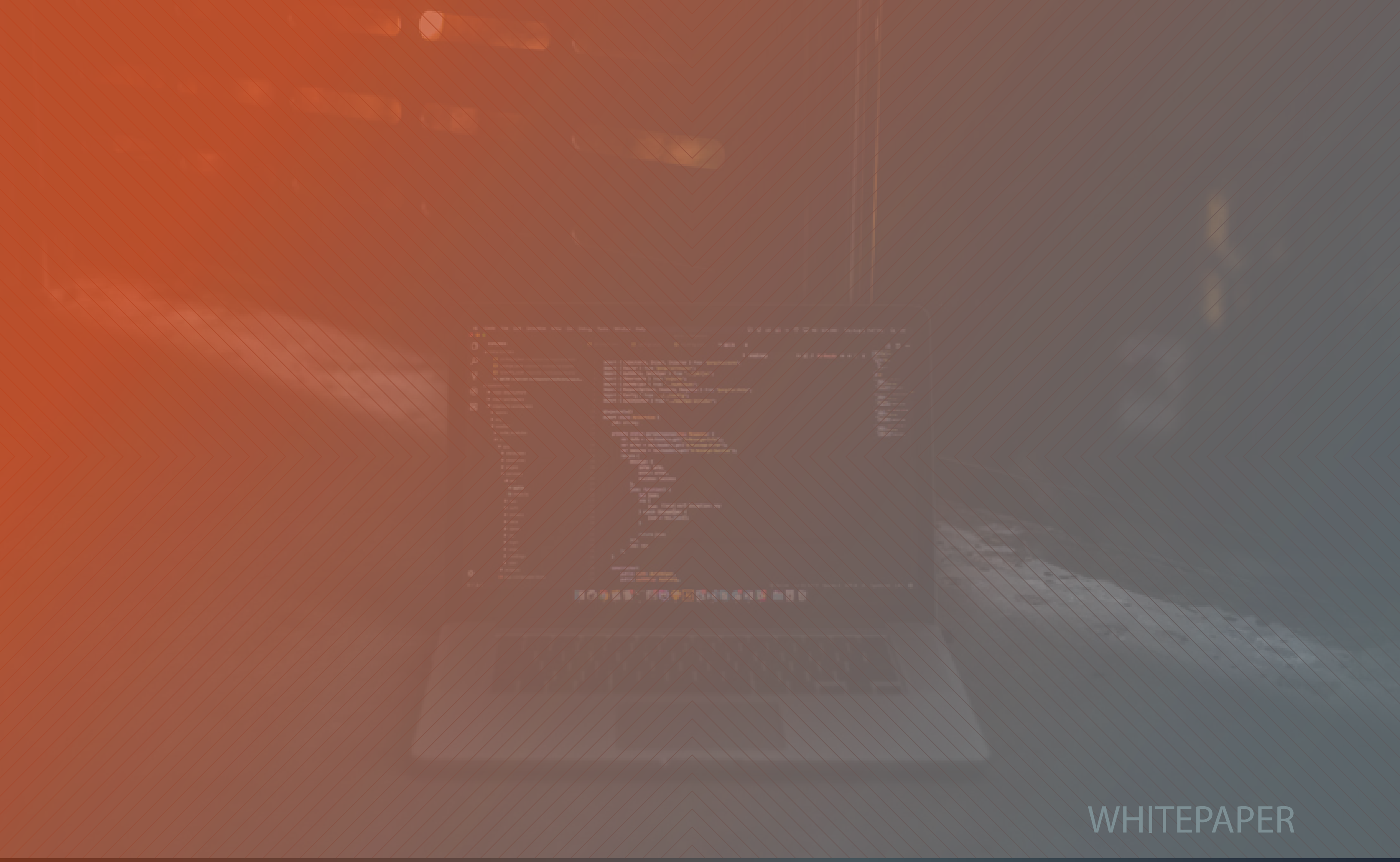

SRC CYBER SOLUTIONS LLP

THREATX

Implementing a Full-Spectrum Approach to AppSec

Introduction

Application Security has undergone massive transformation in recent years. This transformation has spurred the creation of a wide variety of new, specialized products and approaches in security. As this new era of AppSec continues to mature, organizations increasingly need a more unified approach to security. This is true both for the operational needs of the organizatio as well as the quality and effcacy of the security solution.

From an operational perspective, most organizations are plagued by having too many products to manage, too many alerts to address, and not enough coordination and time to make use of all the data they generate. A modern AppSec platform should tame product and alert fatigue, and comnine the myriad of security disciplines and techniques into a unified approach. A Next-Gen AppSec platform can blend varied capabilities into a single offering:

- Application profiling
- Behavioral attacker detection
- API protection
- Deception
- Anti-bot
- DDoS
- Virtual patching
- Edge caching
- SIEM/SOAR integration

This approach delivers high-confidence answers with minimal alerts and analysis and is far greater and more efficient than the sum of its parts.
While this unified approach is helpful for security operations, it is absolutely critical for security. The modern threat landscape continues to evolve and techniques used by one type of threat often blend into another. Bots may attempt to abuse exposed application functionality. Automated attack platforms are used for reconnaissance and exploitation. DDoS attacks can be large-scale, volumetric attacks or target critical application-level functions via an API.

All of these threats will attempt to obfuscate their true origin from security defenses and constantly move to evade simple reputation rules. As boundaries between these types of threats become blurred, it is critical that an enterprise approach to security addresses all types of threats, regardless of their type, including:

- Traditional and signatureless threats
- Bot-based and human attackers
- Web front-end and API attacks
- Traditional and microservice architecture
- Volumetric and Layer 7 DDoS

With these requirements in mind, this paper explores some of the key requirements of a Next-Gen AppSec platform and how it can be used to build a coordinated, full-spectrum approach to application security.

Learn more at www.threatx.com

More Than the Sum of Its Parts

Before diving into specific capabilities and details, it is important to note that a modern AppSec platform needs to be more than just a collection of features. The many techniques and perspectives within the platform need to work together to deliver the best possible decisions and conclusions, no matter which solution elements are at work.

An attack may (and most likely will) use entirely different techniques during the reconnaissance phase than it does during the attacking phase. An AppSec solution may, likewise, employ different detection strategies during each phase of mitigation: application profiling to detect reconnaissance phase; active deception during an intrusion attempt, for example. To make smart decisions based on a specific threat, these techniques need to inform a cumulative risk profile that persists and adapts over time.

Understanding Cumulative Risk

The system needs to recognize relationships between different types of events, behaviors. All perspectives and context must be integrated into a single "total risk" view for a given entity. This can be accomplished by risk engines, decision engines, or other higher level policy managers. Most importantly, the many disparate security techniques must culminate in a clear, consolidated result that doesn't depend on staff or third-party correlation analytics.

Temporal Context and Fingerprinting

In order to maintain this context, a platform must have the ability to track an attacker over time, often as the attacker shifts between disparate IP addresses and locations. This is particularly important to connect different malicious actions across the attacker kill-chain. For example, attacker profiling can be used to identify specific traits and behaviors that are distinctive for particular attackers. Hosts can be used to marked and tracked with various types of cookies and injection techniques in order to maintain context between visits. This information can be identified and learned on a specific application or enterprise them shared globally with other enterprises. Working together, these techniques ensure that the platform can see and correlate even very low-and-slow attacks, and deliver a complete picture of the risk facing the application.

Ensuring Application Performance and Availability

For some organizations, the availability, reliability, and overall performance of an application is as important (if not more so) than security. Even the best security has limited value if the application being protected isn't available in the first place. And while application availability and security can be addressed by separate teams and solutions, many modern application teams are finding it is much easier and more efficient to ddress both with a unified platform. At a high level, an AppSec platform can help ensure the health of enterprise applications in two key ways:

1. Optimizing the content and user experience for valid users
2. Repelling DDoS attacks designed to disrupt the application

Let's take a look at how this is accomplished.

Integrated CDN Services

A content delivery network is becoming a core component of AppSec platforms and is crucial both for ensuring end-user performance as well as stopping DDoS attacks. First, a CDN should ensure quality performance and user experience for end-users accessing dynamic content. Global POPs allows organizations to scale content delivery to support new applications or sporadic high-load events. Additionally, the CDN can distribute and serve user requests and content directly from edge servers to further minimize latency and impact on origin servers. Having CDN and security services integrated lets both areas work together rather than relying on separate components to manually integrate and analyze.

DDoS Protection Across All Layers

In addition to optimizing for performance, a CDN provides an ideal way to scrub high-volume DDoS traffic directed at an application. DDoS attacks can come in many forms including attacks at the application level that can overwhelm it with expensive functions or queries. This variability requires the solution to monitor and learn the behavior of an application and its components to recognize when the application is being unduly taxed. Ultimately, an effective AppSec platform must be able to address both volumetric DDoS attacks as well as the more sophisticated Layer 7 attacks. This can require different types of intelligence and enforcement in different locations. For example, volumetric attacks might be best addressed in the cloud, while Layer 7 attacks may require behavioral analysis and enforcement at the WAF layer.

Multiple Styles of Threat Detection

Applications face an incredibly diverse landscape of threats, and no single technique can reliably catch them all. As a result, modern AppSec platforms require an ensemble of detection methodologies that work together. Let's briefly take a look at a few analysis methods that a solution sholud employ.

Traditional Threat Detection

While threats continue to advance, the traditional attacks against applications remain as relevant as ever. Various types of injection attacks, XSS, XSRF, authentication, and access control weaknesses all remain daily concerns for any application. While these and other OWASP Top 10 threats are well known, they remain incredibly popular attack vectors in the wild. As such, it's a basic requirement for any AppSec platform to

Application Profiling

Behavioral analysis offers a new and powerful approach to identifying threats and problems in an application without relying on rules and signatures. This is particularly important for modern AppSec because new threats may not have a known signature. Alternatively, threats such as bots may not use an exploit at all, and instead, try to abuse exposed functions of the application.

Application profiling learns the normal behavior of an application and its services and can recognize deviations that may signal a threat. For example, attackers enumerating application services or looking for vulnerabilities typically have a very different intensity than normal users and will progress through forms or other application functionality differently than a human visitor.

As mentioned earlier, DDoS attacks can often target computationally expensive functions in an app, which can lead to slow response times. Application profiling can detect these signs of an attack and raise the risk. In many cases, however, application profiling may not be conclusive on its own. Not all anomalies are signs of malicious behavior, but they can provide a critical perspective for seeing the overall scope of an emerging attack.

Attacker Profiling

Attacker profiling uses a blend of behavioral analysis, machine learning models, and statistical analysis to identify the unique signs of attackers. Again, this approach is able to detect threats without the need for signatures or predefined IOCs. Instead of an inward view of the application, these threat-facing models look outward at the attackers. These models can look across thousands of behaviors and traits to identify the hidden indicators that distinguish attackers from valid users. This can include low-level traits of an attacking host, such as unique combinations of browser versions, user agents, access behaviors, just to name a few of the hundreds of possibilities.

In addition to detecting threats, attacker profiling is essential for quickly developing intelligent responses when an attack is detected. For example, the platform may use a combination of application profiling, attacker behaviors, and active engagement to conclusively identify a coordinated attack against an app. Attacker profiling can then be used to identify what makes the attacking traffic unique from normal visitors. This enables the attack to be safely mitigated without disrupting availability or the valid user experience.

Attacker Engagement and Deception

Analytical models are great tools for detection, but they are also typically passive in nature. By actively engaging with attackers and suspicious visitors, we can gain critical threat insights that wouldn't be possible with passive techniques alone. For example, if a visitor is suspected to be a bot or part of an automated attack framework, confirmation of that suspicion can be validated by challenging the visitor with javascript or cookies to solicit a response. Likewise, injecting fake fields into a form that are not visible to human visitors can provide a clear sign that a visitor is a bot.

Additionally, active deception can be used to gain further insight into the goals and intent of the attacker, while also mitigating the damage. Including honey content or fake resources can let security follow the progression of an attacker without putting actual application resources at risk. Alternatively, techniques such as tarpitting can slow an attacker's progression to the point that their scripts or automation is no longer effective. These approaches are often the most valuable later in the detection and enforcement process, as they can confirm suspected threats, while shifting into the protection and enforcement phases.

Anti-Bot and Automation

Detecting and mitigating bots and malicious automation is an essential requirement for a modern AppSec platform. Malicious bots often account for 20% or more of the traffic on an application, and they can be used in a variety of ways. The vast majority of attacks are highly automated throughout the reconnaissance and exploitation phases.

What's more concerning is that bots can abuse exposed functionality of an application without the need for exploits at all. Bots can use credential stuffing techniques to break in and take over user accounts. They can be used in carding attacks to validate stolen credit cards or automate the creation of bot-controlled accounts for astroturfing or buying out scarce products.

As automation has become central to a wide variety of attacks, it is increasingly critical for anti-bot capabilities to be integrated into a comprehensive AppSec platform rather than a standalone product. As we have seen in earlier examples, application profiling, attacker profiling, and active engagement can all play a role in distinguishing bots from valid human visitors. This ability to distinguish humans from bots can not only prevent new classes of threats, but it adds crucial context that we can use in risk-based decision engines.

Ensuring Full Coverage Across the Enterprise

Thus far, we have focused on the techniques and intelligence used to protect applications. However, a true AppSec platform must be able to extend these protections to all parts of an application and to all application architectures.

Security for APIs

Today, APIs are a fundamental building block of modern applications. Allowing developers to quickly access and integrate functionality into their applications, while also providing a standard way to access application functionality on a variety of platforms is essential. However, these APIs can expose the inner workings of an application to attackers and they typically lack the same level of protection found at the web frontend. While API gateways can provide logical balancing and access controls, they often lack the threat detection and prevention capabilities of a WAF.

A modern AppSec platform needs to be able to natively support the security needs of APIs. The platform must be able to natively decode and detect threats such as SQL injection even within JSON or Websockets. Security must also have the ability to recognize reconnaissance, enumeration, and fuzzing against APIs. Ideally it should also be able to enforce policies based on risky calls like 'changeAdminPassword' or expensive calls like 'createImage'. Obviously, appropriate policies will vary from application to application, but the AppSec platform must be able to align to the unique needs and risk tolerances of the APIs.

Microservice Architectures

Microservice architectures have made applications far more modular, while enabling development pipelines that are faster and more efficient. However, traditional appliance-based approaches to security have failed to keep pace with these changes as application functionality is split into more and more self-contained modules.

It's important for modern solutions to automatically integrate into this new application fabric as new modules are developed and deployed. Instead of models based on physical or virtual appliances, security must often take the form of a Kubernetes sidecar that can ensure security is built-in at the level of a Kubernetes pod. This not only ensures protection against threats but also allows the platform to monitor API connections between modules, while also profiling normal behavior to identify any deviations. Bottom line: organizations need to be able to defend all of their applications consistently regardless of how the application is architected internally.

SIEM and SOAR Integration

In addition to supporting the ways applications work, an AppSec platform also needs to work with other security tools and support the overall process of security operations. And while the overarching goal should be to deliver high-confidence decisions and actions within the platform itself, the data is often invaluable throughout the organization. The platform should provide fine-grained insight into security events for SOC analysts to further verify, investigate, or hunt for threats. Naturally, some of this analysis occurs on aggregated datasets collected from a variety of products, and as such, AppSec tools should work seamlessly with SIEMs and other security analytics tools.

Likewise, the solution needs to work with and empower the overall SecOps processes. This often requires the solution to have its open APIs to share and take in information from other systems. In particular, the platform will need to integrate tightly with security orchestration and automation or SOAR platforms. This ensures that the information within the platform can be shared and available wherever it is needed in the organization, while also driving responses beyond the scope of the platform itself.

Conclusion

As the application landscape grows more complex, enterprises increasingly need an integrated platform that can simplify the security and availability of all their applications. Instead of fracturing application security into countless point products, a unified approach is both more effective and operationally efficient. By blending multiple detection strategies (traditional, behavioral, active engagement, deception, etc), ThreatX is able to detect all types of threats (known, unknown, and bots) with high confidence across all phases of an attack. With integrated application performance optimization and DDoS protection, the platform ensures that applications not only remain secure, but also deliver the best possible experience for end users. And with the ability to align with virtually any architecture, ThreatX ensures that your application security program can grow in lockstep with your applications. To learn more, see the technology in action during this brief demo.

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.