WEDGE NDP-1038T

The Wedge Networks™ NDP-1038T was built for enterprises and SMB's with a concurrent user base of between 2,000 and 4,000 individuals and is the platform of choice for enterprises with fibre connectivity, or a need to store a large amount of security events within the box.

As a multi-gigabit Deep Content Inspection security appliance, the WedgeOS™-based appliance can be easily deployed into any network to transparently enforce Deep Content security policies such as blocking infected traffic at wire line speeds. It is a purpose built appliance for protecting web surfing PCs, laptops, and smartphones from infections, for defending web and application servers against malicious attacks, and for enforcing company policies while not impacting the end-user perception of internet performance and reliability.

Purpose Built From the Ground Up

The Wedge NDP - 1038T was built from the ground up with a focus on catering to those high bandwidth users for which other solutions are unable to protect. Based on Wedge Networks'™ award winning WedgeOS™ Deep Content Inspection platform, this hardware / software combination provides the next generation of Network Based Deep Content Inspection solutions. It incorporates the best of breed content security techniques to protect the network by inspecting commonly used application layer protocols, such as HTTP, SMTP, POP3, IMAP and FTP, effectively eliminating threats before they reach network endpoints (servers, desktops and mobile devices).

Integration

Fully Integrated for use with the many *Cloud Network Defense™ Security Suite services such as APT/Anti-Malware, Anti-Spam/Anti-Spear Phishing, DLP, Mobile Security, Next Generation Content Filtering, Application Control, Web Application Firewall, etc.* to allow dedicated security policies to be deployed across the web and email with a single appliance.

Built for performance with the *SubSonic Engine's*™ unique traffic handling, the resource needs for anti-malware defense are easily administered while allowing room for organizations to grow and add additional protection services without altering user experience.

Seamless network integration with the ability to deploy as a transparent inline bridge, the Wedge Content Security appliances can be deployed into your network with no need for costly and disruptive network outages and reconfigurations. In addition, other deployment modes such as WCCP, ICAP, etc. allow for maximum flexibility.

KEY MARKETS
SMB's with Fibre Connectivity
Educational and Government Institutions that require security event logging

AVAILABLE SECURITY SERVICES
- APT/Anti-Malware
- Anti-Spam/Anti-Spear Phishing
- Data Loss Prevention
- Mobile Security
- Next Generation Content Filtering
- Application Control
- and more...

PROTOCOLS INSPECTED
The Award Winning WedgeOS™ brings together malware protection for both e-mail and web traffic by fully supporting Bi-Directional Scanning of HTTP, FTP, SMTP, POP3 and IMAP Content.

FOR ORGANIZATIONS NEEDING
High Throughput Requirements
High Accuracy
2,000+ User Concurrency

LEVERAGING THE POWERS OF
WedgeOS™
SubSonic Engine™ Technology
Green Streaming™
Open Service Bus™
Deep Content Inspection
Transparent Malware Protection Services

AWARDS
THE GOLDEN BRIDGE AWARDS — GOLD — BEST 2012 — BUSINESS WORLD

SC MAGAZINE ★★★★¾ — UTM Category 2012

Info Security Products Guide 2015 — GLOBAL EXCELLENCE — GOLD ★★★★★

SC MAGAZINE ★★★★★ — Anti-Malware Gateway Category 2011

wedge networks
securing the cloud connected world

Specifications

NDP-1038T

Performance

Email (messages per hour)	1,200,000+
HTTP (requests per hour)	Up to 2,000,000
Concurrent Users	2,000+

(actual number of users is much higher depending on network characteristics)

Hardware

CPU	Intel® Xeon™ 3.5 GHz
RAM	16 GB
Storage	256 GB SSD
Network Ports	8GbECopper + 4GbE SL w/ LAN Bypass
Power Supply	200W ATX Power AC/DC 100-240V full range 4.5A @ 50 ~ 60 Hz
Command Console	COM (RJ-45)
Peripheral Ports	USB 2.0 × 2,VGA

Physical/Operational

Form Factor	1U Rack mount
Height, Width and Depth	16.8" × 18.9" × 1.7"
Weight	28.60 lbs
Operating Temperatures	0°C to 40°C
Storage Temperatures	-20°C to 75°C
Relative Humidity	5% to 90%
Power Consumption (W)	98.6
MTBF (hours)	64,789
Certifications	CE, FCC, RoHS, PSE

Functions Available on the Cloud Network Defense™ Security Suite

APT/Malware Defense combines real-time sandboxing with the broadest threat intelligence and Deep Content Inspection (DCI) to secure against all malware attacks, persistent threats, network abuse, and blended attacks across all networked devices.

Anti-Spam/Anti-Spear Phishing combines real-time intelligence of over 2 billion sensors worldwide with behavioural analysis and DCI to secure against all messaging threats; rapidly deploying into even the most complex of networks with transparent (non-MTA), two-way protection.

Data Loss Prevention detects and prevents the leakage of structured and unstructured data, effectively stopping confidential data escaping via web and email.

Mobile Security enables the secure usage of mobile devices, solving the phishing, malware, network abuse, blended attacks and data security within your network or while roaming.

Next Generation Content Filtering uses the largest web classification database with the most comprehensive categories, augmented with human reviews, producing industry-best accuracy. This enables organizations to understand, filter, monitor and report on Internet usage, allowing employees to take full advantage of the Web without compromising business goals.

Application Control combines real-time network Flow security with the broadest threat intelligence and DCI to enable the detection and blocking of traffic that are detrimental to an organization's productivity and image.

Web Application Firewall is designed to scale instantly to preserve performance and filter attack traffic close to the source, keeping essential web applications up and running. It delivers protection of web applications and secures sensitive database content by blocking threats such as cross-site scripting, SQL injection, buffer overflows, file inclusion, DoS, cookie poisoning, schema poisoning, and countless other attacks.

Unequaled Performance

The NDP-1038T was built with organizations such as government and educational institutions in mind, allowing them to add an extra layer of protection for all of their users, providing the accuracy and performance needed, while adding additional storage to enable the storage of large amounts of security events that typically need to be tracked.

RUNNING ON wedgeOS

Wedge Networks™, Inc.

is transforming how network security is delivered. Its innovative Cloud Network Defense™ is a true cloud network security platform designed to deliver the elastic, embedded and comprehensive security that is required to combat the shifting threat landscape associated with today's cloud connected world. Unlike first generation security products, cloud-assisted appliances or even dedicated security clouds, Cloud Network Defense™ enables inline inspection of both inbound and outbound traffic embedded within the cloud layer across all platforms and device types without latency. Wedge's products are deployed globally, delivering security protection for tens of millions of users in Fortune 500 companies, government agencies, Internet 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 Wedge VM™ 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