| DATASHEET

WEDGE ENTERPRISE-PREMIUM (BANDWIDTH-BASED) SECURITY-AS-A-SERVICE PACKAGE

Deliver Security-as-a-Service to Broadband Customers From the Cloud

Wedge's innovative Subscriber Bandwidth-Based SECaaS packages allow service providers to market and price a variety of SECaaS offerings based on the subscriber's broadband bandwidth, consistent with how broadband services are marketed and sold. This approach eliminates the complexity of tracking per user or per device licensing and closes critical security gaps resulting from the inevitable connectivity of unprotected devices.

The result is a simple to market and easy to administer SECaaS set of offerings, with specific security packages that can be priced and sold based on the security services included with the package and the combined upstream and downstream broadband connection rate of the subscriber's broadband service.

Even better, this approach enables a superior security service by enabling the SECaaS to protect all devices connecting to the network, without requiring any software to be downloaded to devices or appliances to be deployed at the customer's location. Simple, easy, and superior – a winning combination!

Premium Enterprise & App Server Security Delivered as a Service

Wedge Networks™ SECaaS Enterprise-Premium package provides a specialized SECaaS license consisting of Anti-Spam, Anti-Malware, Web Filter, Data Loss Prevention, Mobile Security, Safe Search, Application Control, Server Security and Web Application Firewall security applications. These security applications are orchestrated in conjunction with Wedge Cloud Network Defense™ enabling service providers to deliver premium cyber security as a service to enterprise customers with locally hosted servers requiring additional protection.

This powerful combination of security applications works in concert with Wedge's patented Deep Content Inspection (DCI) to provide:

- **Email & Web Security:** detecting and blocking spam, phishing, malware and other malicious web threats in real-time;
- **Data Loss Prevention:** monitoring and preventing the leakage of critical data from the network that is often targeted by these threats;
- **Web Content Filtering:** facilitating the safety and management of web access and Web 2.0 applications to ensure that the network is being used efficiently and for business compliant purposes from all devices, including mobile.
- **Application Server Protection:** blocking attacks against Web, VoIP, and other application servers and network applications.

The Difference

Wedge's SECaaS Enterprise-Premium package applies a portfolio of security applications deep into subscriber's content, with cloud-based scalability for industry leading Enterprise-grade security, with Carrier-grade scale and reliability, plus protection of locally hosted application servers for unmatched threat management effectiveness and throughput, featuring:

Email Security:

- **Most accurate detection and blocking of spam and phishing attacks** – with micro updates every minute, real-time spam identification through behavioral analysis, and WedgeIQ's™ global threat intelligence network.
- **World's largest threat intelligence network** – over 2 Billion sensors in over 165 countries collaborating to identify and block globally encountered threats.
- **Stops blended, multi-channel messaging attacks** – fully integrated solution over all web and email protocols.

EMAIL SECURITY PROTECTION

- Advanced Threats
- Phishing
- Trojans
- Worms
- Zero Hour
- Targeted Attacks
- Malware
- Spam Botnets
- IP Blacklisting
- Blended Attacks
- Messaging Abuse

wedge networks

securing the cloud connected world

Web Security:

Web Threat Protection

- **Most accurate detection and up-to-date detection and blocking of network attacks** – with comprehensive best-of-breed signatures updated hourly, leveraging the combined knowledge across WedgeIQ's™ global threat intelligence network.
- **The only solution with multiple full signature databases** – industry-leading accuracy rates are achieved as a result of scanning against multiple complete signature databases.
- **Real-time sandboxed behavioural heuristics detect zero-hour attacks** – the ability to see all content and discover the "intent" of malware within embedded sandboxes - zero-hour attacks can be stopped in their tracks.
- **Protecting all operating systems and all devices** – with built-in cross-session learning, Wedge can identify malware on one operating system and block it on all others.

Safe Web Surfing and Application Control

- **Leading Content Provider policy integration** – seamless web application control for Google Safe Search, YouTube, and more.
- **Most comprehensive web classification database** – 280 million top-level domains spanning more than 95 categories for accurate and effective web filtering.
- **Application Control to prevent the usage or to at least control the bandwidth consumption of specified applications and application types** – giving network administrators greater control over valuable network resources.

Data Security:

- **Flexible data loss prevention criteria** – protecting against unauthorized transmission of specified content.
- **Largest coverage of file formats and protocols for inspection** – with coverage of 400+ file types and multiple protocols for industry leading DLP inspection.
- **Highest accuracy with two staged scan** – ability to rapidly scan streams and extract suspicious content for more comprehensive evaluation, all in real-time.
- **Built-in compliance support** – easily monitor and enforce compliance based on pre-loaded policies and reports.

Mobile Security:

- **The application of the above policies to mobile phones** – protecting users, enforcing compliance, and securing content even when access is via mobile devices.

Application Server Security:

- **Detection and blocking of traffic matching the behaviour or various common internet server attacks** – protecting application servers and all devices from BOT and DOS attacks, exploits, SQL injections and more.
- **Web Application Firewall (WAF) real-time HTTP traffic monitoring** – providing constant visibility to users' interactions with web applications as well as access control to limit surface attacks.

Disclaimer: This specification sheet provides a brief overview of features and capabilities. Please refer to the most current user guide for additional details.

WEB SECURITY

- Advanced Threats
- Web Threats
- Trojans
- Worms
- Zero Hour
- Targeted Attacks
- Malware
- Key Loggers
- Viruses
- Rootkits
- Spyware
- Bots
- Malicious Apps
- Blended Attacks
- URL FIltering
- Web Content Filtering
- Safe Search

SECURES DATA IN ALL APPLICATIONS

- Web
- HTML5
- Games
- Email
- Mobile Apps
- Social Networking
- SMS/MMS
- Mobile Payments
- App Stores
- Content on Demand

wedgecloud
network defense

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.

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