BROCADE

AT-A-GLANCE

Balancing Application Performance and Security

SUMMARY

As digital transformation creates new demands for IT, there is a growing tension between the need to protect applications and data and the need to deliver exceptional digital experiences to customers. Organizations need security solutions that assure reliable performance as well as protection.

Delivering Application Agility, Predictable Performance, and Security to Meet the Demands of Digital Commerce

Organizations seek to deploy more applications faster than ever before, but this can increase the risk of errors and the potential for security breaches. It also places new pressures on legacy systems that can threaten the stability of operations and digital services. Security remains high on the business agenda for organizations increasing their digital footprint, but legacy solutions can delay application deployment and slow testing, and are unable to provide the consistency of performance and robust security required in the face of new and changing threats. Security itself is becoming broader in scope as it now incorporates technologies such as the Internet of Things, biometrics, and cloud computing. All of these challenges require an integrated application security and protection approach designed for the business demands and technology of today.

But with security perceived as a bottleneck that can impede application responsiveness and business growth, there is a growing tension between the need to protect applications and data, and the need to deliver exceptional digital experiences to customers. In fact, 59 percent of business department decision makers admit they are more concerned about applications failing during peak usage periods than ensuring those applications are secure.[1]

A Need for Stability, Speed, and Security

Customers of digital services demand ease of use, speed, and security. With studies showing that customers will only wait a matter of seconds online before disengaging and moving to a competitor site, many organizations have focused on speed and availability. However, given the potential reputational damage and costs through penalties, loss of business, and remedial action of fixing a security breach, faster application development, deployment, and performance cannot be prioritized.

[1] "Why Smart Organizations Maximize Application Performance, 2016," *Vanson Bourne*, 2016.

87 percent of decision makers state that protecting applications from external attack will become more of a priority than user-related security breaches with the next few years.[2]

A quarter of organizations predict the number of applications they use will increase by more than 20 percent in the next few years. A complex matrix of in-house-built, off-the-shelf, and hybrid applications is standard in many organizations. The increasing rate of change, scale, and speed is placing developers and application vendors under extreme pressure. In this fast-paced and highly complex environment, flaws in code that may compromise security are probable and can take months to identify and fix. Patches may not be released and applied for weeks or more. This can leave applications vulnerable to attack, presenting attractive "open doors" to those seeking to gain entry and secure access to privileged or sensitive data.

Consistent Application Performance and Solid Security Requires a Virtual Solution

Traditional, appliance-based Web Application Firewalls (WAFs) provide some application protection, but are inefficient and cumbersome in todays' complex, multilayer IT environments, especially when used in cloud infrastructures. Limited policy management tools mean WAFs become bottlenecks, slowing data transfer and impacting application performance. Each WAF can only address the requirements of a single client application, requiring a significant investment in hardware and slow, manual application of upgrades and updates device by device. Deployment of new applications and ability-to-scale is curtailed by the level of manual programming and installation required. In addition, wherever security is not holistically addressed, updates, fixes, and patches may not be deployed systematically and this will create risk and weak spots in the overall environment.

20 percent of business departments globally rolled out applications without IT involvement, citing the need to bypass IT's security controls in order to function.[2]

Web Application Security for digital businesses and cloud-enabled IT environments must be easy to manage and cost-effective, while reducing or eliminating the need for manual management. A virtual Web Application Firewall (vWAF) can deliver the same resilience and protection as its hardware predecessors as well as offer these additional capabilities:

- **Massive scalability:** With its ability to dynamically scale across CPU, computer, server, rack, and data center boundaries, the vWAF can meet quickly changing and ever-increasing application demands.
- **Cross-platform portability:** Data centers becoming increasing virtualized, and a vWAF can accommodate and secure a hybrid environment of virtual and physical solutions.
- **Distributed and delegated management:** For efficiency and effectiveness, configurations should be tailored and granular with multi-administrator privileges. A vWAF's distributed management and automation makes policy update and patch deployment much easier, cascading changes across the entire environment in minutes rather than months.
- **Detection and protection:** A vWAF can test new policies in "detection-only" mode, providing full transparency to administrators and enabling them to identify the impact of policy changes and avoid false-positives. A vWAF's automated policy management provides immediate end-to-end protection while retaining control.
- **Application shielding:** Proactive security is critical to avoid breaches occurring. A vWAF's authentication framework consolidates applications under one management plan, reducing complexity while providing additional layers of security.
- **Full integration:** Security solutions must be layered to create strong protection at every level. A vWAF can interoperate with multiple systems and applications, extending its automation and security capabilities across multi-vendor systems.

Over half of decision makers state that the speed of identifying and resolving security problems when it comes to updating or deploying applications is "critically important".[2]

[2] "Why Smart Organizations Maximize Application Performance, 2016," *Vanson Bourne*, 2016.

Security and Performance with the Brocade Virtual Web Application Firewall

The Brocade® Virtual Web Application Firewall (Brocade vWAF) is a scalable solution for application-level security, providing intelligent protection against external attacks. As a virtual device, it can be easily scaled and optimized to provide the required level of protection and policy enforcement without impacting performance, removing bottlenecks from the network, and optimizing application availability. It supports both off-the-shelf solutions and complex custom applications, including third-party frameworks. It also integrates easily into any environment, including hybrid environments where virtual, physical, and cloud-based resources are in use.

The Brocade vWAF shields applications by inspecting and blocking attacks such as SQL injection and Cross-Site Scripting (XSS)—identified by the Open Web Application Security Project (OWASP) as among the top ten most critical Web application security risks—by applying business rules to online traffic. Its distributed and automated policy management ensures that all changes and fixes are deployed system-wide in real time, reducing any window of opportunity for attackers.

The Brocade vWAF also provides filtering of outgoing traffic to help to mask privileged information such as credit card data and personal information, supporting compliance with industry regulations such as PCI-DSS and HIPAA.

Learn more about Brocade virtual Web application solutions at www.brocade.com/appsec.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE