WedgeSecure Cloud – Data Sheet

December 2025

Overview

- Cloud-native security and orchestration platform for protecting systems connected through software-defined networks, including:
  - VPNs
  - SD-WAN
  - Software-defined virtual networks
  - Inter-cloud communications
- Delivered as a multi-tenant cloud service running clustered virtual instances of:
  - WedgeSecure IQ (analytics, orchestration, and reporting)
  - WedgeSecure Engine (inspection and enforcement)
- Provides inline security for tunneled and inter-cloud traffic using:
  - Deep content inspection
  - AI-based malware prevention
  - Policy controls for web, SaaS, and cloud-to-cloud traffic

Features and Benefits

- **Cloud-Native Deployment**
  - No on-premises appliances required
  - Centralized cloud service activation across multiple sites
- **Inline Threat Prevention**
  - Real-time blocking of malware, exploits, and policy violations as traffic traverses secure tunnels
  - Designed to protect cloud-connected workloads and users in motion
- **AI-Powered Anti-Malware**
  - Detects and blocks known and unknown threats using deep-learning models
  - Targets zero-day and ransomware-style attacks in addition to signature-based detection
- **Secure Web Gateway Controls**
  - URL/category filtering and safe-search enforcement
  - Blocks common web risks including phishing destinations and malicious websites
  - Controls access to proxy-avoidance and other high-risk browsing paths
- **Intrusion Detection and Prevention**
  - Network-based protections including:
    - DoS/DDoS patterns
    - Exploit and injection attempts (for example, SQL injection)
    - Botnet command-and-control (C2) activity
- **Network-Layer Data Loss Prevention**
  - Deep inspection of data in motion
  - Policy-based controls to reduce sensitive data exfiltration over network traffic

- **LLM-Based Content Policy Enforcement**
  - Context-aware policy enforcement for web and SaaS traffic (beyond keyword matching)
  - Supports governance use cases such as:
    - Safer use of generative AI tools
    - More accurate content control for sensitive or inappropriate data
- **Centralized Orchestration and Analytics**
  - Unified policy management, event analytics, and reporting
  - Threat intelligence and forensic drill-down capabilities
- **Secure Connectivity and Scaling**
  - Tunnel support: IPsec and WireGuard
  - Elastic scaling from small deployments to high-throughput environments
- **Multi-Tenant Operations for MSPs**
  - Tenant isolation and delegated administration
  - Supports large customer fleets from a single platform
  - Enables branded / white-label Security-as-a-Service delivery
- **Subscription Model**
  - Pay-as-you-grow consumption model
  - Automatic updates without hardware maintenance

Use Cases

- **Cloud-Edge Organizations**
  - Secure inbound and outbound traffic routed through:
    - VPN hubs
    - SD-WAN overlays
    - Cloud-based egress points
  - Suitable for:
    - Headquarters and large campuses using cloud egress
    - Data centers with cloud-connected workloads
    - Cloud-first organizations consolidating security enforcement in the cloud
- **Managed Service Providers (MSPs/MSSPs)**
  - Deliver multi-customer Security-as-a-Service from one platform
  - Use cases include bundling security into:
    - Managed connectivity services
    - SD-WAN offerings
    - UCaaS or managed network services
  - Capabilities typically delivered per tenant:
    - Threat prevention, web filtering, IDPS, and DLP controls

Technical Specifications

- **Platform Architecture**
  - Cloud-native, multi-tenant service
  - Clustered virtual instances for scale and resiliency
  - Core components:
    - WedgeSecure IQ (orchestration/analytics)
    - WedgeSecure Engine (inspection/enforcement)
- **Inspection and Enforcement**

    - Deep content inspection for tunneled and inter-cloud traffic
    - Inline enforcement for threats and policy violations
- **Policy and Compliance Controls**
    - Tenant-aware policy framework for shared environments
    - Audit-ready logging designed to support common governance and regulatory needs
- **Security Capabilities**
    - AI/ML-based malware prevention
    - Secure Web Gateway controls (URL/category filtering, safe search)
    - Intrusion Detection and Prevention (network attack detection/mitigation)
    - Network-layer Data Loss Prevention (DLP)
    - Context-aware content policy enforcement using LLM techniques
- **Connectivity**
    - Secure tunnel support: IPsec and WireGuard
    - Supports SD-WAN and VPN-connected architectures
    - Scales across a wide throughput range (deployment-dependent)
- **Operations**
    - Centralized management console
    - Multi-tenant administration with delegated roles
    - Reporting and forensic drill-down tools

Software Specifications

Software Specifications	
Threat Prevention	Dual-engine signature + AI/ML anti-malware (zero-day detection in milliseconds) Sandbox detonation for greyware New-Gen IDPS (DoS, SQLi, exploits, Bot C&C, CVEs, etc.) Advanced Web Filter (categorized filtering, malicious content blocking, safe search) Keyword-based network DLP
Secure Connectivity	High-performance VPN termination (BYOE/BYOK support) Post-quantum-safe management plane High-availability with automatic failover and load balancing
Deep Visibility & Analytics	Actionable dashboards, forensic drill-down, customizable reporting Intelligent SIEM with Data Fusion High-throughput telemetry ingestion & SIEM-friendly log export
Orchestration & Operation	Full RESTful API suite for orchestration Policy, data, and system operation
Performance & Scale	100 Mbps (SOHO) to >100 Gbps (large providers) Real-time processing of multi-petabyte datasets Elastic cloud scaling (AWS, Azure, GCP, private cloud)

Configuration Specifications

Configuration Specifications	
Product Components	WedgeSecure Nucleator WedgeSecure IQ WedgeSecure Engine

Deployment Environment	Public cloud (AWS, Azure, GCP, Oracle, etc.) or private cloud Supported Hypervisors: ESXi, VirtualBox, ProxmoxVE, KVM
Deployment Modes	Router Bridge TAP Explicit proxy ICAP WCCP
Throughput	100 Mbps – >100 Gbps (elastic)
High Availability	Active-active clustering with load balancing and automatic failover
Secure Tunnel	IPSec VPN WireGuard Support SD-WAN