radware

Financial Services & Web Application Security:

Taking Stock of Application-Layer Security Threats

The financial services industry is, by its very nature, inherently risk adverse. The sheer volume of transactional data moving through networks can be staggering and protecting that data from cyber-threats is strategically and fiscally critical. To understand how financial service executives keep their most prized applications secure, Radware surveyed over 600 chief information security officers (CISOs) and other security leaders across financial services, retail and healthcare industries. This article provides an overview of key findings from Radware's web application security report: *Web Application Security in a Digitally Connected World*.

This emphasis on security and control within the financial services industry is supported by the fact that most surveyed financial service companies have more security controls in place around their applications than counterparts in the retail or healthcare industry (see Figure 1).

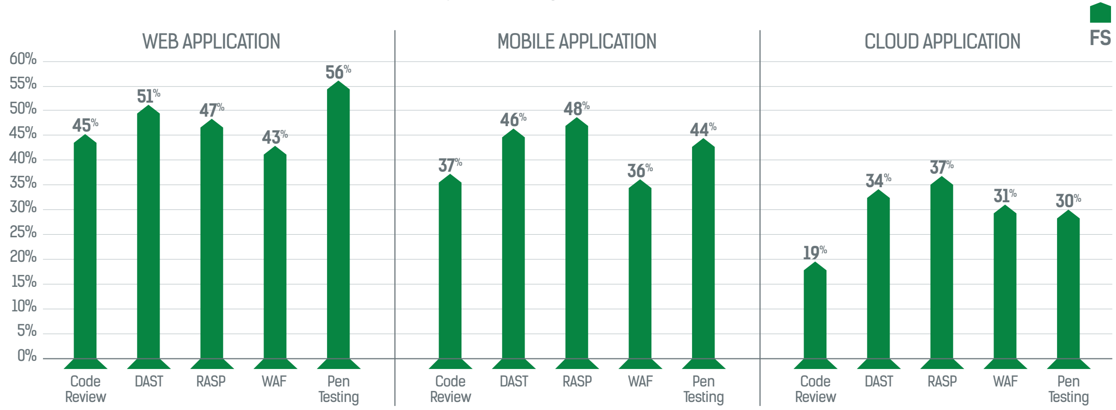


Figure 1: Frequently used security controls

Even with more security controls and investment in place than other industry sectors, recent global geopolitical, economic and technological disruptions continue to have transformative impact on how financial services address and mitigate risk.

- The emergence of cryptocurrencies and blockchain is revolutionizing transactions and interactions throughout the global financial community and resulting in new financial technology players that challenge the entire financial landscape as we know it.
- The digitization of the financial services market empowers consumers and institutional clients, altering the way financial services companies communicate and conduct business. Third-party mobile payment vendors such as Venmo, ApplePay and PayPal adds levels of sophistication and multiple touchpoints that increases the potential for significant threats and attacks.

As financial services institutions address these critical business and technological challenges, they also must fortify their institutions from the onslaught of potential threats. Over the past 12 months, 35% of respondents have experienced Brute Force attacks, 27% Web scraping attacks and 45% data security breaches. They must also address the growing threat of Layer 7 DDoS attacks as 64% find them most difficult to prevent, detect and contain while more than 65% lack confidence they could mitigate such an attack on the application layer.

So where does that leave the financial services sector? Security executives and influencers (from five continents) who responded to the survey collectively lack the confidence they can detect, mitigate and contain security threats. Here are key reasons this crisis of security confidence exists for our financial services survey respondents.

CONFIDENCE AND MITIGATING RISK

From a detailed analysis of survey results, financial services institutions are concerned they have the necessary security framework in place to successfully mitigate or protect their applications from a variety of potential application-layer threats. Only 40% feel strongly that they can safeguard customers' financial data and payment records while nearly half do not analyze API vulnerabilities prior to integration.

> Though nearly 60% of network traffic is generated by bots, only 25% of all financial services responders felt with certainty they could distinguish between good and bad bots.

THE AUTOMATED SECURITY AND CODE TESTING GAP

Statistical evidence from the survey demonstrates that the accelerated rate of application delivery and changes, coupled with emerging technologies, causes security gaps and instabilities, negatively impacting the way internal organizations as well as third parties share data. Only 33% of financial services security executives and their teams are aware of frequent changes made by in-house applications and APIs within the software development environment, while only 41% are able to track data with third parties after the data leaves the corporate network.

The security vulnerabilities and threats that increase from these process fractures could be addressed by automated security solutions and code testing. However, only 19% are using API gateways, 25% WAFs and only 36% are using both while only 25% of respondents made significant investment in security controls following an industry-wide security breach.

Even though nearly 75% share username and passwords and 50% payment details via APIs with third parties, only 53% use encryption when exposing data to third-party APIs and less than half of respondents require authentication from thirty-party APIs or who use a single sign-on (SSO) solution. Without tighter security controls and protocols, financial services institutions, which have large multinational ecosystems of partners, are open to hacks, threats and attacks that can have millions of dollars in financial, productivity and brand loss.

BEST PRACTICES IN APPLICATION SECURITY

To take the critical steps toward a more secure future, first start with a security gap assessment, identifying and analyzing where risks exist in processes, systems and security tools. This should include WAF requirements and maintenance, frequency of policy and signature updates across all security devices and the ability to distinguish between good and bad bots.

Determine how to augment existing tools, skills and capabilities with industry-leading security solutions that have demonstrable results in mitigating attacks from emerging technologies. Ensure that security and application development teams have a real-time communications methodology to minimize threats to mobile, Web and third-party applications. Finally, develop a realistic budget that ties security investment to quantifiable ROI but also accounts for emerging threats and new technologies.

During this process, keep in mind that WAF technology is central to application security. Businesses require a next-generation WAF that is flexible enough to adapt to changing IT infrastructures and the evolving threat landscape and change based on the needs of the business. Here are seven characteristics to look for when considering a WAF offering.

1. **Agility Equals Security Risks** – DevOps and agile development practices are great at creating new applications quickly and efficiently. Unfortunately, the fluidity of these environments also creates a bevy of unintended security risks. Ensure any WAF solution can automatically detect and protect applications as they are added to the network by automatically creating new policies and procedures.

2. **Cover That Top Ten List** – Industry pundits and experts at security consortiums and communities continue to categorize and identify the greatest Web application security risks facing organizations. A WAF solution should provide complete coverage, including all OWASP Top 10 risks.

3. **Device Fingerprinting** – Bots, crawlers and spammers, using new techniques to disguise malicious traffic, can exhaust resources and scrape sensitive information from websites or cloud-based assets. A good WAF needs to sniff out these clandestine cyber assaulters. Device fingerprinting identifies, blacklists and blocks machines used for attacks regardless of the IP they hide behind. Even if the bot dynamically changes its source IP address, its device fingerprint does not change.

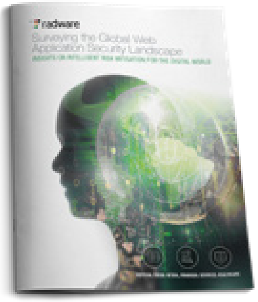
4. **Negative + Positive = Zero-Day Protection** – Advanced application and "smoke screen" attacks that use DDoS assaults to mask other tactics are becoming commonplace, while zero-day assaults swiftly exploit newly discovered vulnerabilities. Negative and positive security models that automatically detect application domains, analyze potential vulnerabilities, and assign optimal protection policies are critical.

5. **Who's Knocking at the Door?** – Enforcing Web access control policies and security procedures is a bread and butter function of any WAF. How to do it is where the devil is in the detail. Ensure any WAF offering supports user authentication and single sign-on (SSO) functions. This applies two-factor authentication and enables access to premise-based applications from outside the enterprise network. In addition, it ensures access to data based on a user's role/business needs.

6. **Two Minds Are Better Than One** – Cyber-attacks are increasing in severity and complexity, making it difficult for organizations to stay ahead of the rapidly evolving threat landscape. To assist, a WAF vendor should provide options for fully managed services for both on-premises and cloud-based WAF deployments. This provides the organization with the insight and expertise from security experts that can assume full responsibility to configure and update security policies as well as actively monitor, detect, alert and mitigate attacks in real time.

7. **Protection Via Unification** – Leading analysts agree that the best WAF solution is one that provides both on-premises and cloud-based offerings. It provides a unified solution that ensures complete availability and protection with no security gaps between on-premises and Web applications, and facilitates quick and easy migration of applications to the cloud.

In conclusion, ensure that any WAF solution your organization is evaluating covers these critical security solution fundamentals - complete OWASP Top 10 vulnerabilities, effective API security, HTTP DDoS mitigation. By evaluating existing security processes, systems and security tools, and implementing application security solutions and practices that augment and enhance these capabilities, organizations will build the foundation for an application-secure infrastructure.



DOWNLOAD ***Web Application Security in a Digitally Connected World***

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.