

| DATASHEET

WEDGE ENTERPRISE-BASIC (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!



Robust Web and Email Security

Wedge Networks' Enterprise-Basic SECaaS package provides a specialized SECaaS license consisting of Wedge's Anti-Spam and Anti-Malware security applications orchestrated in conjunction with Wedge Cloud Network Defense™ enabling service providers to deliver robust web and email security for their enterprise customers of all sizes.

Wedge Networks™ carrier-grade Anti-Spam Network App combines real-time intelligence of over 2 billion sensors worldwide with behavior analysis and Deep Content Inspection (DCI) to secure against all messaging threats. Anti-Spam services are supported with transparent (non-MTA), two-way protection which provides in-line protection without the need to redirect email to a different server for processing.

Wedge Networks Anti-Malware Network App combines real-time sandboxing with the industry's broadest threat intelligence and DCI to secure against all malware attacks, persistent threats, network abuse, and blended attacks across all networked devices. The combination of Anti-Spam and Anti-Malware with Wedge's patented DCI provides robust web and email security with industry leading performance.

The Difference

Wedge Cloud Network Defense™ with the SECaaS Enterprise-Basic package applies Anti-Spam and Anti-Malware deep into subscriber's content, with cloud-based scalability to deliver Enterprise-grade Email and Web security, and with Carrier-grade scale and reliability 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 WedgeQ's™ global threat intelligence network.
- **World's largest messaging intelligence network** – over 2 Billion sensors in over 165 countries collaborating to identify and block threats encountered globally.
- **Stops blended, multi-channel messaging attacks** – fully integrated solution over all web and email protocols.

Web Security:

- **Most accurate and up-to-date detection and blocking of network attacks** – with the industry's most comprehensive best-of-breed signatures updated hourly, leveraging the combined knowledge across WedgeQ'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.
- **URL filtering based on parameters such as time interval and key word patterns** – enables organizations to effectively manage risk by controlling access to web content across users, groups, devices and locations.
- **Real-time sandboxed behavioral 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.

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

EMAIL SECURITY PROTECTION

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

WEB SECURITY

- Advanced Threats
- Web Threats
- Trojans
- Worms
- Zero Hour
- Targeted Attacks
- Malware
- Key Loggers
- Viruses
- Rootkits
- Spyware
- Bots
- Malicious Apps
- Blended Attacks



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.