The bridge to possible

SD-WAN Security

Right security, right place

Protect enterprises and evolve to a SASE architecture

SD-WAN offers total transport flexibility and efficient access to cloud applications in Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) multicloud environments. While the resulting efficiency creates a better user application experience and reduces the cost for organizations, the solution must also address increasingly sophisticated security threats and offer protection against network vulnerabilities.

How do you enable security with SD-WAN and protect your network from 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? And most importantly, how do you evolve to a Secure Access Service Edge (SASE) architecture?

Cisco® SD-WAN offers engineering leadership in both networking and security, including full-stack multilayer security capabilities on the premises and in the cloud. The integrated security arms IT with advanced threat defense where and when it is needed — for branches connecting to multiple SaaS or IaaS clouds, to data centers, or to everything on the internet — and accelerates the transition to a SASE architecture in a secure and agile manner.

Security benefits of Cisco SD-WAN

- Constant protection against all internal and external threats, from branches to SaaS
- Improved user experience via secure direct internet and cloud access
- Increased overall network efficiency and reliability with micro-segmentation and identity-based policy management
- Centralized visibility and control for all internal, inbound, and outbound traffic
- Reduced cost and complexity using a single product for networking, security, and cloud.

The bridge to possible

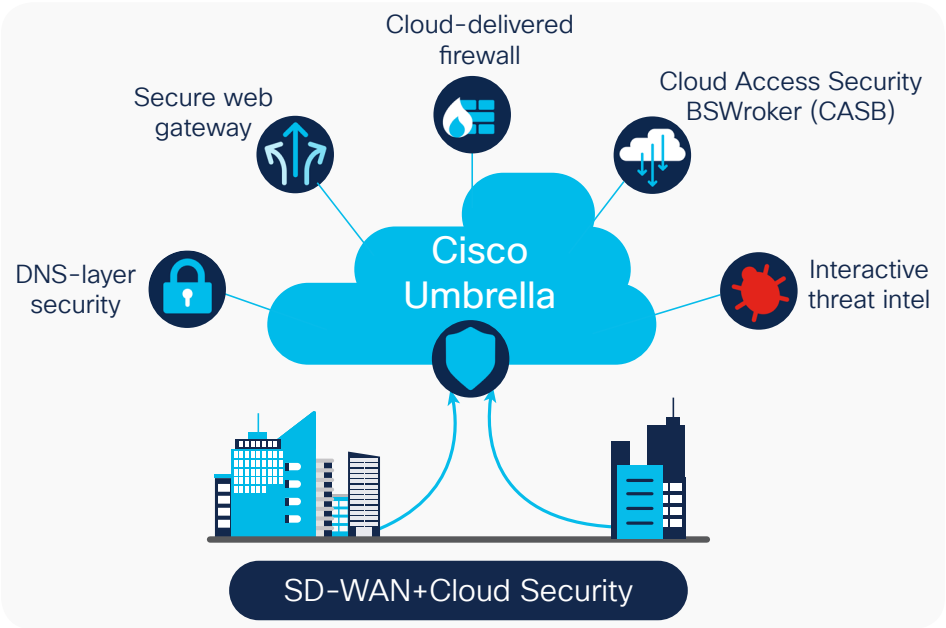
Built-in full edge security stack

Cisco SD-WAN offers a full security stack for protection against web attacks.

Cloud security and SASE

Cisco SD-WAN is fully integrated with cloud-delivered Cisco Umbrella®, which offers protection against security blind spots and cyberthreats. Powered by the Umbrella global network and Cisco Talos® threat intelligence, it's the easiest way to deliver protection to users anywhere they access the internet and cloud apps.

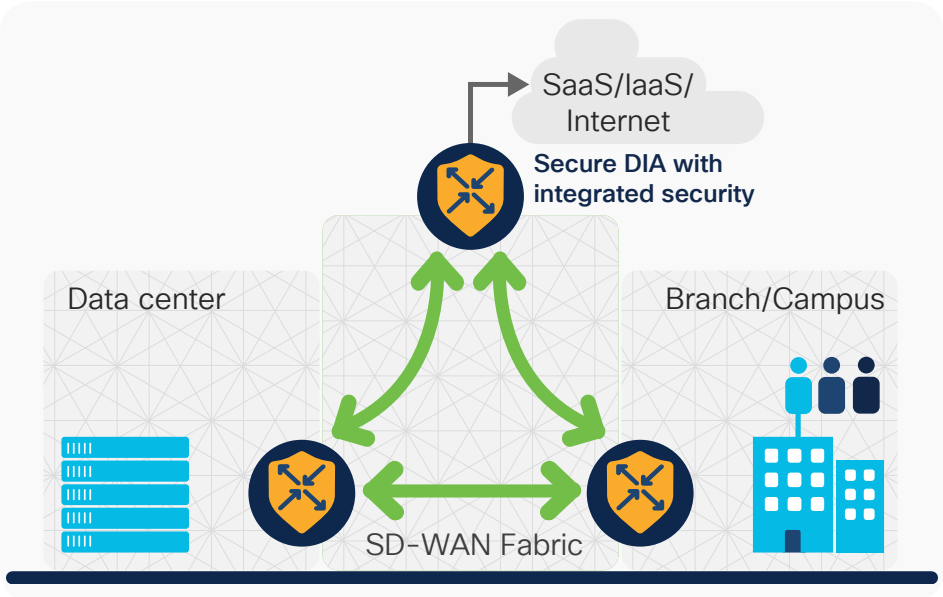
Figure 1. Cloud security and SASE



On-premises security

Cisco SD-WAN offers embedded SSL decryption, enterprise firewall, intrusion prevention, URL filtering, and malware sandboxing. Together, these capabilities provide secure WAN access and help users meet compliance demands onsite while offering constant protection against internal and external threats from a range of sources.

Figure 2. On-premises security



The bridge to possible

Firmware security in SD-WAN

Over the past few years, firmware attacks on infrastructure have proliferated, increasing by 500% and costing businesses an average of $8MM per breach. Only Cisco SD-WAN builds edge platforms and routers with advanced Trust Anchor capabilities to defend against firmware attacks.

The latest Cisco Trust Anchor provides the most advanced firmware defence via:

Embedded security: Hardware-anchored root of trust and Secure Boot are combined into a single security chip embedded onto the device console, protecting firmware from exploits

Enhanced visibility: Customers are able to see and verify their device integrity while managing their Public Key Infrastructure (PKI) and certificates

Self-healing: Cisco SD-WAN edge platforms and routers are flexible and able to upgrade their firmware and crypto capabilities in case of corruption or attack. In the event of a vulnerability or exploit, Cisco SD-WAN devices can self-heal and are not rendered inoperative

[1] Catalyst 8000 Edge Platforms Family

Cisco's open, integrated secure SD-WAN and SASE architecture

Cisco SD-WAN offers a full range of integrated security functionality that can be enabled on-premises and using the cloud-delivered Cisco Umbrella. The full stack multilayer security consists of four major security categories: micro-segmentation, enterprise firewall, secure web gateway, and DNS-layer security. Each security category itself spans a different combination of security features. These features and capabilities are:

Micro-segmentation: Secure isolation of different portions of the enterprise at a granular level to protect critical assets

Identity-based policy management: Enforcement of a common set of access control policies uniformly across campus and branches

Enterprise firewalls: Granular policy and control of thousands of applications

Secure web gateway: Full protection against all kinds of web-based attacks, including SSL inspection

DNS layer security: Significant reduction in incidents by stopping threats at the earliest point

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

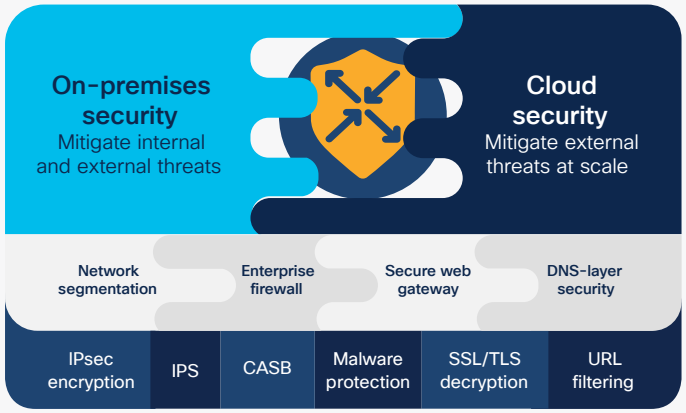
Cloud Access Security Broker (CASB): Protection against account compromises, breaches, and other major risks in the cloud app ecosystem

Malware protection: An extended security feature across both on-premises and cloud security using Cisco AMP and Threat Grid to prevent and 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

Figure 3. SD-WAN security features



The bridge to possible

Learn more

To learn more, please visit cisco.com/go/sdwan-security or contact your account representative.

C45-743155-03 03/21

Key SD-WAN security use cases

Secure direct internet access

Cisco SD-WAN security delivers full protection and control against all major web attacks arising from SaaS and internet access. The integrated security solutions provide the best balance of security and user experience for direct internet access.

End-to-end micro-segmentation and identity-based policy management, at scale

Cisco SD-WAN enables you to extend micro-segmentation and identity-based policy management across Cisco Software-Defined Access (SD-Access) and non-SD-Access branches, driving consistent multidomain policy enforcement, all from a single pane of glass.

Branch security

Cisco SD-WAN provides constant protection against all cyber threats, from branches to multicloud SaaS environments. It also meets comprehensive data compliance requirements in every major vertical, including highly regulated industries such as financial services, healthcare, utilities, and government.

Enforce regulatory compliance

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

Table 1. 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