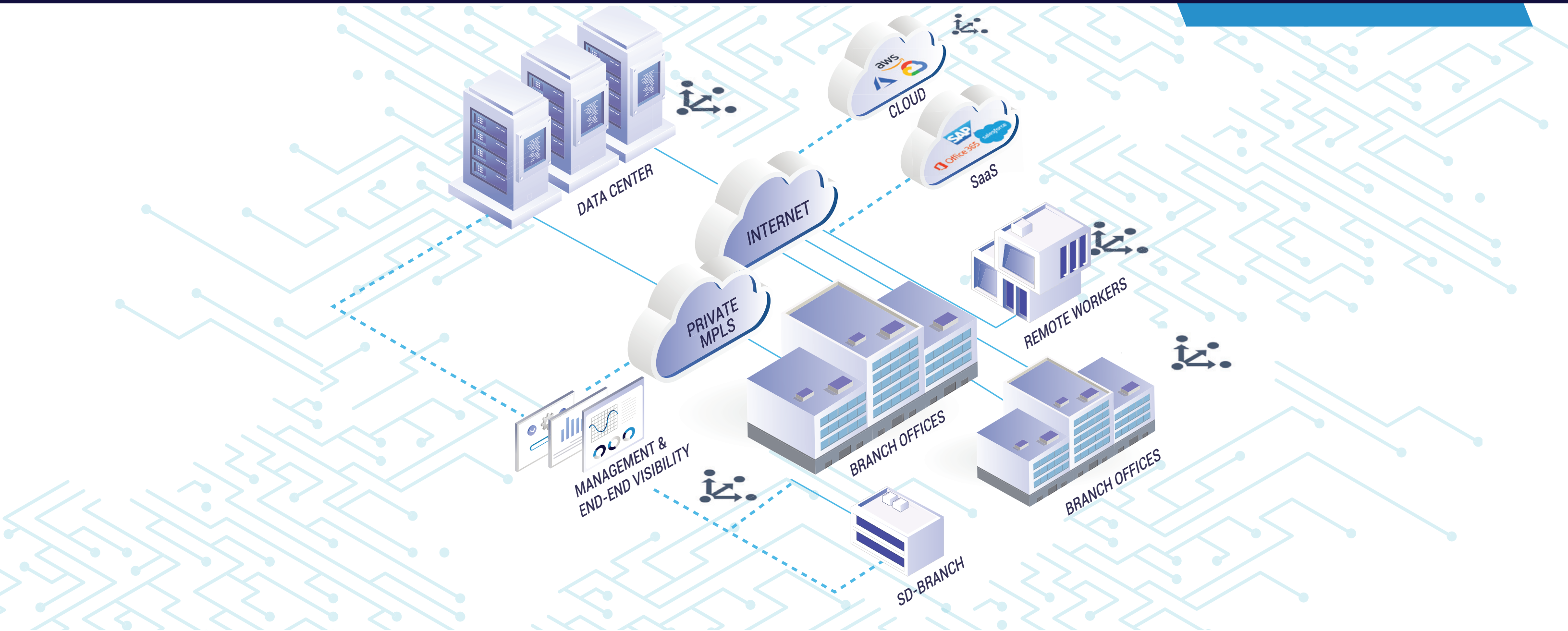
CONTERRA NETWORKS

Fiber Driven. People Powered.

DATA SHEET

Conterra Secure SD-WAN



Feature

- World's only ASICaccelerated SD-WAN
- 5000+ applications identified with real-time SSL inspection
- Self-healing capabilities for enhanced user experience
- Cloud on-ramp for efficient SaaS adoption
- Simplified operations with NOC management and analytics
- Enhanced granular analytics for end-to-end visibility and control
- Foundational for a single vendor SASE
- Gartner Magic Quadrant Leader for both SD-WAN and Network Firewalls

A Secure SD-WAN, Powered by a Single OS, to Transform and Secure the WAN

As the use of business-critical, cloud-based applications continues to increase, organizations with a distributed infrastructure of remote offices and an expanding remote workforce need to adapt. The most effective solution is to switch from static, performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures.

Traditional WANs may utilize SLA-backed private multiprotocol label switching (MPLS) or leased line links to an organizations' main data centers for all application and security needs. But that comes at a premium price for connectivity. While a legacy hub-and-spoke architecture may provide centralized protection, it increases latency and slows down network performance to distributed cloud services for application access and compute. The result is operational complexity and limited visibility associated with multiple point products. This scenario adds significant management overhead and difficulties, especially when trying to troubleshoot and resolve issues.

Conterra's SD-WAN Solution is built on an organization's network infrastructure and security architecture, enabling networks to transform at scale without compromising security. This approach provides consistent security enforcement across flexible perimeters by combining a next-generation firewall with advanced SD-WAN networking capabilities. This combination paves the way to a Fortinet's Single-Vendor SASE approach, empowering organizations to consistently apply enterprise-grade security and superior user experience across all edges, converging networking and security across a unified operating system and agent. Furthermore, infrastructure networks are simplified by extending SD-WAN into wired and wireless access points of branch offices.

UPDATED JUNE 2024

Business Outcomes

Improved User Experience

An application-driven approach provides broad application steering with accurate granular identification, advanced WAN remediation, and accelerated cloud on-ramp for optimized network and application performance.

Accelerated Convergence

The industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables Secure Edge (FortiGate SD-WAN) and Thin Edge (FortiExtender Wireless WAN) to transition to their Single-Vendor SASE solution to secure all applications, users, and data anywhere.

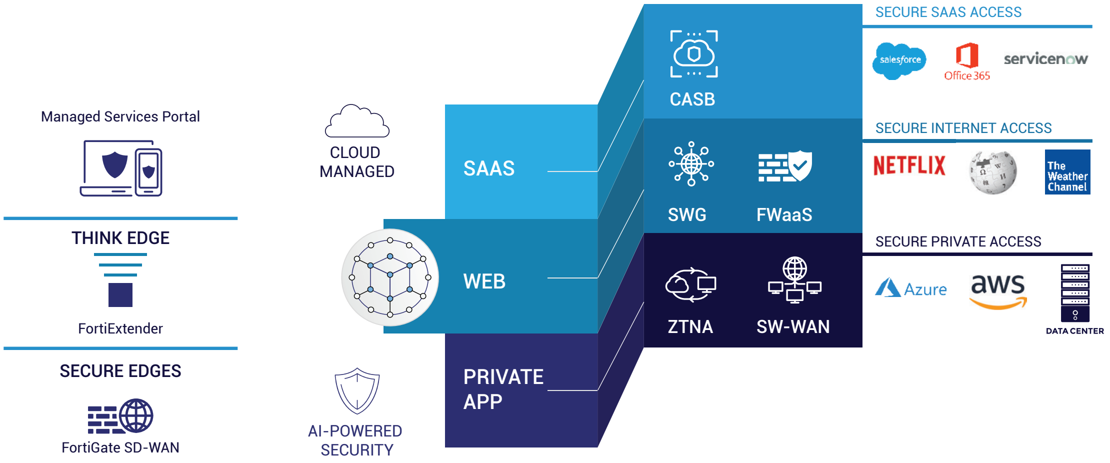
Efficient Operations

Simplify operations with centralized orchestration and enhanced analytics for SD-WAN, security, and SD-Branch at scale.

Secure SD-WAN Is Foundational for a Seamless Transition to SASE

Secure SD-WAN enables organizations to transition to a single-vendor SASE by extending secure access and high-performance connectivity to users regardless of their geographic locations. SASE delivers a full set of networking and security capabilities including secure web gateway (SWG), universal zero-trust network access (ZTNA), next generation dual-mode cloud access security broker (CASB), Firewall-as-a-Service (FWaaS), and secure SD-WAN integration. With a unified solution, you can:

- Overcome security gaps.
- Simplify operations and enhance security and networking analytics.
- Shift to an OPEX business model with simple user-based tiered licensing.



Core Components

Conterra has partnered with Fortinet to provide Secure SD-WAN which consists of the industry's only organically developed software complemented by an ASIC-accelerated platform to deliver the most comprehensive SD-WAN solution.

FortiGate

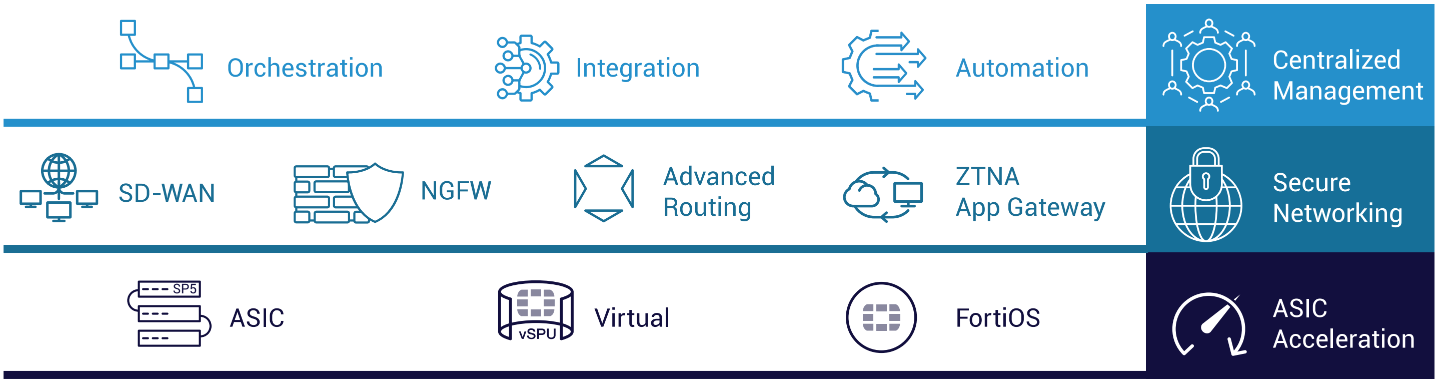
Provides a broad portfolio available in different forms, physical appliance and virtual appliances, with the industry's only ASIC acceleration using the SOC4 SPU or vSPU.

- Reduce cost and complexity with next generation firewall, SD-WAN, advanced routing, and a ZTNA application gateway on a unified platform that allows customers to eliminate multiple point products at the WAN edge
- ASIC acceleration of SD-WAN overlay tunnels, application identification, steering, remediation, and prioritization ensure the best user experience for business-critical, SaaS, and UCaaS applications

FortiOS

Fortinet's unified operating system delivers a security-driven strategy to secure and accelerate network and user experience. Continued innovation and enhancement enable:

- Real-time application optimization for a consistent and resilient application experience
- Advanced next generation firewall protection and prevention from internal and external threats while providing visibility across the entire attack surface
- Dynamic Cloud connectivity and security are enabled through effective cloud integration and automation



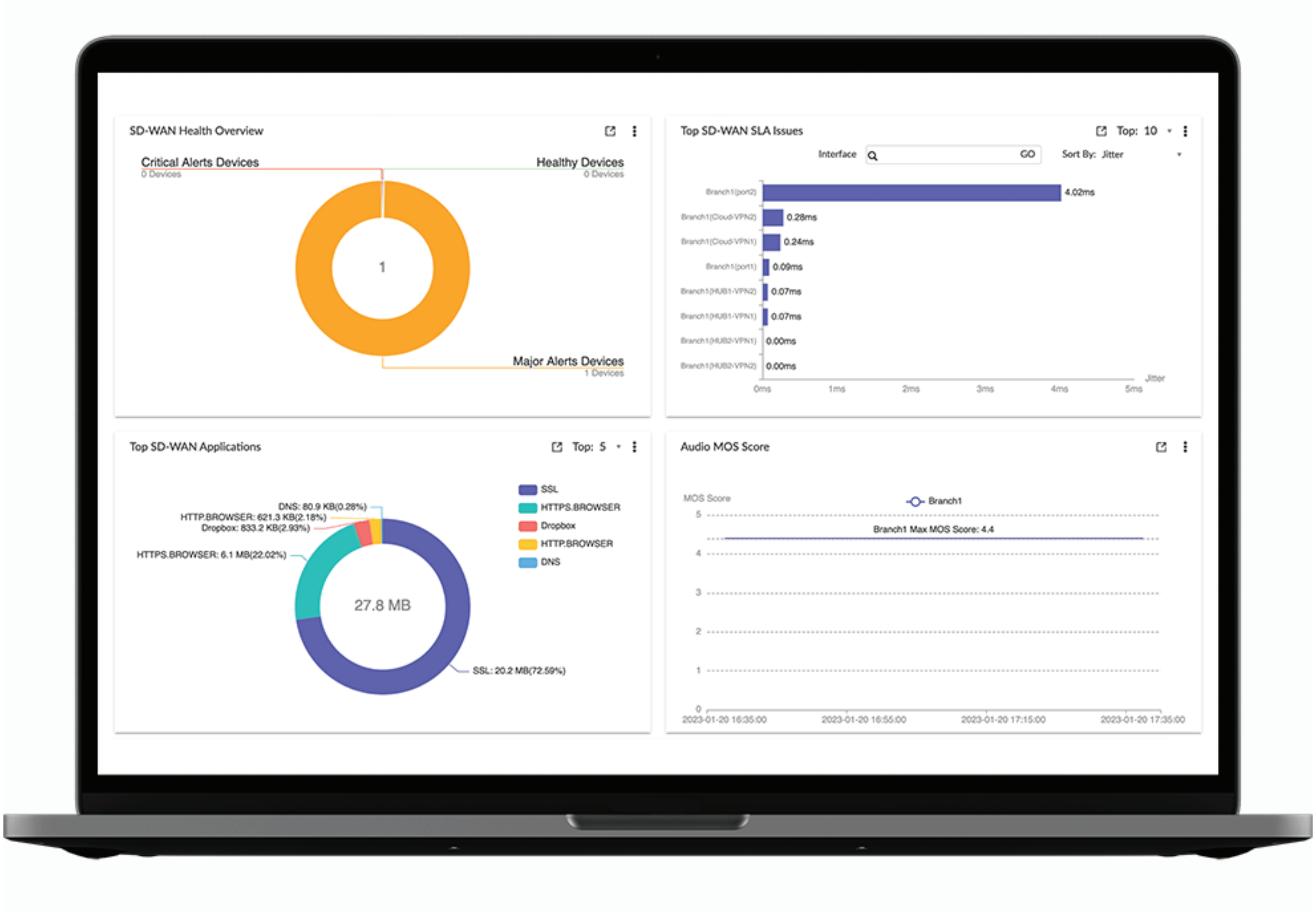
Orchestration
Integration
Automation
Centralized Management
SD-WAN
NGFW
Advanced Routing
ZTNA App Gateway
Secure Networking
ASIC
Virtual
FortiOS
ASIC Acceleration

Core Components

NOC Operations

Simplify centralized management, deployment, and automation to save time and respond quickly to business demands with end-to-end visibility. With a single-pane-of-glass management that offers deployment at scale, customers can:

- Centrally manage devices, including firewalls, switches, access points, and LTE/5G extenders from a single console
- Provision and monitor Secure SD-WAN at the application and network levels across branch offices, datacenters, and cloud
- Role-based access control to provide management flexibility and separation



Feature	Feature	Description
SD-WAN	Application Identification and Control	5000+ application signatures, first packet Identification, deep packet inspection, custom application signatures, SSL decryption, TLS1.3 with mandated ciphers, deep inspection
	SD-WAN (Application aware traffic control)	Granular application policies, application SLA based path selection, dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, application session-based steering, probe-based SLA measurements
	SD-WAN (Application aware traffic control)	Forward Error Correction (FEC) for packet loss compensation, packet duplication for best real-time application performance, Active Directory integration for user based SD-WAN steering policies, per packet link aggregation with packet distribution across aggregate members
	SD-WAN deployment	Flexible deployment – hub-to-spoke (partial mesh), spoke-to-spoke (full mesh), multi-WAN transport support
Networking	QoS	Traffic shaping based on bandwidth limits per application and WAN link, rate limits per application and WAN link, prioritize application traffic per WAN link, mark/remark DSCP bits for influencing traffic QoS on egress devices, application steering based on ToS marking
	Advanced Routing (IPv4/IPv6)	Static routing, Internal Gateway (iBGP, OSPF v2/v3 , RIP v2), External Gateway(eBGP), VRF, route redistribution, route leaking, BGP confederation, router reflectors, summarization and route-aggregation, route asymmetry
	VPN/Overlay	Site-to-site ADVPN – dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESP-HMAC support, symmetric cipher pre-shared (IKE/ESP): AES-128 and AES-256 modes: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication with RSA certificates, Diffie-Hellman key exchange (Group 1, 2, 5, 14 through 21 and 27 through 32), MD5, and SHA-based HMAC
	Multicast	Multicast forwarding, PIM spare (rfc 4601), dense mode (rfc 3973), PIM rendezvous point
	Advanced Networking	DHCP v4/v6, DNS, NAT – source, destination, static NAT, destination NAT, PAT, NAPT, Full IPv4/v6 support

Feature	Feature	Description
NOC Operations	Centralized Management and Provisioning	Managed Services Portal, centralized configuration, change management, dashboard, application policies, QoS, security policies, application-specific SLA, active probe configuration, RBAC, multi-tenant. Fabric Overlay Orchestrator capability built directly into FortiOS, allowing automatic connectivity between devices without FortiManager.
	Cloud Orchestration	Managed Services Portal, single sign-on portal to manage Fortinet NGFW and SD-WAN, Cloud-based network management to streamline FortiGate and management, extensive automation-enabled management of Fortinet devices
	Enhanced Analytics	Bandwidth consumption, SLA metrics (jitter, packet loss, and latency), real-time monitoring, filter based on time slot, WAN link SLA reports, per-application session usage
	Cloud On-ramp	Cloud integration – AWS, Azure, Alibaba, Oracle, Google. AWS transit, direct and VPC connectivity, transit gateways, Azure Virtual WAN connectivity, Oracle OCI connectivity
FortiGate	Redundancy/High-availability	FortiGate dual device HA – primary and backup, FortiManager HA, bypass interface, interface redundancy, redundant power supplies

Considerations for Branch and Hub Selection

Selecting the Branch or Hub devices depends on multiple factors that are unique to each deployment. Speak with a specialist for assistance selecting the right devices for your environment. Below are the most common selection criteria and some commonly selected Hub devices, based on deployment sizes (for reference purposes only).

Branch Selection

- Security requirements
- Number of users
- Throughput
- Interface connectivity
- Wireless requirements
- Redundancy (WAN, Power, IPsec Tunnels, Device)

Hub Selection

- Security requirements
- IPsec throughput
- Total IPsec Tunnels
- Interface connectivity
- Redundancy (Ports, Device, Power, Intra-site)
- AC or DC Power

Frequently Asked Questions

What level of visibility will I have into the SD-WAN network performance?

The Managed Services Portal, included with all Managed SD-WAN solutions, provides unparalleled visibility and control into your Conterra Managed SD-WAN solution. It is the central hub for real-time insights into network performance and SD-WAN routing.

How frequently can I make changes to the SD-WAN configurations and how long does it take for the requested changes to be implemented?

There are no limits on the quantity or frequency of changes to your SD-WAN environment. Users can make most changes within the Managed Services Portal and experience those in near-real time.

I don't see any Orchestration models or pricing, is that an additional cost?

Conterra centrally manages and monitors your SD-WAN devices at no additional cost. The Managed Services Portal allows for self-management of your SD-WAN infrastructure.

Are Connections to WAN Ports limited to one Provider?

Conterra Managed SD-WAN solution is designed to meet the needs of your business. The solution supports various Internet connections carrier agnostic.

Which interfaces can be utilized as WAN ports?

There is no restriction on how you use any of the interfaces. Physical models will traditionally have designated "WAN" ports but you may also utilize any of the available LAN or DMZ ports as a WAN interface.

Why is "Maximum IPSec Tunnels" omitted for Branches?

IPSec Phase1 interfaces have no hard limit and are only limited by system memory. Our tests have shown they support several hundred tunnels on even the smallest box, but that can vary based on many factors.

CONTERRA™
NETWORKS

Fiber Driven. People Powered.