Legacy WAF is Failing

- Static, rule and signature-based approaches simply can’t keep up with modern, evolving threats...

- No integrated solution to scale and cover complex app environments...

- Constant tuning and increased monitoring places huge operational burdens on security teams...
Defining the Next-Gen WAF

**Behavior-Based**
- Detection based on application & attacker behavior
- No need to manage & tune signatures

**Attacker-Centric**
- Go beyond anomalies to identify fundamental attacker actions
- Actively engage, challenge, & deceive attackers

**Cloud-Native**
- Plugs into any architecture
- Cloud, APIs, & microservices
- Stay in step with DevOps
- Rapid time-to-value
The Kill Chain Approach

**Active Tracking and Engagement:**
- IP Fingerprinting/Interrogation
- Deception
- Tarpitting

**Request and Entity Blocks:**
- Low False Positives
- Low False Negatives
# Deployment & Pricing

<table>
<thead>
<tr>
<th>Basics</th>
<th>Can Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on production app coverage</td>
<td>DDoS</td>
</tr>
<tr>
<td>Includes on-boarding &amp; baselining</td>
<td>Edge Caching</td>
</tr>
<tr>
<td>Expert managed services &amp; 24x7 SOC</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>Annual contracts</td>
<td>Defacement Protection</td>
</tr>
</tbody>
</table>
THANK YOU!
Global POPs

Atlanta
Boston
Chicago
Dallas
Denver
Houston
Los Angeles
Miami
Montreal
New York
New Jersey
Northern Virginia/D.C.
Oakland
Phoenix
Querétaro
Sao Paulo
Seattle
Silicon Valley
Toronto
Raleigh

Amsterdam
Barcelona
Dublin
Ehningen
Frankfurt
London
Marseille
Milan
Montpelier
Oslo
Paris
Winterthur

Beijing
Chennai
Hong Kong
Melbourne
Osaka
Seoul
Singapore
Sydney
Tokyo
Global CDN Features

- Deploy in unlimited POPs per-region (NAM, EMEA, APAC)
  - Over 40 well-connected POPs worldwide
  - Multi-Terabit, low-latency connectivity at major peering points
- Static and Dynamic Caching
- Content and Network Optimization
- Volumetric DDOS Scrubbing
- 24x7 SOC
Bot Protection

- **Entity Analysis** - ThreatX applies machine learning and heuristic analysis to all entities to help distinguish bots from true human visitors.

- **Active Interrogation** - ThreatX actively engages potential threats. At the highest level, this includes injection of cookies and JavaScript.

- **Application Analysis** - ThreatX monitors the application for signs of bot-based attacks. The power of bots often lies in their scale, and ThreatX continually analyzes the intensity of traffic to alert staff to bot-based attacks.
Bot Protection

- DDOS
- Scraping
- Credential Stuffing/ATO
- Fake Account Creation
- Carding
Defacement Protection

Traditional WAF protects web sites from front-end attacks:

- SQL Injection, XSRF, XSS, etc.
- OWASP top 10
- Bots
- DDOS
But for many hosted sites, the back-end is unprotected, which can lead to defacement.
Defacement Protection

ThreatX Defacement Protection detects site defacement and keeps users from seeing the altered content. ThreatX will detect defacement and notify the customer of site changes for approval or rollback.
API Protection

- Block unauthenticated requests
- Tarpit L7 DOS queries
- Block SQLi within the JSON request body
- Block API Mapping
- Block Brute Force attacks
- JSON in Websockets support

```
$ curl -u admin@securedmz:unused -X POST -d \"id\":5,\"name\":\";UNION SELECT 1, version() limit 1,1--\" https://api.securedmz.com/api/v1/users
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>403 - Forbidden</title>
<h2>Forbidden - ID: 496ab6e88416426b325522e16623c295</h2>
```
## Comparing Legacy WAF with ThreatX

<table>
<thead>
<tr>
<th>Legacy WAF</th>
<th>ThreatX Next-Gen WAF</th>
<th>ThreatX Customer Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat identification through application traffic analysis looking for predefined signature matches.</td>
<td>Threat detection through attacker tracking, behavioral modeling, and risk measurement. Enables zero-day threat ID. Known bad traffic blocked immediately.</td>
<td>High Accuracy Threat Detection</td>
</tr>
<tr>
<td><strong>Result:</strong> High false positives, and limited zero-day threat identification</td>
<td><strong>Result:</strong> High true positive, high true negative threat detection and protection</td>
<td><strong>Right-Time Risk Based Blocking</strong></td>
</tr>
<tr>
<td><strong>Result:</strong> App protection requiring extensive administration by SecOps</td>
<td><strong>Result:</strong> App protection that evolves with the attack landscape and application</td>
<td><strong>Tuneless Administration</strong></td>
</tr>
<tr>
<td>Threat analysis performed on a per application basis.</td>
<td>Threat analysis performed across all apps and all customers worldwide obfuscating PII.</td>
<td><strong>DevOps Aligned with Ubiquitous Deployment</strong></td>
</tr>
<tr>
<td><strong>Result:</strong> New threat identification restricted to individual apps.</td>
<td><strong>Result:</strong> Fast identification and protection from emerging threats</td>
<td><strong>Access to Expertise</strong></td>
</tr>
<tr>
<td>Threat protection updates through manual signature and rule updates.</td>
<td>Threat protection automatically generated based on attacker tracking and real-time app profiling.</td>
<td></td>
</tr>
<tr>
<td><strong>Result:</strong> High burden for constrained security teams</td>
<td><strong>Result:</strong> Minimal maintenance and tuning burden</td>
<td></td>
</tr>
<tr>
<td>Appliance and SaaS deployment options.</td>
<td>Cloud-native, container based, auto-scaling with world-wide footprint.</td>
<td></td>
</tr>
<tr>
<td><strong>Result:</strong> On-prem deployment with lift/shift to cloud, WAF deployment and tuning can be out of sync with DevOps</td>
<td><strong>Result:</strong> Auto-tuning/scale/update aligned with DevOps, support for legacy and cloud app deployments</td>
<td></td>
</tr>
<tr>
<td>Reactive managed service. Customer burden to upgrade, &amp; maintain</td>
<td>Proactive and consultative security experts that continually assesses target apps and vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td><strong>Result:</strong> Substantial customer staff investment required</td>
<td><strong>Result:</strong> Minimal customer investment and expertise required</td>
<td></td>
</tr>
</tbody>
</table>
## ThreatX Behavior Analysis Capabilities

<table>
<thead>
<tr>
<th>Application Profiling</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine learning that determines appropriate application inputs and responses while continuously adapting to application and environmental changes</td>
<td>Rapid application baselining</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous baselining as application evolves/changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faster threat identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fewer false positives</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entity Behavior Profiling</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time and continuous threat behavior identification, classification, and correlation for all suspicious IPs/entities across all applications and customers.</td>
<td>Automated behavior recognition and dynamic rule generation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instant visibility to highest risk attackers and targeted applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete visibility to attack profile and targeted application weaknesses</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attacker Fingerprinting</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookie injection, JavaScript injection and IP profiling to fingerprint suspicious IPs for future identification and event correlation</td>
<td>Botnet Detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Correlation of events for attacks executed from multiple IP’s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ability to track multiple users behind the same IP address</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Deception</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injection of fake fields, URLs, error codes, headers, JavaScript, etc. for bot identification</td>
<td>Differentiates between legitimate users and bots</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reduced server load from botnet traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protection from Account Take Over and other bot attacks</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cross Customer Correlation</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk analysis, and active blocking based on suspicious entity behavior correlated across applications and customers over time and the ability to define appropriate action as risk escalates</td>
<td>Highly accurate decision/response engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fewer false positives without creating backdoors/false negatives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dramatic reduction in threat analysis and response workload for overburdened security teams</td>
<td></td>
</tr>
</tbody>
</table>
“...We add and acquire new apps and properties all the time, so ensuring uniform threat protection across a geographically dispersed product group is critical for us. Threat X has given us the deep visibility we need into our attack surface, all from a centralized, cloud-based solution that we can deploy across new apps in a matter of hours. Now I can look at our threat profile and vulnerabilities from one risk-based dashboard while relying on the Threat X SOC team as trusted advisors for the latest information and analysis on evolving threats.”

- Bryan Becker, Director of Information Security, Kroenke Sports and Entertainment

- Wide range of applications that support media properties, sporting teams, and venues
- Need to ensure uniform threat protection across a geographically dispersed product group
- Able to deploy Threat X across new apps in a matter of hours
"...We deployed Threat X in days across our complex application environment and instantly had a holistic, risk-based view of all threats and vulnerabilities. Threat X’s unique “kill-chain” based approach immediately reduced our false positives, allowing us to move to blocking mode in days versus the several weeks required by our prior WAF solution. My team trusts the experts in the Threat X SOC to engage us when new threats emerge, and they take full advantage of the automated threat correlation capabilities to significantly reduce their analysis workload."

- Sloane Stricker, CISO and VP Global Operations and Infrastructure, GHX

- Largest footprint in the healthcare supply chain, serving 5,600 providers and 750 manufacturers
- Robust mix of best-of-breed web apps, deployed globally as both cloud and on-premise infrastructure
- In blocking mode in days vs the several weeks required by the previous WAF solution
## The Problem With Legacy WAF Signatures

<table>
<thead>
<tr>
<th>Precise Signatures</th>
<th>Generic Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow protection</td>
<td>Broad and less accurate</td>
</tr>
<tr>
<td>Lower false positive rate</td>
<td>High false positive rate</td>
</tr>
<tr>
<td>Easy to evade and high false negatives</td>
<td>Blocks valid customer/user traffic</td>
</tr>
</tbody>
</table>

### Example:

- **Precise Signature**: *Do not allow Pat in the door if wearing a red hat*
  - *Pat puts on a blue hat and is allowed in*

- **Generic Signature**: *Do not allow anyone in the door wearing a red or blue hat*
  - *Stops Pat and all customers with red or blue hats*

**Signature-based protection is incomplete and un-manageable**
Today’s WAF Buyers are Seeking...

- Full attack spectrum coverage
- Near zero false positives and negatives
- Minimal administration
- Ubiquitous deployment options and cloud native
Information from various sources and behaviors are corroborated in real-time for near 100% attacker validation.

**Primary Abnormal Behavior Detection**
- Scanning, Reconnaissance, etc.

**Interrogation**
- Cookie injection
- Javascript injection
- IP profiling

**Deception/Manipulation**
- Injection of fake fields
- Tarpitting

**Detection of Advanced Abnormal Behavior**
- Brute Force, Exploitation, etc..

**Cross-application attack correlation**
- Shared threat analytics
- X-customer correlation

**External Threat Intelligence**
- Licensed, opensource
ThreatX Detection Model

- Tracks intensity, inputs, responses...
- Finds deviations that reveal signs of attack

Risk-Based
Complimentary Perspectives
Attacker-Centric

- Identifies the unique behaviors of attacks
- Tracks attack in kill-chain context

Active Engagement
Application Behavior
Attacker Behavior

- Actively challenges suspicious behavior
  - Fingerprinting
  - Injection
  - Manipulation
  - Deception