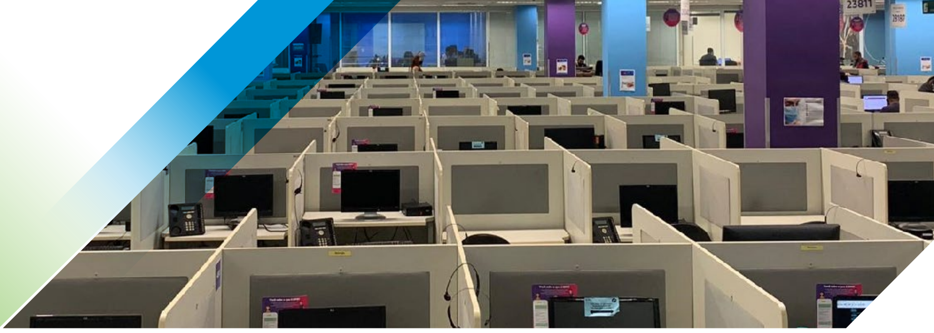
Customer
Case Study



LIQ Reinforces Security With VMware Carbon Black and VMware SASE

Pioneer in the all-line relationship approach in the country, LIQ integrates technology to deliver innovative solutions, bridging the entire journey between shoppers and brands. As one of the main leaders in the sector, it offers complete solutions to the market, with a presence in 90 percent of Brazilian states, more than 700 cities and around 13,000 points of sale.

Industry

Business Services

VMware footprint

- VMware Carbon Black®
- VMware Carbon Black Workload®
- VMware Carbon Black EDR®
- VMware SASE®
- VMware Cloud Web Security®
- VMware Secure Access®

With numerous ransomware attacks in Brazil last year, LIQ has witnessed some of its customers and service providers experiencing breaches. Security has always been a very important issue for the company, and knowing that the network structure was its main vulnerability, LIQ needed to focus on protecting endpoints. After talking to organizations that were directly impacted by ransomware attacks, the company received recommendations for using the solutions VMware Carbon Black, VMware SASE, VMware Cloud Web Security and VMware Secure Access. One month post-deployment, LIQ was able to identify around 30,000 incoming threats before they became attacks.

Delivering brand names closer to consumers

LIQ is the leading customer experience company in Brazil. With around 20,000 employees and 11 units spread across nine states in the country, the company registers more than one billion interactions per year, always working with the objective of bringing brands closer to their consumers. LIQ bets on a human perspective and on an all-line approach, which integrates retail, voice, chat, email and digital solutions to offer intelligent, dynamic and end-consumer-centric resources. Using modern and multichannel technologies as tools for the digital transformation of the consumer experience, the company has complete and integrated solutions in CRM, trade and live marketing and BPO. It also stands out for promoting diversity and having social inclusion as one of its main pillars.

> “We’ve always taken security seriously and we’ve never had a significant breach. But new threats emerge all the time and we need to make sure our security is strong enough to stop them.”
>
> Nicolas Ramirez, Director of Technology and Innovation, LIQ

LIQ REINFORCES SECURITY WITH VMWARE CARBON BLACK AND VMWARE SASE

Careful analysis identifies security breaches

LIQ employees are constantly transmitting and receiving data. The company also needs to comply with strict security regulations around data. Faced with the abrupt increase in the number of ransomware attacks in Brazil, the company saw that, without proper monitoring and security actions, this is a gateway to intrusions that could easily spread across the entire network. As a result, LIQ had to reassess its stance, as it was not fully confident that the existing tools it had would be enough.

To begin, the company decided to focus on endpoint protection—the main vulnerability. After talking to companies that were directly impacted by ransomware attacks to understand what they thought went wrong, VMware Carbon Black Workload and VMware Carbon Black EDR were recommended, and, after reviewing, LIQ was impressed.

LIQ implements VMware solutions to solve problems

In November 2021, after implementing Google Cloud VMware Engine solution, which generated great business results, LIQ contacted VMware to begin negotiations on security. Four months later, VMware Carbon Black, VMware Cloud Web Security and VMware Secure Access solutions were implemented. At the end of May 2022, the company already had the technologies deployed on more than 10,000 machines.

“We were looking for a unifying strategy that would provide a way to manage and secure all our cloud and on-premises environments with consistency, as well as being able to understand what is happening to reduce risk. We started with the EDR system, but we are also concerned with all the other layers, from the perimeter to the applications, APIs and data. Security threats can come from multiple sources, so we really need to protect everything. VMware is proving to be an excellent ally in this mission,” explains Nicolas Ramirez, director of technology and innovation at LIQ.

The company’s VMware SASE solutions work together to provide conditional access and data loss prevention, or DLP. Conditional access, part of a Zero Trust architecture, bases access to sensitive data on a user’s identity instead of whether they are inside or outside a network perimeter—making remote access much more secure. DLP is an important SASE feature that helps prevent data breaches.

“We were looking for a unifying strategy that would provide a way to manage and secure all our cloud and on-premises environments with consistency, as well as being able to understand what is happening to reduce risk. We started with the EDR system, but we are also concerned with all the other layers, from the perimeter to the applications, APIs and data. Security threats can come from multiple sources, so we really need to protect everything. VMware is proving to be an excellent ally in this mission.”

Nicolas Ramirez, Director of Technology and Innovation, LIQ

Vulnerability management at LIQ

In just one month with the new solutions operating, LIQ identified a significant advance in terms of the security of its business. VMware Carbon Black prevented more than 28,000 malware and identified 420 endpoints with critical vulnerabilities.

The future of network and cloud security convergence for LIQ

Now, LIQ is in the process of introducing VMware SASE into its business in order to achieve convergence between network and cloud security with simplicity, scalability and flexibility. Through this technology, combined with the VMware Carbon Black solution, the company will have an advanced Zero Trust architecture for the endpoints and workloads, being able to identify suspicious behavior and neutralize it before it affects the organization.