SECURITY SOFTWARE COMPANY

CATO NETWORKS

CASE STUDY

VERTICAL:	**Technology**
HEAD OFFICE:	**United States**
GLOBAL FOOTPRINT:	**USA. Europe, Asia-Pacific**
LOCATIONS:	**5**

Security Software Company Maximizes Global R&D Productivity With Cato Cloud

About Security Software

Security Software Company, an anonymous Cato customer, provides security services to enterprises around the world. The company has a headquarters and four branch offices across US, Europe, and the Asia-Pacific. Firewall appliances in each location established IPsec VPNs to one another and across local Internet connections.

Mission Impossible: Open an Office in Days Without Compromising Network Performance

The company was looking to expand its workforce by hiring developers in Europe. The challenge? They needed a new facility – and gave the IT team five weeks to open the location.

At first, the technical approach appeared straightforward — connect the location into the company's Internet VPN. Firewall appliances at other company locations already established IPsec tunnels into the headquarters. Contractors and remote users accessed Jira, as well as the company's Docker containers, by running mobile VPN clients on their devices and connecting to an assigned firewall. From there, they traversed the VPN to headquarters and onto their destination. The approach seemed obvious.

But there was no onsite IT personnel in the European branch office, and an IT person is exactly what would have been needed to configure and deploy the local firewall. The developers were going to work in a shared office space, like WeWork or NextSpace. While the shared office provided Internet access, NATing was being used. Without a dedicated, public IP, a local firewall would need its configuration "tweaked" just to establish a VPN to other firewalls.

And for every location added to the VPN, the IT manager found deployment to take exponentially

longer. He and his team needed to configure tunnels from the new location to every other company location. It was an arduous process requiring them to establish the tunnels to each site, design specific firewall rules for each tunnel, and factor in user issues, such as whether or not to allow remote access. "It was about 1.5 hours of work per tunnel per site. We could spend a few days just configuring the VPN for a new location," he says. The IT team was also unsure of the availability of his Internet path.

"The European branch office required 100 percent uptime," he says, "With the Internet, you can't promise that. Your traffic still goes through several unknown ISPs. You can't ensure that every hop is not a single point of failure."

Another approach was needed. MPLS sounded like the logical choice. It would address his performance concerns. But getting an MPLS line installed in time was going to be a problem. "Just taking delivery of a 20 Mbits/s MPLS circuit would require about a month-and-half in total and three weeks after signing the purchase order," he comments. Far too long for his five-week window.

Cato Cloud: Fast Deployment and Faster Applications

The IT manager looked around for alternative solutions when a friend suggested he investigate Cato Cloud, Cato's cloud-based and secure global SD-WAN. Cato Cloud would use his existing Internet line to connect locations, mobile users and, when he's ready, cloud resources into an affordable, SLA-backed alternative to MPLS. Once in the Cato Cloud, all traffic is protected by a converged suite of advanced security services that includes next-generation firewall (NGFW), secure web gateway (SWG), URL filtering, and advanced threat protection.

For a company where the Internet and mobile connectivity already played such a key role in its networking strategy, Cato Cloud sounded very attractive. By relying on Internet last mile, deployments would be much faster than MPLS. And since Cato uses zero-touch provisioning, the company could avoid the time spent individually crafting each VPN configuration. IT initially installed a Cato Socket, Cato's SD-WAN appliance at the remote European office, and at the headquarters behind the existing firewall. With users connecting directly to Cato, he did not need to add a firewall at his new location. During the next phase, he rolled out Cato to all offices. Mobile users were equipped with the Cato Client to connect directly to Cato Cloud.

Performance Improves, Costs Fall with Cato Cloud

With Cato, IT did far more than just deploy a new location. It improved the users' application

experience, made the team more efficient, and reduced costs. "Cato certainly met my expectations," he says. Cato Cloud incorporates a range of network optimization that significantly reduces data transfer times.

"Cato's optimizations make all the difference. As one Atlanta user remarked to me 'This is unbelievable. I work with our main server in the datacenter and I feel like it is right here in the office.'

IT agility has also improved significantly in many ways. Deploying new offices is no longer a matter of days or even hours. "Onboarding is very fast," he says, "From the time you put in the Socket, minutes are needed to deploy a location." New account configuration is particularly easy. "The LDAP integration really helps. We just imported hundreds of users right into Cato. No need to type in configuration profiles," he adds.

Ongoing management has also become simpler and more efficient with Cato. He monitors his branch sites from one screen using the Cato Management Application. "Managing the solution is very intuitive," he says, "I gave the Cato Management Application to one of the IT engineers and she quickly adapted to the platform."
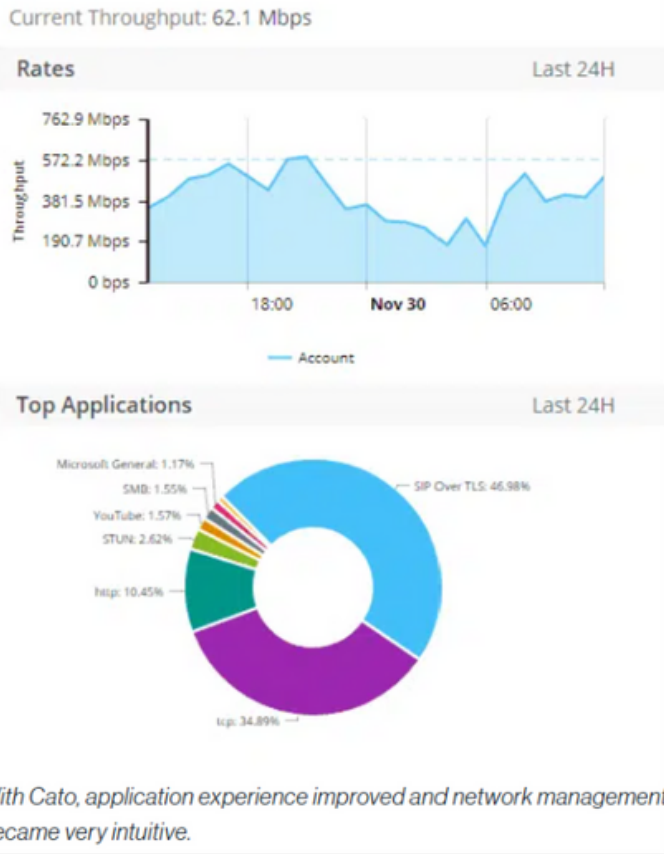
Cost avoidance Was Also Realized in Several Areas.

Cato saved the company from having to purchase an MPLS connection at $4,800 per month. The company also avoided paying for firewall licenses. "We planned on spending $600 per branch firewall and another $400 per year for our licenses," he says, "but many firewalls had to be upgraded because they couldn't handle activating the IPS, the number of active security rules, or the amount of bandwidth. We would end up spending $1,600 per branch firewall and $950/year for the license and that doesn't include the time or cost of upgrading to the new appliance."

Any deployment requires close cooperation with the service provider and on that, Cato gets high marks. "Cato support is unlike any other support that I've experienced. Our interaction is almost like working with an extension of our team," he says.

Security Robust Enough for the Experts

Moving forward, he is looking at replacing the remaining firewall appliances with Cato Cloud. He also wants to enable Cato IPS and Cato's advanced threat protection knowing that unlike an appliance, performance will not degrade with the new capabilities.

Current Throughput: 62.1 Mbps

With Cato, application experience improved and network management became very intuitive.

Overall, he doesn't have regrets with the transition, but he does have an answer for those questioning his decision to go with Cato.

"As you can imagine there were more than a few skeptics in the room when I pitched Cato. MPLS was the safe bet," he says. "But when I went back to one of the VPs and said 'Did you ever imagine that with the money we were going to spend on connectivity alone for the European branch, I could now connect our US support team and customer focus groups, and still provide remote access to all employees? He didn't believe me until I showed him the bills."

IT Manager
Security Software Company