FireHost Receives Network Edge Protection with Radware's Attack Mitigation System

firehost™
SECURE CLOUD HOSTING

Business Need

As a leading secure cloud hosting provider, FireHost needed a solution to secure its network infrastructure and provide real-time attack protection of mission-critical systems for its clients.

Why Radware's Solution

Radware's Attack Mitigation System (AMS) offered rapid detection and mitigation of network attacks including denial-of-service (DoS), distributed-denial-of-service (DDoS), network and application-level flood and zero-day attacks.

Solution

Built with award winning products including DefensePro, Radware's AMS is a real-time network and application attack mitigation solution.

Benefits

The integration of Radware's AMS system provided FireHost customers solace regarding security, uptime, and performance of sensitive information.

Overview

Headquartered in Richardson, TX, FireHost specializes in protecting websites and applications of companies with compliance and high traffic needs, such as eCommerce, SaaS and healthcare IT providers. Since 2009, they have made hacker awareness, management and preventions a standard part of every customers secure cloud hosting environment. As a leader in secure cloud hosting, capable of protecting sensitive data and brand reputations of the world's enterprises, FireHost offers the most comprehensive fully managed cloud infrastructure-as-a-service (IaaS) available today, built specifically for the needs of companies governed by PCI and HIPAA compliance regulations. A reputation built on security and availability, FireHost provides services from Dallas, Phoenix, London and Amsterdam to some of the largest companies in the world.

"Radware's Attack Mitigation System fits perfectly within our secure cloud hosting architecture. The ability to stop a variety of multi-level attacks at the edge of our networks in North America and Europe empowers FireHost to provide the best protection in the industry"

- Chris Drake, Chief Executive Officer at FireHost

FireHost Challenges

As a cloud hosting provider, FireHost is responsible for protecting sensitive data and brand reputations for companies of all sizes, including many Fortune 50 organizations. FireHost customers handle sensitive information such as credit card numbers and personal identifiable information that needs to remain secure and available. As an organization, they are known for meeting high traffic and high availability requirements for SaaS application providers and online retailers. As FireHost began to search for a seller to replace its existing infrastructure, they pursued a vendor that met their customers' requirements for availability, performance, resiliency and security with scalable and cost-effective features that facilitate future growth.

The Solution

FireHost selected Radware's Attack Mitigation System (AMS), a real-time network and application attack mitigation solution that protects the application infrastructure against network and application downtime, application vulnerability exploitations, malware spread, information theft, web service attacks and web defacement. Complete with award-winning products such as DefensePro, a network security appliance, AMS secures FireHost network infrastructure and provides real-time attack protection of mission-critical systems for its clients.

Benefits

Upon deployment of Radware's AMS solution, FireHost received extremely rapid detection and mitigation of network and application attacks including denial of service (DoS), distributed denial of service (DDoS), network and application-level flood and zero-day attacks. This capability allows FireHost to provide continuous uptime to its clients, even when they are under heavy attack from hackers. FireHost clients, particularly those handling sensitive information such as credit card numbers and personal identifiable information, have received expert mitigation of known and emerging attack vectors. By integrating Radware into FireHost's network architecture, customers have achieved consolation regarding their security, uptime and performance.

CRP-FireHost-CS-01-2013/05 - US

radware