CATO
NETWORKS

# Companies Boost Home/Mobile Remote Access Performance, Scalability, and Security with Cato

# Delivering Networking and Security Ready for Today and Positioned for Tomorrow

The COVID-19 pandemic led to the largest global work-at-home experiment in history, forcing organizations to scale their mobile VPN solutions to capacities previously unheard of. Unfortunately, mobile and home users often wrestle with the slow performance, latency and unreliability that come with backhauling remote connections to a data center or other location before sending them to applications and the cloud. With thousands working at home full time, poor performance means poor productivity. This is how three organizations delivered equally fast office and remote access connections with Cato. Cato connects mobile and home users to the same fast converged backbone as office users and provides IT with a single set of IT security and management capabilities for all three.

AdRoll

AdRoll Transforms Global Access to Amazon AWS with Cato →

ASM INTERNATIONAL

ASM Boosts WAN and Mobile Performance, Cuts Costs with Cato →

Geosyntec

Geosyntec Connects 60+ Locations, Improves Remote Access Punch with Cato →

# AdRoll Transforms Global Access to Amazon AWS with Cato

**Adrian Dunne**
Global Director of IT

AdRoll provides a marketing platform for creating personalized advertising campaigns using an advertiser's website data.

## Mobile and MPLS Challenges

Adroll has approximately 500 employees spread across six main global locations and 350 offsite contractors. A cloud-centric business, Adroll deploys three datacenters in Amazon AWS. Before Cato, offsite contractors connected via VPN's to AdRoll's San Francisco firewall and from there to the Internet and AWS. The company had dual firewalls at each location but no geo redundancy.

### Performance

Traffic backhauls created a chokepoint, adding latency and saturating the San Francisco Internet connection.

**"Once, the VPN on our primary firewall rebooted. Suddenly, 100 engineers couldn't work anymore."**

### Deployment

Onboarding new users was cumbersome, particularly for contractors whose machines AdRoll did not control.

**"Using the Mac's management software to push out VPN configurations to users was a pain."**

### Security

There were security issues as the VPN required users to be granted access to all network resources, not specific applications.

**"Traditional VPNs meant opening the door to everything."**

# The Cato Experience

### Performance

With Cato, Dunne solved his contractors' latency problems.

**"Traffic from mobile users is sent across the optimized backbone directly to AWS. Eliminating the San Francisco chokepoint also reduced the congestion on the San Francisco Internet line."**

### Deployment

Cato has made deploying mobile employees and contractors much simpler.

**"With Cato, we just send a user an invite to install the client. It's very much like a consumer application, which makes it very easy for users to install."**

### Security

Cato also gave AdRoll better control over permissions for mobile users, determining the resources they can access at a very granular level.

**"With Cato, we can control what VPN access looks like for our contractors, salespeople, and locations and that really spoke to us. Now there's no concern about users getting into our routers."**

## Traditional Mobile VPN Challenges

Like many companies, AdRoll saw networking pains grow as the company matured. Internet performance was a problem for the company's offsite contractors. They had to establish a virtual private network (VPN) connection to the company's San Francisco firewall and from there they connected to the Internet and AWS. The traffic backhauls created a chokepoint, adding latency and saturating the San Francisco Internet connection.

Redundancy was also an issue. Locations were equipped with dual firewalls for local redundancy, but there was no geo-redundancy. Should the San Francisco site become inaccessible, the contractors were unable to work. "It puts a lot of stuff in one basket,'" says AdRoll's Global Director of IT, Adrian Dunne, "Once, the VPN on our primary firewall rebooted. Suddenly, 100 engineers couldn't work anymore."

Onboarding new users was cumbersome, particularly for contractors whose machines AdRoll did not control. Dunne and his team had to send them configuration instructions for their VPN clients. "Using the Mac's management software to push out VPN configurations to users was a pain," he says.

There were also security issues as the VPN required users to be granted access to all network resources, not specific applications. Nothing prevented a user who only needed access to the company's Web application, for example, from using SSH to connect to the company's routers. "Traditional VPNs meant opening the door to everything," says Dunne.

Ultimately, Dunne found the appliance-centric approach to mobile connectivity constrained his operation. "When we moved our San Francisco office, we had to treat our firewall relocation like an organ transplant," he says. "We ran down the stairs with the firewall, jumped into a running car, drove across the city, and ran it up the stairs to minimize downtime. That's not scalable or how I want to live my life."

## Cato Globally Optimized and Secure Mobile Access

Dunne and his team had already experienced the value of cloud services with AWS. It provided his broader IT efforts with redundancy, geo coverage, and backhaul elimination. He wanted to mirror that success with his VPN solution, which is why he turned to Cato.

Cato provides a global, SLA-backed backbone that connects remote mobile workers and branch offices to corporate resources, such as cloud datacenters, and enforces granular access policies.

With Cato, Dunne solved his contractors' latency problems. Instead of backhauling their traffic to San Francisco, contractors now run the Cato mobile client and connect to Cato. AdRoll's Amazon AWS datacenter connected to Cato using a Cato initiated IPsec tunnel. With both users and datacenters connected to Cato, a single network is formed. Traffic from mobile users is sent across the optimized backbone directly to AWS. Eliminating the San Francisco chokepoint also reduced the congestion on the San Francisco Internet line.

> **"Onboarding new users became much simpler. With Cato, we just send a user an invite to install the client, It's very much like a consumer application, which makes it very easy for users to install."**

Perhaps the best measure of his success has been what users haven't said. "From our users, we have peace and quiet," he says, "Nobody will come and say, 'Thank you for the VPN.' They expect it to work, but silence is gold."

## Improved Security Posture is Good for Business

Cato also gave AdRoll better control over permissions for mobile users, determining the resources they can access at a very granular level. "With Cato, we can control what VPN access looks like for our contractors, salespeople, and locations and that really spoke to us," says Dunne. "Now there's no concern about users getting into our routers," he says.

> **Dunne and his team have also gained deeper insight into cloud usage. Now we can see who's connecting when and how much traffic is being sent, information that was unavailable with our previous VPN provider, he says. Correct oversight and monitoring of logs ties directly into the bigger security conversation."**

But more than providing "just" better management, Cato has helped AdRoll attract larger customers. "Fortune 500 customers do their due diligence and ask about access control, data flows, log review, and stuff like that in their RFPs," he says, "Cato gives us the ability to tick the "yes" box and shorten the time to get in front of the customer. There was a direct impact on our bottom line."

# ASM Boosts WAN and Mobile Performance, Cuts Costs with Cato

**Ian Bleazard**
IT Director of Infrastructure and Analytics

ASM INTERNATIONAL

ASM SMT is part of the ASM Pacific Technology (ASMPT) Group, a global supplier of semiconductor assembly and packaging equipment and materials and surface mount technology solutions.

## Mobile and MPLS Challenges

The ASM Group is separated into three business segments. The Surface-mount Technology (SMT) sector decided to switch its network to Cato. ASM SMT's main sites are in Munich, Germany; Weymouth, England; and Singapore, with other locations in the U.S. and several countries in Western Europe and Asia. Before Cato, ASM SMT's offices connected over a global meshed VPN topology overlaid on top of MPLS. Local Internet breakouts added Web filtering and WAN optimization hardware. Mobile users connected to firewalls at core regional locations for remote access.

### Performance

Scalability was limited, which had an adverse impact on remote access performance.

**"With shared memory and CPU resources among firewall and remote access functions, the regional firewall appliances were often unfit for increasing demand."**

### Deployment

Before Cato, ASM SMT's offices connected over a global meshed VPN topology overlaid.

**"The solution worked okay, but it was very expensive and took a long time to provision."**

# The Cato Experience

## Performance

Cato improved remote access performance, increasing home and mobile user productivity.

**“The productivity of those on the POC significantly increased and, more importantly, it removed some of daily frustrations.”**

**“Our users really like it and find the Cato VPN client easy to use – and that’s rare.”**

## Deployment

Deploying Cato was quick and simple. The Cato solution provided more bang for ASM’s buck.

**“Cato’s pricing structure allowed a higher bandwidth among sites vs. MPLS.”**

**“We were able to switch over with almost no outage, which is key, as any outage can cause issues with production and other key business functions.”**

## The Challenge: A Fast, Agile Global Network

Global suppliers need fast, agile networks to keep business processes moving among manufacturing plants, warehouses, customers, and partners. As a leading supplier of SMT and semiconductor process equipment for computer chip and circuit board manufacturers, ASM SMT is no exception. With offices spread globally from the west coast of the USA to the east coast of China, ASM SMT found achieving such a goal a tall order.

Before Cato, ASM SMT’s offices connected over a global meshed VPN topology overlaid on top of MPLS. Local Internet breakouts added Web filtering and WAN optimization hardware. Mobile users connected to firewalls at core regional locations for remote access.

“The solution worked okay, but it was very expensive and took a long time to provision,” says Ian Bleazard, ASM SMT IT Director of Infrastructure and Analytics. “We operate in China and Vietnam, where you can be looking at a 180-day lead time for connectivity. Six months can have a substantial negative business impact.”

With a typical office consisting of the usual stack of edge security products, such as firewalls and Web filter, new site deployment was dependent on multiple security vendors delivering on time, which, of course, often led to further delays, according to Bleazard.

In many cases, each appliance had to be managed separately, so configuration was a tedious and sizeable task at scale. Any changes to the regional firewalls had an impact on remote user connectivity.

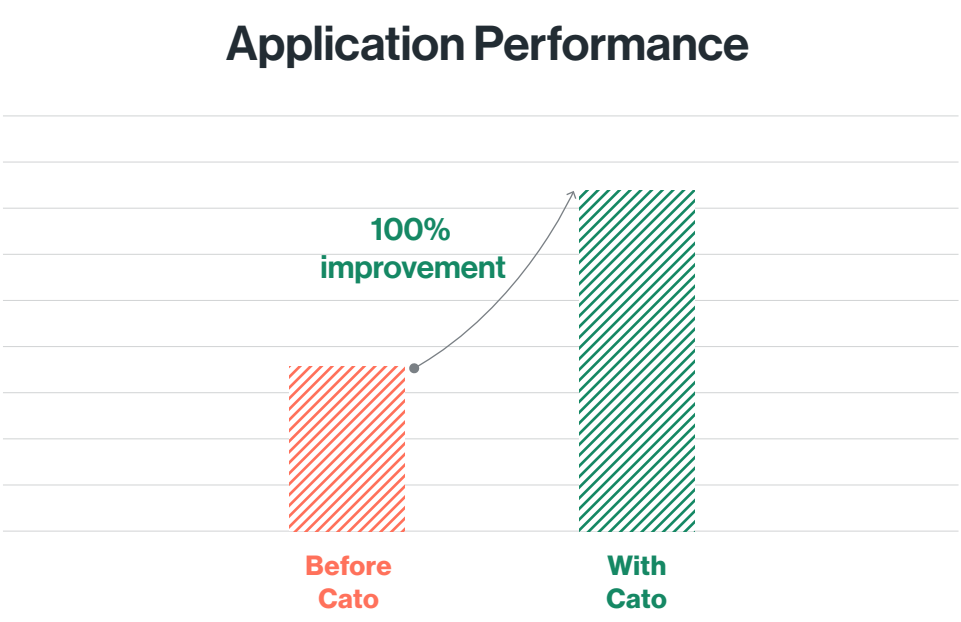
> **“With shared memory and CPU resources among firewall and remote access functions, the regional firewall appliances were often unfit for increasing demand.”**

## ASM SMT Investigates SD-WAN, Chooses Cato

ASM SMT sought a simpler solution that would deliver business agility, security and good performance at a lower total cost of ownership. “SD-WAN was intriguing to us, so we set out to research the technology and some vendors,” says Bleazard. “Three vendors made our shortlist, but it soon became clear that there was only one all-encompassing winner.”

That winner was Cato. “Other vendors either lacked middle-mile backbone solutions, required backhauling of traffic between locations or couldn’t provide built-in WAN optimization and security functionality.” A trusted local vendor introduced ASM SMT to Cato. “Immediately we had a good feeling. Cato had a promising solution that could solve a lot of our issues and they presented it to us in a very honest, upfront manner.”

ASM SMT put together a proof of concept (POC) project with Cato for three business locations. “The idea was to throw some of the major issues we encountered with MPLS at the POC scenario. For example, we wanted to see how Cato would address speed issues with centralized Product Lifecyle Management software, SMB file copy and videoconferencing performance over the WAN.” During the POC, Cato improved performance more than 100 percent vs. MPLS.




> **“It’s rare that you hear from users when things are going well, but, amazingly, during the POC we had users from all over the business thanking us and telling us how much it was improving their daily business productivity.”**

## Cato Delivers Agility and Performance at a Lower Cost than MPLS

Convinced, ASM SMT proceeded with Cato deployment across the other locations. “Our MPLS contract had eight months left, so we could roll out Cato gradually,” says Bleazard. “Cato’s use of BGP made the rollout seamless, with dynamic routes published automatically as soon as a site came online. We were able to switch over with almost no outage, which is key, as any outage can cause issues with production and other key business functions.” The savings and performance grew as MPLS contracts expired and ASM SMT transitioned to Cato.

> **“Cato’s pricing structure allowed a higher bandwidth among sites vs. MPLS and its packet loss mitigation feature helped a lot with VoIP and video packets reaching their destination without a break in communication.”**

Bleazard was very pleased with Cato support. “Cato usually answered our emails within 10 minutes, and we were able to get someone on the phone quickly when something was important,” says Bleazard. “The general feeling was that support was there when we needed it.”

ASM SMT has since begun rollout of the Cato VPN client as a replacement for the internal VPN gateways, a process that accelerated as the COVID-19 pandemic sent workers home, first in China and then everywhere else. “Generally, you don’t transition technology during a crisis, but we felt we had to move a few hundred users – mostly the ones that use a lot of bandwidth – onto the Cato network for VPN and it worked out really well,” says Bleazard. “The VPN provides straight access onto the Cato backbone and the services they need, rather than backhauling everything to the local office. Our users really like the Cato VPN client and find it easy to use – and that’s rare. Having one console for everything makes the whole management process much simpler as well, and very much helped us stay on top of these unique circumstances.”

Overall Bleazard is very pleased with the Cato experience and plans to expand remote access using Cato and deployment to future locations. He adds, “The past eight weeks is one of the few times I’ve ever received emails from users saying thank you.”

# Geosyntec Connects 60+ Locations, Improves Remote Access Punch with Cato

**Edo Nakdimon**
Senior IT Manager

Geosyntec

Geosyntec is a consulting and engineering firm that works with private and public sector clients to address new ventures and complex problems involving the environment, natural resources, and civil infrastructure.

## Mobile and MPLS Challenges

Geosyntec Consultants has more than 80 office locations worldwide. Before Cato, the company's 67 North American sites had 1.544 Mbits/s connections to an MPLS service. Routers at the local branch offices split the traffic, sending voice traffic across MPLS, site-to-site traffic across an Internet-based DMVPN connection, and Internet traffic over the local internet lines. Cloud usage consisted predominantly of instances in Azure connected to the Geosyntec datacenter via a 1 Gbits/s ExpressRoute connection. Remote mobile access was provided via multiple VPN technologies. Critical applications included Skype for Business, Geographic Information System (GIS) software, and CAD.

### Performance

Users initially connected to a VPN server in a Geosyntec location but continued to send data through those offices even when accessing data in a different location, introducing latency and bottleneck issues.

**“**

**If there's any latency, if there's any lag, we're going to hear about it.”**

### Deployment

Like many enterprises, Geosyntec faced the challenges of widespread remote access posed by the COVID-19 pandemic.

**“**

**With the COVID-19 pandemic on the rise, many of our users began to work remotely. Our VPN traffic spiked, in some cases, hitting the limits of our VPN servers.”**

# The Cato Experience

## Performance

By running the Cato Mobile Client, users are automatically connected to the nearest Cato PoP, bringing them the full benefits of Cato's security services and network optimization.

**"By connecting them directly to Cato, we eliminated unnecessary hops across the public Internet core."**

**"My team and I received many emails from employees saying this is the best experience they have had out of all the VPN clients."**

## Deployment

With Cato, Geosyntec connected 67 sites and more than 1200 remote onto the same network all managed through the same console.

**"In a matter of 30 minutes, we configured the Cato mobile solution with single sign- on (SSO) based on our Azure AD."**

## The Challenge: How to Deploy Skype for Business Without MPLS

Collaboration is essential to most enterprises, but voice and video collaboration are too sensitive to route over the Internet and scaling up an MPLS can be very costly. What can IT leaders do without increasing their networking costs? That was the challenge facing Edo Nakdimon, senior IT manager at Geosyntec Consultants.

The environmental consulting service had relied on MPLS service to connect 67 offices across North America with T1 (1.544 Mbits/s) connections. Geosyntec initially ran voice over MPLS using Cisco CallManager in its datacenter. Routers at the branch offices provided local breakout, sending voice traffic across the MPLS circuit and the rest of the traffic across the Internet.

"Enabling voice, video chatting and other collaboration services over a single T1 lines is like trying to push an elephant through a pinhole," says Nakdimon, " For optimal experience, we knew we had to either scale up our existing solution or reearchitect our Wide Area Network environment. Without the proper network design traffic such as voice and video will suffer."

Collaboration, though, wasn't the only application that concerned him. The company's consultants rely on Geographic Information System (GIS) software and CAD for their work. The GIS project files were stored on servers in the respective Geosyntec offices. However, the consultants often had to open files in remote offices, pulling the large files across the DMVPN connections. "If there's any latency, if there's any lag, we're going to hear about it."

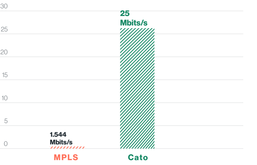
He decided to migrate to Skype for Business and replace the MPLS service with a network architecture that could address all of his application needs.

## Cato Meets Geosyntec's 'Ever Evolving' Needs

Nakdimon initially investigated traditional SD-WAN offerings but was skeptical of vendor claims that they could maintain quality of service (QoS) across the Internet. "I don't care what any SD-WAN provider will tell me; I don't care what any network engineer will tell me. They can't guarantee markings will pass over the public Internet across multiple internet service providers," he says. "Once traffic leaves the endpoint, it's beyond the vendor's control. This is just the way it works."

Cato distinguished itself because its SD-WAN devices connect to Cato's global, private backbone. And with more than 50 points of presence (PoPs) across the globe, Cato was located near Geosyntec's strategic locations. These factors ensured Cato could provide the QoS Geosyntec requires. "I looked and saw that Cato's SD-WAN devices were connecting to its private network and thought that was 'perfect.' It's exactly what I wanted."

Nakdimon conducted a PoC, and "everything worked great," he says. There was no comparison between MPLS's T1 connection and the 25 Mbits/s connections he used with Cato. Since then, he's rolled out Cato across all of his North American locations, replacing MPLS with Cato's Secure Access Service Edge (SASE) platform.




As an early Cato adopter, Geosyntec experienced some "growing pains," he said. He points to problems with firmware upgrades to the Cato Socket, Cato's SD-WAN device, as an example, which needed to be addressed. "I generally found Cato support to be quick and responsive," he says. "Once that was done, we have so far no complaints. If you have complaints, typically it was not on the network side. We've been very happy so far," Nakdimon says.

> **"Day-by-day needs and requirements are changing, and at Geosyntec, we need to constantly research options to meet those ongoing changes and requirements. Cato provides us with a platform for delivering the networking and security capabilities that help our users increase their productivity while allowing our network engineers to concentrate on other projects by reducing the management time and overhead."**

Gradually Nakdimon has expanded beyond MPLS replacement, activating other Cato capabilities, such as Cato security services, to protect branch offices. "Networking is ever-evolving," says Nakdimon. "Day-by-day needs and requirements are changing, and at Geosyntec, we need to constantly research options to meet those ongoing changes and requirements. Cato provides us with a platform for delivering the networking and security capabilities that help our users increase their productivity while allowing our network engineers to concentrate on other projects by reducing the management time and overhead."

## Cato SDP Solves Global Geosyntec's Remote Access Challenge

Remote access has been another service Nakdimon activated for his users. Like many enterprises, Geosyntec faced the challenges of widespread remote access posed by the COVID-19 pandemic. And while Nakdimon had already planned to deploy Cato SDP (Software Defined Perimeter), Cato's remote access solution, before the pandemic. "Corona was just an added reason for me to roll it out," Nakdimon says.

> **"We utilize a few different VPN technologies. With the COVID-19 pandemic on the rise, many of our users began to work remotely. Our VPN traffic spiked, in some cases, hitting the limits of our VPN servers."**

Nakdimon accelerated his Cato remote access adoption in part because of the scalability issues of his VPN servers. "We utilize a few different VPN technologies. With the COVID-19 pandemic on the rise, many of our users began to work remotely. Our VPN traffic spiked, in some cases, hitting the limits of our VPN servers," Nakdimon says.

Not only was scaling VPN servers a problem, but so was performance. Users initially connected to a VPN server in a Geosyntec location but continued to send data through those offices even when accessing data in a different location, introducing latency and bottleneck issues.

Instead, he deployed client-based Cato SDP, equipping more than 1200 remote users with Cato's Mobile Client. "Deployment was quick. In a matter of 30 minutes, we configured the Cato mobile solution with single-sign-on (SSO) based on our Azure AD."

> **"We found that we could reduce network overhead and eliminate bottlenecks for remote users. By connecting them directly to Cato, we eliminated unnecessary hops across the public Internet core."**

By running the Cato Mobile Client, users are automatically connected to the nearest Cato PoP, bringing them the full benefits of Cato's security services and network optimization. "Cato SDP extends the QoS and network policies in our SD-WAN, to our remote users," he says, "We found that we could reduce network overhead and eliminate bottlenecks for remote users. By connecting them directly to Cato, we eliminated unnecessary hops across the public Internet core."

In addition, Nakdimon was able to deliver additional security to remote users. "The easily deployed [single sign-on] and web filtering integration provided us additional layers of security for our remote users," says Nakdimon. "The Cato remote access solution is simple to deploy, yet robust. It improved our employees' ability to securely and productively work remotely."

With Cato, Geosyntec connected 67 sites and more than 1200 remote users (only 101 are currently shown) onto the same network all managed through the same console.

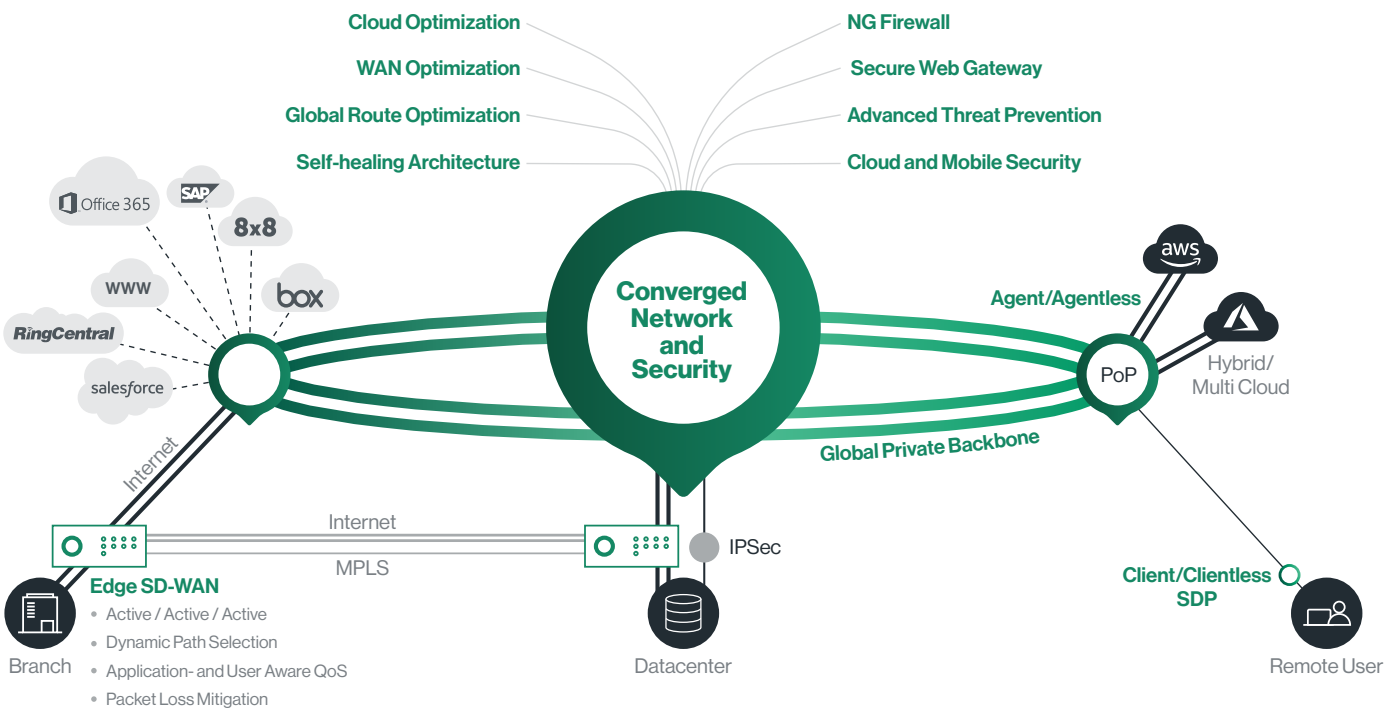
## Geosyntec Looks Ahead with Cato

Looking ahead, Nakdimon hopes to replace its branch firewalls and routers with Cato security services. Overall, Geosyntec credits Cato solutions with streamlining WAN connectivity and remote access, augmenting security, and providing a high degree of user satisfaction, Nakdimon says.

> **"My team and I received many emails from employees saying this is the best experience they have had out of all the VPN clients, Nakdimon says. They email me. They're thrilled. And if users are happy, management is happy."**

# About Cato Networks

Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero trust architecture.




## Cato. The Network for Whatever's Next.

### Cato Cloud

- Global Private Backbone
- Edge SD-WAN
- Security as a Service
- Cloud Datacenter Integration
- Cloud Application Acceleration
- Secure Remote Access
- Cato Management Application

### Managed Services

- Managed Threat Detection and Response (MDR)
- Intelligent Last-Mile Management
- Hands-Free Management
- Site Deployment

ISO 27001 Certified

SOC2 Approved

GDPR Compliant