AppSentinels.ai
Application Security Re-invented

Application Security for Cloud Native Applications

Background

In the digital age, business leaders see software teams as core to the business and are demanding them to innovate faster in response to market and competitive demands. Organizations are on path of fast iteration - experimenting with new products or features, gauge customer feedback, adopt or drop and move to the next thing. The pace of change is not an option but existential for organizations. Organizations that can adapt will gain market shares and organizations that cannot, will cease to exist.

In response to the need, engineering leaders are constantly looking at ways to make software delivery faster and better. Application architectures have evolved as a result with major shifts like-

- Monolithic architectures to Micro-services design patterns
- Mostly internally developed services to higher use of open-sources and 3rd party services.
- Pre-provisioned static infrastructure to cost optimized Pay-As-You-Go shared cloud infrastructure.
- From waterfall releases to agile mode of development and rapid deployments multiple times a day, further different deployment strategies like Blue-Green, Canary etc.
- Docker and Kubernetes simplifying deployments by improving connectivity between components and elastically scale applications based on the usage trends.
- Clients have also evolved. With mobile being primary access mechanism and with adoption of single page applications.

Engineering and Security leaders are working hard to keep up but cannot slow down even if they are not prepared or have blind-spots.

Implication to Security

Business logic that was all embedded in a single application is now distributed across multiple micro-services. Also due to frequent changes, business logic is never static rather it's fluid and constantly changing. Most importantly, business logic that was completely residing with servers is now controlled by clients as clients connect responses from multiple API's and present to the user.

Further, developers write generic API's serving multiple use-cases. This leads to unintended data exposed to the clients.

All of these have large implications for Security. It means authorization needs to be enforced at granular level across the services. This is a much tougher problem to tackle as traditionally RBAC & role authorizations were weak spots of applications, had no standards and is now fully exposed to the malicious users. This exposes many zero-day business logic exploits to the hackers.

Further as applications evolve over time, more API's are added and obsolete APIs remain in the system often undocumented. These are all potential entry points for hackers.

All these are blind spots for traditional application security products. Security leaders should look forward to next generation of application security products that are purpose built to mitigate the new threats.

Characteristics of Next Generation Security Product

Let us look at characteristics a next generation security product should possess -

- Build deep context of application, API structures, API interactions and the dependencies.
- Understand application users and derive roles and associated permissions to incredibly detailed individual object level.
- Continuously learn and quickly update application context for new changes.
- Track application context in real-time for every single user and distinguish legitimate and malicious activity.
- Maintain a data flow map for compliance and privacy observability and track data flows across various application components.
- Consolidated forensic data from all components for faster patient zero analysis and proactive threat hunting requirements.
- Support non-intrusive frictionless deployment in multiple form-factors and deployment modes.
- Zero or minimal impact on application latency, uptime.
- Support elastic scale with ability to ramp up or down with the applications.

Security leaders should keep above characteristics in mind while evaluating vendors for application security products.

Role of Big Data and AI/ML for Next Generation Application Security Product

Endpoints and Network Security verticals have transformed over last few years via EDR and SASE and have shown successful path to do threat analytics in the cloud to protect against advanced threats. We believe a similar shift is needed in the Application Security to protect customers against advanced application threats. However, there are some serious challenges

- Every application has unique business logic that is constantly evolving. AI/ML models for Application Security should be able to train with minimal amount of data available for the specific application.
- Models should be able to train fast to be effective in a constantly changing environment.
- Explain-ability of deep-learning models is a research area in data-science. Application Security ML models should have explain-ability built-in as customers need clear actionable insights.
- The models should also have high accuracy to avoid adding to the alert fatigue already plaguing the industry.

No doubt, delivery from cloud helps simplify management and allow continuous evolvement to cater to new threats. Security leaders looking for next generation application security product should evaluate the solutions against this backdrop.

Summary

There are generational shifts happening in application architecture and delivery. Addressing needs of the next generation applications requires building products grounds up to cater to the requirements. Current generation products like WAF, RASP and SAST/DAST, in any form, cannot fight against the new generation of threats as is evident with the news of API breaches reported on a regular basis. We need purpose-built product to address these requirements.

Application Security must evolve with the Application architectures. We at AppSentinels have built a product that addresses many of these challenges. Let us talk and we will be happy to share with you what we are building.