SaaS Provider of Payment Processing Solutions Protects Business from DDoS Attacks with Arbor Edge Defense

HIGHLIGHTS

The Challenge

- Lack of visibility into ongoing volumetric and application layer attacks
- Existing security solution unable to mitigate or remediate attacks on the business

The Solution

- Arbor Edge Defense with Hardware Security Module

The Results

- Protecting availability to critical SaaS applications for their clients
- Providing visibility and mitigation capabilities reducing risks presented by inbound DDoS attacks & outbound malicious communications

Customer Profile

This global organization is a major provider of software as a service (SaaS) based solutions operating in cloud, for banking, payments and transactional documents, and other areas. Global companies depend on them for application solutions such as digital banking, cloud-based financial messaging, cyber and risk management, along with many other services. Their customers operate in the financial services, healthcare, insurance, and other industries that are highly security conscious. With almost a dozen datacenters around the world and office locations in North America, Europe, Asia, and the Middle East, a relatively small number of IT staff support essential business service offerings for their thousands of customers. For this SaaS provider, the network is the business, and thus any threat to availability of the online services can impact the financial concerns of its customers as well as future revenue.

The Challenge

The biggest challenge facing this organization was visibility into security threats attacking the business. As a payment processor and provider of financial transaction reconciliation, promptness in completing a request is an imperative. Anything impeding the availability of these services to their clients would be financially detrimental to both the clients and the SaaS provider, not to mention the reputation of the provider.

Despite investing in security tools such as a web application firewall (WAF), a DDoS attack impeded access to critical business services for almost half a day. Customers were unable to process payments or reconcile financial transactions while the attack was ongoing. Even though no actual breach occurred, the downtime and reputational damage from an attack had a significant financial impact on the business. Even worse, the existing tools that the security team was using had not helped them detect or mitigate the attack. They needed a new solution that could provide both visibility and counter measures.

Solution in Action

To more effectively protect their business, as well as their customers' business, this organization turned to Arbor Edge Defense (AED) from NETSCOUT®. This stateless packet processing engine functions as a network perimeter enforcement point, detecting and blocking both inbound cyber threats (e.g. DDoS attacks) and outbound malicious communications. Unlike their WAF which only protected web applications, AED protects all services inbound and outbound, providing best of breed DDoS protection and contextual threat intelligence. Essentially, AED delivers both the first and last line of perimeter defense for an organization.

Deploying AED was a complete game changer. Suddenly the IT team was able to both see and mitigate ongoing volumetric and application layer DDoS attacks that they had previously been blind to. They were able to detect both botnet and attack traffic as well as stop new DDoS attacks in their tracks. The ease of configuration and visibility into different types of threats made for quick time to value for this organization.

AED provided the IT team a unique view into the traffic on the network, due to the curated library of threat data it has access to through the ATLAS Threat Intelligence Feed. Armed with potentially millions of reputation-based Indicators of Compromise (IoC), AED could stop inbound IoCs in bulk, taking pressure off of stateful security devices such as the previously deployed WAF. AED was also able to block outbound communication from compromised internal devices to known bad sites on the internet – essentially acting as a last line of defense. Each time an outbound IoC was blocked, AED could provide more context related to the IoC, thus helping the security teams better determine risk and provide additional information for proactive use in other security tools.

The Results

For this customer-centric SaaS provider, protecting availability to critical applications for their clients can now be achieved as a result of their partnership with NETSCOUT. Their new AED deployment is providing much needed threat visibility and mitigation for the security team. Since implementing this powerful solution, they have gained visibility into ongoing volumetric and application layer attacks that was putting their business and that of their customers at risk. With their new improved visibility, they can now protect their end-users from threats thus mitigating business risks and protecting their bottom line.

LEARN MORE

For more information about NETSCOUT Retail Banking solutions visit

https://www.netscout.com/solutions/retail-banking

NETSCOUT®

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us