

Appliance Elimination Makes Security Simple



Wayne Khan
Head of IT

Love, Bonito

Background

Love, Bonito is a fast-growing fashion and retail business in Singapore and the broader Southeast Asian region. A passion project started in 2008 by three teenagers, Love, Bonito started selling directly to customers online in 2010 and launched its flagship retail store in Kuala Lumpur in 2015. The company has three offices located in Singapore, with the main office in Singapore comprised of more than 50 employees, and an AWS instance.

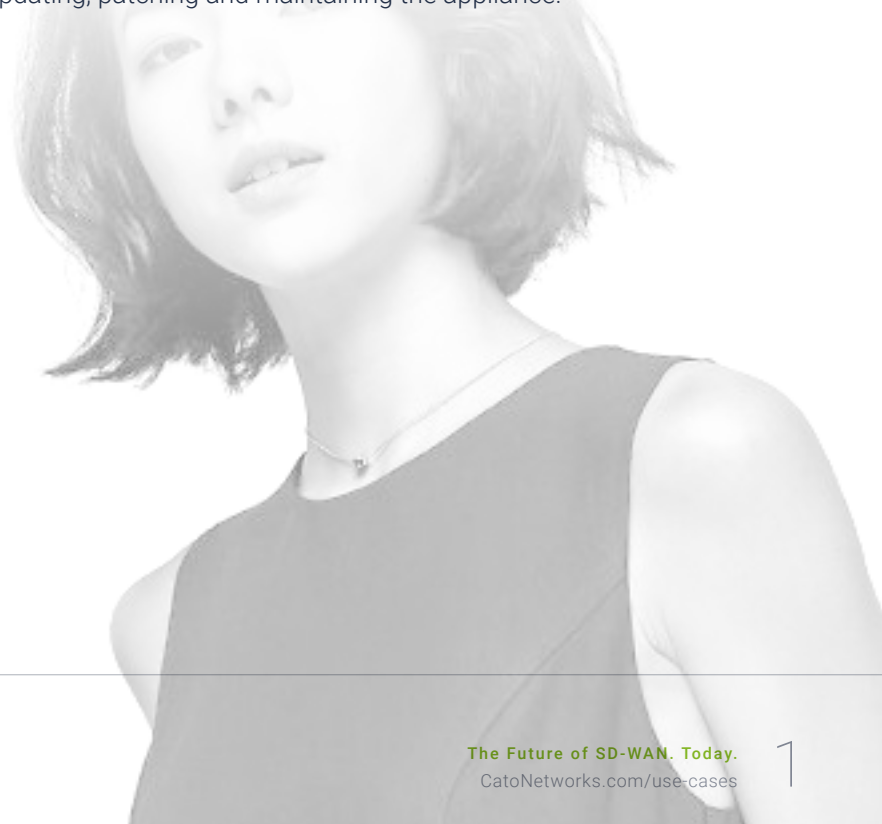
“I wanted to simplify our local infrastructure not make it more complicated. With a UTM, I would have been left updating, patching and maintaining the appliance.”

Challenge

Like many small companies, Love, Bonito relied on the Internet to connect its offices. And like many IT managers of small companies, Wayne Khan, Love, Bonito’s head of IT, found firewall appliances increasingly out of step with his organization. He needed a way to restrict access to recreational sites and protect home users. “The network perimeter is deprecated today,” he says, “We needed to a tool that respected this change.”

Khan considered purchasing Unified Threat Management (UTM) appliances and equipping users with virtual private network (VPN) access, but installing more security appliances didn’t align with his IT objectives.

“I wanted to simplify our local infrastructure not make it more complicated,” he says. “With UTM, I would have been left updating, patching and maintaining the appliance.”



Solution

He liked the simplicity of the Cato Cloud service and flexibility it gave him to activate what he wanted, when he wanted it and wherever he needed it. He could choose whether or not to activate Cato's security and networking services one location at a time, across all locations at once, or even client-by-client.

Khan decided to deploy the Cato Cloud, starting with his main site and his mobile users. He activated Cato's next generation firewall (NGFW), as well as URL filtering for all sites and users.

Every implementation has its own nuances and Love, Bonito is no exception. Khan needed to support a phased deployment, connecting the headquarters first to the Cato Cloud. He also knew he would still need to securely connect to the third-party's site running the company's ERP server.

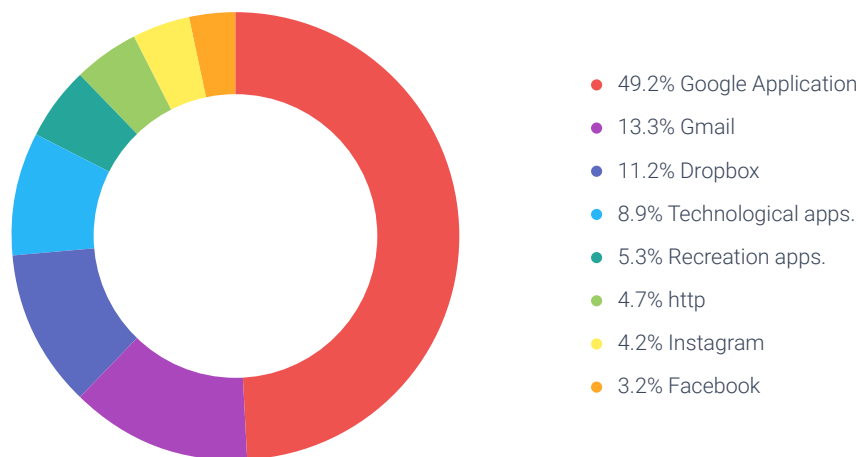
Khan kept Love, Bonito's existing firewall, splitting the outbound traffic with his router. ERP traffic is sent to

his firewall; all other traffic is sent to the Cato Socket, a small appliance connecting into the Cato Cloud network via an IPsec tunnel. Mobile and home users ran the Cato Client software to connect into the Cato Cloud.

With Cato in place, gone are the days when he had to be worried about what users were doing on the Internet. "Cato's URL filtering has made it much easier for us to express Love, Bonito's organizational posture on particular categories of content," Khan says, "We can block unacceptable sites, but prompt when our staff needs (or rather, demands) for their "fix" of Korean drama."

And now he can also offer secure access to corporate systems from anywhere. "The VPN functionality lets staff access our leave management system and other resources even from outside of the office, securely."

"Cato's VPN functionality lets staff access our leave management system and other resources even from outside of the office, securely."



The Cato Cloud gave Love, Bonito deep insight into the applications used by mobile and office users across the company backbone.

The Way Forward

Khan isn't finished yet. He plans to connect his AWS instance to the Cato Cloud this year and as for his firewall, "My goal is to simplify our local infrastructure by moving our ERP system into the cloud and eliminating the firewalled connection to the third-party location," he says

His experience with Cato support has been "excellent" he says. Strategically, Cato put him in a position to move forward with his simplification initiative. "Cato Networks helped us regain control over access to the network and made resources available to our staff."

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](https://twitter.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