radware

Web Application Security in a Digitally Connected World

VERTICAL FOCUS: RETAIL, FINANCIAL SERVICES, HEALTHCARE

Table of Contents

Global organizations stand on a cyber-security precipice. Emerging technologies such as blockchain, artificial intelligence (AI) and Internet of Things (IoT), along with the explosive volume of mobile, Web and cloud apps creates uncharted, highly lucrative pathways to revenue generation, optimized productivity and enhanced brand value. At the same time, the speed and sophistication inherent in these technological advances exposes application vulnerabilities, security risks and skills deficiencies. These compromise compromise sensitive company and customer data, devalue the brand and severely impact financial performance.

The conundrum for any organization is how to take the leap toward these new technologies that help break down the barriers to consumer engagement and deliver substantial economic reward while successfully protecting corporate assets, intellectual property (IP) and personal customer information.

About the Research

Radware, in conjunction with Ponemon Research, surveyed over 600 chief information security officers (CISOs) and other security leaders across six continents. The intent was to uncover the challenges that these new technologies and rapid-fire application deployments are presenting, ascertain how organizations in different industries identified application-layer and API vulnerabilities, measure the impact that bots are having on organizations, how companies combat application-layer attacks (like those listed in the OWASP Top 10) and construct a security roadmap for today and tomorrow. Radware also sought to understand how the exponential number of security breaches against the application layer (such as the recent Equifax attack) would alter the financial and operational actions these companies would take.

Key Findings

- Sixty-eight percent of organizations admit low confidence in information security posture. They also admit they can't assure 24/7/365 availability, and about two-thirds (68%) have not yet integrated security into their DevOps.
- Organizations often leave sensitive data under-protected. Forty-five percent report they suffered a data breach while 52% do not inspect traffic being transferred to and from APIs. Fifty-six percent do not have the ability to track data once it leaves the company.
- Bot traffic represents more than half (52%) the amount of Internet traffic, exceeding 75% of the total traffic among some organizations. Forty-nine percent of all bot traffic is bad bots, yet 33% of organizations cannot distinguish between good and bad bots.
- API security is often overlooked. While 60% both share and consume data via APIs, including personally identifiable information, usernames/passwords, payment details, medical records, etc., 52% don't inspect the data that is being transferred via APIs and 51% don't perform any security audits or analyze API vulnerabilities prior to integration.
- Application-layer DDoS is a greater fear than network-level DDoS assaults. Only 33% feel confident they can mitigate application-layer attacks compared to 50% that feel confident they can protect against network-layer DDoS attacks.
- Seven out of ten businesses (72%) are not fully aware of the frequent change made to in-house applications and APIs within their organizations' software development environment.
- Forty percent of respondents claim their organization updates applications at least once per week, posing a great challenge for organizations.
- Everyone wants the speed and agility that continuous delivery provides but few feel they can achieve it securely. Half (49%) currently use the continuous delivery of application services and another 21% plan to adopt it within the next 12-24 months. However, 62% reckon it increases the attack surface and approximately half say that they don't integrate security into their continuous delivery process.
- Less than a year prior to the due date (May, 2018) for General Data Protection Regulations (GDPR) compliance, 68% of organizations are not confident they will be ready to meet these requirements in time.

CONUNDRUM #1

The Confidence Crisis: Protecting Applications Against Data Theft and Bot Attacks

As the rate and number of new technologies materialize at an accelerated pace, many security professionals face the unprecedented challenge of mitigating a wide swath of threats and attacks that often are byproducts of the evolving IT landscape. Existing security strategies, plans and measures may not measure up to quickly developed malware, floods and other threats. The result is a "crisis of confidence" that can overwhelm skills, deplete budget and resources, chip away at brand equity and fracture customer/partner relationships.

Take the recent Equifax breach[1], which exposed over 145 million individuals and their personal information because of a Web application vulnerability. While there may have been governance and accountability plans in place, there may have been other actions, such as a Web Application Firewall (WAF), which could have mitigated such a massive attack had it been updated properly against known vulnerabilities. A simple question may have been: did the company have the confidence they could protect against a probability of attack or was false confidence in the "impossibility" of such an attack their strategic approach?

The survey suggests companies are not prepared to meet these new challenges and pay an unknown price for it. Nearly 40% of respondents indicate that security issues and concerns frequently delay application delivery while 62% lack or have no confidence they can rapidly adopt security patches and updates without compromising operational performance (see Figure 1).

Periods of high demand represent major revenue opportunities for organizations. In extreme cases, like the retails industry, 20 percent[2] of their annual income can be earned over the holidays. Therefore it is crucial for them to be able to deliver optimal service in peak periods as every fraction of a second converts to revenue. Surveyed respondents see a large security gap around protecting sensitive data. In fact, 68% of retailers lack certainty they could secure credit card data during peak demand periods while 73% of those in healthcare maintain low confidence they can safeguard patients' medical records. 60% of financial services companies lack certainty they can safeguard customers financial data and payment records.

1 Source: New York Times https://www.nytimes.com/2017/10/02/business/equifax-breach.html
2 Source: National Retail Federation https://nrf.com/resources/holiday-headquarters/holiday-faqs

How confident are you that your organization is protected against each one of the below-mentioned attacks? (See Figure 2 for list)

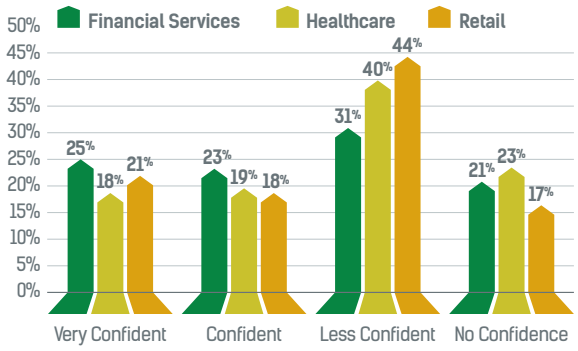

Figure 1: Confidence levels

As Figure 2 statistics indicate, nearly half of respondents have had a data security breach over the past 12 months despite the barricades they use. In addition, 36% of respondents have experienced a Brute Force attack against a Web application - an attack vector that some Web application firewalls in the market today do not fully cover. The growing prevalence of attacks is a known fact, thus the more alarming finding is the uncertainty within these companies that they could even detect, prevent or contain these attacks, especially when it comes to emerging threats such as Layer 7 DDoS attacks. Research shows that 64% of financial services institutions, 62% of healthcare organizations and 58% of retailers acknowledge the difficulty in mitigating Layer 7 DDoS attacks (see Figure 3). In fact, 57% feel similarly about encrypted Web attacks and nearly half about API manipulation (see Figure 4).

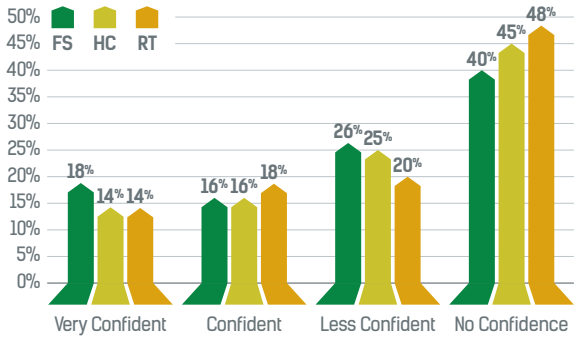

Figure 3: Application-layer DDoS mitigation confidence levels

Everyone suffers attacks

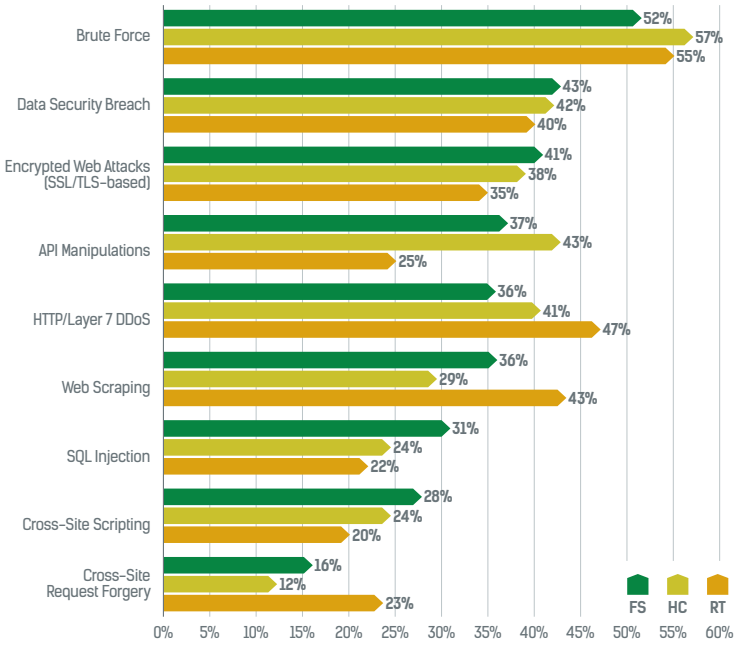

Figure 2: Application and/or Web server attack frequency

Application-Layer DDoS Mitigation

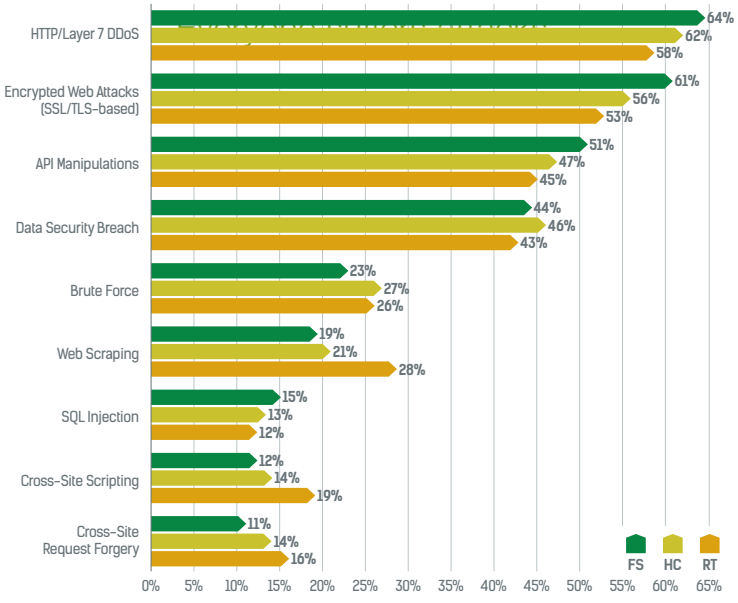

Figure 4: Top most difficult attacks to mitigate

BOT ATTACKS

Automated attack programs, such as 'bad' bots, are the main force behind the majority of the attack landscape today. In fact, bots conduct more than half of all Internet traffic flow. For some organizations, bots represent more than 75% of their total traffic. This is a significant finding considering only one in three (33%) organizations cannot distinguish between good bots and bad ones. Good bots serve critical functions, such as price aggregators to customer service chatbots and search engine spiders. However, for every good bot in the world, there is a bad bot wreaking havoc.

Bots make traditional attack vectors more effective, faster and larger than anything humans can accomplish on their own. Let's examine how many of the application-layer threats and attack types are conducted by bots vs humans.

Completely Bot Driven:

- Web scraping
- Web Application DDoS
- Encrypted (SSL/TLS) Infrastructure and Layer 7 DDoS
- Brute Force

Human Orchestrated/Bot Assisted:

- API Manipulations (primarily a manual process with certain functions automated by bots)
- SQL Injections (in some cases require human direction to be successful)
- Cross-site scripting (requires manual intervention but uses bots to automate much of the attack process)
- Cross-site request forgery (same as cross scripting)

This presents a major challenge for most organizations, whom depend upon traditional detection methods to identify them (see Figure 5). However, bot intelligence has far exceeded many of these tools and it can easily bypass systems like Captcha. Ticketmaster[3] recently experienced this as Web-scraping bots bypassed their Captcha security to purchase all available seats for the popular Broadway play, Hamilton. Therefore, organizations should consider a combination of several techniques designed to determine if their traffic is coming from a human or a bot. By using many techniques like fingerprinting, Captcha, IP-rate based detection, in-session detection and termination, Javascript challenges and dedicated anti-bot solutions, organizations can fortify Web applications exponentially.

What techniques do you use to distinguish between a real user and a bot?	Web Applications	Mobile Applications
IP Rate-Based Detection	49%	46%
In Session Detection and Termination	46%	43%
Captcha	31%	22%
Dedicated Anti-Bot/Anti-Scraping Solution	20%	10%

Figure 5 – Techniques used to distinguish between a real user and a bot

3 Source: IGN http://www.ign.com/articles/2017/10/03/bots-bought-30000-hamilton-tickets-alleges-ticketmaster

DATA LEAKAGE: EVERYONE'S GREATEST FEAR

Data leakage was one of the primary concerns across all of the industries we surveyed.

- Forty-five percent of respondents report that they suffered a data breach, including 45% in the financial services sector, 45% in retail and 46% in healthcare.
- More than 60% are not confident that they can quickly detect application-layer attacks, including 59% in financial services, 67% in retail and 67% in healthcare.
- More than 60% are not confident that their organizations are protected against application-layer attacks, including 52% in financial services, 61% in retail and 63% in healthcare.
- More than 70% are not confident their organization can protect itself against an application-layer DDoS attack, including 66% in financial services, 68% in retail and 70% in healthcare
- Nearly 60% of respondents do not track sensitive data they share with third parties once the data leaves the corporate network.

Even though a 2017 IDC research[4] report indicates global organizations will spend over $100 billion on security hardware, software and services by 2020 (an annual CAGR of 8.3%), Radware's research found that even with security breaches costing millions in productivity and revenue losses, only 40% of respondents made nominal to no investment in increasing security controls following high profile cyber-attacks.

4 Source: IDC https://www.idc.com/getdoc.jsp?containerId=prUS41851116

CONUNDRUM #2

The Continuous Delivery Security Challenge

Organizations are looking for ways to optimize the deployment of application services. Many try to fully automate the cycle of application development, QA, testing, modifying and deploying in staging, and the production environment in what is known as continuous delivery. A successful continuous delivery implementation can yield a competitive edge and save operational expenses. For some of the more dynamic application services, the fast pace is critical as they are required to deploy multiple versions into production per day. The challenge, on the other hand, is to ensure accurate application security throughout the process, as almost two-thirds (62%) believe it increases the attack surface.

Radware's research shows that continuous delivery is high priority for many organizations with half of respondents currently using this approach and another 20% planning to do so within the next two years. Because continuous delivery requires accelerating the pace of application development, changes, fixes, etc., there are inherent exposure points that hamper risk and threat mitigation. Even with sustainable and secure methodologies and processes in place, the new exponential growth in digital touchpoints (Web, cloud, mobile) coupled with applications being developed by both IT and lines of business, may result in major security schisms that spell disaster without automated code reviews and security practices in place. This is especially problematic when business lines do not implement automated testing tools and protocols.

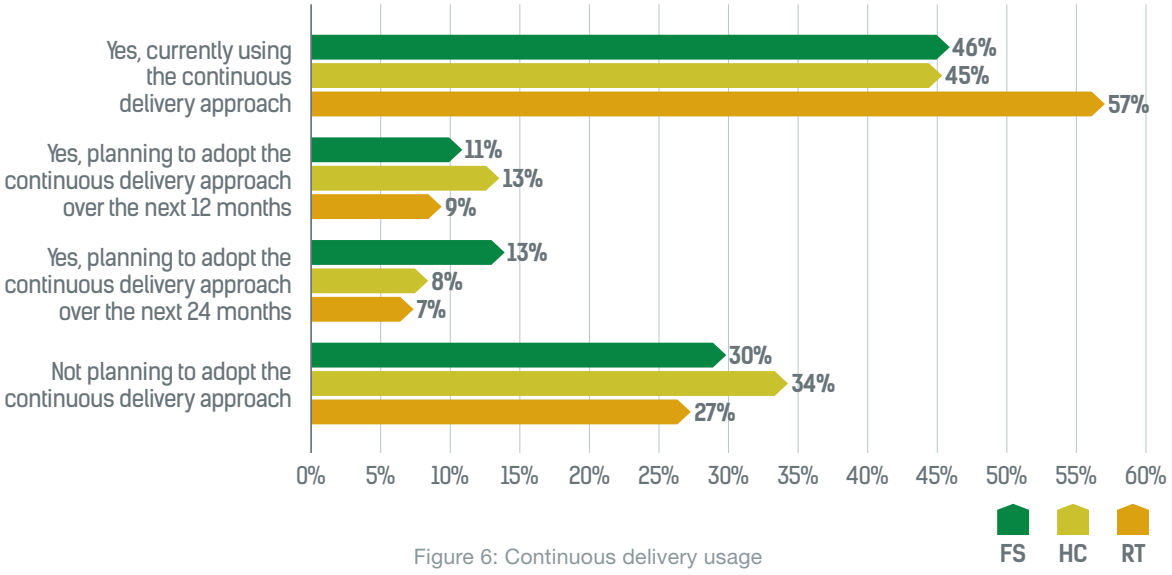

Figure 6: Continuous delivery usage

Radware research indicates security executives and other experts understand the impact continuous delivery is having on their organizations. While sixty-two percent believe continuous delivery increases the attack surface, risks and vulnerabilities, only 25% are confident that security is integrated with continuous delivery of in-house, Web or cloud.

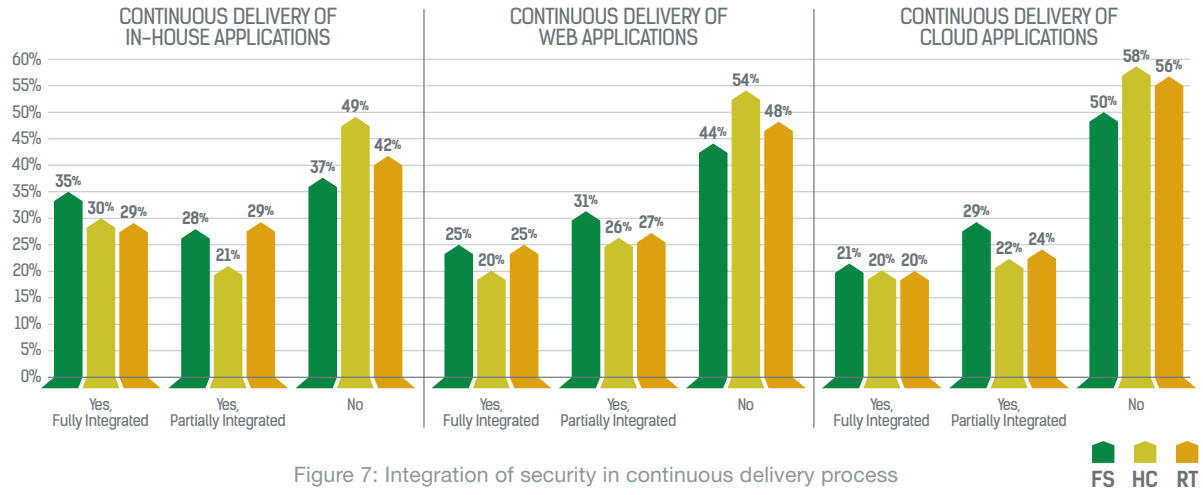

Figure 7: Integration of security in continuous delivery process

MOBILE SECURITY

Nearly 25% of mobile applications undergo changes daily, if not hourly, while nearly half of all mobile applications for financial services undergo change in under a week's time. This exponentially increases the continuous delivery security conundrum as it amplifies the volume of changes moving through an organization (see Figure 7).

		Web	Mobile	Difference
Bot Detection	Captcha	31	22	-9%
	IP Reputation limit	49	46	-3%
	Dedicated anti bot solution	20	10	-10%
	In session termination	46	43	-3%
Apps Undergo Changes	Hourly	3	6	+3%
	Daily	7	18	+11%
	Weekly	14	17	+3%
	Monthly	28	24	-4%
	More / other	48	35	-13%
Security Controls	Code review	38	30	-8%
	DAST	45	41	-4%
	RASP	44	42	-2%
	WAF	41	37	-4%
	Pen Test	52	29	-13%

Figure 8: Variance between mobile and Web application detection and security

The ideal continuous delivery implementation is fully automated, efficient and quick. While this is the primary goal of DevOps teams, sometimes a conflict arises around information security holes that may remain unpatched, as automatic testing tools do not provide hermetic protection against application exploits. So it happens that conflicts might rise between application and IT security teams that care primarily to identify and maintain security in such rapidly changing environments. This gap creates increased exposure for organizations to potential attacks (see Figure 8).

Additionally, these threats are significant and potentially catastrophic as many organizations use limited security tools with only 20% using only API gateways, 23% using just WAFs and only 32% using both. In fact, less than half of all organizations analyze API vulnerabilities prior to integration and greater than 50% inspect data that is being transferred or returned via APIs.

...less than half of all organizations analyze API vulnerabilities prior to integration and greater than 50% inspect data that is being transferred or returned via APIs.

This lack of automated security and vulnerability testing is especially troubling as many of these organizations are required to comply with critical governmental and industry-led standards and regulations, as in the case with HIPAA (Healthcare) and PCI (Retail and Financial Services) where more than 75% of corresponding respondents indicate they must be in compliance. Even with these high levels of compliance (which usually determine how to deal with and protect sensitive information), nearly 60% of respondents do not track sensitive data they share with third parties once the data leaves the corporate network (see Figure 9).

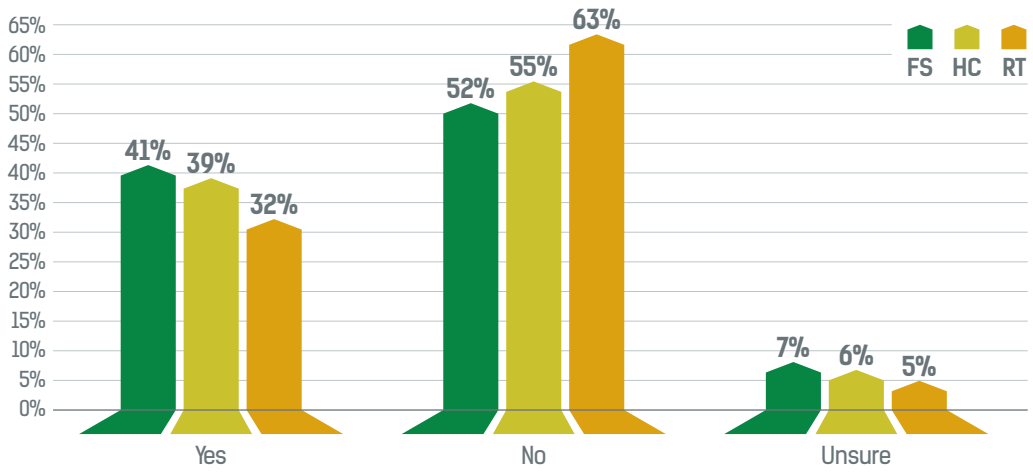

Figure 9: Does your organization have the ability to track the data shared with third parties after it leaves the corporate network?

For continuous delivery/development to be truly effective, security services should be fully integrated into and automated through the DevOps chain[5]. In the case of WAFs, integrating into the chain is too cumbersome. Hence, the best way to address this issue is with an adaptive, positive security model

APIs

An Application Programming Interface (API) is a set of tools and protocols used to develop application software. This interface is a predefined request–response messaging system that exposes reliable content and operation negotiation (typically expressed in JSON or XML).

Publicly available APIs allow sharing of content and data openly between communities and applications. DevOp environments, with the ever-increasing demand for continuous delivery, requires complete process automation utilizing APIs across the board. API vulnerabilities are hard to monitor and do not stand out.

Traditional application security assessment tools do not work well with APIs, leaving Web services such as APIs vulnerable to various types of attacks and abuse of Web applications, such as access violations, code and protocol manipulations, injections, overload (in message size or volume) and data exfiltration. These threats are significant and potentially catastrophic as many organizations use limited security tools with only 20% using only API gateways, 23% using only WAFs and 32% leveraging both. In fact, less than half of all organizations analyze API vulnerabilities prior to integration and greater than 50% inspect data that is being transferred or returned via APIs. Fifty-two percent do not inspect traffic being transferred to and from APIs.

APIs are often overlooked by organizations. While 60% both share and consume data via APIs, including personally identifiable information, usernames/passwords, payment details, medical records, etc., 52% don't inspect the data that is being transferred back and forth via their APIs and 51% don't perform any security audit or analyze API vulnerabilities prior to integration. Fifty-seven percent feel they have no answer to API manipulations.

5 Source: Radware Blog https://blog.radware.com/security/2017/01/devsecops-continuous-security-delivery/

CONUNDRUM #3
GDPR Preparedness Effect

Organizations around the world that do business in or with the European Union (EU) will soon need to meet stricter data privacy laws with the GDPR taking effect in May, 2018. Any organization that offers goods or services to EU residents, monitors personal behavior or processes or handles personal data of EU residents will be impacted by this law. Those who do abide by the regulation will be subject to hefty fines. This is a particular challenge for large multi-national corporations that do business in the EU as well as companies that may be headquartered there.

What does this mean to surveyed organizations, many of whom do business with or are located in the EU? While nearly 60% of respondents were very familiar or familiar with the GDPR, less than 20% were very confident they would be in compliance by May, 2018. (see Figure 10).

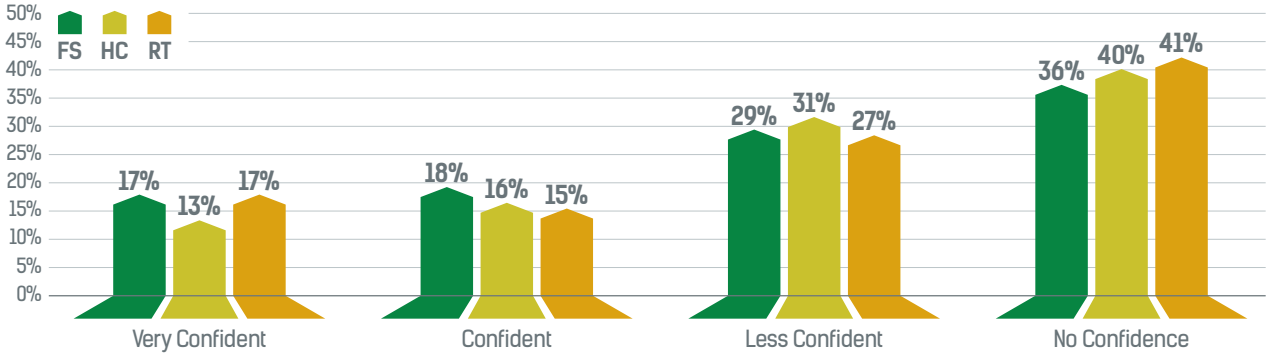

Figure 10: How confident are you that your organization will be compliant with GDPR on or before May 25, 2018 (effective date)?

This sizable compliance gap is alarming as many organizations acknowledge the need to alter how they collect, use and protect sensitive data. Over 25% expect to change their processes significantly due to GDPR while more than half expect to make just some changes. Retailers and financial services enterprises may face the most hurdles regarding GDPR as over 60% of retailers and nearly 50% of financial services firms currently collect customer data for profiling and personalized marketing, yet only 17% of each group type states they will be in compliance with GDPR by the effective date.

Beyond the initial compliance issue, those respondents familiar with GDPR acknowledge it will affect their current security activities. Sixty-seven percent say it will impact cost while 57% state it will require new investments in enabling security technologies. Nearly 90% see it increasing compliance and audit activities and nearly 60% see hiring of additional security experts. Fifty-five percent expect workflows to change.

With GDPR compliance occurring in the first half of 2018, the survey indicates many organizations, whether in the EU or not, need to accelerate their efforts and take scheduled action or incur large financial risk. They have the option to look to third-party security companies who can help them navigate the process; they also can seek information from the GDPR site. Additionally, it should benefit any organization to integrate a GDPR-specific security roadmap into current security strategies and tactics and budget accordingly for the appropriate resources and tools essential to meeting initial compliance dates and ongoing adherence to the regulation.

INDUSTRY SNAPSHOT

Healthcare

The healthcare sector consists of a wide number of segments: payers, such as insurance companies; providers such as hospitals and doctors; and manufacturers, both pharmaceutical as well as medical device and equipment. Because the industry deals with quality of life issues across the spectrum, access to real-time data, especially sensitive data such as patient records, requires both the security and availability of in-house, Web, mobile, or cloud applications.

The digital transformation has led to a staggering amount of video and images produced by the healthcare sector. The healthcare sector has created a virtual always-connected world of medical equipment devices that continually transmit unstructured, and potentially unsecure, data 24/7/365. Beyond the data explosion, the healthcare sector must comply with a broad, highly specific set of governmental- and industry-led regulations and standards (e.g., HIPAA, GDPR, local regulations like the FDA guidelines in the US) that control the collection, use, sharing and transmittal of sensitive personal and clinical information.

Healthcare providers have made large CAPEX investments in sophisticated medical equipment. Due to their long lifecycle, many of these devices are connected to old, unpatched systems. In fact, some still run on Windows XP. Often, IT administrators cannot update or patch these systems for fear of voiding the device's warranty, making equipment manufacturers a weak link in the medical industry when it comes to securing the environment.

As more data moves through networks within the four walls and out, the healthcare segment struggles to keep up with needed security strategies, technologies and resources that address the level of sophistication fueled by digitization. Data breaches, ransomware and security vulnerabilities such as exposed websites, unencrypted mobile applications, phishing and more have exposed tens of millions of patient and medical records in 2017 alone.

It stands to reason that the healthcare sector would invest in skills, tools and solutions that protect their applications and environments. Yet, of nearly 200 security executives surveyed from the healthcare sector (almost 90% having executive authority to direct security activities and investments) found that healthcare lagged behind other industries such as retail and financial services when it comes to mitigating risk. Just 27% of respondents had confidence they could safeguard patients' medical records even though nearly 80% are required to be compliant with governmental regulations.

Just 27% of respondents had confidence they could safeguard patients' medical records even though nearly 80% are required to be compliant with governmental regulations.

CONFIDENCE AND MITIGATING RISK

Analysis of survey feedback paints a portrait of a sector ill at ease with the growing security demands being placed on their institutions. Nearly two-thirds of respondents have little to no confidence they could rapidly adopt security patches and updates without having an operational impact while 70% said less than 50% of data loss incidents over the past 24 months were fully tracked and patched (see Figure 11).

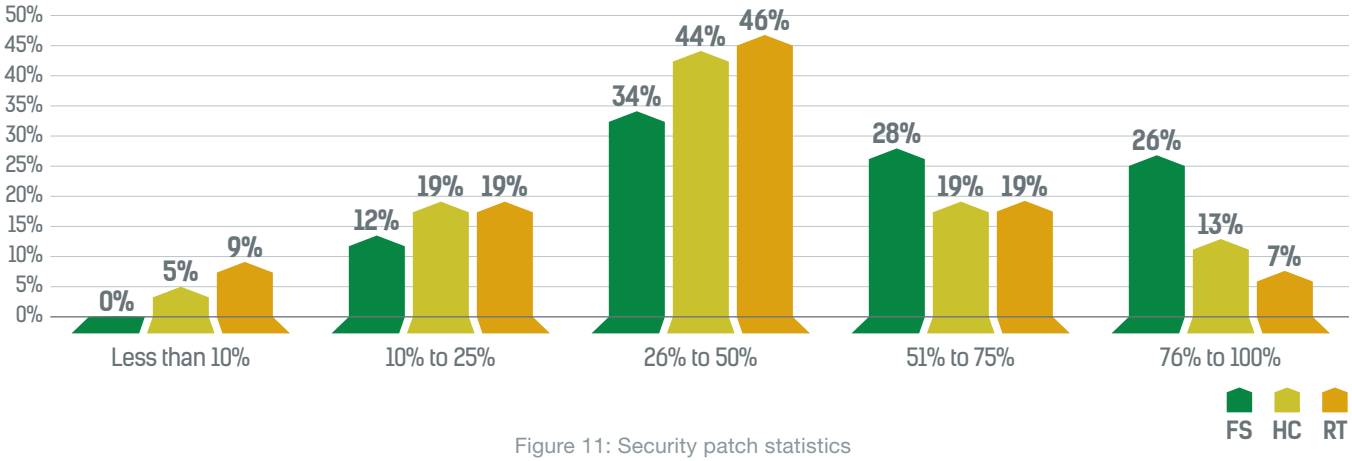

Figure 11: Security patch statistics

While 68% of respondents invested somewhat or significantly in security controls following major industry data breaches or attacks, only 21% use API gateways, 23% WAFs and only 29% use both. Additionally, less than 40% analyze API vulnerabilities prior to integration while less than 40% feel that they could detect or mitigate against attacks such as Brute Force, Web scraping, encrypted Web or API manipulations.

- Only 25% of respondents are fully aware of changes made to in-house applications and APIs within their software development environment.
- Sixty-one percent cannot track data shared with third-parties once it leaves the corporate network and 57% do not inspect data that is being transferred/returned via APIs

THE RISE OF EMERGING THREATS

Beyond addressing existing threats and vulnerabilities that have impacted the healthcare industry over the years, many respondents see the growing threat from emerging technologies. Bots, as with other industries, are becoming more dominant from a generated traffic perspective, with 36% of network traffic in healthcare being bots. However, only 20% of respondents can identify with certainty whether the 36% are good or bad bots.

Because there is more encrypted traffic in healthcare, there is a significant concern regarding encrypted (SSL/TLS) threats and attacks on the application layer. Of all attacks, 41% of respondents indicate that Layer 7 DDoS attacks have occurred more frequently over the past 12 months, though only 30% are confident or very confident they could mitigate one of these attacks against the application layer. Sixty-two percent acknowledge that it would be most difficult to prevent, detect and contain these type of attacks.

INDUSTRY SNAPSHOT
Retail

The retail industry is undergoing a transformative period as the "empowered" consumer, driven by technological advances and breakthroughs, impacts how retailers market, communicate and sell. Retailers continue to erode the barrier to purchase via a myriad of new technologies, such as mobile apps, social media transactions and AI that converse with consumers. They leverage AI to analyze buyer behavior and optimize buyer preferences. Even "traditional" retailers have invested in technologies that track both offline and in-store behaviors to further reduce the barrier to sale regardless of location.

To achieve such pervasive consumer contact, retail technologies depend upon bot automation. Bots have radically altered how consumers connect with retailers and consumer product companies. In retail, bots are everywhere, from electronic couponing to price aggregators, and from programmatic ad buying to app-to-app communications (chatbots).

With the rise of bots comes the security risks of discerning bad versus good bots. Our survey shows that 70% of generated network traffic is bots, but less than 20% of respondents can discern with certainty between good and bad bots (see Figure 12). Bad bots can wreak significant financial havoc on a retailer, stealing intellectual property via Web scraping, undercutting or stealing pricing and disrupting inventory management. For example, "sneakerbots[6]" have transcended the sneaker market and are now buying out all manner of highly anticipated products before they are available online.

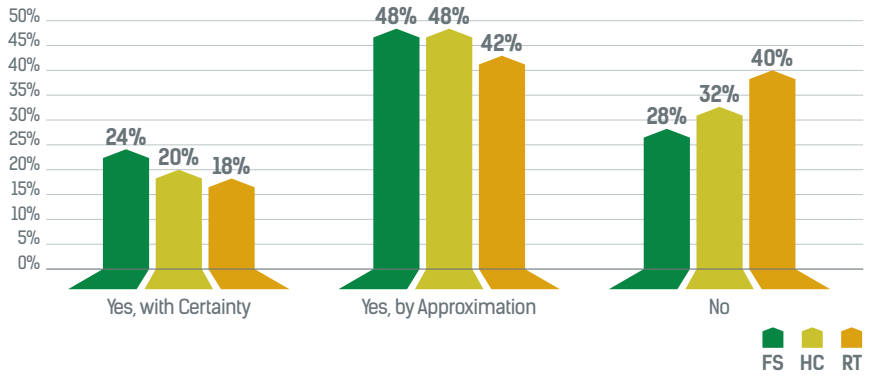

Figure 12: Is your organization capable of making a distinction between good and bad bots?

Because consumers expect the highest level of security from their sites and places they shop, ensuring that the retailer will protect their personal and financial data, retailers must adopt to the accelerated rate of technology change and growing security risks to realize high levels of customer loyalty, brand reputation and customer satisfaction. Let us review some of the security issues facing retailers today and see why these respondents currently lack confidence that they can offer the level of security their customers demand and expect.

6 Source: Recode https://www.recode.net/2017/9/13/16304668/nike-bots-counterfeiters-heidi-oneill-sneakers-retail

BOTS AND EMERGING TECHNOLOGIES

As mentioned previously, bots are a key technology issue of which respondents take serious notice. For those respondents who could distinguish between good and bad bots, bad bots often attack retailers in the form of Web scraping attacks. In fact, 75% of retailers said that Web scraping is a very significant risk to their intellectual property. Radware research indicates that 72% of retailers reported experiencing negative consequences to Web scraping attacks, including gathering of pricing information (56%), held inventory (45%), website copying (39%), and inventory depletion (32%) (see Figure 13).

> In fact, 75% of retailers said that web scraping is a very significant risk to their intellectual property.

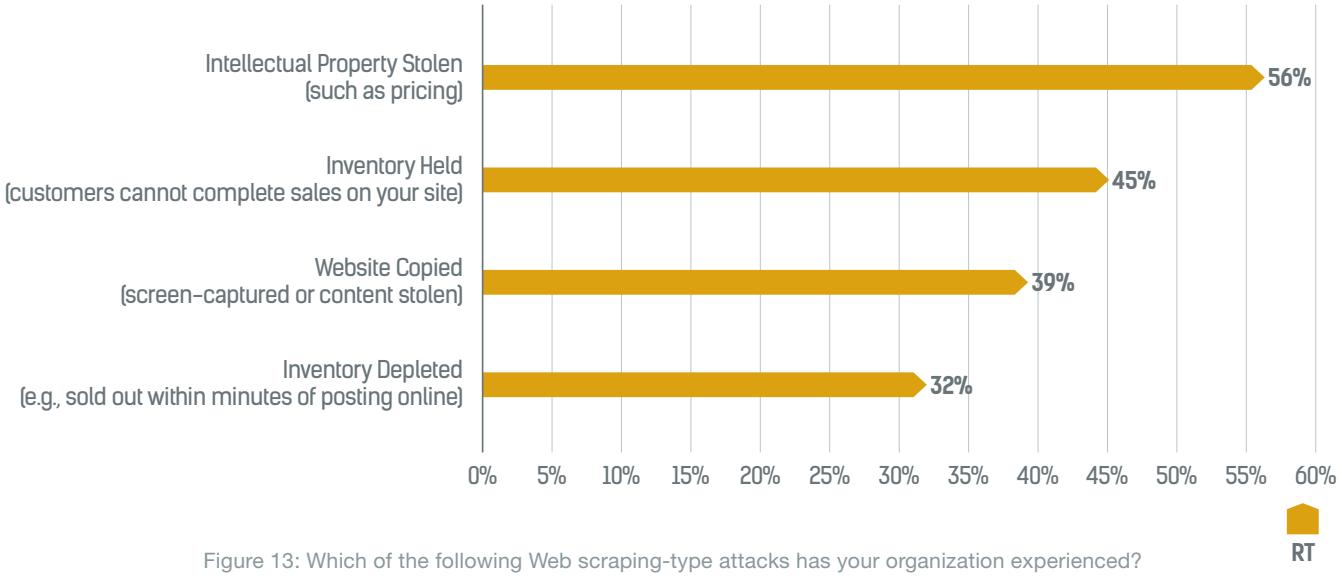

Figure 13: Which of the following Web scraping-type attacks has your organization experienced?

In addition, the increasing risk of encrypted Web attacks, such as Layer 7 DDoS as well as other attack vectors such as Brute Force and data security breaches, are of major concerns to retailers, who may not have the solutions to mitigate the risk. While retail applications and Web servers have experienced Brute Force (36%) and Layer 7 DDoS (25%) attacks over the past 12 months, only 16% of respondents are confident they could quickly detect one of these attacks and only 21% feel very confident they could quickly mitigate it.

CONFIDENCE AND MITIGATING RISK

Insights from the survey regarding retail confidence in mitigating risk demonstrate that retailers are not completely comfortable they have the tools, solutions and proper investments to address the issues. Just 32% have confidence they could secure sensitive data (e.g., credit card) while over 60% cannot track data shared with third parties once the data leaves the corporate network (see Figure 14).

> Just 32% have confidence they could secure sensitive data (e.g., credit card) while over 60% cannot track data shared with third parties once the data leaves the corporate network.

There is also growing concern that this lack of confidence may be founded in the fact that only one in five respondents are fully aware of changes made to in-house applications and APIs within their software development environment. Even though 33% are required to comply with PCI standards, nearly 60% don't inspect the data that is being transferred/returned via APIs and less than 40% analyze API vulnerabilities prior to integration.

As compared to other industries such as healthcare and financial services, surveyed retailers did not respond to industry-wide security breaches with significant investment in security controls, with only 33% significantly increasing their investments. This is alarming since over 60% of respondents collect customer data for profiling and personalized marketing; this lack of investment may make retailers more vulnerable to threats and attacks.

The following statistical analysis from retail respondents demonstrates why many of these enterprises may fall victim to potential application-layer attacks, lacking a comprehensive security framework to identify or mitigate against those attacks. Only 25% of retailers state that they fully integrate security into the delivery of Web applications while only one in three could quickly detect a wide range of threats and attacks. This may be why various retailers around the world have experienced frequent attacks on their applications, making them all too vulnerable to a broad range of threats as well as placing them at a competitive disadvantage (where shoppers will quickly abandon their cart or basket, negatively impacting sales and customer loyalty initiatives).

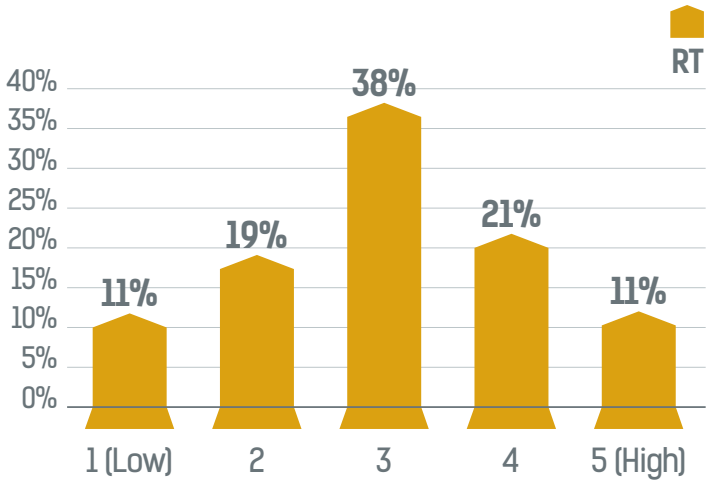

Figure 14: Rate your organization's ability to secure sensitive data (like credit card and customer data) during high demand periods, like during Black Friday and Cyber Monday?

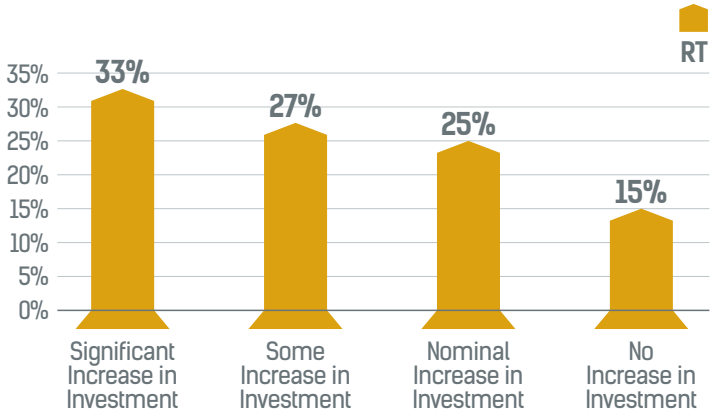

Figure 15: What effect did large retail data breaches have on your organization's investment in security controls?

INDUSTRY SNAPSHOT

Financial Services

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. This emphasis on controls is supported by the fact that most surveyed financial services institutions, across the board, have more security controls in place around their applications than their retail or healthcare industry counterparts (see Figure 16).

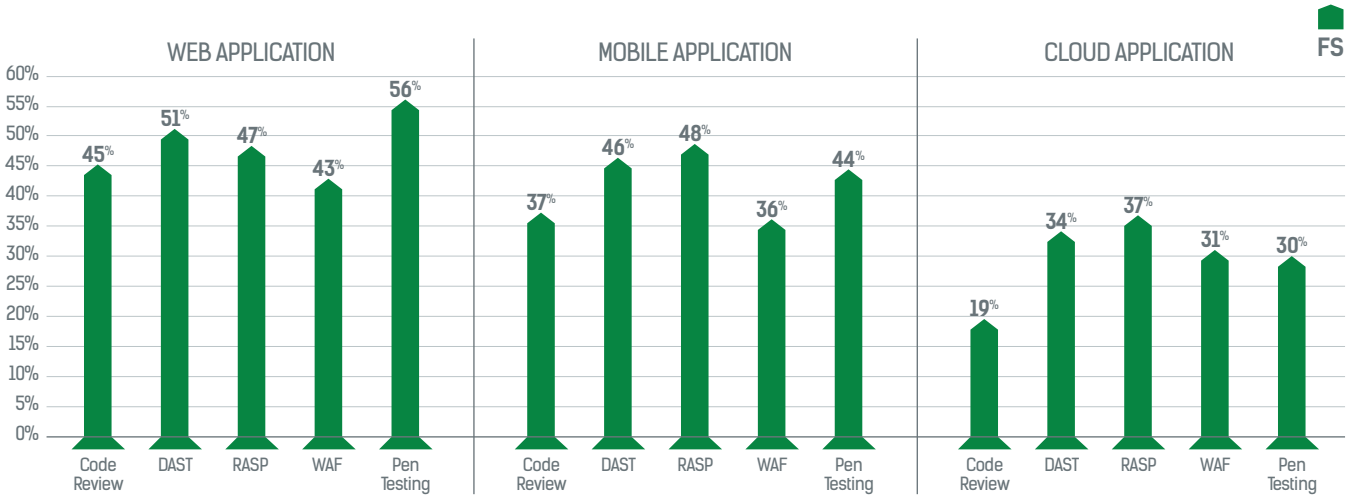

Figure 16: Frequently used security controls

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.

Respondent Profile/Methodology

Radware, in conjunction with Ponemon, conducted an informational survey of the global security community, collecting 644 responses from CISOs, CIOs, and security leaders of large, multinational corporations (ranging from $500M - $25B in annual revenues) around the globe. This objective, vendor-agnostic aimed to learn more about their Web application security solutions needs. The survey focused on three verticals: Retail (202 respondents), Healthcare (183 respondents) and Financial Services (259 respondents). Geographically, 60% of the survey respondents were U.S.-based, while the remaining 40% were diversely spread around the globe (including 18% from Europe).

About the Sponsors

PONEMON INSTITUTE

Ponemon Institute© is dedicated to advancing responsible information, security and privacy practices in business and government. To achieve its mission, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and security practices of organizations across a variety of industries and geographies.

RADWARE

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. Radware Cloud Security Services provide cloud-based infrastructure protection, application protection and corporate IT protection services to enterprise globally. For more information, please visit www.radware.com.