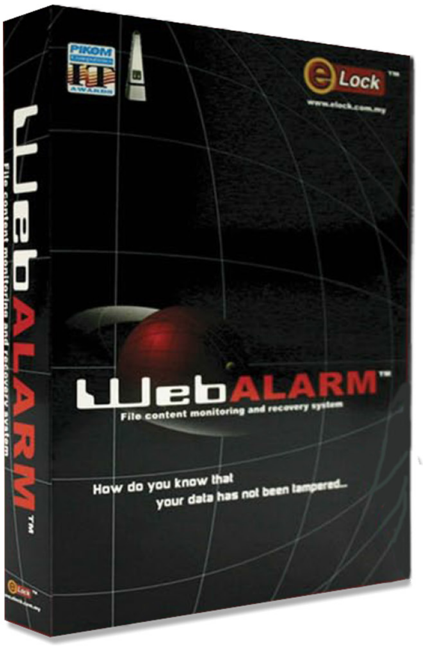
eLock THE DIGITAL SECURITY COMPANY

WebALARM™

THE ANCHOR OF TRUST


PIKOM
eLock
www.elock.com.my
WebALARM™
File content monitoring and recovery system
How do you know that your data has not been tampered...
WebALARM™ File content monitoring and recovery system

MONITORING

PROTECTION

INTEGRITY

FEATURES

FILE & DATA INTEGRITY MONITORING

WebALARM continuously monitors files and folders round the clock to detect any changes made to the monitored data. WebALARM scans each file to check for its existence, integrity and access permissions.

AUTOMATIC RECOVERY

WebALARM will automatically take immediate action upon detection of a data integrity violation event. This is a built-in feature of WebALARM without requiring any additional scripting by the administratior. The available options for automati recovery include:

DATA VIOLATION ALERT

WebALARM will issue alerts upon detection of any data integrity violation. The types of alerts include: WebALARM Console alerts, Network management console alerts, via SNMP, Email alerts, SMS

DATA UPDATE MANAGEMENT

WebALARM allows continuous monitoring without interruption while some part of the data is being updated. It provides two flexibles methods for content owners to update the monitored data without trigger any false alarm.

TECHNICAL OVERVIEW

A two-tier application :

Agent : a system process that runs on the monitored server.

Console : a graphical user interface for managing the Agent.

HOW IT WORKS?

During the initial configuration, the administrator uses the Console to select the files and folders to be monitored by the Agent.

The Agent will then create a backup for all the selected files and generate a list of file signatures using proven hashing algorithms.

The agent will detect changes in real-time and upon detection of any file error conditions, the agent will recover the affected files with their original content and attributes. In addition, the agent will report to the Console as well issuing emails and SNMP traps.

At A Glance

1. Web content protection

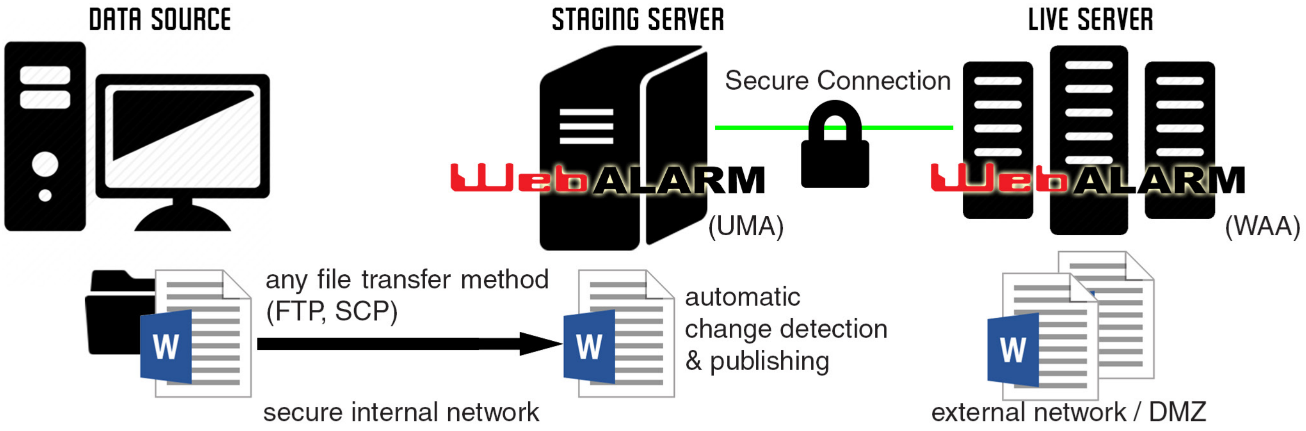
Provides round the clock monitoring of web applications and data with automatic recovery without the need of human intervention.

2. Ensure web server integrity

Protecting DNS records, settings, mail server configurations and controls data upload activities.

3. Provides data and application audit capability

Providing audit trails of file and data modifications.



1. CENTRALIZED USER MANAGEMENT & SCALABILITY

Various agents running on different platforms are configurable via a single console. This proven solution centralizes management and scales to accommodate corporate change and expanding remote needs.

2. EXTENSIVE AUDITING & LOG FILTERING ABILITY

The log file serves as a forensic trail of hacker activity. All events such as file alteration alerts, file uploads and modification details are logged with each events tagged with a time and date. A common problem among security analyst is the sifting of pages and pages of logs. The log filtering ability enables quick filtering and easy searches on specific log events.

3. REMOTE ADMINISTRATION

Agent and Console concept allows user to configure the agent only via the console which can be installed local to the agent or remotely. Remote console configuration is recommended as means of protecting the WebALARM agent in the event of agent host compromise.

4. MULTIPLE USER ACCOUNTS

WebALARM promotes the use of multiple user accounts with explicity assigned permission to support multiple users. Each agent possesses an individual user account database allowing assignments of different administrative and normal user accounts.

5. SNMP/ EMAIL/ SOUND ALERTS

An alert is triggered when unauthorized modification of a monitored file has been verified. The agent can be configured to send out a SNMP trap message or an email or run a platform dependent program in the form of a batfch file or shell script.

6. QUICK RESPONSE TIME

WebALARM uses an integrity monitoring enging that performs real-time surveillance on user selected files/folders and able to instantly detect file modification. The restoration process is simply a matter of replacing the tampered file with a copy of the original instantly upon detection thereby keeping downtime to a minimum

7. LOGIN SECURITY

The Admin user is able to restrict normal log on users to a range of IP addresses making it difficult for a foreign host within the internal network to pose as a valid host. This feature can also be applied to the administrative account. The use of a SSL channel between console and agent and digital certificates authenticate console hosts with valid IP addresses.

8. BACKUP COPY MONITORING

The Backup folder contains the backup copies of the monitored files/ folders that are used by the agent to restore the original. To ensure the integrity of the backup copies, the files/ folders in the backup folder are constantly monitored to retain its authenticity. Backup copies are also compressed to minimize disk space usage. Backup can be stored on a remote server that can be specified via the WebALARM console.

9. SECURE UPLOAD FEATURE

The upload feature of WebALARM allows an admin user to upload modified files to the agent as means of a web site update by allocating the admin user a specified amount of time to upload files. A scheduled upload feature allows upload time to be automatically launched based on a user selected schedule.

e-Lock Corporation Sdn Bhd
Business Suite 19A-26-3, Level 26, UOA Centre, 19 Jalan Pinang, 50450 Kuala Lumpur, Malaysia.
Phone : +603-2166-2981 Fax : +603-2166-2982 Email: info@elock.com.my
Web : www.elock.com.my