The bridge to possible

SD-WAN Security

Right security, right place

Security benefits of Catalyst 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 microsegmentation 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.
- User identity verification, visibility into every device, and adaptive policy enforcement with a zero-trust approach.
- Support for third-party integration with widely popular cloud security vendors for choice of networking and security solutions.

Protect enterprises and evolve to a SASE architecture

As businesses evolve to meet changing demands, many have shifted to hybrid work environments, distributed workforces, and increased cloud adoption. While these changes have enabled greater flexibility and efficiency, they have also introduced new security challenges. With the rise of increasingly sophisticated threats, businesses need robust security solutions to ensure that their networks are secure from potential threats.

Cisco Catalyst™ SD-WAN offers a comprehensive security approach that addresses these challenges, enabling you to provide reliable and secure access, enforce consistent security policies, minimize costs, and improve business agility.

Catalyst SD-WAN's secure architecture has evolved to meet these changing security paradigms by providing a scalable and secure solution that can protect your network from anywhere. Catalyst 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 Software-as-a-Service (SaaS) or Infrastructure-as-a-Service (IaaS) clouds, to data centers, or to everything on the internet – and accelerates the transition to a Secure Access Service Edge (SASE) architecture in a secure and agile manner.

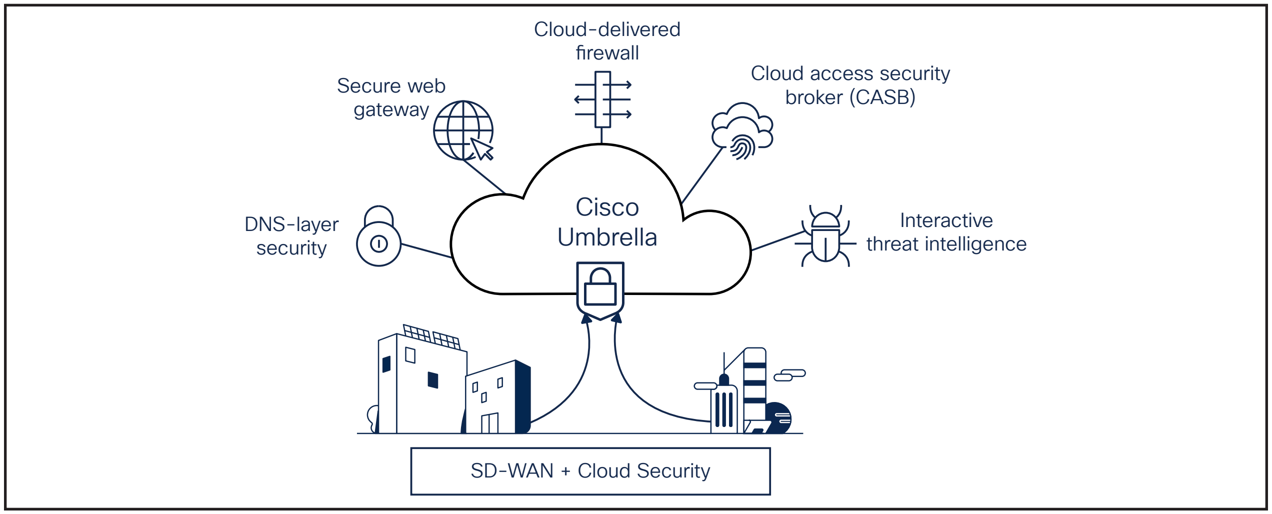

Figure 1. Cloud security and SASE

Built-in full edge security stack

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

Cloud security and SASE

Catalyst 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.

On-premises security

Catalyst 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 data compliance requirements onsite while offering constant protection against internal and external threats from a range of sources.

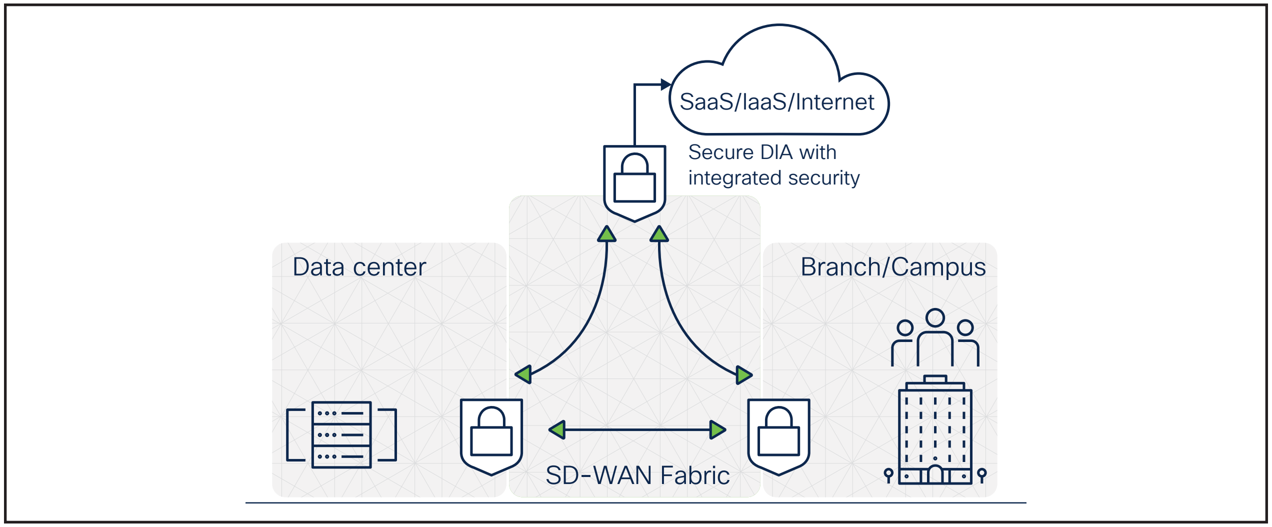

Figure 2. On-premises security

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

Catalyst 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: microsegmentation, enterprise firewall, secure web gateway, and DNS-layer security. Each security category spans a different combination of security features. These features and capabilities are:

Microsegmentation: 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 firewall: Granular policy and control of thousands of applications.

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 $8 million per breach. Only Catalyst 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 defense 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: See and verify your device integrity while managing your Public Key Infrastructure (PKI) and certificates.

Self-healing: Catalyst 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, Catalyst SD-WAN devices can self-heal and are not rendered inoperative.

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 Secure Malware Analytics 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: Extended security across both on-premises and cloud platforms with 80+ web categories covering millions of domains and billions of web pages.

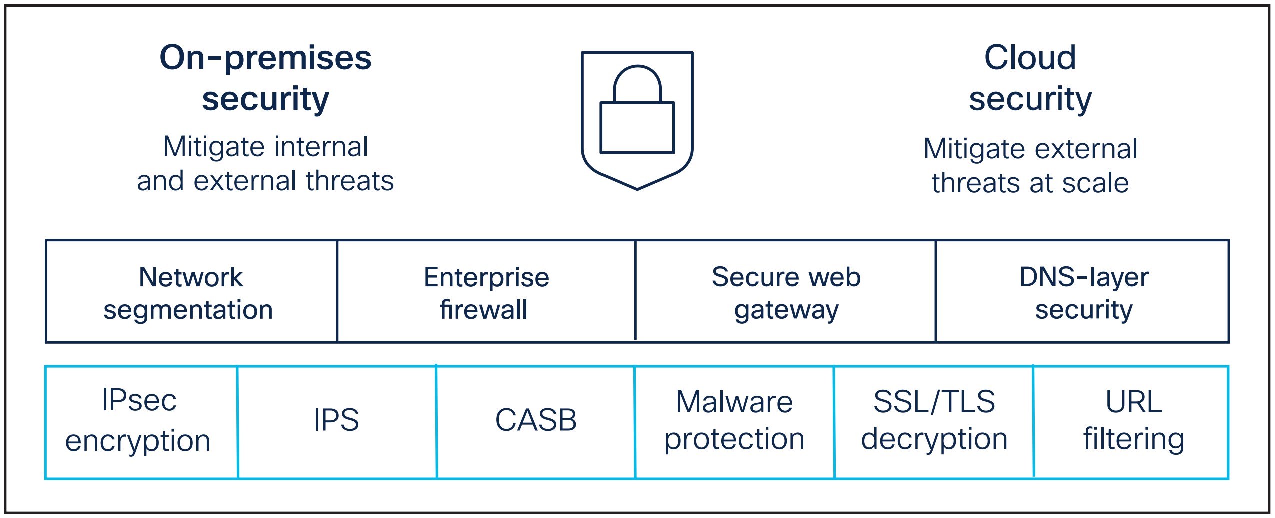

Figure 3. SD-WAN security features

Key SD-WAN security use cases

Secure direct internet access

Catalyst 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 microsegmentation and identity-based policy management, at scale

Catalyst SD-WAN enables you to extend microsegmentation 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

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

Enforce regulatory compliance

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

Cisco SASE- Catalyst SD-WAN integration with Cisco's SSE solution- Cisco Secure Access

As organizations leverage their existing SD-WAN, they may encounter advanced security needs driven by the challenges of today's diverse IT landscape. This can lead them towards a Secure Access Service Edge (SASE) environment, combining their SD-WAN with consolidated, cloud-delivered security (SSE).

Cisco Catalyst SD-WAN facilitates this transition by seamlessly integrating with the SSE solution - Cisco Secure Access. This game-changing integration empowers IT administrators with an automated solution, delivering not only highly resilient cloud security but also an optimal experience for end-users.

Branch offices and roaming users face heightened vulnerability to cyber threats, especially with the growing adoption of Direct Internet Access (DIA). The seamless integration of Cisco Catalyst SD-WAN and Cisco Secure Access within a SASE architecture effectively addresses these concerns by effortlessly extending robust cloud security measures across the entire SD-WAN fabric.

Take advantage of Catalyst SD-WAN and Cisco Secure Access integration to achieve:

- **Enhanced Security with SASE:** Elevate internet and SaaS traffic protection at branch offices with Cisco Secure Access (SSE). Easily steer traffic for additional security.
- **Faster Deployment:** Automatically connect Cisco Secure Access and Catalyst SD-WAN manager through Smart Accounts, enabling effortless deployment across your entire network. This significantly reduces branch office setup time.
- **Simplified Management:** Manage connectivity and provision thousands of sites to Cisco Secure Access in minutes, with just a few clicks from a single, centralized dashboard.

Learn more

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

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 Access Control Lists (ACLs)
Platform	Trustworthy hardware, software, and solution