

# 5 IT Projects to Save Money and Improve Your Productivity



Now's as good a time  
as any to identify the  
trends you can leverage  
to Reduce Costs,  
Improve Agility, and  
Increase Productivity

In speaking with hundreds of IT executives and networking professionals across the globe, five networking and security shifts demand particular attention.



From MPLS to SD-WAN

---



From Proprietary Cloud Connectivity to Cloud Access Optimization

---



From Security Appliances to Security as a Service

---



From "Shadow IT" to Controlled Cloud Access

---



From UC to UCaaS

---

# From MPLS to SD-WAN

SD-WAN adoption is booming and for good reason. CIOs and their teams have taken to SD-WAN to reduce costs and improve their agility. The high-cost of international MPLS connections have given way to SD-WANs with affordable, SLA-backed private backbones.

Replacing MPLS's high costs and inflexibility is often an imperative of WAN transformation initiatives for which many organizations turn to SD-WAN. By using affordable Internet capacity, SD-WANs let companies slash monthly bandwidth spend.

## SD-WAN Benefits

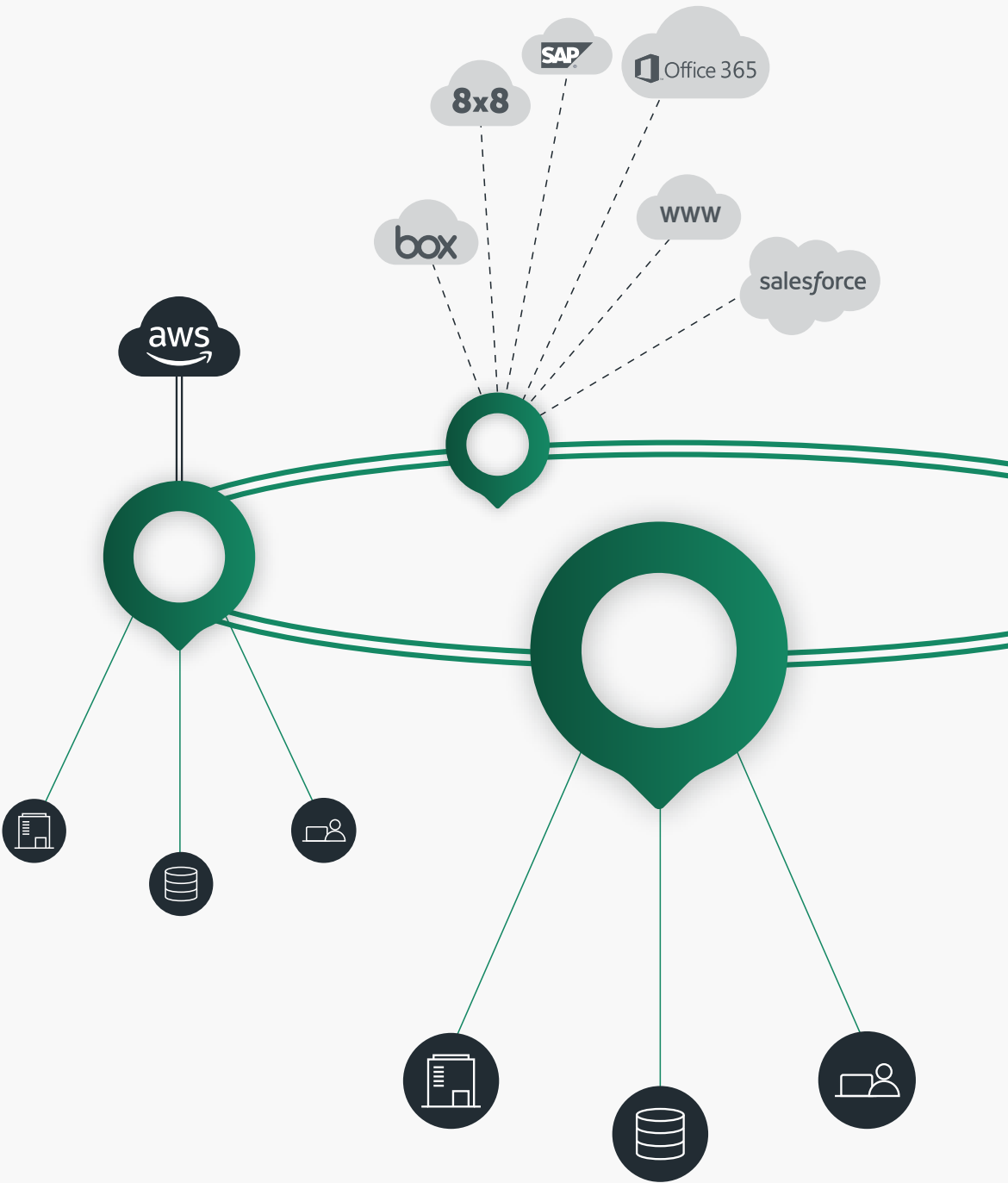
Internet connectivity also afford SD-WANs other benefits. Sites can be deployed in minutes not months. Network uptime can reach five 9s as even small locations can be equipped with last-mile redundancy. And with more bandwidth and application-aware routing, applications perform better — at least in certain scenarios.

## The Next Challenge

At the same time, though, Internet-based SD-WANs show problems when used for worldwide application delivery. The suboptimal routing of the Internet core is often too unpredictable with too much latency to deliver a responsive, predictable application experience. Many CIOs find themselves stuck with MPLS and all of the costs and limitations that implies.

## The Solution: Affordable, Private Global Backbone

Packaging an affordable, private global backbone with SD-WAN frees companies from their MPLS dependency. Managed private backbones avoid the problems of the Internet core. Ubiquitous IP capacity reduces capacity costs. Building a managed, private IP-based backbone gives global SD-WAN services MPLS-like performance at a fraction of MPLS's cost.



# From Proprietary Cloud Connectivity to Cloud Access Optimization

With the cloud, IT is challenged to provide the same seamless experience as when users accessed applications in private datacenters. Those challenges can be easily met by optimizing the network for cloud access. IT professionals know well the value of cloud services but integrating the cloud into legacy MPLS network deployments remains challenging for many reasons:



**Erratic Internet performance** disrupts the cloud experience. Cloud datacenter and cloud application traffic must leave the controlled world of MPLS and traverse the Internet core with its congestion and unpredictable routing. Proprietary cloud connectivity options, such as AWS Direct Connect or Azure ExpressRoute, addresses the Internet performance issue but requires additional investment and does not address the backhauling problem.



**Backhauling cloud traffic** to a centralized, secure Internet gateway has been the norm for enterprise networks but adds latency to the cloud session.



**Capital and operational expense increase significantly** when companies secure the cloud. Many organizations find they must set up and maintain virtual firewalls for every cloud datacenter.



**Poor multicloud user experience** ensues as users end up juggling numerous logins when connecting to different clouds.

## The Solution: Native Cloud Connectivity

By building native cloud connectivity, network optimization, and security into a global SD-WAN, enterprise can deliver users a superior cloud experience while meeting enterprise requirements for security and control.

Users authenticate once against the SD-WAN (using multi-factor authentication) to access multiple clouds. Cloud resources are more responsive thanks to the SD-WAN's numerous network optimization techniques, some designed specifically for the cloud. All the while IT can protect cloud resources and users from Internet-borne threats using the same SD-WAN security services that protect the rest of the enterprise.



# From Security Appliances to Security Services

Security appliances have long burdened IT with their operational overhead. Firewall-as-a-Service (FWaaS) addresses those limitations, letting companies improve their security posture and reduce operational expenditures (opex).

Security teams have long relied on security appliances, and with each security appliance comes a hefty capital outlay and plenty of operational overhead. FWaaS replaces the traditional branch firewall appliance with a network security stack in the cloud. It's a security revolution that delivers four elusive benefits:

## No capacity constraints

Traffic growth or activating processing-intensive features on the firewall often necessitate appliance upgrades outside of budgetary cycles. FWaaS avoids those problems by leveraging cloud scalability and elasticity.

## Maintenance and vulnerability patching

FWaaS avoids the immense effort and potential failure points introduced by the appliance lifecycle of handling, maintenance, configuration, and upgrades. With FWaaS, the provider, not IT, handles software updates and patching without additional cost or sudden hardware upgrades.

## Simplified management

Firewall administrators are all too familiar with the challenges of maintaining consistent security policies across sites and managing multiple brands of firewalls. With FWaaS, one logical rule set defines access control across all relevant enterprise resources.

## Universal traffic inspection

To protect their sites, organizations must either deploy appliances at every location, increasing costs and complexity, or backhaul traffic to a site for security processing, adding latency. Regardless, separate security tools are still needed for the cloud and mobile users. FWaaS provides visibility into and control over all WAN and Internet traffic for fixed and mobile users.








# From “Shadow IT” to Controlled Cloud Access

The benefits of cloud applications are well documented, and so are the problems of unauthorized cloud application access (aka Shadow IT). Making cloud access and security part of a global SD-WAN service, puts IT in control of the cloud.

While the cloud brings many benefits, IT executives have also grappled with the downsides caused by users accessing unauthorized cloud applications:

- 

**Risk of infiltration** grows from users accessing malware-infected cloud services.
- 

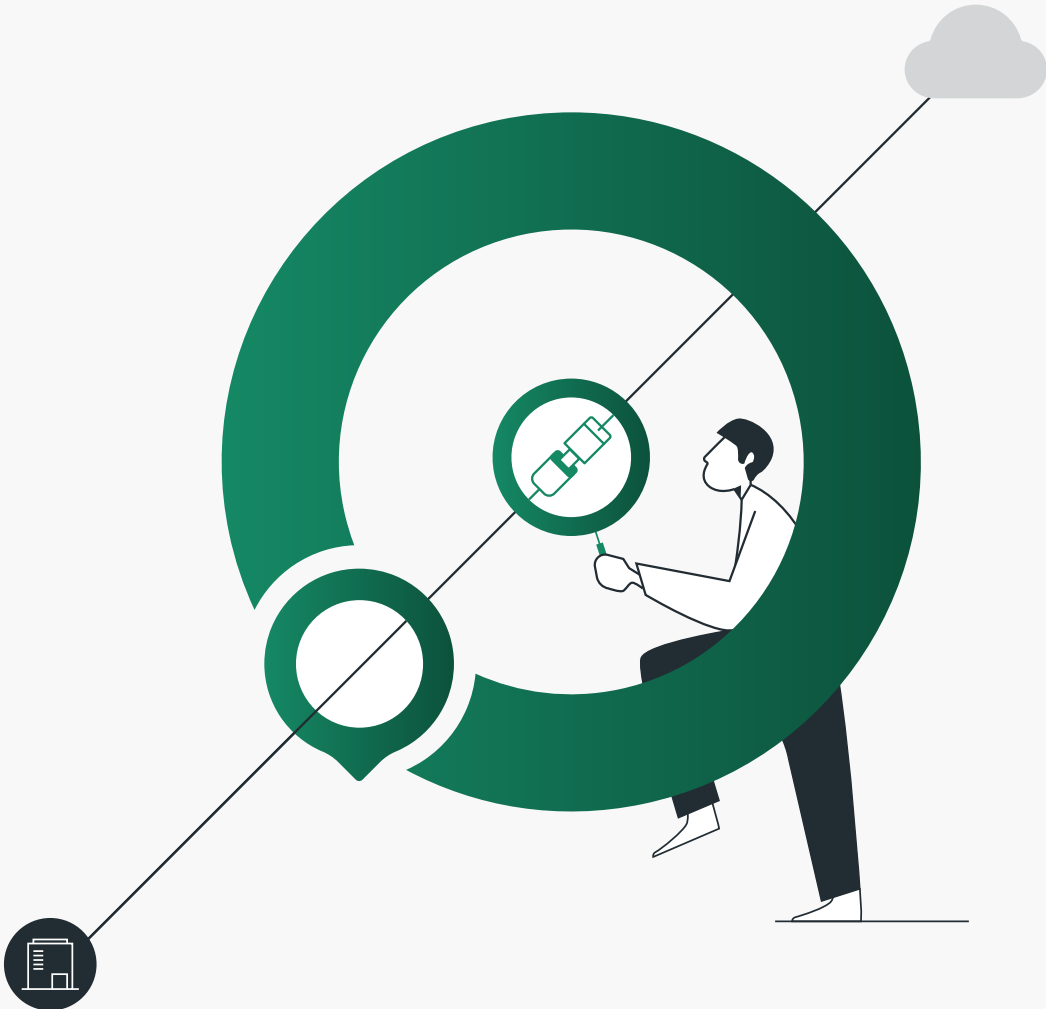
**Data loss** becomes a pressing concern whether because users fail to implement the necessary backup procedures, or because users can leak business-critical information undetected.
- 

**Protecting data privacy and enforcing compliance** with GDPR and other standards and regulations becomes far more difficult.

Cloud Access Security Brokers (CASB) provide an enforcement point for enterprise security policies as users access cloud-based resources. But CASBs introduce yet another security element to purchase and deploy. Additional security policies must be created and maintained, increasing an enterprise's operational overhead and fragmenting IT's view into their security infrastructure.

## The Solution: Make Cloud Access and Security Part of the SD-WAN


CASB becomes inherent to the service. The same policy set used for governing access to internal resources extends to SaaS applications and the Internet. IT gains full visibility into SaaS usage with analytics showing which locations and users, fixed or mobile, are accessing which SaaS applications. SaaS performance improves as a global SD-WAN service avoids the congestion of the public Internet, routing SaaS traffic across their optimized backbones and exiting at the PoP nearest to the customer's instance in the SaaS service.





# From UC to UCaaS

Unified communications changed how we communicate; UC-as-a-Service (UCaaS) changes how we consume UC — avoiding overhead, reducing downtime and deploying in minutes.

As many distributed enterprises have already seen, the integration of voice, video, messaging into a UC system can dramatically improve collaboration. At the same time,

- 

**Increased opex** — Like any on-premise application, delivering a functional UC system requires significant capital investment. By contrast, UCaaS allows you to switch to an opex model, avoiding the costs and complexity of deploying and maintaining UC infrastructure.
- 

**Improved uptime** — Resiliency is also higher with UCaaS offerings, as they're less susceptible to single-event outages that can plague UC systems. Yes, you can build single-event resiliency into a UC server, but that requires increasing investment in redundant hardware, local failover for branch offices, and more.
- 

**Lightening fast deployment** — As a cloud service, UCaaS can deploy in minutes, far faster than setting up a UC server and the supporting infrastructure.

UCaaS works even more effectively across SD-WAN. The Internet backhaul typical of MPLS networks translates into inefficient routing of UCaaS voice traffic, often degrading call quality. SD-WAN allows for local Internet breakout, eliminating the backhaul problem.

UCaaS sessions, particularly those with video conferencing, require significant bandwidth. MPLS, of course, comes with a hefty capacity price tag. Approximately 38% of companies benchmarked by Nemertes Research saw their WAN costs rise when adopting UCaaS.

**When implementing SD-WAN as a global service, UCaaS traffic can be carried across an optimized global connection to doorstep of the UCaaS service, eliminating Internet's performance problems.**



# Cato Networks: Reducing Networking Costs and Improving Agility

Addressing those five technology changes from an infrastructure perspective requires a global networking service with its own backbone, built-in security capabilities, and the ability to connect sites, cloud resources, and mobile users. We call these services cloud-native service and Cato is the world's first cloud-native carrier.

The Cato Cloud Network is a global, geographically distributed, SLA-backed network of PoPs, interconnected by multiple tier-1 carriers. Cato Security Services is a fully managed suite of enterprise-grade and agile security capabilities, built into the network. By converging networking and security onto an SLA-backed backbone, Cato Cloud lets organizations drop MPLS without compromising network performance or reliability, eliminate branch appliances, gain direct, secure Internet access everywhere, and seamlessly extend the enterprise WAN to mobile users, cloud datacenters, and cloud applications.

**For more details, please contact us**

To learn more visit our website at  
[www.CatoNetworks.com](http://www.CatoNetworks.com)  
or contact us for a short and enlightening demo

**CONTACT US**

