Channel Partner Perspectives

Managed IT Provider Eliminates Appliance Sprawl, Improves Security Capabilities with Cato Networks

Paul Breitenbach
Chief Information Officer

Background

For more than 14 years, WorldwideIT has delivered managed IT solutions to businesses, nonprofits and government. WorldwideIT (WWIT) provides customized solutions designed to meet the unique needs of each customer and proactively manage the ever-changing demands from today's IT solutions.

The underlying security architecture used by WWIT was to deploy and connect a firewall at each customer premises. WWIT managed the customer's firewalls, ensuring they provided the necessary performance and security capabilities. When customers needed advanced security services, such as SSL traffic inspection, WWIT found the firewalls too limited.

Expensive upgrades were needed, prompting WWIT to look for a new architecture. Ultimately, WWIT settled on the Cato Cloud. Initially, Cato's scalable SSL inspection drew WWIT, but quickly WWIT's leadership team became intrigued by Cato's full firewall capabilities. Paul Breitenbach, Chief Information Officer at WWIT, talked with us about that journey and why his company ultimately adopted Cato's Firewall as a Service (FWaaS).

The Journey to Cloud-based Security Services

> “ The flexibility we got with Cato Cloud, and particularly with the SSL inspection, meant we didn’t need to upgrade any hardware on-premise to inspect all of the traffic we needed to keep customers safe ”

Why were you looking to change your security architecture?

We initially went out to market because of SSL inspection. Our firewall appliances did not have the necessary capacity. The capability was available with additional licensing, but not the capacity.

What approaches did WWIT consider?

We evaluated and did a lot research on many vendors and then tested a smaller pool of them. The second choice was a leading Secure Web Gateway (SWG) provider. The company really provided a web filtering solution with Data Loss Prevention (DLP) and other features built-in. The offering didn’t have full firewall capabilities so we couldn’t replace the customer’s firewall appliance, which would have led to higher costs and more management overhead.

Why did you choose Cato?

The flexibility we got with Cato Cloud, and particularly with the SSL inspection, meant we didn’t need to upgrade any hardware on-premise to inspect all necessary traffic to keep customers safe. Looking at Cato’s overall platform, I think there’s a more complete vision than other vendors who are primarily web gateways. The tipping point was Cato’s easy deployment and ability to rollout rapidly to customers.

> “ Our firewall appliances did not have the necessary capacity. The capability was available with additional licensing, but not the capacity ”

The Benefits of Cato’s Firewall as a Service

A converged security service aligned well with WWIT’s need?

That’s right. A lot of the competitors we reviewed were simply web filters with a lot of services built on top of that. None of them were true cloud FWaaS with additional security services. I think even though Cato is a startup and a much newer company than some of the others we evaluated, the Cato leadership has a vision and approach to make the Cato Cloud a platform rather than just a single service offering. It’s a distinction I like. I also liked the team behind Cato. The executives’ track records in previous companies, and the work they did in building innovative solutions is a plus.

Sounds pretty compelling. Is there any reason why someone may opt not to deploy the Cato platform and remain with an appliance?

Playing the devil’s advocate here, you’re relying on Cato to handle all of your traffic and security services. You must ensure anyone doing that has a robust platform, the uptime to meet your needs, and those sorts of things. From a purchasing standpoint, it’s the sort of thing that would have to be vetted by any organization. I looked at the Cato Cloud architecture and was very impressed by the degree of redundancy built into the network.

How does Cato help with the biggest security threats concerning your customers?

Our customers are particularly concerned with web-based threats, more specifically a lot of the newer variants of ransomware and crypto-types of malware. Those are really rampant. They may come in as an email, but they’re just a link to a web-based threat. Cato gave us the ability to actively scan traffic and stop those attacks. This is particularly valuable for small offices that lack the resources to purchase a robust network security stack. With Cato, we could provide them affordable protection with the same kinds of policies and robustness that might have only been available in high-end appliances.

How are customers using Cato today?

Most of them are multi-offices and we use Cato to unify the policies and protection across them. For a lot of customers, it’s just to add extra layers of security. You can deploy Cato with Cato Sockets (Cato’s hardware endpoints) or you can send your traffic through the existing firewalls. In some cases, we’re leaving existing firewalls in place because they’re new. Cato adds an additional layer of filtering and the capacity to do SSL inspection, which is one of the more important things with Web-based traffic. It’s not just distributed offices that describes customers, it’s also the need for extra security and eventually to replace their firewall as it ages and is no longer needed.

The Business Impact of the Cato Partnership

> “ Cato seemed to be both very channel-focused and very flexible. Cato’s open to getting ideas from us, and are capable of incorporating them into their platform very quickly ”

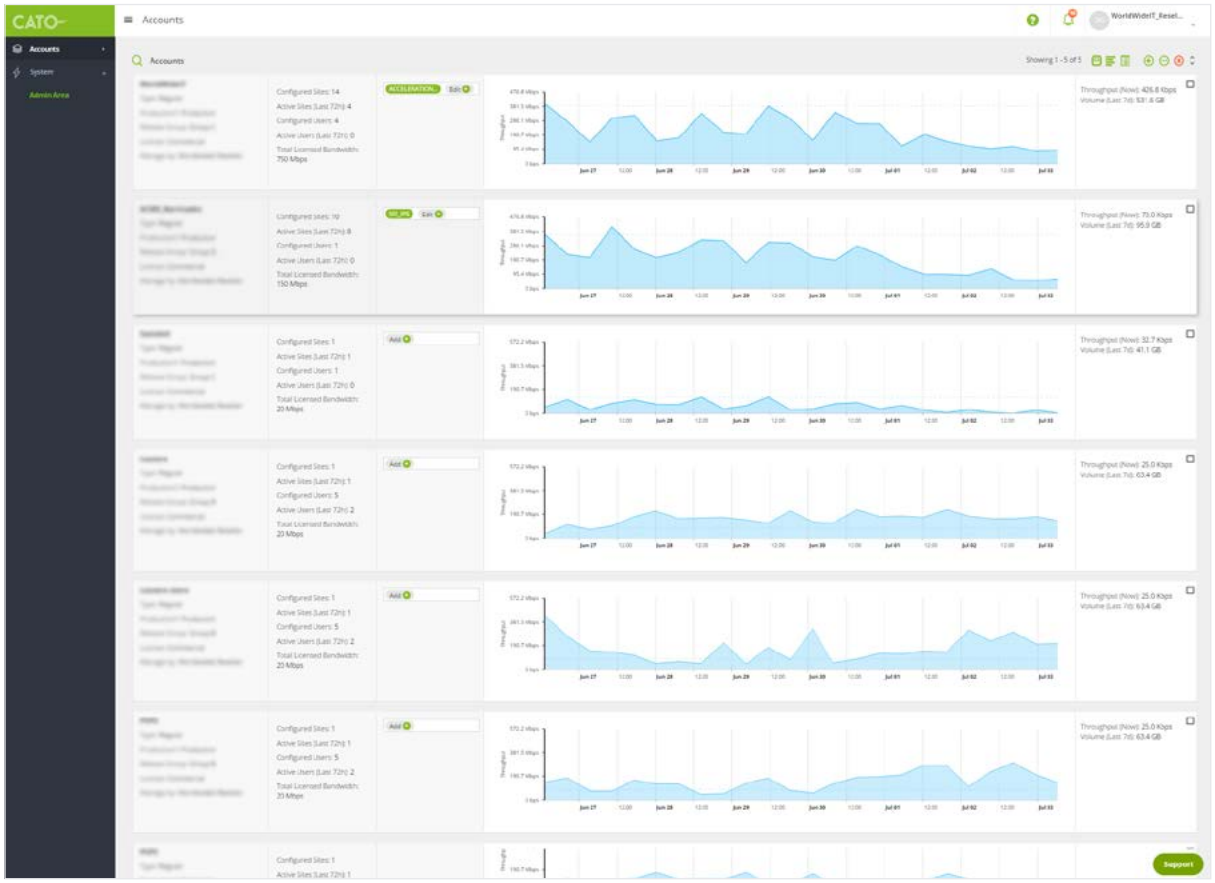
With which kind business problem did you find Cato especially helpful?

Acquisition in particular is a good example. We have customers who need offices brought online and connected in a very quick and efficient manner without a lot of upfront costs. Cato really fits that need to a “T”. One customer of ours has acquired many smaller shops in their industry. Rather than having to build the technology infrastructure stack at each new location, the customer utilizes Cato for connectivity and security in a very simple manner.

Paul, can you describe your relationship with Cato so far from a partner perspective?

To us, Cato seemed to be both very channel-focused and very flexible. I think that’s an important distinction. A lot of vendors are not easy to work with and not flexible at all in what they offer partners. Cato’s open to getting ideas from us, and are capable of incorporating them into their platform very quickly.

With Cato, partners can manage all of their customers from one view.



CATO NETWORKS

About Cato

Cato Networks provides organizations with a cloud-based and secure global SD-WAN. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people and data.

The Cato Cloud reduces MPLS connectivity costs, eliminates branch appliances, provides direct, secure Internet access everywhere, and seamlessly integrates mobile users and cloud infrastructures into the enterprise network. Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, who previously cofounded Check Point Software Technologies and Imperva, and Gur Shatz, who previously cofounded Incapsula.

For more information:

www.CatoNetworks.com

@CatoNetworks

Where do you want to start?

SECURE AND OPTIMIZED SD-WAN

SLA-BACKED, AFFORDABLE WAN

SECURE DIRECT INTERNET ACCESS

APPLIANCE ELIMINATION

HYBRID CLOUD NETWORK INTEGRATION

MOBILE WORKFORCE, SECURE CLOUD ACCESS