DEFENDER

Intrusion Detection Systems

"Transforming Network Data into Security Knowledge"

K2-Defender Product Overview

The Product

K2-Defender is an Enterprise-wide Security Monitoring Platform.

By aggregating and displaying sensor information in a central location, K2-Defender transforms data about your network into actionable Security Knowledge. K2's unique design gives you the ability to fuse data from all over a network, bringing both real-time **and** historical security information together onto a single screen. This innovative capability gives you access to a single comprehensive view of your network security posture.

K2-Defender sets a new standard for Network Security Monitoring. By managing and interpreting data, the system reduces the business risk associated with internal and external threats to your network.

Features

Effective

- Network aware -reduces false positives
- Threat based alert escalation
- Transforms unmanageable data into useful alert summaries
- Ability to drill down to packet payload level
- Traditional 'packet pattern' rules
- Statistics-based rules
- Pass rules, enabling 'white' listing
- All components managed from a single location

Sophisticated Incident Reporting

- Store and retrieve reports from the central database
- Drag and drop any event element into a report
- Comprehensive template creation facility
- HTML output
- Quickly find all reports relating to a packet
- Data recorded in reports protected from data cleaning

Secure

- Undetectable sensors
- Sensors boot from CD
- Physically separate management network
- Encrypted heartbeat betweenkey components
- Fault tolerant design

Extensible

- Dynamically reconfigurable from a central location
- Support for additional network protocols
- Support for additional application layer protocols
- Run-time signature reconfiguration
- Run-time software upgrades

Performant

- Distributed three-tier architecture
- Non-intrusive network sensors
- Designed from the ground up as a distributed system

Scalable

- Dynamic data scalability
- Dynamic processing scalability
- Dynamic bandwidth scalability

Based on Open Standards

- POSIX
- CORBA
- XML
- J2EE
- HTML

Intrusion Detection Systems

K2-Defender System Architecture

The Architecture

K2-Defender is a distributed system coordinated via a dedicated network. This architecture enables K2-Defender to accommodate the demands placed on a monitoring system by the scalability and distributed nature of today's Enterprise networks. This approach avoids performance bottlenecks and enables K2-Defender to produce an accurate, timely and centralised view of the security posture of your network.

Components

Analyst Console

- Java Based
- Real-time alert monitoring
- Report generation and retrieval
- Forensic analysis
- Analyst-to-analyst whiteboard

Database

Central storage for:

- Packets
- Rules
- Alerts
- Configuration
- Data
- Reports

Application Server

- Secures database by acting as a proxy
- Scales console connections
- Provides distributed help facilities
- Hosts analyst collaboration tools
- HTTP server

Configuration Manager

- Java based
- Rule creation
- Rule deployment
- System configuration and tuning
- User management
- System configuration change review

Network Sensors

- Passive connection to enterprise network
- Active connection to management LAN
- Intelligent rule matching
- Statistics gathering

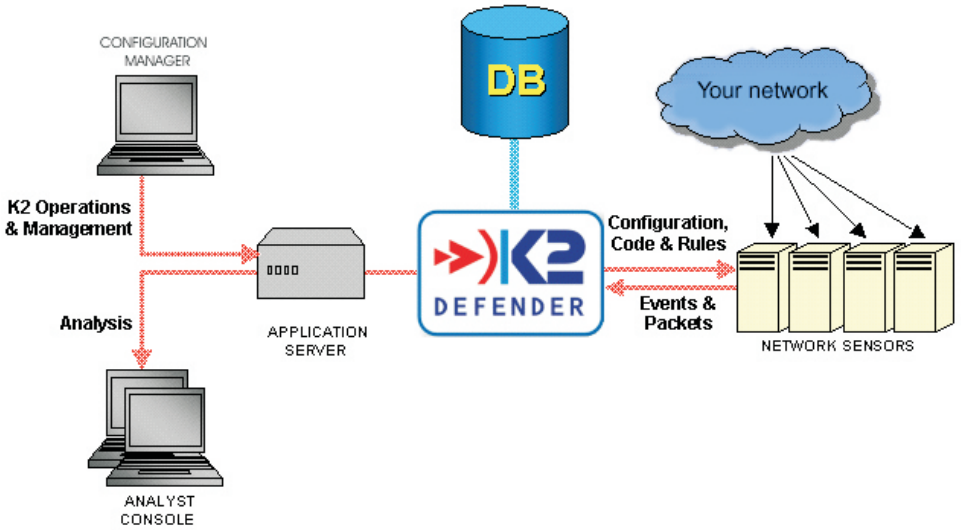

Figure 1: K2-Defender Architecture

For further information contact:

K2 Defender Ltd.
Garden House
Cloisters Business Centre
8, Battersea Park Road
London SW8 4BG, UK
http://www.k2defender.com

K2-Def-PROV-V4.1