SRC CYBER SOLUTIONS LLP

THREATX

WAF to WAAP++

A 3-Step Plan to Modernize Your AppSec

Executive Summary

As web applications and their threats have evolved, traditional WAFs have struggled to keep pace. Applications are built and deployed in new ways, are accessed in new ways, and face an increasingly broad and sophisticated set of risks and threats. Originally coined by Gartner, Web Application and API Protection (WAAP) introduces a modernized approach to application security that addresses these new challenges.

At its highest level, Gartner defines WAAP as the *"evolution of cloud web application firewall services, expanding scope and security depth."* And while APIs are called out in the name, this expanded "scope and depth" covers a variety of additional functionality, including bot protection, DDoS attack mitigation, and in some cases, security services. ThreatX uses the term WAAP++ as a reminder that WAAP is not simply WAF + API security, but a true evolution of modern application security.

Since WAAP is defined as an evolution of the WAF, it may seem like a WAAP (or WAAP++) is simply an old fashioned WAF with some new features bolted on. And that's exactly what many traditional WAF products have done to position themselves as a WAAP provider. However, simply adding on to an already-bloated WAF architecture makes things worse not better. With more policies to define and manage and more alerts to analyze, costs will rise while performance and reliability take a hit.

A native, purpose-built approach to WAAP++ can solve these problems. In this paper we lay out some of the core concepts of the ThreatX approach to WAAP and how it can deliver a far more effective and efficient approach to application security.

WE TACKLE THIS IN 3 BASIC STEPS:

1. How to Protect All of Your Applications
2. Get Protection Against All Types of Threats
3. Vastly Simplify Your Security Operations

1 How to Protect All Your Applications

Before a security solution can be used to manage or mitigate risk, it has to be deployed to its target systems. This seemingly obvious prerequisite has been a glaring challenge for WAFs over the years. Cumbersome deployment, time-consuming customization, and ongoing tuning of WAFs meant organizations had to focus their efforts on a select few applications. And, in recent years, that coverage problem has grown considerably worse. This is due to a variety of factors:

Most organizations struggle to protect even 15% of their applications.

Gartner, Magic Quadrant for Web Application Firewalls

WAF Challenges

More Applications to Protect: Organizations simply have far more applications today than ever before. More applications mean more application attack surface, and each new application multiplies the amount of work required for AppSec and security teams.

Diverse Deployment Options: Traditional WAFs were designed first and foremost as appliances to be deployed in front of application front-ends. This appliance-first architecture has struggled to adapt to today's mix of local, cloud, and hybrid application deployments. This has led to increased deployment complexity and inconsistent protection depending on where an application is deployed.

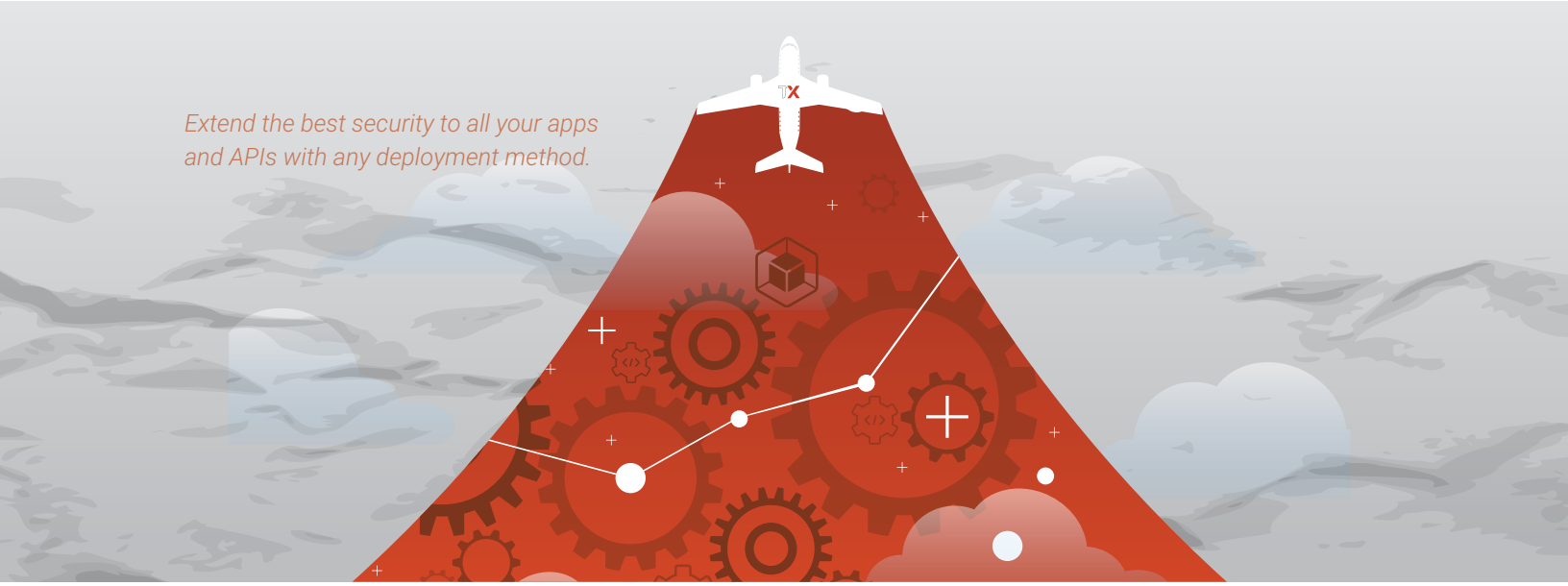
New Application Architectures: With the rise of containerized applications and microservice architectures, an appliance-based approach has grown obsolete. Instead of a monolithic architecture with a single front end, these newer applications consist of logically separated and decentralized modules that can require their own unique protections.

The Rise of APIs: WAFs have struggled to provide coverage for the APIs that modern applications increasingly depend on. APIs have their own protocols, unique risks, and attack models, and expose new powerful paths to the internal workings of an application. The traditional WAF architecture has struggled to extend coverage to these critical APIs, and in most cases, protections are limited to a subset of the capabilities taken for granted at the web frontend.

For these reasons, it is no surprise that in the recent Magic Quadrant for Web Application Firewalls, Gartner found that most organizations struggle to protect even 15% of their applications.

How the ThreatX WAAP++ Helps

ThreatX provides a native approach to WAAP++. Unlike WAFs that attempt to force an appliance-based architecture to do things it was never designed to do, ThreatX is built from the ground up as a cloud and API-native solution. This translates into deployment that is far simpler and protections that are consistent, ensuring that organizations can extend their best security to all their apps and APIs.



Cover All Deployments

ThreatX deploys easily on premises, in hybrid environments, or in the cloud, using the ThreatX cloud or within any cloud service provider. ThreatX's cloud-native architecture quickly extends equal protection to all apps. Deployment is achieved with a simple DNS update, often discovering and protecting apps and APIs that were overlooked or forgotten.

API-Native Protection

ThreatX also provides native support for APIs. This includes decoding JSON to detect threats in API calls, native support for WebSockets, tarpitting Layer 7 DOS attacks, and protection from a wide variety of additional API specific threats and reconnaissance techniques. Instead of bolting on a few API features, ThreatX is designed to address the unique threats APIs face.

Microservices and DevOps Ready

ThreatX easily aligns with the latest application architectures and development methods. ThreatX functionality can be deployed in a Kubernetes sidecar deployment (among others), allowing protection to extend to the individual module or workload. Just as importantly, DevOps teams can ensure that security is built in even as new components are deployed.

Read on for step 2

2 Get Protection Against All Types of Threats

As web applications have evolved, so too have the threats that target them. Over the past few years the threat landscape has undergone a transformation in terms of sophistication, diversity, and sheer volume of attacks. Sophisticated threats often patiently develop attacks over time, employing a variety of evasion techniques to avoid traditional detection.

At the same time, organizations face completely new classes of threats such as bots and malicious automation, and new DDoS and Layer 7 attacks. And with the inherent exposure to the Internet, web-based threats of all types can be automated at scale, leading to an overwhelming volume of daily attacks.

The sophisitcation and volume of attacks continues to evolve and increase.

WAF Challenges

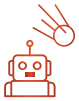
It is no coincidence that these changes have put unique stress on traditional WAFs. In many ways, threats have evolved to take advantage of inherent weaknesses in conventional WAFs. Evasion techniques can circumvent the rules and signatures that traditional WAFs rely on. Slowly-evolving attacks can stay hidden in the noise of low-level events without ever being seen as significant. Bots can be indistinguishable from regular visitors and abuse application functionality without ever triggering a block.

To adapt, many WAFs have attempted to layer additional modules or even separate products on top of their core signature-based detection engines. This has led to greater complexity for AppSec teams. Each component module or product typically requires its own configuration and policies, generates its own alerts, and incurs its own costs both financially and in terms of performance.

How the ThreatX WAAP++ Helps

ThreatX is built on a unified approach to threat prevention. The ThreatX solution is organized around a central decision and risk engine that looks at all types of threats, using multiple forms of analysis, and across all phases of attack. This provides a single solution for traditional WAF threats, anti-bot defenses, and DDoS protections.

Most importantly, these protections are not simply a collection of separate features. ThreatX uses an ensemble-based detection engine that blends signatures, behavioral analysis, active interrogation, and deception to deliver a single automated answer that clearly defines the threat and its risk to the organization. Key capabilities include:



Bot Protection and DDoS Mitigation: A true WAAP solution must include protection from malicious Bots and DDoS attacks. ThreatX brings together a variety of application and attacker profiling techniques to detect bots malicious automated attacks including account take-over (ATO), credential stuffing, carding and much more. ThreatX is able to provide protections from both volumetric and Layer 7 DDoS attacks. These DDoS protections extend to API functionality where attackers can often attempt to drag down the application with expensive API calls.

Risk-Based Decision: ThreatX brings together all of its many contexts to deliver a single, continuously updated risk score associated with an attack. The risk score incorporates all detection methodologies and all correlated events. By incorporating many perspectives and contexts, the risk score can be used to drive automated blocking protections with very low risk of false positives. Not only can this risk score be used to automatically block a threat, it can also be used to automatically unblock once the threat has passed.

Correlation and Context over Time: Modern attacks often go through a variety of stages from initial reconnaissance and mapping, to exploitation, to the ongoing command and control of malware or compromised applications. ThreatX automatically fingerprints and tracks attackers over time so that the full narrative of an attack remains in context. This allows security teams to see the full scope of an attack and the significance of small events that might seem insignificant on their own. This automated correlation of events within the WAAP solution means that teams can get better answers faster without relying on external correlation in SIEMs or analytics platforms.

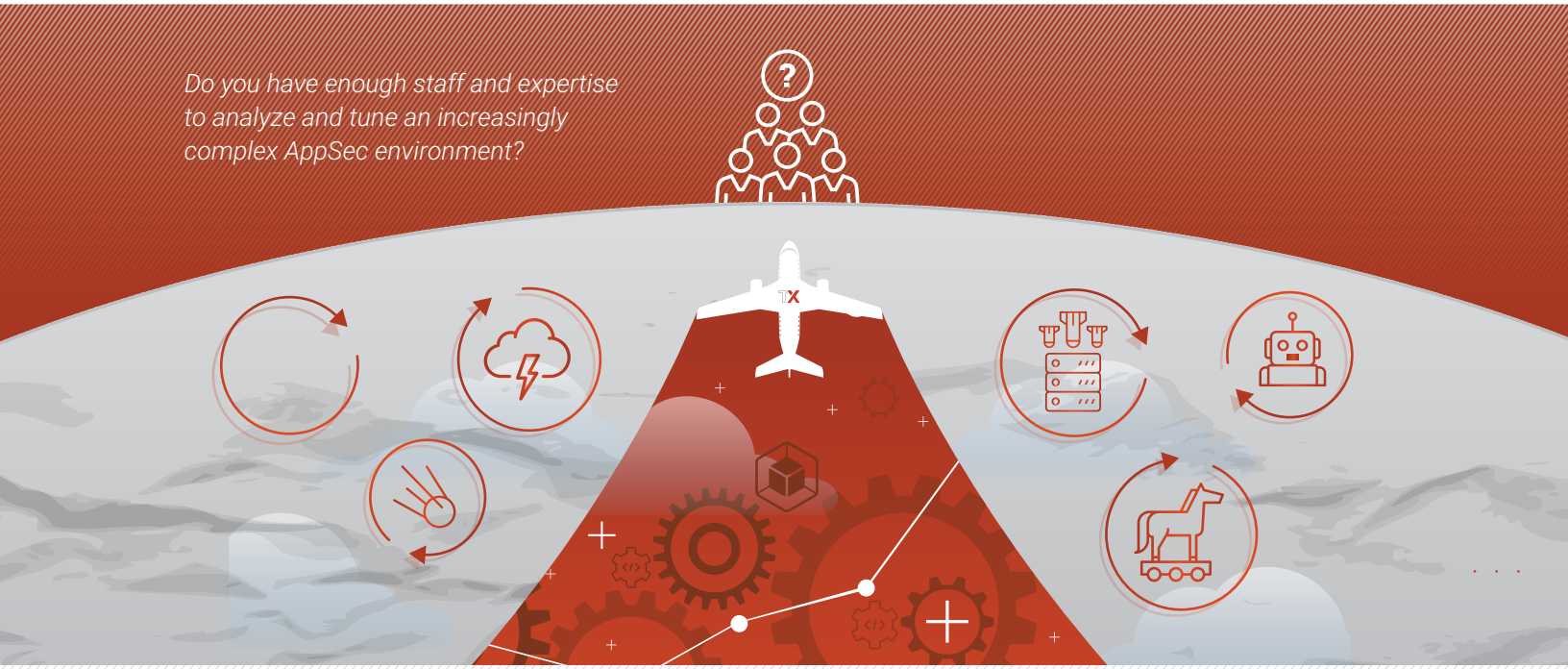
Ensemble Detection Model: Security tools often specialize in one style of analysis, and likewise excel at detecting one style of threat. ThreatX brings together multiple techniques that are automatically integrated to provide a single answer based on all available contexts. This includes application profiling to identify potential signs of abuse that would not be seen by signatures. Attacker profiling that reveals the unique behaviors, traits, and tools associated with attackers and threats. The ThreatX platform can then proactively interrogate and challenge suspicious visitors to distinguish true threats from benign visitors. When needed, the solution can further apply deception or tarpitting to respond to threats.

Read on for step 3

3 Vastly Simplify Your Security Operations

A true AppSec solution should ultimately make security operations simpler and easier to manage. However, adding AppSec tools and modules often increases the workload on security staff. More security tools often means more alerts and anomalies to investigate, more policies to tune, and more data to correlate.

To make matters worse, skilled cybersecurity staff are in incredibly short supply. A recent study from (ISC)² found that there is a global shortage of more than 4 million cybersecurity professionals, with a shortage of more than 500,000 in the United States alone. Likewise a study from Tripwire found that 82% of security teams were understaffed, and 85% found it was more difficult to hire security professionals.



The combination of too much data and too little security staff can quickly overwhelm an AppSec team and leave even the best security tools ineffective.

How the ThreatX WAAP++ Helps

ThreatX allows organizations to remove the bottlenecks in their security operations and free their security staff to focus on high-value work. This is made possible by internal efficiencies of the ThreatX platform itself combined with access to ThreatX built-in Security Operations Center (SOC) service.

Reduction in Alert Fatigue: ThreatX's internal correlation and risk engine allows organizations to reduce the number of alerts that need to be manually processed and analyzed by staff. Multiple detection contexts and multiple events over time are internally correlated to provide a singular up-to-date view of a particular threat. Staff still retain the ability to dive into full detail of every supporting event for analysis and confirmation of a threat, and likewise all logs can be shared with external SIEMs for additional analysis. But more importantly, block decisions are viewable at a higher level of abstraction, reducing workload to manageable levels.

AppSec-as-a-Service (ASaaS): One of the important aspects of ThreatX's WAAP++ is the inclusion of security services as part of the platform. Customers are free to use services as much or as little as they need to get support for things like alert monitoring, incident response, development of custom policies, system administration and much more. This allows organizations to offload specific tasks to the ThreatX team to free in-house talent to focus on other priorities.

Access to Expertise: In addition to operational horsepower, ThreatX also provides access to some of the most highly trained AppSec talent in a variety of disciplines. For example, while targeted and customized Bot-based attacks are increasingly common, many organizations do not have an in-house Bot expert. In this case, customers can leverage the ThreatX experts who have extensive experience developing countermeasures for these types of application-specific attacks. This access applies to all other disciplines as well including DDoS and API based threats.

Conclusion

AppSec is undergoing profound changes. As threats and challenges evolve, so too must the security tools that are trusted to keep applications safe. Unfortunately, aging WAF architectures have struggled to keep pace with these changes. ThreatX provides a new purpose-built approach known as WAAP++.

WAAP++ BENEFITS

1 Protection for All of Your Applications

Cover all applications including local, cloud, and API assets.

2 Protection from All Types of Threats

Coverage from all types of threats from traditional OWASP threats, bots, DDoS attacks and more.

3 Simplfied Operations & Access to Experts

A highly efficient approach to security and the ability to access expert services as needed to ensure that security capabilities and security operations are always in sync.

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