WEDGE OS 5.0

Overview

Wedge's patented Cloud Network Defense™ platform is purpose-built to address the next generation of threats associated with mobility, cloud, social media and internet-of-things. It enables augmented capabilities of key security applications through technology designed to deliver security as a real-time, elastic, and transparent layer of the network fabric.

Powering Cloud Network Defense™ is the WedgeOS™, which utilizes both a Patented Deep Content Inspection (DCI) Engine and Deep Packet Inspection (DPI) Engine, either of which can be run separately from each other or in tandem. It allows all current and future network security functions to be implemented with high performance and robustness. WedgeOS™ is composed of a variety of technologies and is pre-bundled into Cloud Network Defense™ with a set of award winning security applications such as email security, web security, web application firewall, DLP, APT defense, content filtering and mobile data security; all enabled by the underlying DCI and DPI engines.

WedgeOS™ is a high performance 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, can be packaged as Virtual Machines, and can be deployed in a Cloud-based environment through Network Functions Virtualization for Security (NFV-S). To date, thousands of instances of WedgeOS™ have been deployed in service providers, enterprises, and SMBs worldwide, carrying out high performance DCI and DPI functions for these organizations.

Features

• Enhanced multi-CPU/multi-core support with real-time scheduling to deliver high performance and robustness for DCI and DPI 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;
• Rapid time-to-market with the Open Service Bus architecture enabling the implementation of new DCI and DPI applications;
• Patented optimization algorithms (USPTO 7,630,379) which deliver thirty times (30X) performance improvements over conventional approaches.

SubSonic Engine™

The outstanding network data processing ability of the WedgeOS™ is accomplished by the patented SubSonic Engine. It contains a set of architectural components that work in tandem with delivery performance: a multi-thread network data processing mechanism that scales to tens of thousands of concurrent data sessions; an application content recognition module that dramatically reduces the network data processing latency; and an adaptive resource allocation algorithm that improves the overall processing performance for all data sessions. The SubSonic Engine was designed from the ground up to delivery low-latency, high concurrency and Gigabit throughput for Deep Content Inspection of all the commonly used application layer network protocols and data compression formats.

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. By applying an optimized, linear complex fingerprint algorithm instead of the polymorphic scanning on repeated content, SCR accelerates content inspection exponentially by retrieving rather than reapplying resource expensive content inpsection algorithms. It effectively and efficiently processes data payloads without compromising network speeds.

wedge networks
securing the cloud connected world

Deep Content Inspection (DCI)

Deep Content Inspection (DCI) 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 accuracy and high performance, the DCI 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, including the patented SubSonic Engine™ and GreenStream™ technologies.

The key technical requirements of implementing a DCI application:

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

Benefits

Compared with other Data in Motion inspection technologies, DCI technology in the WedgeOS™ provides:

- The ability to extract digital objects in real-time from the Data In Motion sessions leads to the complete comprehension of the intention of the sessions.
- The ability to correlate the comprehension of the digital objects transmitted in many communication sessions leads to new ways of network performance optimization and intelligence.
- The ability to support ICAP and WCCP for explicit proxy mode deployments reduces the cost of network reconfiguration.
- The ability to support transparent proxy mode deployments eliminates the cost of network reconfiguration and supports unlimited VLANs.

Open Service Bus™

The Open Service Bus™ (OSB) provides cross-protocol content inspection services for the SubSonic Engine™. These services could include anti-virus scanning, anti-spam scanning, and more. The OSB provides a unified layer around the content inspection services to present a set of consistent invocation methods / standardized interface for the SubSonic Engine™. It insulates and manages the third party services in separate process spaces to limit the impact of possible faults. This architecture allows the distribution of the inspection workload to multiple processors / machines.

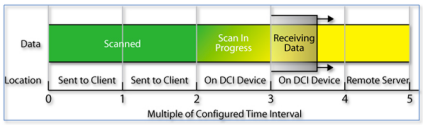
GreenStream™

GreenStream™ is a content inspection technology that provides full inspection of a continuously arriving stream of content; scanning and releasing at regular intervals to lower network latency exponentially.

GreenStream™ continuously scans all data received up to that point as a whole and streams it to the end-user devices at each instance of the configured time interval.

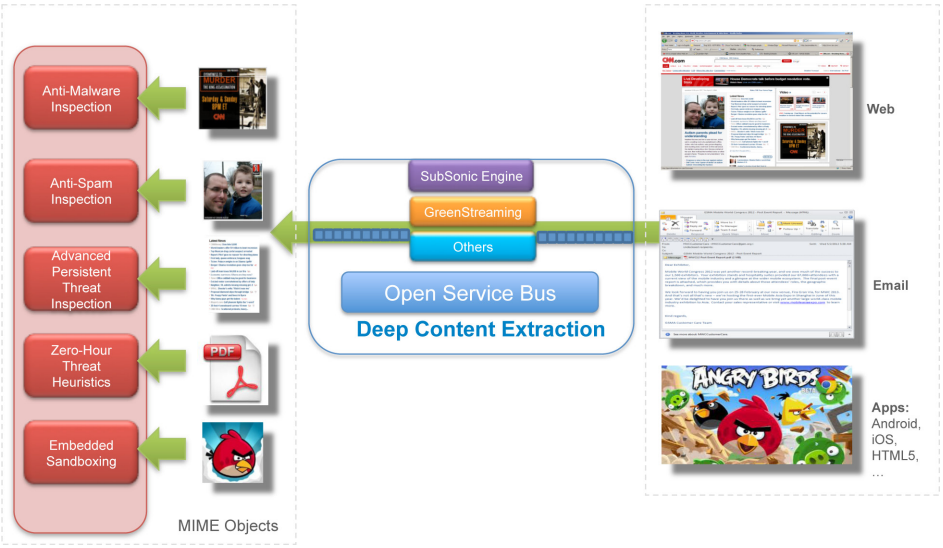
This provides the following benefits:

- Reduces the network latency introduced by a security system.
- Automatically adjusts to the network speed by using a configured time interval as opposed to a configured data chunk size.
- Full context scans without sacrificing detection accuracy, especially when combating malware that spans across a large portion of content.



Deep Content Inspection: How it Works

The illustration outlines 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:

- Direct-In-Memory Traffic Object Flow Inspection of web traffic to the session based thread for DCI analysis
- Interception of the packets that are carrying the payload in order to reconstruct a copy of the payload
- Files are extracted from any archives, binders, packers or scramblers so that Deep Content Scanning can occur
- 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.
- If specific /flagged objects are detected, the transmission is interrupted and the content is replaced with a proper, customizable warning message.

wedgecloud network defense

RUNNING ON wedgeOS

Awards

Info Security Products Guide 2016 GLOBAL EXCELLENCE GOLD

Info Security Products Guide 2015 GLOBAL EXCELLENCE GOLD

CIO Review 50 MOST PROMISING INTERNET OF THINGS SOLUTION PROVIDERS 2015

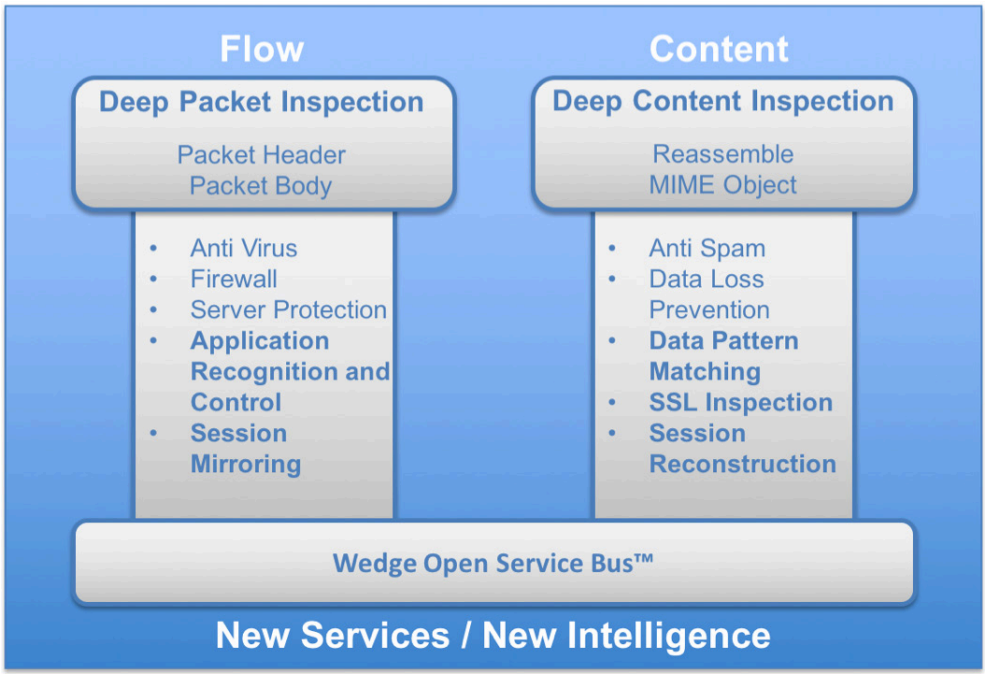
Deep Packet Inspection (DPI)

Deep Packet Inspection integration in the WedgeOS™ provides the platform with Flow security. The integration of DPI allows the WedgeOS™ to inspect both packet header and body, with network traffic being compared against Flow Security signatures, enabling a wide range of services such as AV, Firewall and Server Protection, in addition to application control.

Benefits

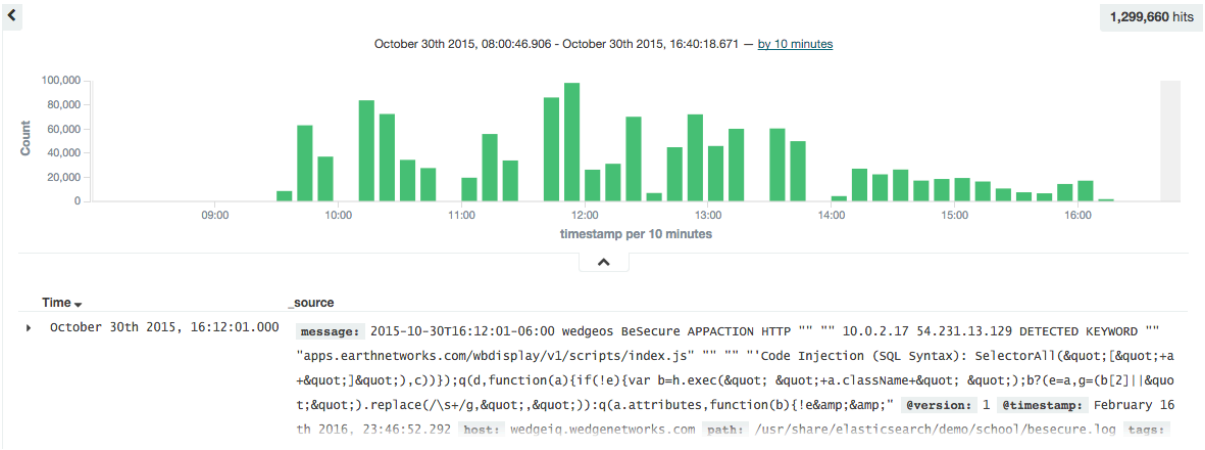
DPI integration enables Wedge to offer:

- **Detect and Block BOT Command and Control** - traffic from a regularly updated list of known botnet command and control servers.
- **Critical Infrastructure Protection** - protect against the use of insecure data transfer methods and known vulnerabilities of various SCADA software packages, such as PcVue, Sunway ForceControl, Siemens FactoryLink, and more.
- **Recognize and Stop Denial of Service** - with the ability to see traffic and DoS attacks on a variety of servers and network appliances.
- **Protect Against Server Exploits** - including a variety of known exploits on many different software applicaions, including PDF readers, Microsoft RDP and Windows Media Player, VNC Server, Java-base programs, JavaScript, and many more.
- **SQL Injection Protection** - including methods of compromising SQL-based RDBMSs, such as Oracle.

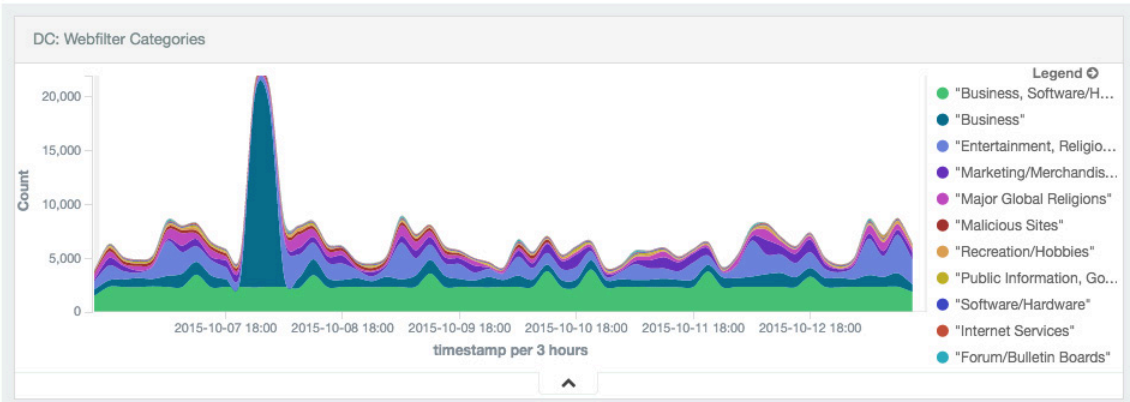


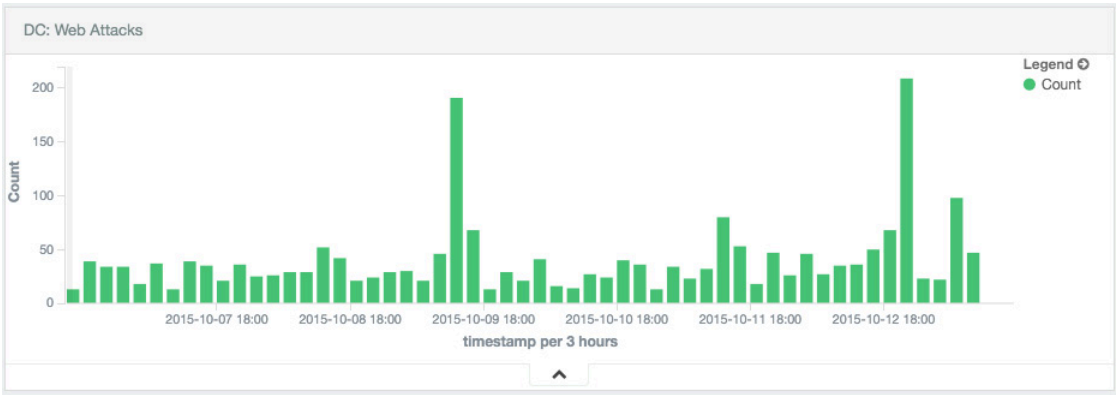
Expandable Platform - Future Services with WedgeOS™

Sample Log Records from WedgeIQ™

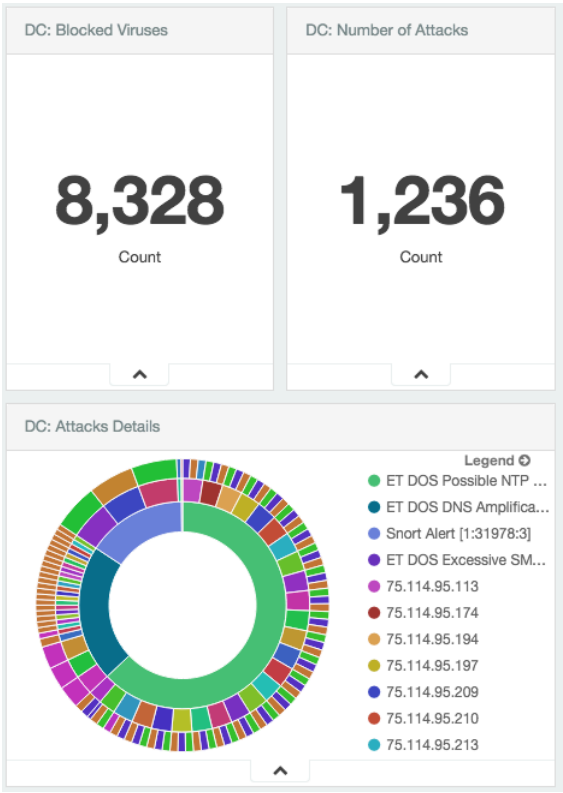


Sample Dashboard Analytics from WedgeIQ™

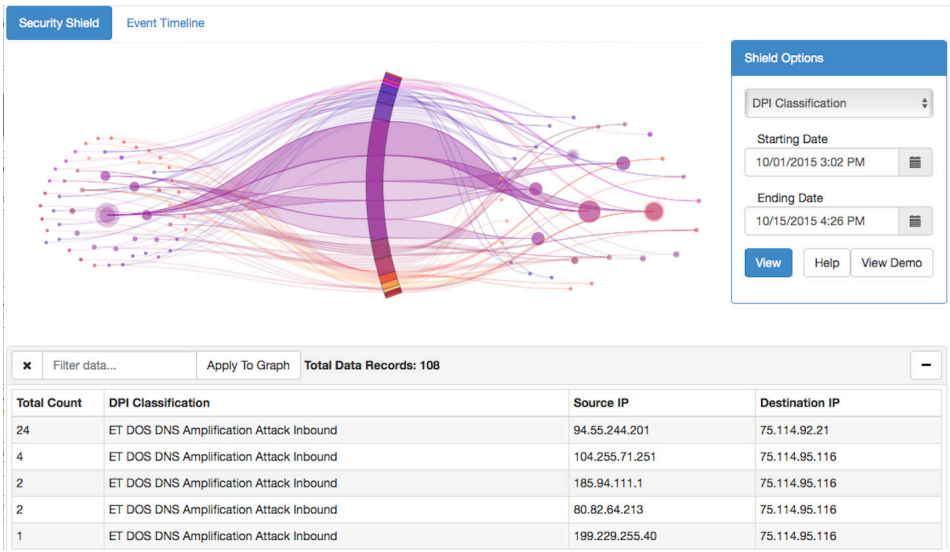




Sample Dashboard Analytics from WedgeIQ™



WedgeIQ™ Security Shield Analytics



Total Count	DPI Classification	Source IP	Destination IP
24	ET DOS DNS Amplification Attack Inbound	94.55.244.201	75.114.92.21
4	ET DOS DNS Amplification Attack Inbound	104.255.71.251	75.114.95.116
2	ET DOS DNS Amplification Attack Inbound	185.94.111.1	75.114.95.116
2	ET DOS DNS Amplification Attack Inbound	80.82.64.213	75.114.95.116
1	ET DOS DNS Amplification Attack Inbound	199.229.255.40	75.114.95.116

Wedge Networks™, Inc.

is transforming the way security is delivered. Powered by the innovative WedgeOS™, Wedge Networks' Cloud Network Defense™ is an orchestrated threat management platform designed to combat the shifting threat landscape associated with cloud, mobility, bring your own device, Internet of Things and consumerization of IT. By applying security policies at the cloud-layer, enterprises and network operators offering security-as-a-service can achieve more effective security, using best-in-class multi-vendor technologies, with greater efficiency and scale. The award winning Wedge Platform™ is deployed globally, delivering security protection for tens of millions of users in Fortune 500 companies, government agencies, internet and broadband service 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.

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