Gigamon

POSITIVE TECHNOLOGIES

Joint Solution Brief

Intelligent and Automatic Protection of Business Applications with Positive Technologies and Gigamon

The Challenge

Almost every modern enterprise uses hundreds of web, mobile or ERP applications to run operations. Often created in-house, these applications can contain security vulnerabilities – with nearly 70 percent of critical severity – that traditional security scanners cannot always detect.

Integrated Solution

Integrated with the Gigamon GigaSECURE Security Platform, the Positive Technologies Application Firewall (PT AF) proactively and continuously blocks attacks on web applications of all sizes and types, across a broad range of industries.

Joint Solution Benefits

- The GigaSECURE Security Delivery Platform inline bypass functionality supports failover protection and maintains traffic continuity for PT AF in the event of a network outage or tool failure.
- SSL decryption from the GigaSECURE Security Delivery Platform helps eliminate unnecessary processing by PT AF while enabling visibility into encrypted sessions.
- Filtering of relevant traffic to PT AF accelerates processing throughput and ensures analysis of only traffic that presents a security risk.

Introduction

According to the Verizon 2017 Data Breach Investigation Report (DBIR), attack patterns vary widely by industry. However, when including bot data, the top attack vector in 2017 remains the same as the previous year: non-secure web applications. Seventy-seven percent of breaches within this pattern were the targets of botnet activity, which uses strength in numbers to spew unwanted traffic at victims' infrastructure.

Often, web applications are developed in-house and contain vulnerabilities that predominantly stem from developer errors, which for several reasons, cannot always be detected by traditional security scanners, intrusion detection or prevention systems (IDS/IPS) or firewalls. For example, signature analysis becomes obsolete when attackers exploit zero-day vulnerabilities; and due to a deluge of "suspicious event" alerts, IDS/IPS systems lack the physical capacity to process and sort them to identify actual threats in real time.

Even well-known vulnerabilities cannot be fixed immediately. Patching code requires time, resources and sometimes even pausing of critical business processes. Moreover, for customized applications with unique vulnerabilities, adequate defense requires a thorough analysis of application structures, user interaction models and usage context.

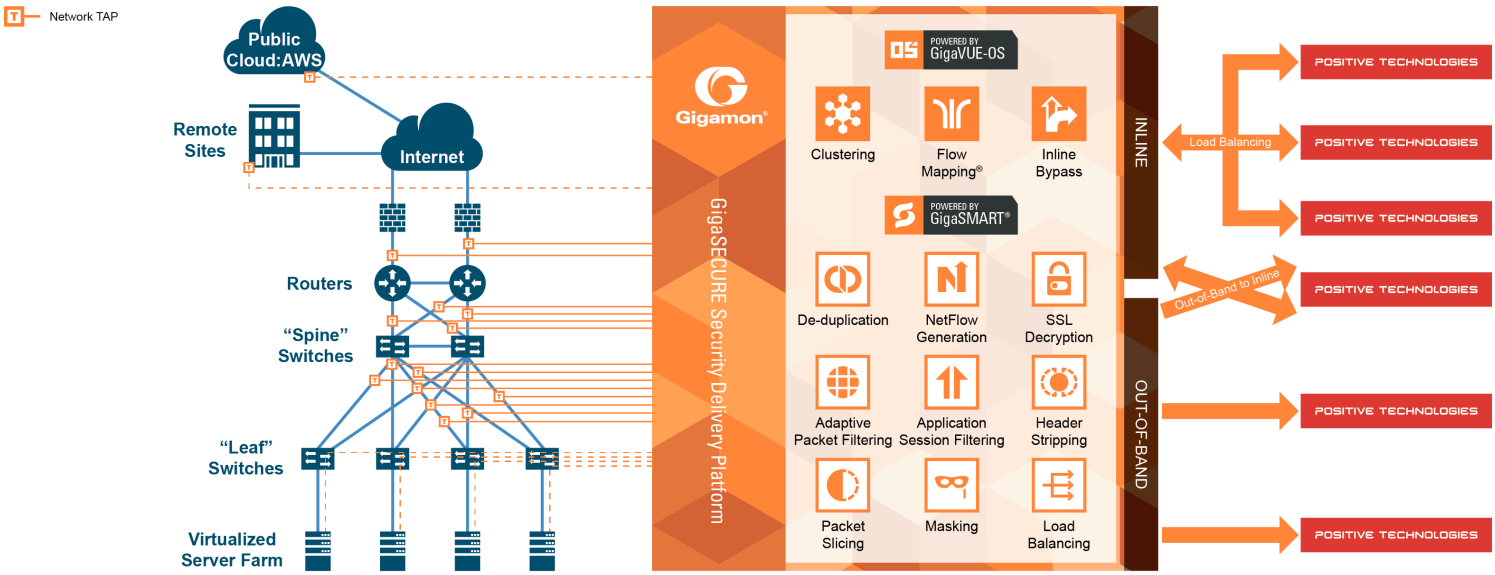
The Gigamon and Positive Technologies Joint Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform for greater traffic visibility, Positive Technologies Application Firewall (PT AF) helps organizations — no matter the industry — protect critical web applications and distinguish real attacks from normal application operations. The solution provides protection not only from all common vulnerabilities, but also zero-day attacks, client attacks, automated attacks and Layer 7 Distributed Denial of Service (DDoS) attacks.

PT AF combines powerful machine-learning techniques, smart event correlation mechanisms and advanced virtual patching to detect and counteract attacks and emerging threats with greater accuracy than other web applications firewalls (WAFs). Its behavior analysis capabilities help uncover suspicious user activity and prevent automated attacks — for example, scanning, brute force, DDoS, fraud, data leakage — on web portals and ERP systems, mobile and cloud applications, online financial services and industrial control systems. Moreover, by enforcing a secure software development lifecycle that automates vulnerability detection and mitigation in the early stages of development, the solution also helps avoid losses that can result from lingering vulnerabilities at the production stage.

[1]PT Application Firewall Product Brief, Positive Technologies Research, 2016.

© 2017 Gigamon. All rights reserved.



Key Gigamon solution features that augment the value of Positive Technologies deployments include:

Inline bypass for efficient and resilient deployment: The GigaSECURE Security Delivery Platform inline bypass functionality provides physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure. As required, any number of PT AF devices can be deployed to manage traffic — regardless of the speed and utilization of monitored network connections — or moved in and out of line at the touch of a button.

SSL decryption: Real-time SSL decryption integration increases traffic visibility for the PT AF solution. The Gigamon Visibility Fabric can be used to decrypt SSL encrypted traffic for inspection by security inline tools and then, if passed, re-encrypt the traffic for onward delivery. Decrypted traffic can also be sent to any other device connected out of band.

Traffic filtering: The GigaSECURE Security Delivery Platform sends specific traffic or sessions — for example, HTTP and HTTPs — to PT AFs so that the devices do not become overloaded with irrelevant traffic.

Easier control of asymmetric routing to ensure session information is kept together: Most security devices require all the packets in a session to be inspected by the same device as incomplete sessions risk being blocked. The GigaSECURE Security Delivery Platform provides an intelligent and efficient way to ensure this inspection happens in most architectures.

Learn More

For more information on the Positive Technologies and Gigamon solutions, contact:

POSITIVE TECHNOLOGIES
www.ptsecurity.com

Gigamon®
www.gigamon.com

© 2017 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

3236-01 07/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com