Customer Case Study

Blender Breaks Free from the Box

Boaz Aviv
Chief Technical Officer

blender
Loans Between People

Background

Eliminating borders for both lenders and borrowers worldwide is at the heart of Blender's peer-to-peer lending platform. Founded three years ago, Blender's service gives borrowers and lenders a simple and easy alternative to traditional banks lending that offers more attractive rates to both parties.

Currently servicing more than 10,000 clients, the company has offices in Israel, Italy and Lithuania with plans to expand to two new territories in 2017. To be competitive, the organization must also run especially lean, both with its network architecture and IT staff.

> *" Even if the time required to manage your firewall is just 10 hours a month, that's still 10 hours you've lost "*

Challenge

When Blender originally started out of their headquarters in Israel they had installed a firewall appliance from one of the top tier vendors. Chief Technical Officer (CTO) Boaz Aviv found it complex to manage, upgrade and patch. "Owning these boxes is expensive and they need constant management. Even if the time required to manage your firewall is just 10 hours a month, that's still 10 hours you've lost," explains Aviv. Blender depended on an IT integrator for installation and support of the firewall appliance. When they experienced a system failure over the weekend, their IT integrator was not available to support them. This resulted in long downtime and impacted their business.

"We are a global operation and we keep it very lean and mean," says Aviv. "In order to do this you need to minimize hassles that don't directly relate to your business. So it's very important to optimize resources, time and people needed to manage your network and security. That's why I've always preferred the simplicity offered by cloud solutions like Cato."

When the time came to expand to their new offices in Italy and Lithuania, the team at Blender stopped to reevaluate how their office network security footprint would impact cost and capacity going forward. Without dedicating personnel to support remote appliances with upgrades and patches, Blender would be dependent on costly third-party assistance with unreliable coverage.

Also, as a financial technology organization, Blender continuously seeks to upgrade into better security services, "Although we are a young company, we never compromise on security," says Aviv. As a cloud-centric business that is subject to regulations and stores most of its data in SaaS applications and a IaaS datacenter, Blender specifically needs to secure data access.

Solution

When Aviv initially learned about Cato Networks and its cloud-based secure network, he saw it as a perfect fit for Blender. "The only metal I had in my office was our telephony machine and the firewall — and I wanted to get rid of both of them" explains Aviv. "I felt that as much as we grow, the more these boxes would grow right along with us, as would the burden of managing and supporting them."

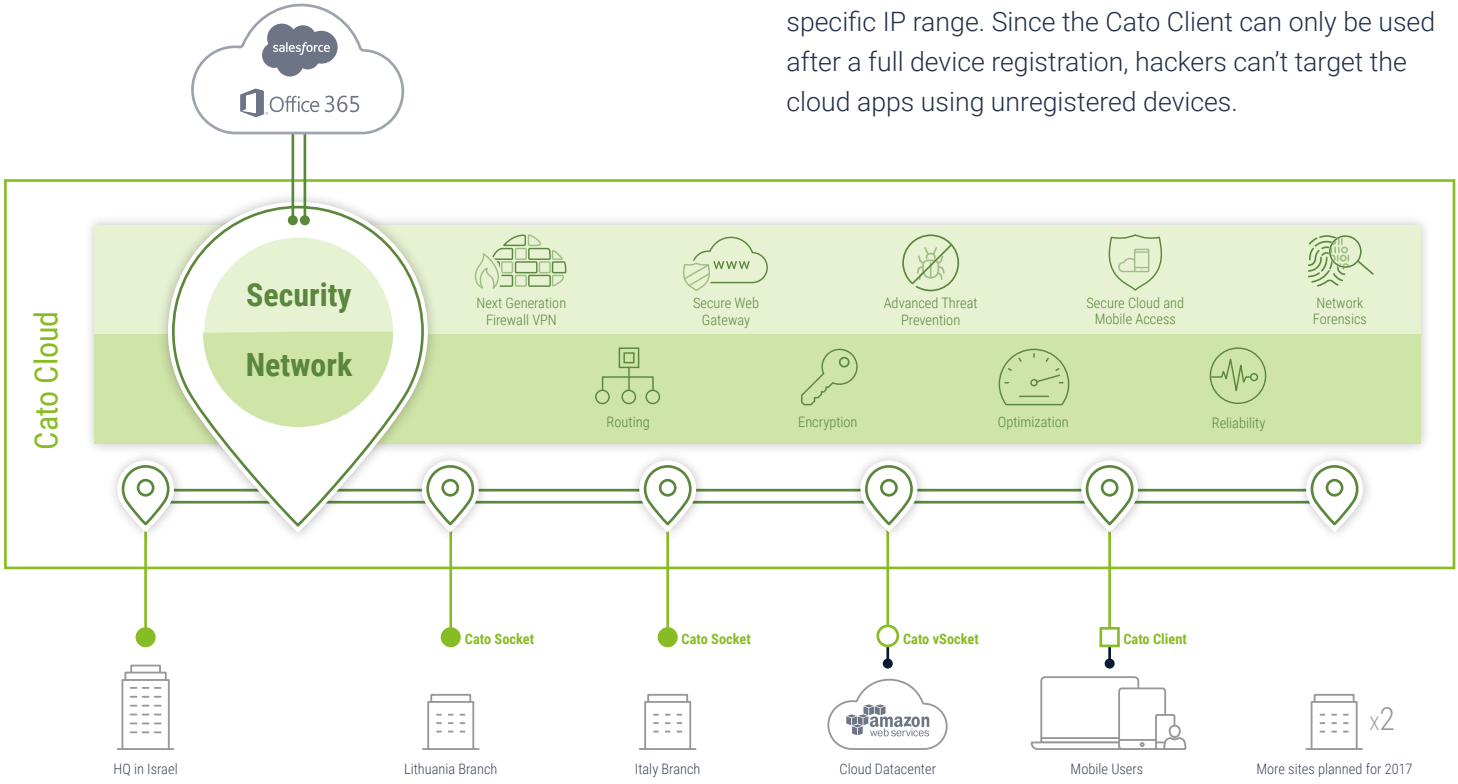
To deploy Cato, Blender simply replaced the incumbent firewall in the main office with a Cato Socket — a small, zero-touch, tunneling device to forward traffic from the office to the Cato Cloud. Connecting their branch offices was simple and required zero technical expertise.

> *"We shipped the Cato socket to Italy and Lithuania and all the local team had to do was plug it into the wall. It was done, and we didn't need IT to install it."*

All locations were now using secure internet access via Cato. A full security stack, including Next-Gen Firewall, application control, and URL filtering inspects Blender's traffic, which is fully encrypted between branches and the Cato Cloud.

Managing network security centrally in the cloud enables a unified policy for all users, locations and applications. Prior to Cato, Aviv had planned to purchase more appliances to support the company's disaster recovery (DR) sites. Installing Cato now allows him to avoid the significant expenses and IT resources it would take to manage additional appliances. Instead, his team is securely connecting the DR sites to the Cato Cloud and from there to the rest of the business.

Blender employees access Office 365, Salesforce and Amazon AWS apps on-the-go using the Cato Client app on their mobile devices. The Cato Client establishes a secure tunnel to the Cato Cloud and all cloud traffic is protected by Cato. To prevent unauthorized access and protect against credential theft, Blender is using a unique Cato feature that allows them to configure their SaaS applications to accept traffic only from the Cato Cloud specific IP range. Since the Cato Client can only be used after a full device registration, hackers can't target the cloud apps using unregistered devices.



The Way Forward

A year into production, Blender is meeting industry security audits while scaling capacity in step with its growing business, and easily enabling users to access network resources using the cloud-based management application. Aviv has been impressed with the level of support he's received throughout. "Any time I've had an issue that needs troubleshooting or had a question, there's always been someone there to help me."

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