BrightCloud®
OpenText Security Solutions

CASE STUDY

BrightCloud Powers Citrix ADC and WAF with the Most Comprehensive IP Reputation Threat Intelligence

citrix®

AT A GLANCE

COMPANY
Citrix

INDUSTRY
Cloud computing, Virtualization, Computer software

PRODUCTS
BrightCloud Threat Intelligence (BCTI)

KEY FINDINGS

- Enables Citrix to integrate and deliver real-time IP address inspection to its customers
- Reduces threat risk by filtering unknown exploits
- Reduces inspection overhead such as CPU utilization

Partner Overview

Citrix provides server, application and desktop virtualization, networking, software as a service and cloud computing technologies to enable business productivity and continuity. Used by over 400,000 organizations, Citrix is a pioneer of remote access and collaboration, breaking the constraints of time, place, infrastructure, networks and devices.

Citrix's Application Delivery Controller (ADC) and Web Application Firewall (WAF) solutions provide comprehensive security for web apps and APIs both on premises and as a cloud service, enabling holistic and layered protection against known and zero-day application attacks. The solution keeps all application types secure across multi-cloud with a WAF, bot management, API security and DDoS protection to maintain a consistent security posture.

The Challenge

In order to deliver thorough application protection to customers, Citrix ADC inspects client requests for attack traffic. This requires processing power, which could require customers to devote large amounts of resources to handle the high level of usage and massive consumption of CPU resources. A more efficient way to accomplish this objective is to filter requests based on a fixed element – the IP address – which significantly speeds up inspection and protection.

However, the sources of attacks change constantly, making it unrealistic for customers to always maintain updated static lists. Citrix needed a comprehensive and dynamic threat intelligence source to identify problematic IP addresses. In addition, the threat intelligence needed to be reliable, simple to use and easy to integrate with Citrix's product to enable rapid identification of requests from known bad sources.

The Solution

After evaluating several threat intelligence vendors, Citrix selected BrightCloud® IP Reputation Service to augment its intelligent security systems. Specifically, the BrightCloud IP Reputation Service optimizes Citrix's WAF, by filtering IP requests that the system does not want to process, and allows it to reset, drop a request or even configure a responder policy to take a specific responder action.

The BrightCloud IP Reputation Service is bundled with Citrix's Premium edition at no additional charge to allow Citrix customers to quickly and simply filter out known bad requests, However, the application can be used with any function on the ADC, such as the WAF, bot management, Access Control List and responder. It can even conduct contextualized IP reputation analysis by incorporating elements like geolocations, time of the day, user group, user properties, user persona and more to regulate different actions such as dropping and limiting requests.

The BrightCloud IP Reputation Service is also used for forward proxy. For example, when users are going outbound to an IP address that is known to be infected, Citrix can block that user's access.

Citrix's research shows that BrightCloud's IP Reputation Service offers the most comprehensive database of known problematic IP addresses. In addition, BrightCloud's contextual mapping across different vectors such as file, domain and malware data, allows it to continuously update the IP reputation score and highlight typically less obvious connections to potential threat actors. Updating every five minutes, it provides the most up-to-date protection to Citrix's customers, with the ability to add additional inspection for decision making. Reliable, simple to use and easy to integrate, BrightCloud brings the best value to Citrix's customers.

Business Benefits of BrightCloud to Citrix

- No need to monitor the Internet for the IP address of bad actors
- Saves Citrix's customers from having to inspect requests from every single IP address to find well-crafted attacks
- Reduce inspection overhead such as CPU utilization and eliminate the need for expensive and bigger ADC/WAF boxes
- Decrease the amount of throughput and enhance performance for legitimate IP requests
- Lower the threat risk by filtering unknown exploits that otherwise might get through

Testimonials

"BrightCloud's IP Reputation data is comprehensive, dynamic and always up-to-date with the latest malicious IP addresses. It's flexible and easy to work with. It simplifies security with an all-inclusive license, so our customers have the security they need with granular control."

- Jason Poole, Director of Product Marketing, Application Security, Citrix

---

"Citrix's WAF embedded with BrightCloud® Threat Intelligence helps our customers reduce their risk exposure through granular, policy-based control for access to their web applications. Through BrightCloud's IP Reputation Service, the contextual insights coupled with the history across 4B+ IP enables us to deliver real-time protection to our customers."

- Jason Poole, Director of Product Marketing, Application Security, Citrix

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size. Discover more at BrightCloud.com.

BrightCloud®
OpenText Security Solutions