

Insight into

Network Traffic and Security Events

Key Features »

- Auto-Discover in Network Topology
- Smart Log Finder Embedded
- Visualization in Device Map
- Support for Multiple Firewall and IDP
- Robust Data Analysis on Attack, Event Logs
- Custom User Report Formats
- Real-time Network Device Monitoring
- Centralized Database Management

Overview

KDware Security Analyzer is an edge solution to provide in-depth analysis of network traffic in collection of security device's logs, including firewall & IDP, with automatic aggregation, correlation, intelligence analysis, as well as network management features in devices monitoring, security alerts, and scheduled operations.

Today's Solution

In security concerns of connecting a local network to the internet, firewall & IDP become an integral component of network implementation in every organization. However, security products, which generates huge amount of security and traffic events each day with especially for different syslog message formats in different brands, leads system administrator hardly in identifying security threats and understanding the traffic patterns. Such un-manageable situation draws seriously security concerns to many corporations in both managerial and operational views.

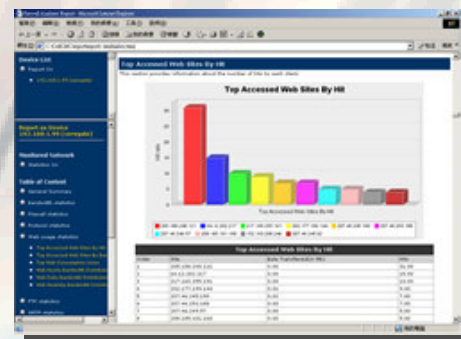
KDware Security Analyzer extends the value of your firewall by monitoring and providing essential information about network activity, displayed in comprehensive, easy-to-interpret reports, as well as value-added network management features, which empower network administrators to move beyond reactive operations to proactive network management, and eliminating risks before security issues raised.

Helps you understand

- Hacker attacks, security breaches, and virus activity
- Attacks & virus such as type, source, destination, port, etc.
- Protocol usage by user and department
- Incoming and outgoing traffic or bandwidth patterns
- Web usage by department and individual employee
- Blocked web site access
- Bandwidth utilization by client and protocol
- Inappropriate internet usage by employees
- Bandwidth allocation and utilization reports
- Activity trends over time

Benefits to Users

- **Cuts costs by using bandwidth more efficiently**
- **Supplies proactive security protection**
- **Reduces productivity losses and liability**
- **Delivers critical insight into firewall activity**
- **Ensure business running and safe**



Features

Device Map Visualization – helps you to visualize and configure the network topology.

Auto Discovery of Network Topology – instead of manual configuration, it supports auto-scan of the network, discovers each machine for traffic analysis and network management.

Enhanced Support for Multiple Firewall - scalable and ease of implementation across different security products.

Profile Setting – provides unlimited number of profiles in reporting scope for various devices in the network topology.

Profile Manipulation and Exchange – provides import and export functions in profile setting.

Monitoring and alerting functions - monitors multiple firewalls, IP devices or services running on your servers. If a device or service goes down; or any critical security event detected, it generates real-time alert to you by email.

Cost-effective Solution - efficiently manages huge amounts of security events and false alarms in a most cost effective way.

Build-in Syslog Server & Processing – embeds syslog server to collect and parse syslog messages from multiple firewalls.

Syslog Archiving – supports syslog message backup and restore for analysis and reporting.

Automated Devices Monitoring and Alerts – 24x7 devices monitoring and automatic alerts; protects your important computerized assets and business information in safe.

Powerful and Comprehensive Report - generates easy to understand report with graphics, tabular, high-level summary.

Robust Data Analysis – offers extensive correlation analysis and pattern creation capabilities.

Flexible Report Generation Using Template – more than 100+ report templates and individual IP reports for selection.

Unlimited Custom Reports – unlimited free report formats where user can make custom report for specific purpose.

Automated Report Generation & Distribution – with scheduling feature to generate user pre-defined report and automatically send to the recipients via email.

Centralized Management - centralized reporting on multiple and distributed firewalls or VPN devices.

Build-in Database & ODBC Support – embeds database for syslog storage, and supports ODBC connection to MySQL.

Simple Setup and Installation – easily installs on Microsoft Windows NT/2000/XP/2003 with simple clicks.

System Requirements

- PIII – 1 GHz or above
- System Space – 60 MB
- RAM – 512 MB or above
- Resolution – 1027 x 768
- Log Space – 800 MB or above

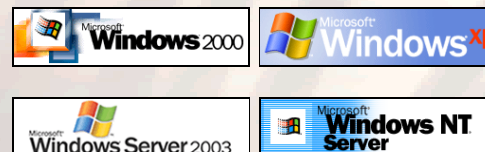
Languages Supported

- English
- Traditional Chinese
- Japanese (coming soon)
- Simplified Chinese

Device Compatibility

- Check Point Firewall-NG
- CISCO PIX - Secure Firewall v4.x, 5.x, 6.x
- FortiGate family v2.8
- NetScreen -5, -5XP, -10, -25, -50, -100, -500, -1000 v4.0, 5.0
- ServGate PointForce, EdgeForce, EdgeForce Plus, EdgeForce Accel
- SonicWALL TELE, SOHO, PRO, GX v4.10, 5.x, 6.x
- WatchGuard - Firebox Models v2.x, 3.x, 4.x, 5.x
- McAfee IntruShield, NetScreen IDP, Snort IDS

Platforms Supported



About KDware

KDware, means "Knowledge Discovery Ware", is a leading provider and innovator of hidden pattern discovery solutions and applications, specialized in security logs, events, and incidents analysis, using Data Mining technology. Our applications, serve for telecommunication industry, government, global enterprises, and small businesses, are widely adopted and distributed.