Right Tool but Wrong Model

Are your defenses against web application attacks falling further behind?

Stratecast | FROST & SULLIVAN

An Executive Brief Sponsored by Threat X

Michael Suby
Vice President of Research

June 2018

INTRODUCTION

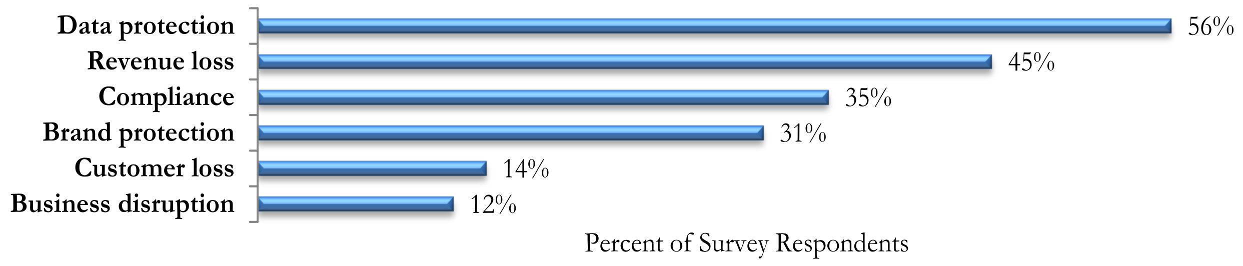
Well-known fact: web applications are essential to all businesses and critical to consumer (B2C) organizations. As a result, an organization's website is often the 'face' for customer encounters. A poor experience not only negatively impacts the brand and degrades customer trust and confidence; it is also directly correlated with increased customer churn and decreased customer lifetime value. Beyond initial impressions, B2C websites are storefronts that provide unlimited impressions and are much more effective in reaching and serving more customers when compared to human interactions.

The same digital transformation exists in business-to-business (B2B) supply chains and business-to-partner engagements. Whether a single or multi-link chain, web applications are foundational for highly scalable, anywhere accessible, and reliable cross-business and inter-departmental interactions. Organizations leverage an expanding array of web applications to support numerous human resource and business objectives: improve individual and team productivity, engage and support personnel, and reduce costs. Correspondingly, from a security risk perspective, the collective attack surface of B2B and B2C web-accessible applications is increasing daily.

Web applications are also highly dynamic. Frequent upgrades and new capabilities are essential to attract and captivate site visitors, and meet business objectives. This dynamism, however, breeds sophistication as well as complexity, which also contributes to configuration and programmatic vulnerabilities. Moreover, with accelerating development cycles and the increasing density of API and micro-services, comprehensive scanning for internal and third-party vulnerabilities prior to production releases may not always be feasible. Often unintentional but nevertheless very real attack vectors are inevitably created.

With web applications being such a critical workhorse, but also a prime target for threat actors covering a gamut of motivations (financial, political, personal, and competitive), securing web applications is just as essential as the capabilities of the web applications themselves. According to a recent survey conducted by Ponemon Institute, a mix of strategic and compliance reasons were noted by organizations for securing their web applications.[1]

Reasons to Secure Web Applications (two responses allowed)



Source: Ponemon Institute

Another well-known fact among organizations is that their web applications are constantly being compromised. According to the same Ponemon survey, 73% of the surveyed organizations are using a web application firewall (WAF) to protect their web infrastructures. Effectiveness, however, is not a certainty. Twenty-six percent of the

[1] *Trends in the Cost of Web Applications and Denial of Service Attacks*, September 2017

surveyed organizations stated their web applications were compromised ‘frequently’ in the past 12 months; an increase from 22% from a comparable 2015 Ponemon survey. Another 54% in the 2017 survey stated they were compromised ‘sometimes’.

Is this paradox the result of deficient WAFs? The answer is not binary, but close. A WAF designed to counterbalance the many contributors to an increasing barrage of web application attacks is essential. At the same time, trained and experienced security practitioners are critical to optimizing a WAF’s effectiveness, and closing the gaps that give rise to damaging web application attacks. Therefore, the answer is a bit of both in a correlated fashion.

We invite you to read on as we share our perspective. In this white paper we discuss the reasons for increases in web application attacks, how those reasons are driving the design characteristics of an effective WAF, and why security technology and human talent need to coexist. We end this paper with an introduction to Threat X, a provider of a true ‘next-generation’ WAF solution.

WEB APPLICATIONS ARE UNDER ATTACK FOR MANY REASONS

Attacks on web applications are on the rise. In its research, Akamai notes that web application attacks are significantly more common than DDoS attacks; and in its most recent research, web application attacks increased in number by 10% year-over-year.[2] Verizon adds, in its *2018 Data Breach Investigation Report*, that attacks on web applications are the number one contributor to data breaches, a finding that materialized even after filtering out botnet-related attacks on web applications using credentials stolen from customer-owned devices. Also, it is no surprise, given these findings, that database and web application servers were the first and fourth most targeted assets (respectively) involved in data breaches (POS terminals and controllers ranked second and third) in Verizon’s documented data breaches.

If there were only a single contributor to web application attacks, then possibly the means to defend against them would be straightforward. In reality it is not that simple. As described in this section, a number of factors contribute to the expanding risk of web applications attacks.

1. The attack surface is broadening

Cloud adoption has become strategic. Moreover, in becoming strategic, demands on development speed and functionality have intensified, forcing organizations to rely increasingly on APIs and micro-services to quickly augment their web applications. Consequently, the attack surface is not only broader, it is also deeper. The attack surface is broadening as web and legacy apps, APIs, and micro-services are merged with on-premises apps, and meshed together in a public-facing cloud environment. Depth is simultaneously increasing as software code is a churning amalgamation of internally developed code and third-party code and libraries.

On the increasing strategic value of cloud services, Frost & Sullivan’s 2017 Cloud Survey revealed the following:

- Two-thirds agree or strongly agree with the statement “We believe a cloud strategy is essential to remaining competitive in our industry.”
- Tactically, 69% list “deliver services and applications faster” as either 6 or 7, on a 7-point importance scale, as a factor in deciding to implement cloud solutions for some or all of their workloads. Only “manage data growth” (71%) and “reduce costs” (76%) ranked higher in importance.

[2] Akamai’s *State of Internet Security - 4Q2017 Report*

Further expanding the attack surface, the shift to the cloud is neither immediate nor uniform. For most organizations, a variety of environments are employed. As shown in the survey results below for web hosting and data storage (primary and object) workloads, there is no dominant environment.

What is your primary environment or deployment model (one chosen per workload)?

Percent of responses	Web Hosting	Primary Storage	Object Storage
Public cloud	18%	8%	23%
Hosted private cloud (single tenant)	21%	23%	12%
On-premises physical servers	17%	22%	17%
SaaS	13%	7%	7%
Bare metal cloud	8%	9%	7%
On-premises virtualized or private cloud	7%	11%	9%

Source: Frost & Sullivan 2017 Cloud Survey

Placing an explanation point to the hybrid or mixed nature of workload deployments, one-third of the survey respondents stated that web hosting is split over multiple environments. Only email and databases were higher, at 41% and 37%, respectively.

Considering the challenges of managing web application security consistently over a hybrid environment and one that includes highly adaptable cloud deployments, security best practices can become a casualty. Accordingly, security concerns are palpable among the surveyed organizations. A majority identified security as the top reason for not implementing cloud solutions. Regarding specific security concerns in cloud deployments, 65% rated "unauthorized access to my data or applications" as either a 6 or 7 on a 7-point criticality scale; and 55% rated "inability to meet compliance requirements" also as a 6 or 7.

2. Frequent and rapid changes in web applications contribute to vulnerabilities

According to Trustwave,[3] 100% of the web applications it tested had at least one vulnerability; and the median number of vulnerabilities was 11. Digging deeper on critical vulnerabilities, 13.8% came from "web pages intended for authenticated users that attackers nevertheless accessed without a valid session identifier." Of high-risk vulnerabilities, nearly 9% were vulnerable to cross-site scripting exploits (i.e., "web applications that do not properly validate user-supplied inputs before including them in dynamic web pages").

Another important aspect of these vulnerabilities is that attackers are adept at compromising 'soft targets' or 'weak links', and then moving laterally to their prized targets. Assisting the attackers, organizations often prioritize their security efforts (e.g., vulnerability scanning, patching, and hardening) to their most 'critical applications'; leaving non-critical applications, or soft targets, highly exploitable. Once these soft targets are compromised, attackers move laterally to other assets, such as critical applications, databases, and file shares. In essence, if the front door is locked, attackers look for the hidden key or try a less visible backdoor or an unlocked window. Many aspects of this very common weak link scenario are detailed in *You're Only as Strong as the Weakest Link in Your Web App Fence*, authored by Andrew Useckas, Threat X CTO.

[3] Trustwave's *2018 Global Security Report*

3. Precautionary scanning for vulnerabilities lacks regularity

According to the previously referenced Ponemon survey, only 45% of web applications, on average, are tested for vulnerabilities; 41% of surveyed organizations have "no regular interval" to test web applications for vulnerabilities; and only 15% test "every time the code changes."

4. Even when scanning occurs, and vulnerabilities are identified, time is required to fix

Fixing identified vulnerabilities is seldom instantaneous. Forty-six percent of the Ponemon survey respondents stated that multiple days are required to fix one compromised web application. Another 20% stated that the time to fix extends into weeks. With vulnerabilities pervasive but also not routinely found, and when time to resolve is measured in days or weeks, other protections, such as WAFs, are essential to combat attackers. However, as stated previously, WAFs are not stopping all attacks.

5. Common attack methods are used repeatedly, but uncommon approaches are evolving too

In Trustwave's research on web application attacks, a variety of common attack methods are used.

	Attack method as a % of total
Cross-site scripting	40%
SQL injection	24%
Local file inclusion	4%
Path traversal	7%

Compounding these attack methods, attackers are not constrained to approaches that are common or traditional. For example, in zero-day attacks, the attacker succeeds by devising an attack method that has previously not been seen or is tailored to a specific target or an undocumented vulnerability. Therefore, detection of the attack based on known patterns, behaviors, or vulnerabilities is an inadequate defense.

Another development in attack methods is the increase in DDoS amplification attacks. Verizon determined that DDoS amplification attacks have exceeded non-amplified attacks since 2015, and are continuing to grow at a faster pace. In amplification attacks, small spoofed packets are sent to the web application in exchange for larger packet responses, with the objective to exhaust available web infrastructure resources. Configuring web infrastructure to scale for the DDoS amplification attacks, as well as other types of DDoS attacks, is a costly proposition in terms of resources, and can be risky (i.e., uncapped auto-scaling fees). Conversely, inability to block incoming DDoS packets places the online experience of legitimate visitors at risk (i.e., revenue and customer loss). Bottom line: effective web application protection must be comprehensive in addressing a myriad of attack methods.

6. Attackers' motives are not limited to extracting valuable data

Verizon also noted that data extraction is not the only motive in web application attacks. Secondary motives to alter web server integrity for illicit repurposing (send SPAM, participate in DDoS attacks or phishing campaigns, store and deploy malicious code) are also common. Over 23,000 repurposing incidents were documented by Verizon. In these incidents, once an attacker has compromised a web application, the attacker moves laterally within and even outside the web infrastructure to hijack resources, leveraging weak administrator oversight and configurations to repurpose existing resources, and even uncover additional resources.

THE COST OF A WEB APPLICATION ATTACK IS SIGNIFICANT AND RISING

Ponemon estimated that the average cost of a web application attack is $3.7 million, 18% higher than the $3.1 million estimated by Ponemon two years prior. Adding to the significance of this cost analysis is its comparison to the average cost of a DDoS attack (more than two times greater) and nearly half of the cost of web application attacks attributed to internal IT and security reactions, such as: post-attack technical support, incident response, and damage or theft of IT assets and infrastructure. At this level of post-attack reactionary costs, shouldn't more attention be spent on preventing web application attacks before they cause material harm?

WEB APPLICATION FIREWALLS NEED A MODEL UPGRADE

With the strategic value of web applications ramping upward, along with the rising frequency and financial severity of attacks, the market for WAFs has been growing rapidly. Frost & Sullivan determined that the global market for WAFs reached $708 million in 2017, an increase of 16% over 2016, and we project annual spending on WAFs to surge to over $1 billion by 2020.[4]

Market demand, we believe, would be even greater if perennial buyer concerns were addressed. Those concerns fall into two primary camps:

- **WAFs have a history of complexity**, for example, lengthy periods of application learning, constant re-tuning for changing circumstances (app capabilities, vulnerability discovery, and attack methods), and the lengthy, end-to-end rule writing process (preparation, testing, implementation, evaluation, and modification).
- With the complexity and challenging circumstances, deployed **WAFs have tended to produce an excessive number of false positives**, and run the risk of blocking legitimate traffic.

One major and unfortunate consequence of WAF complexity is that WAFs are not deployed broadly, and blocking mode is only turned on sparingly. The result is twofold. First, a potentially sizable portion of an organization's web application portfolio is essentially in 'open season' for attackers; and that portion contributes to the previously described weak link scenario—backdoor attacks on critical applications. Second, with WAFs operating solely in monitoring mode, the organization is placed in a reactionary predicament of recognizing and mitigating attacks before the attacker can cause harm. This is certainly not a desirable position considering that WAFs exist to protect business operations and sensitive data. Ultimately, the WAF is not fully preventive.

[4] Frost & Sullivan's *Global Web Application Firewall (WAF) Market Analysis, Forecast to 2021 - New Threats and Increased Competition Drive Innovation*, October 2017

Attributes of a New WAF Model

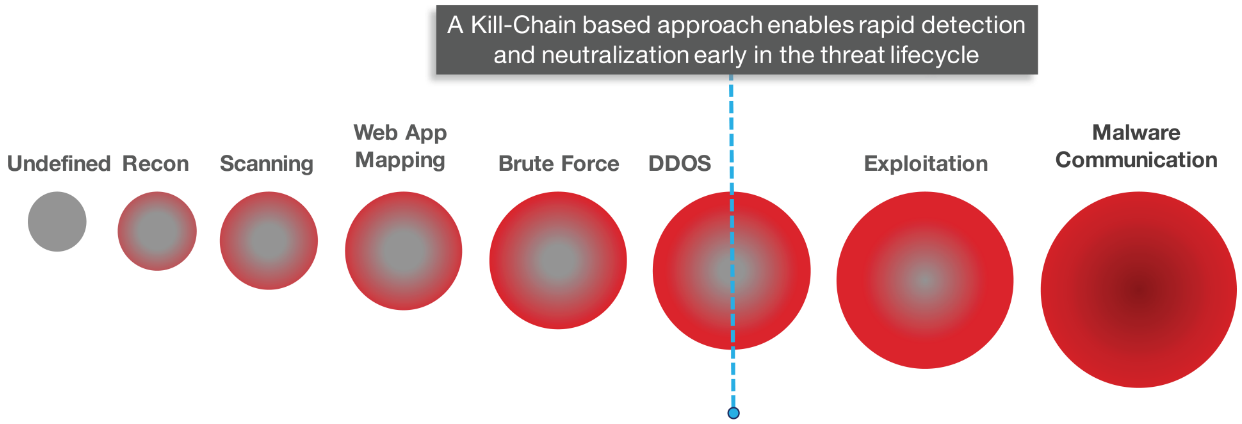
With the critical need for securing web applications confirmed, but traditional WAFs lacking the means to deliver the needed threat protection, a new WAF model is required. The following are our commonsense attributes that any new WAF model should cover:

- **Environment-agnostic** – Simply, wherever web applications reside—public cloud platforms, private clouds, on-premises data centers, or any combination—protection must be consistently delivered.
- **Cloud Consume-ability** – Cloud services have forever changed user expectations. Rapid on-boarding, instantly scalable, always available, highly and easily configurable, and usage-based pricing are no longer 'nice to have' features. They are expected.
- **Dynamic Defense** – Web applications and attackers are moving too quickly to rely on the weight of reactively prepared and static rule sets for protection. A new model is needed—one that leverages behavior-based machine learning, extensive knowledge of attacker methods, attacker tagging to adapt defenses in real-time as attacks unfold, and surgically intercede before damage ensues. To learn more about dynamic defense, we invite you to download and read our insight, *Dynamic Cyber Defenses: A Fresh Approach to an Old Problem*, by clicking here.
- **Low Burden** – Pertaining to managing WAFs, Ponemon reports that more than half of its surveyed organizations believe that three or more full-time equivalent (FTE) employees are needed to properly manage a WAF. Considering the tight labor market in security and the associated costs of acquiring, training, and retaining specialized security practitioners, three or more FTEs is simply prohibitive for many organizations. Alternatively, as mentioned earlier, organizations restrict their WAF deployments and roll the dice on attack potential and severity. The new WAF model must have a low impact on the organization for web application protection to be effective and more broadly applied.

WHY THREAT X

Threat X offers a new model and a truly next-generation approach to WAFs. Operationally, Threat X utilizes a behavioral based, kill-chain focused threat detection and neutralization approach to protecting web applications. By focusing on the attacker, rather than the attack, Threat X builds threat and application vulnerability scores, and elevates engagements for each Internet Protocol (IP) address as the attacker attempts movement along the kill-chain (see following illustration).

Web Application Kill-Chain


A Kill-Chain based approach enables rapid detection and neutralization early in the threat lifecycle
Undefined
Recon
Scanning
Web App Mapping
Brute Force
DDOS
Exploitation
Malware Communication

Source: Threat X

Through behavioral interrogation of each IP, Threat X rapidly determines if an IP is:

- Friend (legitimate application traffic and/or IP) or foe
- Human or machine
- And if foe (human or machine), interrogation and assessment continues to ascertain evolving threat severity as the threat actor attempts to move along the kill-chain

By continuously tracking and assessing threat actors, Threat X is gathering intelligence on their tactics and techniques, and determining when to neutralize their advances.

Scoring Threat X on our four attributes of a new WAF model returns high marks:

- **Environment-agnostic** – Situated in-line with web application traffic but not co-located with the web application, Threat X delivers web application protection independent of where web applications are hosted.
- **Cloud Consume-ability** – Threat X was designed with cloud-native and SaaS deployment capabilities for today's complex, hybrid technology environments. These design characteristics alleviate the burden of deployment complexity, configuration, and management from security and IT teams. Threat X is also compatible with Docker containers hosted on-premises, in private or public clouds (e.g., AWS, Azure, and Google Cloud Platform).

- **Dynamic Defense** – Threat X's approach is truly dynamic. It responds in real-time to what is encountered both in qualifying intent and in neutralizing the threat. As circumstances change with the web applications themselves and attacker methods, adaptation is immediate. A testament to the value of dynamic defense, Threat X customers are blocking, not just monitoring, attacker traffic within 24 hours of turning on the Threat X service.
- **Low Burden** – Threat X is a rules-free approach to WAFs. There are simply no rules or static signatures to create and maintain to block threatening behaviors. Moreover, confidence level is high and analyst time is low as few false positives are produced through the Threat X machine learning technology. Finally, as a cloud-based solution, provisioning and scalability are a snap.

Dynamic defense, static rule sets rendered obsolete, few to no false positives, and snap provisioning and scalability—Threat X unburdens security practitioners and opens the door wide to extend protection to an organization's entire population of web applications.

Even with the operational savings benefits of Threat X's approach, the pervasive talent shortage in security practitioners faced by most organizations cannot simply be eliminated. Security teams not only need the capability to protect all their web applications with greater effectiveness, but also to greatly limit their day-to-day involvement. These organizations have many other areas where they need to direct their limited, but highly strategic, security talent (e.g., accelerating detection and response across its entire IT footprint, driving security best practices into software development, and assessing and mitigating security risks in cloud migrations).

To relieve overburdened security teams, Threat X offers a managed service option: Threat X Labs. Threat X Labs combines the collective threat intelligence and analysis produced within the Threat X platform with a managed service that includes 24x7 proactive monitoring and response; so, organizations gain complete confidence in their ability to detect and respond to web application attacks. In collaboration with customers, Threat X analysts establish risk parameters on when to neutralize threat actors' advances. In rare instances, when the established parameters are not black-or-white, Threat X analysts engage with customers to make joint decisions. Ultimately, Threat X customers receive maximum protection for their entire web application portfolio from the Threat X Labs service without having to dedicate staff to learn and stay current on the constantly evolving nature of threat actors and their methods.

THE LAST WORD

The future of B2C and B2B engagements is already here, and it entails massively available access to resources. Brokering resources is through web applications. These applications both enable and enhance user experiences, and deliver on business objectives. They are workhorses.

Unfortunately, web applications also provide a window of exploitability. Left unchecked, the intended purpose of web applications can be upended and sensitive data placed at risk. This is where WAFs come into play. They are the essential gateways in filtering out the unintended and malicious exploits of various threat actors.

Michael Suby

VP of Research
Stratecast | Frost & Sullivan
msuby@stratecast.com

Silicon Valley
3211 Scott Blvd
Santa Clara CA, 95054
Tel: 650.475.4500
Fax: 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:

Frost & Sullivan
3211 Scott Blvd
Santa Clara CA 95054

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Detroit
Dubai
Frankfurt
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mumbai
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Sarasota
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC