

FlexSD-WAN & SASE

Cloud-Delivered Security and WAN Performance

High-Performance SD-WAN Connectivity for distributed Networks

FlexSD-WAN provides application-aware WAN connectivity for distributed environments with multiple access links and increasing cloud traffic. This product delivers intelligent traffic steering, multi-link aggregation, and centralized policy control to ensure predictable application performance and resilient connectivity across branch offices, data centers, and public cloud environments.

FlexSD-WAN can be deployed as a standalone SD-WAN solution or extended with optional SASE security capabilities through FlexSD-WAN & SASE.

Key Benefits

- ✓ Multi-link aggregation and seamless failover for continuous connectivity.
- ✓ Application-aware traffic steering for SaaS, cloud, and critical workloads.
- ✓ Centralized orchestration with zero-touch provisioning.
- ✓ Real-time visibility into applications, links, and bandwidth usage.
- ✓ Scalable bandwidth per site from 30 Mbps to 2 Gbps.
- ✓ Optional SASE Add-Ons.



Unified Connectivity



Advanced Security



Cloud Optimization



Simplified Management



Flexible Hosting

SASE Add-Ons

Secure Access Services Delivered as an Extension of SD-WAN

FlexProtect SD-WAN & SASE extends FlexSD-WAN with cloud-delivered security services integrated into the WAN architecture.

Security inspection and policy enforcement are performed at hosted or customer-managed Points of Presence (PoPs), while WAN connectivity remains at the branch via the SD-WAN Agent.

SASE Add-Ons are available only with FlexSD-WAN and may be activated individually or combined.

FlexSD-WAN Hardware



Silicom Ibiza



Armortec NC-C632D

Category	Medium Device	Large Device
	Silicom Ibiza	Armortec NC-C632D
Form Factor	Fanless appliance with integrated antennas	Fanless appliance
CPU	Intel® Atom® x7405C (4 cores)	Intel® Atom® C3558 (4 cores)
Memory	8 GB	8 GB
Storage	64 GB	64 GB
Ethernet Interfaces	4 × 2.5 Gbps RJ45	6 × 1 Gbps RJ45
Fiber Interfaces	1 × 1 Gbps SFP cage	2 × 10 Gbps SFP+ cages
Console Port	-	1 × RJ45
USB / Video	-	2 × USB, 1 × VGA
Expansion Slots	1 × PCIe	1 × Mini-PCIe
LTE Support	Up to 2 × 4G LTE dual-SIM radio cards (optional)	Via Mini-PCIe (optional)
5G Support	Up to 2 × 5G sub-6 dual-SIM radio cards (optional)	Via Mini-PCIe (optional)
Wi-Fi Support	Wi-Fi AP / client card (optional)	-
SIM Support	Integrated (per radio module)	External SIM expansion slot
Primary Use Case	Multi-access branch with wireless WAN	High-throughput edge / aggregation

Package Contents

SD-WAN Hub Deployment options:

- Co-managed (at the network edge) SD-WAN Gateway and optional SASE Add-Ons
- Hosted (by Adaptiv Networks) SD-WAN Gateway and optional SASE Add-Ons
- Cloud Orchestration (Adaptiv Networks)

Cost-effective device on-prem

Software

- BATM OS and Adaptiv Networks SD-WAN agent (bit rate license up to 4 Gbps full duplex)

Platinum support package (3 years):

- 24×7 technical support
- Device RMA

SD-WAN Tiers

All tiers support scalable bandwidth from 30 Mbps to 2 Gbps per site.

SD-WAN Business

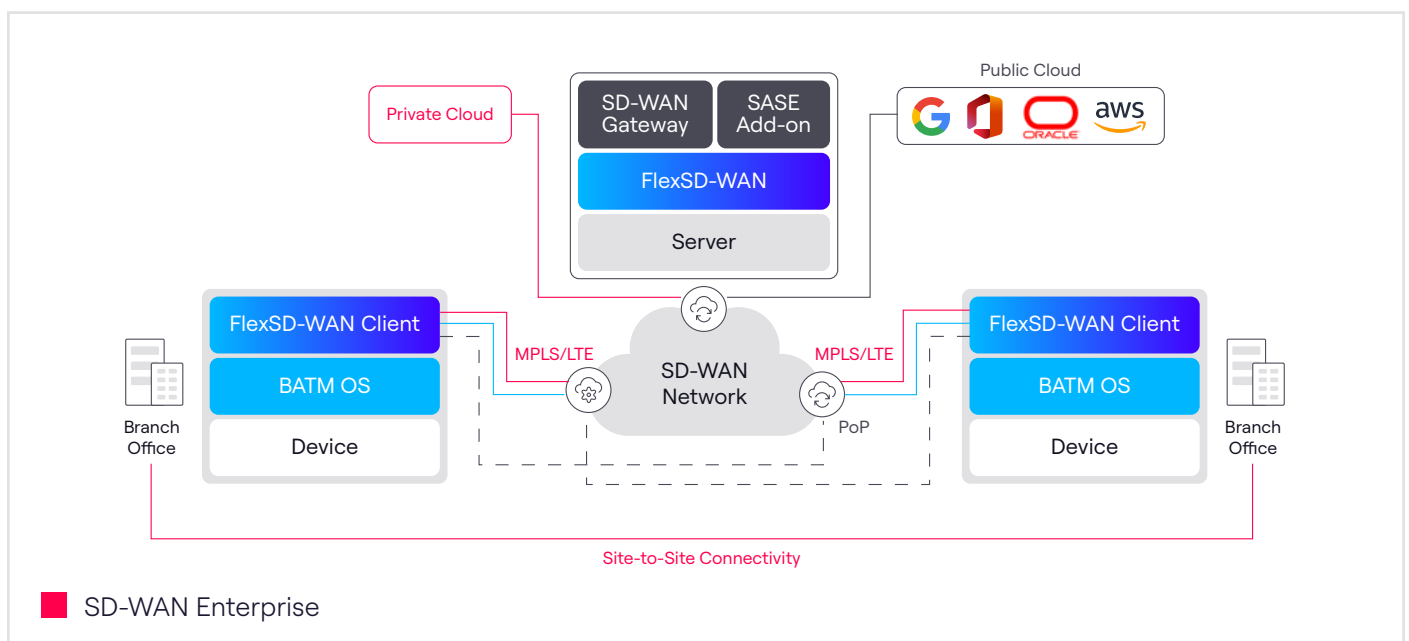
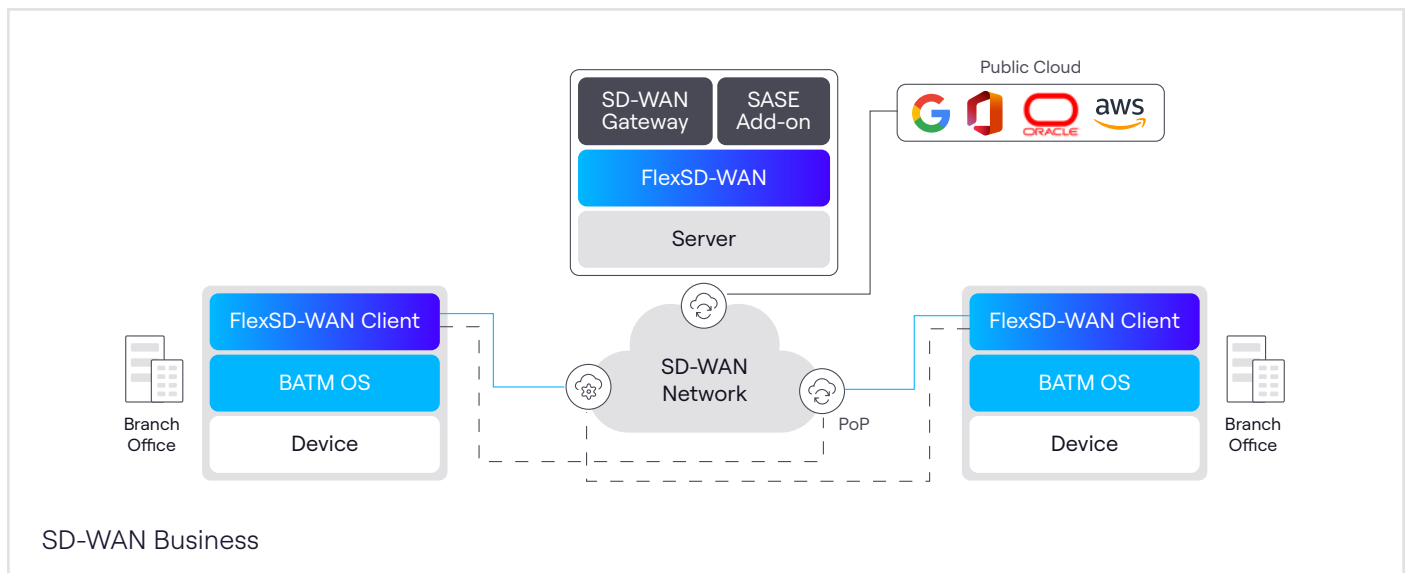
Optimized connectivity for SaaS and public cloud environments with simplified operations and application-aware performance.

- Reliable and secure optimized connection to the cloud
- Effortless multi-link network management
- Applications performance optimization
- Cost-effective scalable networking
- Reliable secure access

SD-WAN Enterprise

Includes all Business tier capabilities, plus advanced hybrid networking, secure site-to-site connectivity, and private cloud access.

- Seamless failover across broadband, MPLS, and LTE
- Secure site-to-site connectivity for private networks
- Optimized access to private data centers and cloud environments
- Application-aware routing with multi-link aggregation
- Scalable networking for distributed enterprises
- Zero-touch provisioning for simplified management



SD-WAN Features	Business	Enterprise
Network Orchestration		
Cloud Management Portal	✓	✓
Zero-Touch Provisioning	✓	✓
Site Status Configuration	✓	✓
Application Visibility & Control	✓	✓
Link Monitoring Tools	✓	✓
Bandwidth Utilization Reporting	✓	✓
Remote Troubleshooting	✓	✓
Smart Connectivity		
Multi-Link Aggregation	✓	✓
MPLS Support	✗	✓
LTE Support	✗	✓
Site-to-Site connection	✗	✓
Intelligent Path Steering	✓	✓
Seamless Link Failover	✓	✓
Application Recognition	✓	✓
Bi-directional application priority	✓	✓
Public Cloud App Prioritization	✓	✓
Private Cloud App Prioritization	✗	✓
Branch Networking		
Cloud-Managed Edge Device	✓	✓
Full DHCP Server High Availability	✓	✓
NAT Port/IP Forwarding	For local breakout traffic only	
Additional IP Addresses	Not included in basic license	
Security		
Site-to-Site Encryption	✗	✓
Internet Access Encryption	✓	✓
Zero Trust Network Access	✓	✓
Stateful Branch Firewall	✓	✓
Custom Firewall Support	✓	✓
Network Routing		
Intelligent Cloud Gateway	✓	✓
Gateway Internet Breakout	✓	✓
Branch Internet Breakout	✓	✓
Private IP (CGNAT)	✓	✓
Max Bandwidth Throughput	2 Gbps	

01

EdgeSecure Web

DNS-and URL-based security controls applied to internet-bound traffic.

URL & DNS Filtering

Controls access to web content by blocking malicious or unauthorized websites. Ideal for business looking to reduce security costs.

Legal Risk Protection

Restricts access to content tied to illegal activity (e.g., drug trafficking, adult content, gambling) using 20M+ categorized URLs.

Security Risk Protection

Blocks access to phishing, spyware, and malware-infected websites to reduce exposure to common internet-based threats.

02

EdgeSecure Network

Deep traffic inspection and threat detection for SD-WAN traffic flows.

Application-level analysis and security inspection are performed at the network edge for cloud, internet, and private application traffic.

Network Traffic Visibility

Offers comprehensive monitoring and analysis of network traffic for enhanced security and performance management.

Deep Packet Inspection

Provides in-depth visibility into network traffic, classifying applications and detecting threats in real time to enhance security and performance.

Feature

Traffic Classification	Uses OpenAPPID and Asymmetric Web Filtering to identify and categorize network traffic based on applications and services.
DoS and Exploits Detection / Blocking	Leverages Snort syntax to detect and mitigate Denial of Service (DoS) attacks and exploit attempts.

Deep Content Inspection

Analyzes files, MIME types, compressed archives, and application-layer protocols to detect hidden threats and enforce security policies.

Feature

MIME Types	Supports all IANA-registered MIME types to analyze and filter content.
Unarchiving and Unpacking	Detects over 500 distinct runtime packers and 3000+ versions, supporting formats like .zip, .rar, and newer compression types like Google Brotli.
Application Protocols	Inspects multiple application-layer protocols including HTTP, FTP, SMTP, IMAP, POP3, SOAP, MAPI, XML/HTTP, and popular webmail services.
TLS Versions	Supports TLS v1.1, v1.2, and v1.3 for encrypted traffic inspection.

AI/ML For Advanced Threats

Leverages artificial intelligence and machine learning to detect and prevent sophisticated cyber threats, including zero-day attacks and advanced persistent threats.

Feature

Protected Endpoint Operating Systems	Covers major OS platforms including Windows, Linux, iOS, Android, and macOS for threat detection.
AI / ML Algorithms	Utilizes deep learning models such as CNN, GCNN, and FM for detecting sophisticated threats.
Analysis Types	Performs real-time static analysis, behavior simulation, and in-situ monitoring to prevent advanced persistent threats.

Security Functions Orchestration

Integrates multiple security technologies, such as IDS/IPS, malware protection, data loss prevention, and compliance measures, to provide a comprehensive security framework.

Feature

Intrusion Detection and Prevention (IDS/IPS)	Detects and blocks malicious activities using real-time signature and anomaly-based detection.
Malware Protection	Uses multi-signature databases, AI/ML techniques, and dedicated malware analyzers to detect and mitigate threats.
Data Loss Prevention	Employs automation, regex-based filtering, and network-based detection to prevent unauthorized data exfiltration.
MDR / EDR Integration	Compatible with security solutions like Cylance and TriagingX for endpoint detection and response (EDR).
GRC Compliance	Ensures adherence to legal requirements such as ETSI 103 for lawful interception and governance, risk, and compliance (GRC) standards.
Application Control	Monitors and restricts access to web chat applications and VoIP services for security and compliance.

BATM enables enterprises, communications service providers, and system integrators to build and operate resilient, secure, and flexible networks across distributed environments.

For more information contact us at salesnetworks@batm.com.