



SD-WAN Security

Right security, right place

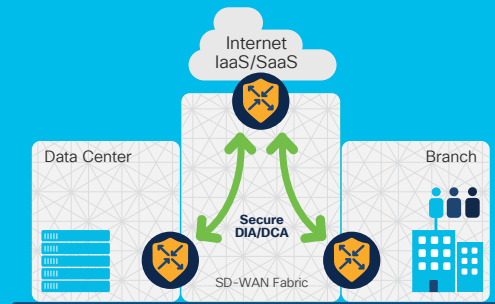
Protect users, connected devices, and all traffic across the WAN

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. The network efficiency that comes with SD-WAN creates a better user application experience and reduces cost for organizations. Unfortunately, all these benefits have a tradeoff – rearchitecting the enterprise WAN and branch networks into SD-WAN creates exposure to threats and additional security complexity.

How do you protect your newly implemented SD-WAN against internal and external threats? If you plan to deploy additional security devices or services on-premises, in the cloud, or both, could you scale easily for future traffic growth? How do you reduce the complexity of deploying and managing security solutions from multiple vendors? How about your visibility into traffic to or across branches and data centers?

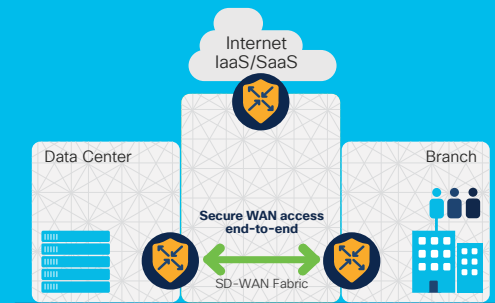
Cisco® SD-WAN offer engineering leadership in both networking and security to include full-stack multilayer security capabilities on the platform and in the cloud. Its integrated on-premises and cloud security arms IT with advanced threat defense wherever it is needed – for branches connecting to multiple SaaS or IaaS clouds, to data centers, or everything on the internet.

Built-in Full Edge Security Stack



Cloud Security

Integrated connectivity and cloud-delivered security provides secure access to the internet and SaaS applications and scales for future traffic growth.



On-Premises Security

Embedded enterprise firewall and intrusion prevention in addition to URL filtering and malware sandboxing provide secure WAN access and meet compliance demands onsite.

Security benefits of Cisco SD-WAN

- Constant protection against all internal and external threats from branches to IaaS
- Improved user experience via secure direct internet and cloud access
- Centralized visibility and control for all internal, inbound and outbound traffic
- Reduced cost and complexity using a single product for networking, security, and cloud

Learn more

To learn more, please visit [cisco.com/go/sdwan-security](https://www.cisco.com/go/sdwan-security) or contact your account representative.

Cisco's open, integrated SD-WAN security architecture

Cisco SD-WAN offers an integrated on-premises and cloud security solution spanning four security categories: network segmentation, enterprise firewall, secure web gateway, and DNS-layer security. Each security category itself spans a different combination of security features. These security features are:

IPsec encryption: An underlying WAN fabric for securing on-premises WAN access and direct internet access

IPS: A built-in intrusion prevention system within an on-premises enterprise firewall based on Snort® and powered by Talos®

App controls: A built-in security practice within every part of the security stack, able to control 1400+ apps using on-premises enterprise firewall

Malware protection: An extended security feature across both on-premises and cloud security using Cisco AMP and Threat Grid to prevent/detect malicious files with sandboxing

SSL/TLS decryption: A security feature with unlimited scale for either cloud security or on-premises security with sufficient resources

URL filtering: An extended security feature across both on-premises and cloud platforms with 80+ web categories covering millions of domains and billions of web pages

Key SD-WAN security use cases

Secure direct internet access

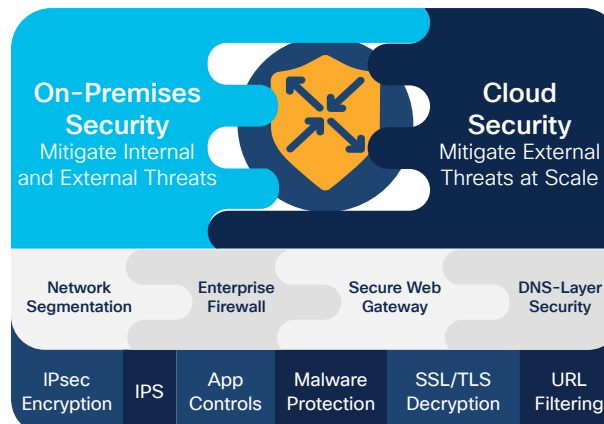
Cisco SD-WAN provides centralized control of the flow of internet-bound traffic using built-in security features. The integrated security solutions provide the best balance of security and user experience for direct internet access.

Secure end-to-end segmentation, at scale

In addition to extending branch segmentation into the data center and the cloud, Cisco SD-WAN protects users and devices within a specific segment from any internal and external threats. With Cisco SD-WAN you are able to manage segmentation policies across the entire network from a single pane of glass and to adapt automatically to any network's changes.

Enforce regulatory compliance

Cisco SD-WAN addresses compliance in a holistic way by offering a comprehensive set of security controls.



Components	Security controls
Control plane	Zero trust security model
Data plane	Integrated on-premises and cloud security layers
Management plane	Role-based access control and ACLs
Platform	Trustworthy hardware, software, and solution