WEDGE OS 5.0

Overview

While network packet analysis has been around for a long time, it can no longer meet the security and compliance requirements of today's enterprises and service providers. To meet these requirements, one needs the ability to provide real-time object level analysis of network traffic. This ability is referred to as Deep Content Inspection (DCI). With DCI, not only can one understand the bits and bytes within the network packets, but they can also "see" the digital objects that are carried over many network packets. It is an enabling technology for many new network applications that digest, route, and manipulate Data In Motion, such as network based anti-malware, DLP, XML routing, object encryption, content annotation, etc.

What Is It?

WedgeOS™ is a high performance Deep Content Inspection (DCI) platform developed by Wedge Networks™, Inc. As a software based Operating System, it can be installed on Common Off The Shelf (COTS) hardware appliances and servers, or can be packaged as Virtual Machines. To date, thousands of instances of WedgeOS™ have been deployed in service providers, enterprises, and SMBs worldwide, carrying out high performance DCI functions for these organizations.

What Does It Do?

The key technical requirements of implementing a DCI application can be summarized as the following:

1. Performance requirements when conducting Deep Content Inspection at the network transport layer
2. Accuracy requirements when enforcing security protection or content accessing policies
3. Transparency requirements when deploying a network layer solution into an existing enterprise or service provider's network
4. Manageability requirements so that the DCI application can be effectively managed as an IT/network asset
5. Reporting requirements providing visibility of application objects

With a set of coherent building blocks, in the form of runtime components and adaptation frameworks, WedgeOS™ enables DCI applications to meet these technical requirements.

BUILDING BLOCKS

Deep Content Inspection Engine
GreenStream™ Technology
High Availability Network Stack
ICAP Network Stack
Open Service Bus
Policy Manager
Session Based Thread Management
SubSonic™ Content Recognition
Traffic Object Streaming
WCCP Network Stack
Enhanced Kernal w/ latest virtualization support
Enhanced Policy and Event API
Policy-based Mail Archiving

DEEP CONTENT INSPECTION ENGINE

This is an architectural abstraction through which MIME objects transmitted through the network are extracted and subjected to different content scanners (i.e. Anti-Malware, Anti-Spam, etc.).

To provide for both high accuracy and high performance, the Deep Content Inspection Engine uses a massive threading framework with every network session mapped to a highly efficient lightweight OS level thread.

Each of the session-based threads use a set of proprietary high performance technologies developed by Wedge Networks™ and its partners, including the patented SubSonic Engine™ technology and GreenStream™ technology.

SUBSONIC CONTENT RECOGNITION

SubSonic Content Recognition (SCR) is a systematic approach of recognizing content that are inspected in other application sessions across many users and application protocols. As a key piece in the patented SubSonic Engine technology, SCR is a pivotal component of the Wedge Networks Operating System (WedgeOS); a set of architecture components that work in tandem to deliver performance, integration and accuracy.

wedge networks
securing the cloud connected world

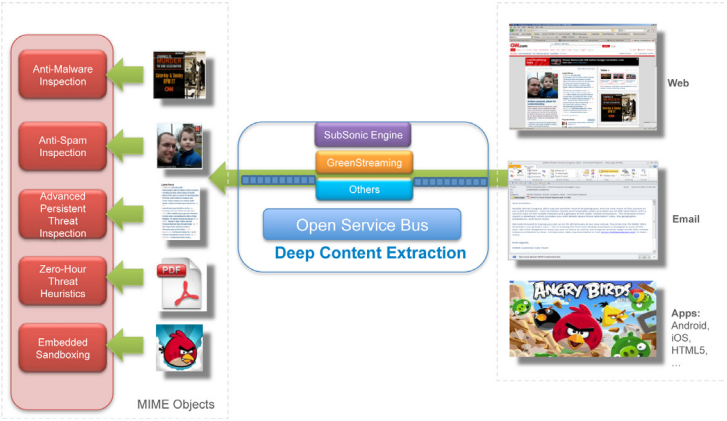
Features of WedgeOS™

WedgeOS™ provides the industry's most comprehensive platform for application-layer security and compliance functions, with the following benefits:

• Enhanced multi-CPU/multi-core support with real-time scheduling to deliver high performance and robustness for Deep Content Inspection functions;
• Optimized transmission and receiving mechanisms to provide line speed Deep Content Inspection throughput;
• Lower Total Cost of Ownership (TCO) due to Stealth Routing based on Transparent Object Flow Inspection (TOFI) that enables plug-and-play network integration capability;
• Deep Content Scanner modeling mechanism to allow for the robust implementation of Deep Content Inspection for new application layer protocols;
• Rapid time-to-market with the Open Service Bus architecture enabling the implementation of new DCI applications;
• Patented optimization algorithms (USPTO 7,630,379) which deliver thirty times (30X) performance improvements over conventional approaches;

WedgeOS™: How It Works

The following figure illustrates the typical process of how WedgeOS™ performs DCI for a normal Web session.



If the DCI application is to prevent malicious content from being downloaded to a user's browser, WedgeOS™ will execute the following steps:

1. Direct-In-Memory Traffic Object Flow Inspection of web traffic to the session based thread for DCI analysis
2. Interception of the packets that are carrying the payload in order to reconstruct a copy of the payload
3. Files are extracted from any archives, binders, packers or scramblers so that Deep Content Scanning can occur
4. Partial payloads are progressively scanned, intercepting specific objects, keywords, malware, etc. if found, while passing on clean content to its destination (i.e. GreenStreaming™). The payload can be subjected to multiple scanners (e.g., anti-malware signature-based scanner, anti-malware heuristic scanner, anti-spam scanner, etc.) simultaneously.
5. If specific /flagged objects are detected, the transmission is interrupted and the content is replaced with a proper, customizable warning message.

Wedge Networks™, Inc.

is transforming the way security is delivered. Powered by the innovative WedgeOS™, Wedge Networks' Cloud Network Defense™ platform is designed to combat the shifting threat landscape associated with cloud, mobility, Internet of Things and consumerization of IT. By embedding security within the network as an elastic, scalable service, it is the only cloud security solution to perform high-performance content inspection without requiring traffic to leave the network. The Wedge Platform™ is deployed globally, delivering security protection for tens of millions of users in Fortune 500 companies, government agencies, internet services providers, and across all industry verticals. Wedge Networks™ is headquartered in Calgary, Canada and has international offices in Dallas, USA; Beijing, China; and Manama, Bahrain.

RUNNING ON wedgeOS

vm wedge

wedgecloud network defense

Wedge Instant-On Program

The WedgeOS™ is available for free trial through the Wedge Instant-On program. The free evaluation comes with 45-day trial license for all services.

Our extensive Product Evaluation Programs allow you to experience the Wedge Content Security platform as part of your decision process.

Call 1-888-276-5356 or visit wedgenetworks.com today for more information.

North America 1 888 276 5356 sales@wedgenetworks.com
USA Headquarters Dallas, TX USA //+1 888 276 5356
Corporate Headquarters Calgary, AB CAN // +1 403 276 5356
APAC Headquarters Beijing, CHINA // +86 400 099 3343
www.wedgenetworks.com