IDC
Analyze the Future

IDC CUSTOMER SPOTLIGHT

Liquid Web Tackles DDoS Challenges with Corero Solution

October 2016

Sponsored by Corero

Introduction

Liquid Web Inc. is a privately held managed web hosting and datacenter company founded in 1997. It operates three wholly owned datacenters in Lansing, Michigan, and a fourth location in Scottsdale, Arizona. The company fills a niche in the public cloud space focused on providing premium web hosting capabilities upmarket from traditional shared hosting. It currently has 25,000–30,000 customers and has been named one of the Inc. 5000 fastest-growing companies for the past 10 years. Liquid Web support teams are certified by Cisco and Red Hat and available onsite at each of the datacenters on a 24 x 7 basis. The company's 400 support engineers have specialties in technical support, server setup, database administration, advanced networking, security, migrations, system restoration, and other areas.

Solution Snapshot

Organization: Liquid Web Inc. is a privately held managed web hosting and datacenter company founded in 1997.

Operational challenge: DDoS attacks had become significantly more prevalent in and disruptive to the company's core business. The challenge was to arrive at a hybrid solution that included an existing product used for attack detection.

Benefits: Decreased incidence of DDoS attacks and improved customer satisfaction.

Over the past few years, Liquid Web found that distributed denial-of-service (DDoS) attacks had become significantly more prevalent in the public cloud space, thereby affecting its core business. These attacks could be either volumetric or nonvolumetric in nature. The company had an existing solution in place from a security provider that was used for attack detection. However, that solution was not doing enough to deal with mounting DDoS problems.

This IDC Customer Spotlight discusses how Liquid Web enhanced its overall security profile by partnering with Corero Network Security. Corero, based in Hudson, Massachusetts, provides real-time, high-performance DDoS defense solutions for service providers, hosting providers, and online enterprises. It employs technology that eliminates DDoS threats through automatic attack detection and mitigation, coupled with network visibility, analytics, and reporting.

Project Implementation

When DDoS attacks were made on the Liquid Web network, incidents needed to be identified, isolated, and mitigated. Before Liquid Web onboarded the Corero solution, such attacks were routinely detected but not prevented. Another challenge was that "innocent bystanders" (i.e., other customers on the network) could be impacted by a network slowdown even though they weren't the specific target of a DDoS attack. This was likely to occur if they were sharing the same switch or the same section of the datacenter.

A Hybrid Approach

The Liquid Web management team and IT team were concerned about the impact of these attacks on both larger and smaller customers. It seemed clear that the company needed to develop a more proactive approach to avoid customers having a poor overall experience with the services they subscribed to. Accordingly, the company started the process of looking at alternative DDoS security network implementations.

After a lengthy evaluation process, the IT implementation team opted for what is fast becoming a common approach: a hybrid scenario. The hybrid scenario involved keeping the company's existing on-premise solution, which had been traditionally used for detection. The plan was to add a Corero DDoS solution, which would be used in a complementary fashion by adding an automatic mitigation capability. This approach gave the company a multilayer DDoS mitigation strategy that prevented illicit traffic from entering the network while the existing solution continued to be used for detection and mitigation.

Avoiding False Positives

One of the key justifications for this approach was the avoidance of false positives. If traffic is blocked as a result of a false positive, customers will be irate. Establishing the right mix, therefore, is a key success factor for the company. For example, blocking traffic that shouldn't be blocked or not blocking enough illicit traffic is less than optimal.

During the trial period, the implementation team was convinced that it wasn't seeing false positives being blocked and there was a dramatic decrease in the malicious traffic that was getting through. This meant that the existing detection solution was more effective because the team was chasing fewer incidents — an unforeseen benefit in that it made the existing tool more effective because of increased focus. For example, if a hundred attacks were entering the network on a daily basis, the existing solution would chase each of them down and figure out which attacks were real or not real as well as what needed to be mitigated. If five attacks got through, the hybrid system prevented that traffic from even entering the network.

Implementation Approach

The entire implementation effort was led by the platform group, which consisted of datacenter, network, and security teams. The Corero product was trialed over a period of several months. The first implementation focused on a portion of Liquid Web's Lansing, Michigan, datacenter, which handles over 90% of the company's customer traffic. This effort involved installing the Corero appliance and border routers in the network on an inline basis and making sure that the configuration included the possibility of bypass mode.

While the other datacenters are considered important, the company had an acute focus on the Michigan resources. Once the trial was completed, the effort to extend the implementation to the rest of the Lansing datacenter was relatively easy. Subsequently, it took another three months to complete implementation in all of the datacenters, protecting more than 100G of Internet bandwidth.

Benefits

In the past, Liquid Web had experienced several large volumetric attacks that created collateral damage in the network environment, so the company was very pleased with the dramatic improvement seen in using the Corero service. In terms of metrics, the most critical improvement was the decrease in the outage minutes associated with large volumetric attacks. The concern was losing groups of customers during these outages prior to a solid hybrid DDoS solution being established. Multiple incidents in the past had raised this as a real possibility.

However, other ancillary benefits were realized as well. The 24 x 7 security operations team indicated that it needed more staff because of time spent processing so many security incidents. As a result of the Corero implementation and the ability to reduce the incidence of DDoS attacks, personnel could focus on other key aspects of customer-related security issues such as virus- and malware-related incidents.

In addition, Corero established a security operations center (SOC) support offering. This involved providing first-level support, monitoring attacks that were being blocked, and alerting the security team when events had occurred. Over the short term, the Liquid Web security team elected not to manage or monitor the traffic flow, but eventually it will take over this function from the Corero SOC team.

Challenges

The new approach represented a significant level of investment, and one of the challenges was internal cultural alignment concerning the new approach. So-called "religious wars" inside the IT group centered on the notion of whether prevention or detection should represent the approach best taken. However, there was a "breakthrough moment" for the company in that the team recognized that both functions could be combined in hybrid fashion, thereby optimizing the functionality of both solutions.

One aspect of the hybrid solution was the recognition of the customer impacts and calculating to the extent possible the true cost of disruption and customer churn. For example, large customers can become very unhappy when the performance they experience is impacted by a smaller customer. Several large customers strongly expressed their concerns about DDoS security issues, and this potential risk of lost business elevated management's level of interest in arriving at an effective solution.

Methodology

The project and company information contained in this document was obtained from multiple sources including information supplied by members of the Liquid Web technical support team and its partners, questions posed by IDC directly to Liquid Web employees, relevant corporate documents, and publicly available information.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com