Microsoft Azure App Service Site Extension

Summary

Companies leverage Microsoft Azure App Service (AAS) to run the apps and APIs driving their business. With a one-click deployment, the Signal Sciences site extension protects applications hosted on AAS, enabling enterprise companies to protect their business-critical apps and APIs.

Enterprises use Azure App Service, Microsoft's serverless Platform-as-a-Service (PaaS), to run the applications and APIs that drive their business. But DevOps and security teams also need to protect those digital assets against layer 7 attacks without major changes to their operational procedures—and now they can with the Signal Sciences site extension for AAS.

Unlike other WAF and RASP site extensions that are programming language-specific, Signal Sciences Azure Site Extension integrates at the platform layer instead of the code layer. This makes it compatible with any web app that can run on IIS within AAS.

Protect any App or API in Azure App Service

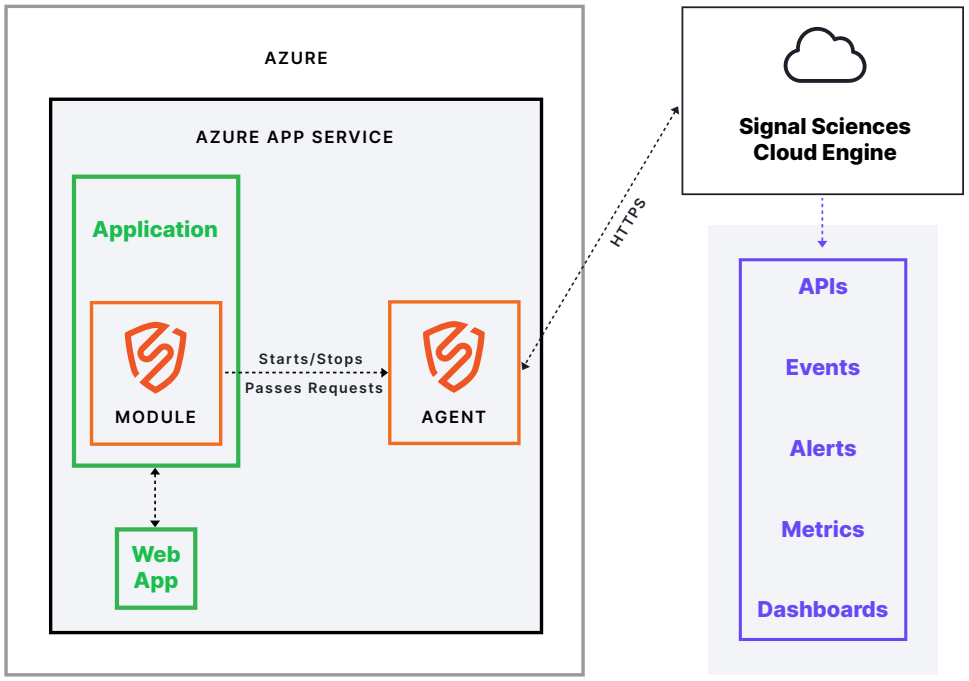
The Signal Sciences site extension for Azure App Service provides detection and protection capabilities for companies running apps on AAS, which is popular with enterprise customers due to its compatibility with legacy applications that run on Internet Information Services (IIS).

How It Works

The site extension automates the deployment of the Signal Sciences agent and IIS module to the customer's AAS environment to protect applications hosted there. It's easy to get started with this native AAS integration:

- Download and install the Signal Sciences Azure App Service site extension with just one click within the Azure Portal.
- Configure the Signal Sciences site extension with your Signal Sciences license key in the web app configuration in the Azure Portal.
- The site extension downloads and installs the Signal Sciences Agent and IIS module into the App Service environment.

Once the site extension is added to your application, the Signal Sciences Agent and IIS module inspect incoming web requests and protect your App Service application.



The Signal Sciences module passes request data to the agent for decisioning. Any requests determined to be malicious by the agent are blocked by the module so they are not passed to the web application. The agent also asynchronously connects to the Signal Sciences Cloud Engine to download the latest WAF rulesets and upload inspection and detection information that can be accessed via the management console.

Features & Benefits of Azure App Service Site Extension

Features

- **Attack protection for any app deployed on Azure App Service**
- **DevOps-focused security alerts across security, engineering, and operations teams**
- **Always-on network flow monitoring to inspect incoming traffic**
- **Scalable protection against both OWASP Top 10 and advanced application layer attacks**
- **Unified management view across your entire app footprint**

Benefits

- **Integration at the platform layer:** Compatible with any web app running on IIS, while still protecting apps and APIs on AAS that drive your business.
- **Automatic protection:** Detect and mitigate attacks without additional operational or management overhead.
- **Cost-effective:** No additional charges for Signal Sciences customers running apps on AAS.
- **Lightweight module:** The extension runs directly in your web servers or application code using a patented, fail-open architecture to communicate with a local agent to ensure your site stays up and runs fast. SmartParse, our patented architecture and proprietary detection technology, eliminates false positives by making instantaneous decisions inline to determine if malicious or anomalous payloads are present.
- **Scalable protection:** Built for the cloud to evolve and scale as your app footprint grows over time.
- **Coverage against all threats:** In addition to the OWASP Top 10 injection attacks, gain protection against advanced web attacks like credential stuffing, bot-generated traffic, web app business logic abuse, and more.