1. Software-only Solution
   - No need for expensive, purpose-built appliances

2. Flexible Deployments
   - Deployable on-premises, in the cloud, across any number of locations

3. No In-line Detection
   - Does not rely on in-line detection, which can introduce additional latency to the network

4. Application Discovery
   - Automatically discovers all web, mobile, and API application assets across the organization

5. No JavaScript or SDK
   - Does not require use of time-consuming JavaScript or mobile SDK modifications

6. Application Firewall
   - Prevent zero-day attacks and address OWASP TOP 10 & PCI 6.6 requirements

7. Economic Value
   - Reduces infrastructure costs, financial loss, business disruption, and damaged reputation

8. Open Architecture
   - Allows data to be shared with SIEMs, WAFs, and more to improve workflows and response time

9. Automated Mitigation
   - Stops attacks fast with customizable, automated mitigation policies - including blocking, rate limiting, and deception

10. Bot Attack Defense
    - Provides effective attack defense against all channels – web, mobile, and API apps

11. AI-Powered Platform
    - With machine learning to provide attack detection/analysis in real time

12. "Baked in" Security
    - Predefined profiles & machine learning eliminate deployment bottlenecks