DIAMOND BRACES

CATO NETWORKS

CASE STUDY

VERTICAL:	Healthcare
HEAD OFFICE:	United States
US FOOTPRINT:	32 Outlets
AREAS:	New York, New Jersey, Pennsylvania, Connecticut

Diamond Braces Uses Cato to Boost WAN Security, Performance, and Reliability

About Diamond Braces

Headquartered in New York City, Diamond Braces consists of 32 orthodontist offices in New York State, New Jersey, and Connecticut. Before Cato, most Diamond Braces' locations were connected through broadband and Internet VPNs. Only the main office and call center used fiber. Security came from a firewall gateway/VPN appliance installed at each location.

The Challenge: Easy Deployment and Management; Fast, Reliable Connectivity

Doctors' and dentists' offices have stringent security requirements, thanks to HIPAA and other regulations for protecting patient data. They work with large X-ray image files and many have been moving medical management applications to the cloud. For dentist office chains, such as Diamond Braces, fast, secure, reliable communications among locations and the cloud are an absolute requirement.

The Diamond Braces network spans 32 orthodontist locations in New York State, New Jersey, and Connecticut, with headquarters in New York City. Before Cato, most Diamond Braces locations were connected via Internet VPNs, with fiber running only from its main office and call center. Each location ran a separate firewall gateway/VPN appliance, which led to increasing complexity as the number of locations grew. "It was all getting too difficult to manage and it was taking too much time to ensure it worked properly," says Alexander Azikov, IT Manager at Diamond Braces.

For all their complexity, however, the firm's firewalls couldn't filter HTTPS traffic, so Diamond Braces was left without any content filtering capability, unless it added it separately, which would only increase complexity and cost.

"We had people accessing malicious sites, often unintentionally via a typo or spam mail," says Azikov. "We needed the capability to warn them or block those sites. I was also looking to add IPS capabilities and I needed an integrated solution that could do it all with a single-pane-of-glass."

Applications such as Office 365 and the firm's patient management solution were mostly in the cloud, so fast, reliable cloud and office connectivity were vital. Large X-rays averaged 7MB each and the company made extensive use of cloud-based VoIP and videoconferencing, so hefty bandwidth and quality of service were also WAN requirements, as was backup connectivity in the event of service disruptions.

With Diamond Braces adding an average of 10 locations a year, quick deployment and easy, centralized management were also key capabilities that IT was not getting from its VPN's, fiber, and branch-based firewall appliances. "We really needed a scalable solution with unified security and management," says Azikov.

Diamond Braces Taps Cato for Simplicity and Security

Azikov had heard how SASE merges WAN and security in a single cloud-native solution and was pretty sure it was what he was looking for. He considered several vendors, but the only one that filled all the SASE requirements was Cato.

"One vendor had an excellent infrastructure, but very limited security, so we would have had to go to another vendor for content filtering, just like with our current solution," says Azikov. "Another vendor relied to a large extent on its endpoint security appliances, so it wouldn't relieve the complexity of our current appliance-based architecture."

Only Cato offered a completely integrated cloud-native SASE solution with a single management interface for WAN and security. It also had all of the required security functions–firewall, IPS, and content filtering. The only appliance to install was the Cato Socket, which was a cinch to configure and required no real management.

Cato connects all global enterprise network resources — including branch locations, mobile users, and physical and cloud datacenters — into a single secure, global, cloud-native network service. With all WAN and Internet traffic consolidated in the cloud, Cato applies a suite of robust security services to protect all traffic, including anti-malware, next generation firewall, content filtering, and IPS.

Connecting a location to Cato is just a matter of installing a simple preconfigured Cato Socket appliance, which links automatically to the nearest of Cato's more than 65 globally dispersed PoPs. At the local PoP, Cato provides an onramp to its global backbone and security services. The backbone is not only privately managed for zero packet loss and 5 9's uptime, it also has built in WAN optimization to dramatically improve throughput. Cato monitors network traffic and selects the optimum path for each packet across the Cato backbone. Mobile users run across the same backbone, benefiting from the same optimization features and improving remote access performance. Installing the Cato solution was incredibly fast and easy.

"We had a proof-of-concept stage, during which I was able to set up an office myself," says Azikov. "I just had to ask some questions about the best way to do certain things. After the first, I could set up locations without even thinking about it. It didn't take long to set up all 33 locations with 50 Mbits/s Cato connectivity. Once we had it all connected on a single Cato network, everything was so easy and reliable," says Azikov. "We can get by on 25 Mbits/s, but 50 made working very comfortable, and Cato's QOS made for very smooth video. For the central office, Azikov went for 75 Mbits/s.

Cato Brings Security, Reliability, and Easy Management

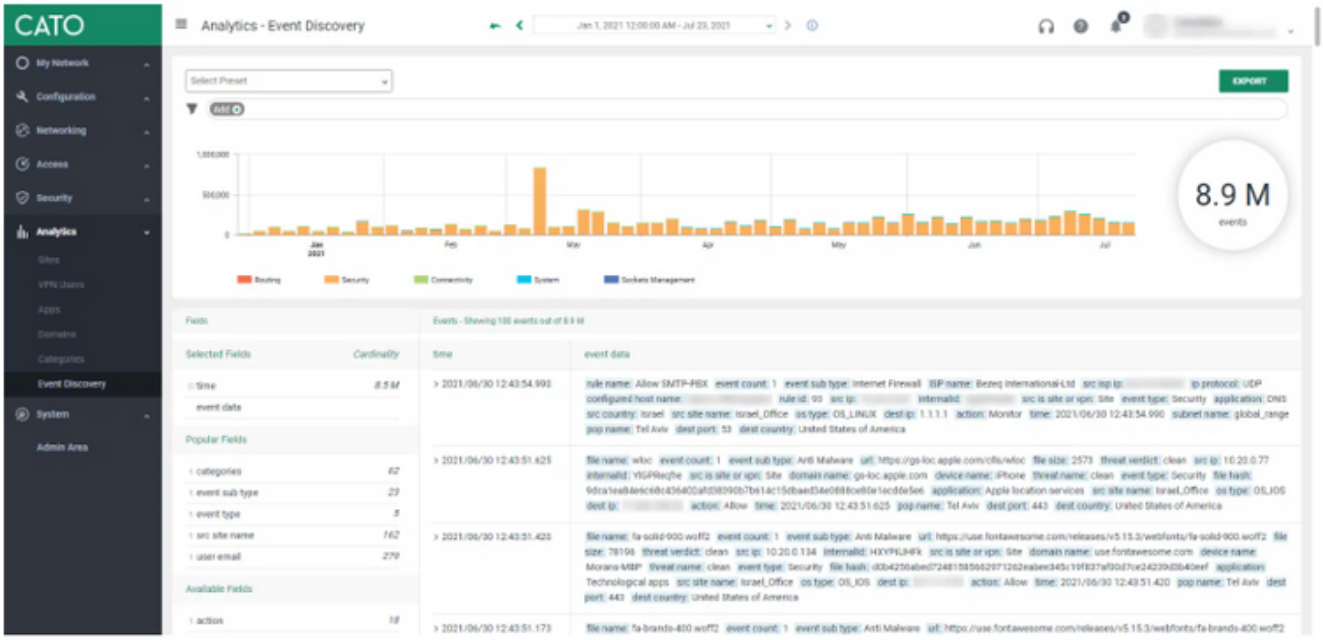
Azikov loves the simplicity and reliability of the Cato solution. "Cato's centralized management saves tons of time," says Azikov. "We troubleshoot issues so much faster. When you have everything in one place you can just switch back and forth and analyze different pieces of the puzzle. IT really ticks all the boxes for us."

With the original firewall solution, Azikov had to copy and paste text-based configuration information from one site appliance to another. Sometimes there were IP address mistakes, which led to hours of troubleshooting.

"With Cato it's all just plug and play," says Azikov. "We don't have to deal with all those IP issues. And when there's a provider issue, I can see it on the Cato interface immediately before employees call me and tell them we're using a backup connection and I'm already working with the provider to get things up again." With easy management, Azikov has more time to research new financial and

project management tools to improve the business.

Azikov's favorite Cato feature is Event Discovery. "I love the analytics Cato provides to help me troubleshoot issues and tweak the system for optimal performance," says Azikov. "Otherwise, I really wouldn't know what to change to make things better. This helps especially with QoS on the slower broadband and LTE backup connections."



With Cato's Event Discovery capability, Diamond Braces can harness detailed analytics to troubleshoot network issues and tweak the network for optimal performance.

In all, Cato has made business much smoother for Diamond Braces and management of WAN and security much easier for Azikov. Perhaps the best thing: "We have a lot fewer complaints from end users," says Azikov.

Alexander Azikov
IT Manager, Diamond Braces