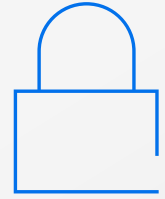# Cloud Security with Cisco+ Secure Connect

Users and applications have moved off premises. So have threats.

Cloud-based architectures allow organizations to become more flexible, efficient and adaptable when business needs change. They also pose new security challenges as more sensitive data migrates from the safety of on-site servers to third-party resources accessed through the internet.

Spectrum Business® Cloud Security with Cisco+ Secure Connect offers a centralized, streamlined platform to implement your security priorities across every cloud and device. Capabilities that include zero trust network access (ZTNA) and a cloud-based firewall allow IT to enforce security measures and device postures for corporate and personal devices. Cloud Security eliminates the need to backhaul remote and branch traffic through the corporate LAN to apply security policies. Simplify cybersecurity without compromising performance using a cloud access security broker (CASB) that gives users secure, direct access to cloud applications. A single portal provides IT teams with immediate visibility across users, network activity, devices and potential threats that include malicious IPs, phishing and malware. Cloud Security simplifies IT operations while strengthening protection against data loss and regulatory violations in an increasingly complex hybrid cloud environment.

Product highlights

- **Secure web gateway (SWG):** Help stop malware and advanced threats with a cloud-based proxy that enforces acceptable use policies.
- **CASB:** Expose shadow IT by detecting all cloud applications in use across your organization. Improve rollout of cloud adoption and reduce risk with visibility into vendors and activity volume.
- **ZTNA:** Establish zero-trust access to clouds and networks based on authorized network, end-user location, group or device security health.[1]
- **Cloud firewall:** Log all user activity and block unwanted traffic using IP, port and protocol rules applied across any network device.
- **DNS-layer security:** Categorize and block traffic to malicious systems and stop threats before they are accessed by customers or employees.

Benefits

- **Identity management:** Authenticate users connecting to a network or cloud application and ensure they only access what they need.
- **Unified management and visibility:** Control access for all users — including those with unmanaged personal devices — and monitor their usage for security risks.
- **Better performance:** Give users direct access to cloud applications without compromising security, on-site or remotely.
- **Work-anywhere support:** Easily apply and manage firewall and malware protection for employees, regardless of location.
- **Regulatory support:** Help secure customer data in regulated industries.

Spectrum
BUSINESS®

FEATURES	ESSENTIALS Securely connect users to apps	ADVANTAGE Data protection/advanced policy
Remote access/ZTNA	● 10 apps	● Up to 300 apps
SWG Proxy and inspect web traffic, URL filtering	●	●
Secure malware analytics	● 500 samples/day	● Unlimited sandbox submissions
CASB Cloud app risk scoring, blocking	●	●
Cloud malware detection	● For 2 applications	● All applications
L3–L4 cloud firewall	●	●
DNS layer security	●	●
L7 cloud delivered firewall and intrusion prevention system (IPS)		●
Inline data loss prevention (DLP)		●

Cloud Security, along with other services from Spectrum Business, can help your organization apply a secure access service edge (SASE) framework to your network. The solution is one of a range of technologies including managed networks, unified threat management (UTM) and distributed denial of service (DDoS) protection, which we can integrate and maintain for a simpler, stronger security experience, backed by 100%, 24/7/365 U.S.-based local support.

Learn more
enterprise.spectrum.com/CloudSecurity

1. Requires Cisco Duo Access subscription.

Spectrum
BUSINESS®