ESG SHOWCASE

Adopting a Risk-centric Approach to WAAP with ThreatX

Date: July 2020 **Author:** John Grady, Analyst

ABSTRACT: Application security controls have not kept pace with changes to application development processes or the increasingly sophisticated tactics of attackers. A new approach providing integrated protection against traditional application threats, API attacks, and machine-generated availability and fraud-based attacks is needed. The ThreatX WAAP++ platform incorporates WAF, bot management, DDoS mitigation, and API protection into a risk-centric approach providing developer and cyber teams with actionable insights to improve application security.

The Modern Application Environment Requires New Defenses

Applications are the backbone of the modern enterprise, with most organizations supporting tens, if not hundreds, of internal applications. In fact, ESG research has found that 88% of organizations have at least 100 business applications in their environment, with 59% reporting that 31% or more are internally developed.[1] Organizations face three key issues with regard to securing modern applications:

1. The distributed and heterogeneous nature of enterprise technology resources. The multitude of applications enterprises use are no longer centralized in a well-segmented DMZ, or even an enterprise data center, but are scattered across multiple private and public cloud platforms, on bare metal and virtualized servers, containers, and even serverless functions.

2. The decentralization of application deployment and maintenance. Whether via DevOps or traditional development methodologies running through the lines of business, the integration of security into these workflows remains a challenge, making it more difficult for centralized security staff to provide consistent risk assessment, remediation, and mitigation for all applications.

3. The skills shortage and its impact on the stratification of applications. Not all enterprise applications are tier-1, meaning the resources and skills allocated to tier-N applications are often limited. In fact, ESG research has found that security practitioners most frequently report application security as the cybersecurity area with the most significant shortage of skills (33%).[2]

The Shortfalls of Traditional Web Application Firewalls

The web application firewall (WAF) remains a staple of application security. However, the high level of adoption does not equate to strong security. Many organizations deploy a WAF to maintain PCI compliance, which, while good for compliance's sake, does not inherently improve security. Further, while the virtual patching capabilities of a WAF provide

[1] Source: ESG Master Survey Results, Trends in Modern Application Environments, December 2019.
[2] Source: ESG/ISSA Research Report, **The Life and Times of Cybersecurity Professionals 2020**, to be published.

protection for vulnerable applications, they do not fundamentally improve the security of the application and should be viewed as a stopgap approach.

WAFs do offer threat protection against exploits such as SQL injections, cross-site scripting, and risks including and beyond the OWASP Top 10. However, these protections are typically signature-based, predicated on a binary allow/block decisioning engine, and often require months of tuning and adjustment to ensure malicious traffic is blocked without introducing false positives. The reliance on these static rulesets and required manual intervention does not scale to address modern CI/CD or DevOps application development methodologies. The process becomes unmanageable for many security practitioners, slowing deployment and ultimately raising the total cost of ownership of the solution.

As a result, the majority of WAF deployments continue to focus on tier-1, public-facing applications, leaving many internal-facing, tier-N applications with inadequate security controls.

To address these issues, some WAFs have been repositioned as "next-generation" in part by incorporating a positive security model that relies more on application behavior to detect and block malicious traffic as opposed to signatures. However, while the approach makes sense in theory, the implementation results have been mixed and fail to address the fact that attacks on web applications span multiple attack vectors beyond those for which WAFs were designed. As a result, the majority of WAF deployments continue to focus on tier-1, public-facing applications, leaving many internal-facing, tier-N applications with inadequate security controls.

The Emergence of WAAP

Over the last few years, much of the security industry has become focused on consolidation and a more platform-centric approach. With WAF, bot management and mitigation, distributed denial of service (DDoS), and API protection all being required for pervasive runtime application protection, a consolidated approach makes sense in the context of application security as well. However, many of today's solutions fail this requirement by maintaining a siloed approach focusing on one aspect of application security or only loosely coupling capabilities. As a result, many organizations continue to buy and deploy multiple application security tools, only adding to the complexities.

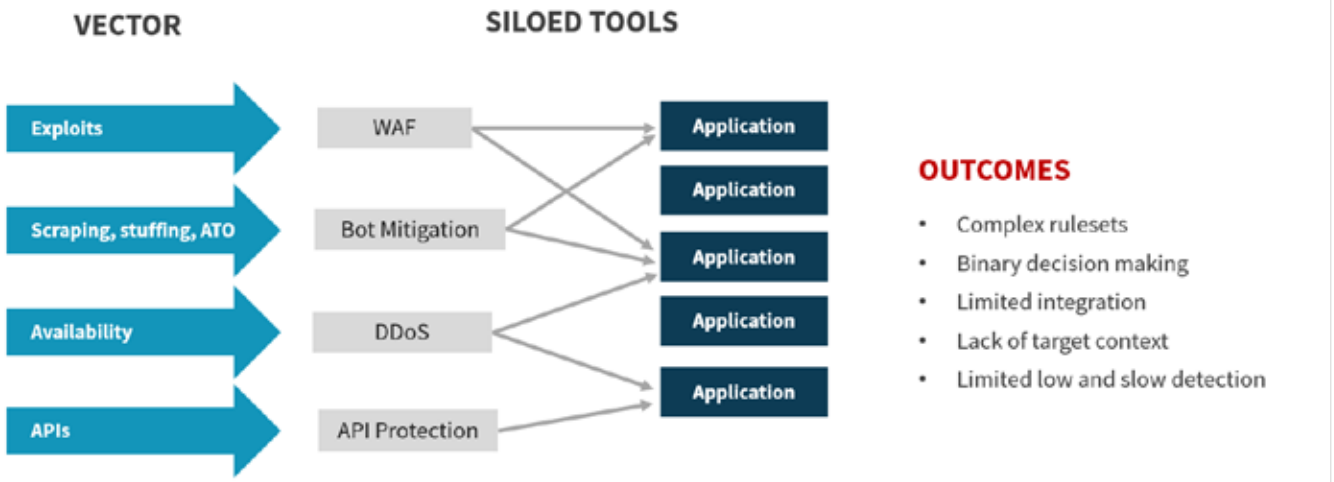
Many WAAP Approaches Only Address Part of the Problem

There has been some progress toward a platform approach to application security over the last year with the emergence of web application and API protection, or WAAP. WAAP solutions incorporate WAF, bot mitigation, DDoS protection, and API protection delivered as part of a cloud-native, auto-scaling infrastructure. Because it seeks to address a significant pain point for many organizations, WAAP has generated a high level of interest despite its recent introduction. However, while generally seen as a positive development, it does leave some important considerations unresolved:

- Reliance on legacy WAF. While a platform approach can provide some reduction in complexity by reducing the number of discrete products and vendors in the environment, WAAPs utilizing a traditional WAF continue to be prone to the same drawbacks previously described relative to deployment, tuning, and ruleset management.
- Lack of integration. The packaging and management of WAAP solutions may be centralized to some extent, but the functionality in many cases remains siloed, meaning security and visibility may not be markedly improved. This is especially important as the prevalence of machine-generated traffic has increased. Solutions that are unable to correlate factors across the different threat vectors they support are destined to be ineffective.

- **Attack-centric protections.** Many WAAPs focus on blocking discrete attacks without the deeper context of what is being targeted, how it fits into the broader application attack landscape the organization is facing, and the risk associated with those attacks relative to the target applications.

Figure 1. Disintegrated WAAP Approach



Source: Enterprise Strategy Group

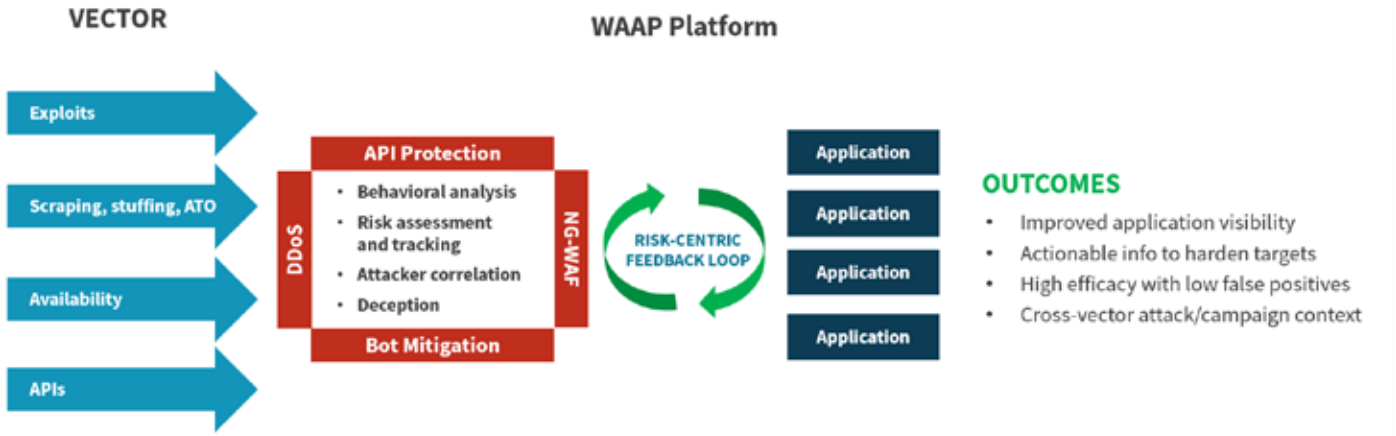
Next-generation WAF, Integration, and Risk-centricity Are Critical for WAAP Platforms

With these issues in mind, the nascent WAAP market must quickly evolve to address the limitations that arise from a centralized yet siloed approach. Ultimately, to truly improve application security, WAAP platforms must present users with a holistic view of the applications in their environment, the cross-vector threats targeting them, and the risk of those attacks to the target application. To accomplish this, the core WAF functionality included in WAAP platforms must provide next-generation capabilities. Rather than looking at a small set of specific requests to match against a rule, the focus should be on how the attacker is interacting with the application and the degree of risk resulting from their actions. This improves not just detection accuracy, but also speeds deployment and eases ongoing management by moving beyond static rulesets.

Further, WAAP solutions should not look at the different types of application attacks in isolation, but rather at all attacks targeting an application comprehensively. Whether protecting against bots launching account takeover attempts, attackers targeting application vulnerabilities, or low and slow DDoS or API attacks, a single-pass, multi-sensor inspection engine should be used to ensure consistency in the protection and centralized visibility of all threats to an application.

Finally, the centralized management console must shift from an attack-based approach to a target-centric view incorporating risk visibility. By combining next-generation WAF with integrated detection capabilities and visibility into application risk, the rich data showing what is happening across the applications in the environment can be turned into actionable insights. These insights can then be disseminated to developers to prioritize reconfiguration, patching, or decommissioning of the applications to improve the security posture of the organization.

Figure 2. WAAP Platform Approach



Source: Enterprise Strategy Group

Enter the ThreatX WAAP++ Platform

ThreatX is a private company focused exclusively on web application protection. The company was founded in 2014 by former CISOs to advance web application security beyond the scope of the traditional WAF. The ThreatX risk-centric WAAP platform includes next-generation WAF capabilities, bot mitigation, API protection, and layer 7 DDoS prevention via a single-pass, multi-sensor scanning engine focused on collecting and analyzing information on attacker interactions with the application. Due to the single-pass, integrated architecture, all four capabilities are included natively in the platform, which ThreatX calls WAAP++.

The ThreatX WAAP++ platform is powered by the Hacker Mind behavioral risk modeling engine, which interrogates attackers to collect metadata through cookie injection, TLS fingerprints, browser fingerprints, and other methods to correlate and group individual sessions and requests into entities. These entities are then given a risk score based on how they are interacting with the application, which is tracked over time. Entities are only blocked when the risk reaches a threshold deemed malicious, allowing ThreatX to collect a sizable amount of intelligence on their profile and tactics without tipping off the attacker. If entities are only acting suspiciously and not maliciously, they are either tracked to gain further intelligence or given delayed responses to reduce the profitability of the attack and hamper bot activity.

The platform sits inline as a reverse proxy, supporting full SSL decryption, and can be deployed via a Docker container into on-premises, public cloud, or private cloud environments. Alternatively, the platform can be consumed as a service through the ThreatX cloud. One of the key differentiators of the ThreatX approach is the availability of security operations center (SOC) experts to provide proactive services support for customers of the platform. Examples include security monitoring, incident response, threat hunting, vulnerability monitoring, and virtual patching support. This offering, called AppSec-as-a-Service (ASaaS), specifically addresses the skill and resource constraints previously discussed, and helps customers turn the intelligence gleaned from the platform into actionable insights to improve application security and performance.

The ThreatX WAAP++ approach provides organizations improved visibility into how users and attackers are interacting with their applications, more streamlined deployment versus traditional WAF tools, reduced false positives via the Hacker Mind correlation engine, and the benefit of a combined product and services approach via ThreatX SOC experts.

The Bigger Truth

Application architectures and development methodologies have changed significantly over the last few years, but the security tools used to protect them have only recently started to evolve. The convergence of WAF, bot mitigation, DDoS protection, and API security tools appears to address this on the surface, but does not specifically solve the most critical issues with application security today: balancing risk with available resources. Application and security teams require actionable intelligence about their environment to keep pace with attackers. The ThreatX WAAP++ platform can help organizations understand their risk and improve their application security posture.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

www.srccybersolutions.com sales@srccybersolutions.com +91 120 232 0960 / 1