# Top Reasons to Replace Your Branch Firewall

There used to be a time when SD-WAN solutions only had a primary focus on WAN virtualizations with less consideration for security. However, with the emergence of advanced secure SD-WAN solutions, the security gap includes the highest threat protection capabilities. **Advanced SD-WAN** has incorporated next-generation firewall capabilities that allow organizations to perform quick and simple deployments without compromising security.
In this blog, we can cover significant reasons one should replace a branch firewall with an advanced SD-WAN to fully embrace the cloud-first era and modernize security and network architectures.

## Delivery of comprehensive security services

Advanced SD-WAN solutions incorporate next-generation capabilities like DDoS protection, intrusion prevention, deep packet inspection, and controlling access through identity-based policies and events logging.
Unlike branch firewalls, advanced **SD-WAN solutions** provide advanced threat protection. It also helps secure untrusted links and seamlessly security policies across the branch offices.

## Simplifying the local operations

In traditional router-based environments, local branches must deal with a sprawl of security and network equipment accumulated over the years. Additionally, local departments often lack experienced IT staff who can maintain and install the equipment.

An advanced SD-WAN is easy to deploy with no-touch provisioning. No experienced IT staff is required locally, and the security policies and configuration are automatically pushed to the branches.

## Support for cloud-first organizations

Organizations routed the traffic to the data center for security inspection. With the moving of organizations, the applications to the cloud and the use of cloud RingCentral, Salesforce, or Microsoft 365 send the traffic back to the data center, negatively impacting the application performance.
With the help of SD-WAN, you can break out the cloud application locally by also eliminating the inefficient backhaul to the data center. It automatically gears up the traffic to the internet based on business policies by identifying the applications on the first packet.

## Securing the IoT devices with the use of micro-segmentation

IoT devices based on simple architecture cannot run the security agents. Thus, organizations need a different security approach for IoT devices to protect networks from potential vulnerabilities.
**Advanced SD-WAN** may go beyond what SASE defines with the next-generation firewall capabilities. It can help implement zero trust network segmentation based on role-based and identity access control.

You can **Contact CloudMyLab** for more information on Advanced SD-WAN.