

SD-WAN to Securely Connect Office or Branch Locations

Solution: Secure Access Services Edge (SASE) ■ **Industry:** Any vertical ■ **Use Case:** Securing Office and branch connectivity

Exium's Secure SD-WAN powered by CyberMesh delivers integrated networking and security as an agile cloud service, with traffic from remote (or edge) locations routed through local Cybernodes (CN) to connect users to the data and computing resources they need without having to backhaul traffic through a data center.

Digital transformation has ushered in a new era of long-lasting IT infrastructure changes. These changes have resulted in new challenges for the network and security teams, such as securing the distributed and hybrid workforce and delivering secure access to business-critical applications across a multicloud environment. In addition, the internet is rapidly becoming the preferred method of connectivity due to cost and availability. Still, it does not provide the security, consistency, visibility, or quality of traditional technologies such as Multiprotocol Label Switching (MPLS) links. IT needs to rearchitect its WAN edge to deliver consistent and predictable digital experiences in a multicloud world.

What is SD-WAN?

A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that allows enterprises to leverage any combination of transport services—including MPLS, broadband internet services, and LTE—to securely connect users to applications.

An SD-WAN uses a centralized control function to securely and intelligently direct traffic across the WAN and directly to trusted SaaS and IaaS providers. This increases application performance and delivers a high-quality user experience, which increases business productivity and agility and reduces IT costs.

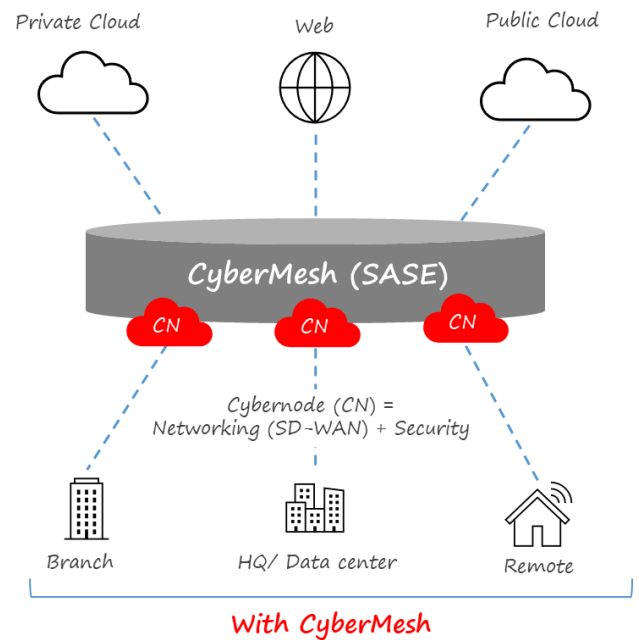
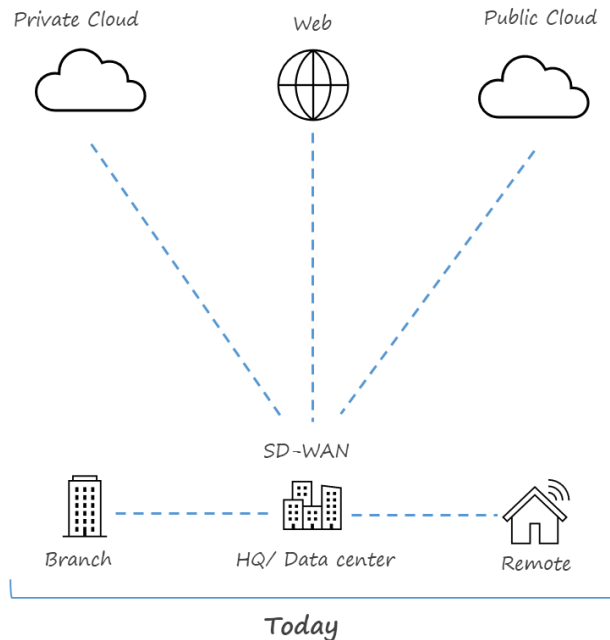
Why SD-WAN?

Times have changed, and enterprises are using the cloud and subscribing to software-as-a-service (SaaS). While users traditionally connected back to the corporate data center to access business applications, they are now better served by accessing many of those same applications in the cloud.

As a result, the traditional WAN is no longer suitable mainly because backhauling all traffic—including that destined to the cloud—from branch offices to the headquarters introduces latency and impairs application performance. SD-WAN provides WAN simplification, lower costs, bandwidth efficiency and a seamless on-ramp to the cloud with significant application

performance especially for critical applications without sacrificing security and data privacy. Better application performance improves business productivity, customer

satisfaction, and ultimately profitability. Consistent security reduces business risk.



SD-WAN architecture

Traditional WANs based on conventional routers were never designed for the cloud. They typically require backhauling all traffic, including cloud-directed traffic, from branch offices to a hub or headquarters data center where advanced security inspection services can be applied. The delay caused by backhaul impairs application performance resulting in a poor user experience and lost productivity.

Unlike the traditional router-centric WAN architecture, the SD-WAN model is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services such as Salesforce.com, Workday, Dropbox, Microsoft 365, and more, while delivering the highest levels of application performance.

How does SD-WAN work?

Unlike SD-WAN, the conventional router-centric model distributes the control function across all devices in the network and simply routes traffic based on TCP/IP addresses and ACLs. This traditional model is rigid, complex, inefficient, and not cloud-friendly and results in a poor user experience.



Exium Secure SD-WAN enables enterprises to securely support application growth, network agility, and simplified branch implementations while delivering high performance, reliable branch access to cloud services, private data centers, and SaaS-based enterprise applications.”

IT Director, Financial Services Provider

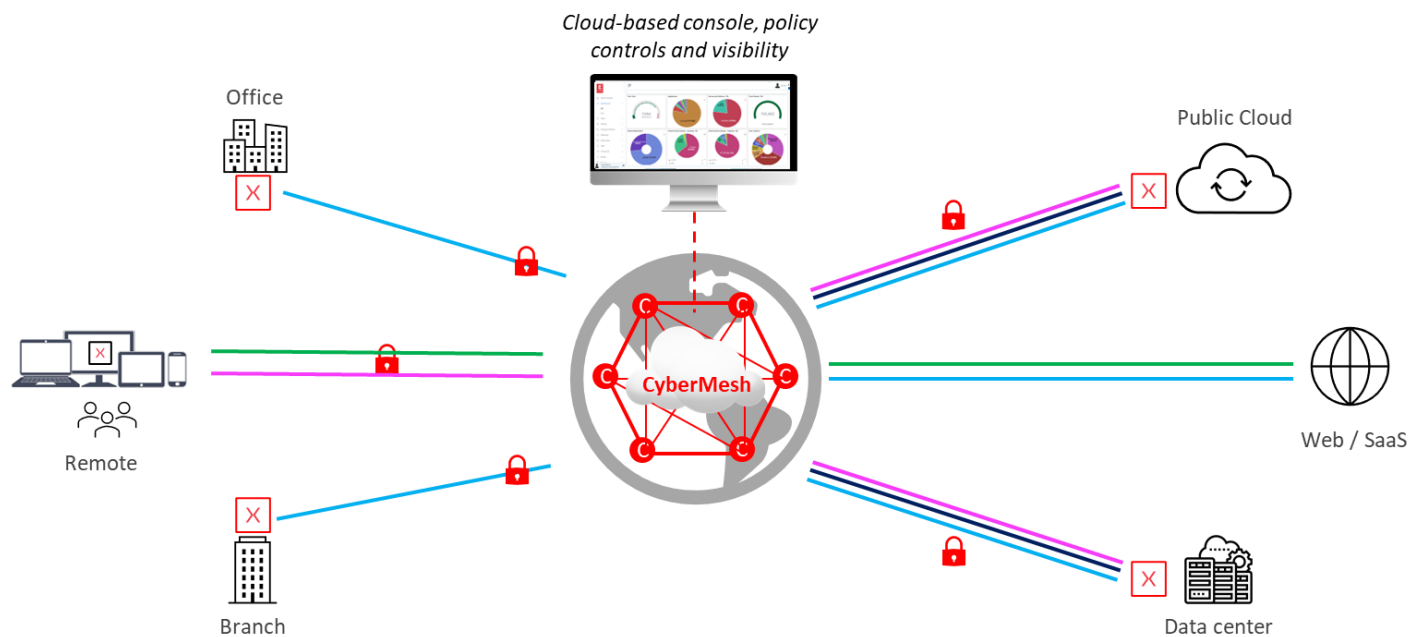
An SD-WAN enables cloud-first enterprises to deliver a superior application quality of experience (QoEx) for users. By identifying applications, an SD-WAN provides intelligent application-aware routing across the WAN. Each class of applications receives the appropriate QoS and security policy enforcement, all in accordance with business needs. Secure local internet breakout of IaaS

and SaaS application traffic from the branch provides the highest levels of cloud performance while protecting the enterprise from threats.

Exium Secure SD-WAN

Secure SD-WAN is a part of the Exium secure access service edge (SASE) platform, which offers converged cloud networking and security services to achieve flexibility, agility, and scale for enterprises of all sizes. As

a cloud-delivered solution, Exium SD-WAN ensures resilient WAN connectivity and allows users to have flexible WAN choices, such as broadband, MPLS, and LTE. Exium SD-WAN offers high application performance and availability while lowering networking costs. It can detect the slightest degradations and dynamically remediate over one or multiple WAN links, resulting in a highly satisfied user experience.



Secure SD-WAN solves network complexity while cutting total cost of ownership. Unlike legacy SD-WAN solutions, Secure SD-WAN combines additional security features for extended protection within a single offering.

Secure SD-WAN connects remote sites to an organization's private network using Exium's CyberMesh. This assures complete site protection from external threats by inspecting and securing all inbound and outbound traffic from the internet, as well as cross-traffic within the site itself.

Deploying Secure SD-WAN can be done quite easily by running Exium's Cyber Gateway (CGW) connector software on your choice of hardware and connecting it to the CyberMesh platform using one or more last mile connections. Flexible hardware support makes deployment and management easy, while enabling organizations to use their existing hardware.

Once deployed, Secure SD-WAN delivers exceptional performance and high availability capabilities, such as active-active link aggregation, and dynamic path selection to overcome network outages or brownouts. Additionally, Secure SD-WAN includes advanced performance features, such as application prioritization and local breakout to ensure superlative quality of experience for end users.

With Secure SD-WAN, remote sites enjoy all the benefits of full-stack, enterprise-grade security without the hassle of having to deploy and manage an array of multi-vendor security appliances at every location. All traffic to and from remote sites gets the benefits of Exium's Defense in Depth security stack, which includes next-generation firewall, secure web gateway, intrusion prevention, anti-malware, and more.

Exium Secure SD-WAN Benefits

Secure SD-WAN offers integrated security, including full-stack multilayer defense-in-depth security capabilities on the premises and in the cloud. This integrated security provides real-time threat protection where and when it is needed — for branches connecting to multiple Software-as-a-Service (SaaS) or IaaS clouds, data centers, or the internet, further accelerating the transition to a SASE-enabled architecture.

Businesses are rapidly adopting SD-WAN technology because of its comprehensive financial and operational benefits.

Lowers WAN OpEx, CapEx, and overall total cost of ownership.

Provides greater business agility and responsiveness to keep pace with IT innovations.

Supports multiple, secure, high-performance connections, eliminating backhaul penalties imposed by MPLS networks.

Improves performance by enabling load sharing across connections and adjusting traffic flows based on network conditions.

Supports the automated provisioning of, and changes to, premium network services such as VPNs, firewalls, security, WAN optimization, and application delivery control.

Supports zero touch provisioning (ZTP).

Improves network security by encrypting WAN traffic and segmenting the network to minimize damage if breaches occur.

Managing the WAN traditionally has been one of the most expensive and rigid aspects of running an enterprise network. SD-WAN eases this burden by proactively responding to real-time network conditions. It uses programmable network devices that you can modify remotely and through dynamic best-path routing, both of which improve cost, agility, and performance.



“As we adapt our network towards hybrid work and cloud migration, the Exium Secure SD-WAN Platform check all the boxes for an agile SD-WAN solution that can deliver the performance, security, and visibility needed to deliver these real-time connected experiences.”

IT Technical Manager, Healthcare provider

Secure SD-WAN Cloud OnRamp for Multicloud

Businesses are using not just one cloud data center in their IT operations, but several clouds across IaaS, SaaS, and Platform as a Service (PaaS). Connecting these workloads and applications together with the WAN and remote users is a challenge.

To help reduce this complexity, Secure SDWAN provides the ability to connect any WAN location to multiple cloud platforms or any other enterprise site, increasing connection speeds and enhancing connection reliability. Secure SD-WAN Cloud OnRamp creates a WAN extension for your IaaS workloads, provides dynamic path selection for optimal SaaS application performance, consolidates branch office egress points into regional colocation facilities, and automates cloud-agnostic branch connectivity with cloud interconnect.

Monitoring underlay performance via the Secure SD-WAN dashboard, Cloud OnRamp automatically selects the fastest, most reliable path to the cloud infrastructure, no matter where your end users are located. In the event

of network service interruptions beyond your control, Cloud OnRamp will adjust paths as necessary, helping ensure continuous uptime and predictable performance.

Secure SD-WAN makes connecting the company WAN to IaaS environments such as AWS, Google Cloud, and

Microsoft Azure simple, automated, and secure — as though the cloud databases themselves are part of the corporate network. Secure SD-WAN applies automated connectivity requirements (loss, latency, and jitter) to find the optimal path to cloud IaaS applications, adjusting the IPsec route as needed to help ensure service delivery and performance while monitoring the hosting infrastructure for anomalies.



The continued proliferation of advanced threats such as ransomware is a disruptive problem for organizations of all sizes. We were looking for a solution where security is built in, not bolted on. The Exium SASE solution is really attractive as it provides the most advanced identity-based access with tightly integrated networking to deliver the greatest performance and security while also improving operational efficiency and lowering costs.”

Director of IT Security Architecture, Fortune 500 Company in the Retail Industry

Analytics and insights

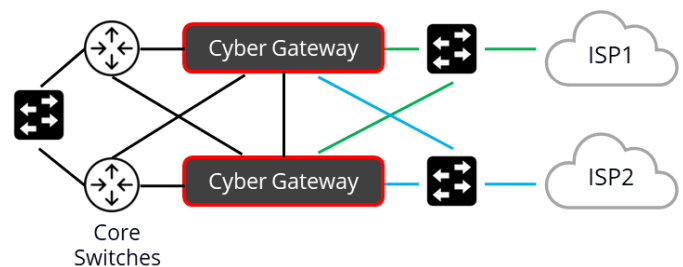
Applications and users are more distributed than ever, and the internet has become the new enterprise WAN. As SD-WAN has evolved to connect users across multicloud, branch, data centers, and a hybrid workforce, enterprises and organizations are constantly challenged to deliver reliable connectivity, application experience, and security over networks and services they don't own or directly control.

Enterprises and organizations need a network analytics solution that provides enhanced visibility and insights to help them take control over such a dynamic environment.

Advances in telemetry and algorithms have transformed network analytics by offering enhanced visibility and improvement in operational efficiency. Exium Secure SD-WAN Analytics solution aggregates a large volume of telemetry data and correlates analytics to provide insights. A highly visualized and intuitive user interface addresses the traditional challenges associated with network analytics for an improved user experience. By aggregating large volumes of telemetry data, establishing historical benchmarks, and correlating analytics to provide actionable insights across the internet, cloud, and SaaS, Secure SD-WAN Analytics transforms network operations from a reactive model to a highly proactive one.

High-Availability (HA)

Secure SD-WAN high-availability allows subsecond failure when an appliance is offline, which allows hitless upgrades. The cyber gateways negotiate the active and standby roles. State information, heartbeat, and surrounding status (for example, WAN and LAN port status) is communicated across the failover link. The same MAC addresses are used on both platforms, enabling the subsecond failover, similar in concept to any first-hop redundancy protocols.



To achieve subsecond failure, both of the next-hop virtual IP addresses (VIPs) on the switches stay the same when a failover event occurs.

Your Needs	Secure SD-WAN Solution
Maximum choice and control	Offers flexibility with a cloud-first architecture to connect any user to any application, across any cloud.
Full SD-WAN feature stack	Provides sophisticated control of the network with a set of features for routing, multicloud, security, and centralized policy control and management.
Multicloud choice and control	Enables a range of optimizations for multicloud applications using the CyberMesh Cloud OnRamp architecture. It optimizes major Software-as-a-Service (SaaS) applications and workflow integrations to major public clouds and colocation providers.
Security that is built in, not bolted on	Enables centralized security policies and provides segmentation across the entire network and a full security stack, either on-premises or in the CyberMesh cloud.
Network services	IPv4, IPv6, DNS, DHCP client, DHCP server, NAT
Dynamic Multipath Optimization	Application and network condition aware sub-second steering, fast intelligent routing, intelligent gateway selection, link aggregation, TCP flow optimization
Forwarding and Quality of Service (QoS)	Classification, prioritization, low latency queuing, remarking, shaping, scheduling, policing, mirroring, NAT/Port Address Translation (PAT)
VLAN tagging	802.1Q, 802.1ad, QinQ (0x8100), QinQ (0x9100), native
WAN overlay support	Public/private/hybrid transport, cloud and on-premises
Routing	OSPF, BGP, static, connected, ICMP probes/responders, overlay flow control, per-packet application aware steering, route filter, route redistribution
Robust IP multicast support	Enables network traffic control, enhances efficiency by eliminating traffic redundancy, and reduces server and CPU load, Internet Group Management Protocol (IGMP) v1/v2/v3 support
Visibility and analytics	Provides granular visibility into applications and infrastructure, enabling rapid failure correlation and mitigation.

Ready to secure Hybrid work, office and branch connectivity?

[Test Drive Here](#)