Cisco SD-WAN Security

At a glance
Public

Cisco protects users, connected devices, and application usage and all traffic across the WAN.

Software-Defined WAN (SD-WAN) is a major step forward in your digital transformation and with it, you can scale your business faster to meet the demands of a rapidly changing market. To help with the ever-increasing adoption of multicloud environments, SD-WAN offers total transport flexibility to connect directly with the cloud using the Internet. Its corresponding network efficiency makes for a better user experience and reduced cost for organizations. Unfortunately, re-architecting the enterprise WAN and branch networks into SD-WAN creates exposure to threats and additional security complexity.

To secure this newly architected environment, customers must use additional physical security devices or third-party security services for their branch connectivity. If your business connects directly to the Internet, or soon will, you need the Cisco® SD-WAN security stack for protection from the branch to cloud edge.

Mitigate all security risks

>90% of SD-WAN vendors are not traditional security vendors

- **Inside-out**
  - Malware infections
  - Command and control
  - Phishing attacks
  - Unacceptable use

- **Internal**
  - Unauthenticated access
  - Lateral movement
  - Compliance violations

- **Outside-in***
  - Unauthorized access
denial-of-service attacks

* Where onsite services or devices are remotely accessible

---

**Edge security devices or services**

Refresh and add layers to the security stack that protects existing Direct Internet Access (DIA) breakouts for some (guest) or all users and some (O365) or all apps.

**Pro:** Improved user experience.

**Con:** Edge management complexity, costly, limited control, and lack of advanced security.

**Cisco SD-WAN security**

Transform the branch with new DIA breakouts at tens to thousands of locations for better security, performance, simplicity, and cost savings.

© 2019 Cisco and/or its affiliates. All rights reserved.
How do I get started?

1. For any WAN topology, Cisco Umbrella™ offers a secure Internet gateway, which improves security at the cloud edge and protects users everywhere.
   - **Learn:** [www.cisco.com/go/umbrella](http://www.cisco.com/go/umbrella)
   - **Try:** [signup.umbrella.com](http://signup.umbrella.com)

2. For lean IT teams wanting a single edge device to secure the branch edge and SD-WAN fabric, Cisco Meraki™ MX is the simplest way.
   - **Learn:** [cs.co/MX-fw-sdwan](http://cs.co/MX-fw-sdwan)
   - **Demo/try:** [cs.co/MX-demo](http://cs.co/MX-demo)

3. For network teams wanting to maximize agility for complex WAN topologies, Cisco SD-WAN is the most flexible.
   - **Learn:** [www.cisco.com/go/sdwan](http://www.cisco.com/go/sdwan)

4. For security teams that want the industry-leading simplicity for multi-factor authentication, deploy Cisco Duo’s core components through a single, extensible platform you enable for adaptive and risk-based application access policies.
   - **Learn:** [duo.com](http://duo.com)
   - **Try:** [demo.duo.com](http://demo.duo.com)

Cisco’s open, integrated SD-WAN security architecture

- **Secure Internet gateway**
  - Secure access to the Internet and multicloud applications with threat protection over all ports
- **Full-stack edge security**
  - Embedded enterprise firewall, intrusion prevention, and URL filtering capabilities for a comprehensive branch edge security
- **SD-WAN**
  - Secure elastic connectivity and agile operations for and by the cloud with application performance assurance
- **Unified access security**
  - Give anytime, anywhere access to all applications based on the trustworthiness of users and devices

Cisco’s solution enables secure branch transformation from the branch to cloud edge without gaps.
Transformative

Cloud-delivered security
Effectively learn, adapt, and protect against where attacks are being staged

Intent-based networking
Constantly learn, adapt, and protect against application performance issues

Advanced analytics
Gain business and IT insights with application QoE models and threat intelligence

Flexible

Full edge security stack
Policy-based, layer 3 to 7 protection from the outside-in, inside-out, and internally

Edge device flexibility
Thin, rich, or full-stack router and firewall options to match onsite IT demands and existing deployments

Open architecture
API to programmable command-line interface for northbound automation and southbound integration

Simple

Software-as-a-Service (SaaS) management
Lower operating expenses by enforcing security and networking at the branch or cloud edge

Zero-touch provisioning
Automate Cloud onRamp for Infrastructure-as-a-Service (IaaS) and SaaS apps

Transport independence
Enable business policy to follow workloads using DIA or a secure VPN overlay

Unlike multivendor solutions, Cisco has the shortest time to threat detection in the industry via Cisco Talos™ threat intelligence. Cisco’s protection constantly learns and adapts with Cisco Umbrella statistical and machine learning models as well as Advanced Malware Protection file reputation and dynamic analysis.

Unlike startups with a handful of good case studies, Cisco built the fastest, most reliable and trustworthy infrastructure used by over 90 million users daily. Cisco’s secure Internet gateway assures 100% business uptime, while Cisco’s SD-WAN assures zero outages for any application.