WedgeSecure Wi-Fi – Data Sheet

December 2025

Overview

- Cloud-managed secure Wi-Fi service that combines:
  - Commercial Wi-Fi access points
  - Cloud orchestration
  - Wedge real-time AI threat prevention
- Edge-to-cloud security model:
  - All traffic scanning, deep inspection, and threat analysis occur in the cloud
  - Policy enforcement and threat blocking occur directly on each access point (AP)
- Eliminates the need for branch security gateways or additional on-site security hardware
- Designed for:
  - Remote, industrial, or temporary sites
  - Pop-up locations, kiosks, and retail
  - LTE/5G/Starlink-connected or space/power-constrained environments
- Zero-touch provisioning simplifies large MSP and distributed enterprise deployments

Features and Benefits

- **Edge-to-Cloud Security Architecture**
  - Cloud-based inspection with enforcement on each AP
  - Inline protection at the wireless edge without gateway refreshes
- **Low-Cost, Hardware-Light Deployment**
  - Security embedded in the AP; no separate security appliance
  - Reduces shipping, installation, and on-site support costs
- **No Gateway Refresh Required**
  - Security anchored at the AP
  - Avoids upgrades of physical security gateways and complex network redesigns
- **Real-Time AI Threat Prevention**
  - Cloud AI/ML engines detect and block:
    - Malware and ransomware
    - Phishing and web-based attacks
    - Advanced persistent threats (APTs)
  - Protects all connected users and IoT devices
- **Compliance-Oriented Design**
  - Supports requirements aligned with HIPAA, GDPR, PCI-DSS and similar frameworks
  - Uses strong encryption, segmentation, inspection, and continuous monitoring
- **Centralized Cloud Management & Zero-Touch Provisioning**
  - Unified, multi-tenant cloud console
  - Zero-touch AP onboarding and configuration
  - Consistent policies across sites and customers

- **Optimized for Space- / Power-Limited Locations**
  - Suited for sites where additional hardware is impractical
  - Works well with LTE/5G/Starlink backhaul and remote industrial deployments
- **OpenWiFi Ecosystem Support**
  - Built on an open, carrier-grade architecture
  - Aligned with the OpenWiFi ecosystem for vendor flexibility

Use Cases

- **Distributed Organizations with Direct-to-Internet Access**
  - Branches connect directly to the internet without central backhaul
  - Provides consistent, cloud-managed security at each site without local gateways
- **Remote or Field Sites Using LTE/5G/Starlink**
  - Temporary, mobile, or satellite-connected locations
  - Enforcement at the AP with cloud inspection protects sites with limited infrastructure
- **SMBs Without Gateway-Based Security**
  - Small and medium businesses gain enterprise-grade Wi-Fi security
  - Simple cloud activation and no extra hardware to purchase or maintain
- **Pop-Up, Kiosk, and Event Deployments**
  - Retail kiosks, temporary stores, and events needing secure Wi-Fi
  - Rapid deployment and recovery with zero-touch provisioning
- **MSP-Managed Wi-Fi Fleets**
  - Multi-tenant cloud management for large numbers of customer sites
  - Simplifies rollout of secure Wi-Fi as a managed service

Technical Specifications

- **Security Architecture**
  - Edge-to-cloud model:
    - Cloud: traffic scanning, deep inspection, AI/ML threat analysis
    - AP: policy enforcement, threat blocking, and inline protection
  - Cloud-delivered service with centralized control
- **Supported Wi-Fi Infrastructure**
  - Access points:
    - Edgecore Wi-Fi APs
  - Controllers / management:
    - Integration with Edgecore ecCLOUD for orchestration
  - Deployment types:
    - Indoor and outdoor APs
    - Wi-Fi standards: 802.11ac/ax/be (Wi-Fi 5, 6, 6E, 7)
- **Security Service Tiers**
  - **Basic Security**
    - Secure Web Gateway (SWG)
    - Anti-malware and web filtering
    - Safe search enforcement
  - **Advanced Security**
    - TLS/SSL inspection
    - Deep content analysis

        - Requires installation of a Wedge CA certificate on user devices
- **Management & Operations**
    - Cloud-based management console
    - Multi-tenant support for MSPs and large organizations
    - Zero-touch provisioning and activation for supported APs
    - Centralized policy definition and reporting across all sites
- **Compliance & Policy Controls**
    - Strong encryption and network segmentation support
    - Full traffic inspection and continuous monitoring
    - Helps organizations meet HIPAA, GDPR, PCI-DSS and similar regulatory requirements

Wi-Fi Access Point Specifications

EAP101	EAP102	EAP104	EAP105	EAP111
Wi-Fi 6 Indoor Access Point	Wi-Fi 6 Indoor Access Point	Wi-Fi 6 Indoor Wall-Plate Access Point	Wi-Fi 7 Indoor Access Point	Wi-Fi 6 Indoor/Outdoor Access Point
Concurrent Dual-Band 2.4GHz & 5GHz	Concurrent Dual-Band 2.4GHz & 5GHz	Concurrent Dual-Band 2.4GHz & 5GHz	Concurrent tri-band 2.4 & 5GHz & 6GHz	Concurrent Dual-Band 2.4GHz & 5GHz
2×2:2 UL MU-MIMO	4×4:4 UL MU-MIMO	2×2:2 UL MU-MIMO	2×2:2 UL/DL MU-MIMO	2×2:2 UL MU-MIMO
Support BLE/Zigbee	Support BLE	Support BLE/Zigbee	Support BLE/Zigbee/Thread	Support BLE/Zigbee/Thread
1 x 2.5GbE PoE WAN	1 x 2.5GbE PoE WAN	1 x GbE PoE WAN	1 x 5GbE PoE WAN	1 x GbE PoE WAN
2 x GbE LAN	1 x GbE LAN	4 x GbE with 1 x PoE Out LAN	1 x GbE LAN	1 x GbE LAN
-	-	-	-	IP55
Support ecCLOUD	Support ecCLOUD	Support ecCLOUD	Support ecCLOUD	Support ecCLOUD

Security Functions

Malware Protection	
Anti-virus	Always-fresh signature and heuristic-based threat intelligence to detect all known malware, such as Viruses, Trojans, Worms, Backdoors, etc.
AI Anti-malware	Artificial intelligence machine learning based malware detection for unknown and never-seen-before malware, such as APT, Zero-day, Ransomware, etc.
Malware Analyzer	Sandbox-based malware detection for greyware and suspicious code, data, and files.
Secure Web Gateway	
Malware sites	Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.
Spyware and Adware	Spyware or Adware sites that gather or track information and pop up unsolicited ads.
Bot Nets	URLs and IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.
Hacking	Illegal or questionable access to or the use of communications equipment/software.

Phishing and Other Frauds	Phishing, pharming, and other sites masquerading as reputable sites that usually obtain personal information from users.
SPAM URLs	URLs contained in SPAM
Confirmed SPAM Sources	Spam Sources include Tunneling Spam messages through a proxy, anomalous SMTP activities, and Forum Spam activities.
Keyloggers and Monitoring	Software agents that track a user's keystrokes or monitor their web surfing Habits.
Proxy Avoidance and Anonymizers	Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring.
Additional Security (Optional) [1]	
Data Loss Prevention	Block or monitor the specified keywords and/or keyword categories.
URL Detection	Block or monitor the specified URLs.
1. Additional security functions are optional and provided upon request.	
Key Features	
Core Features	Instant activation
	Real-time detection and blocking
	Deep Content Inspection (DCI)
	Prevention of unknown malware, such as APTs, in both HTTP and HTTPS traffic
	Web filtering across HTTP and HTTPS connections
	Scheduled Security Event Report