

Cloud Security On The Edge






BaishanCloud Cloud Shield

Overview

In the process of digital transformation, an increasing number of enterprises are devoting more resources to building their web applications and APIs to meet their growing business needs. While it may provide users with the ability and flexibility to interact with their sites, enterprises often fall victim of malicious cyber-attacks which could lead to such devastating results as server down time, user data breach, compromised database and more. Baishan Cloud Shield security solution fully addresses the security issues of customers and provides them with comprehensive security protection on the edge.

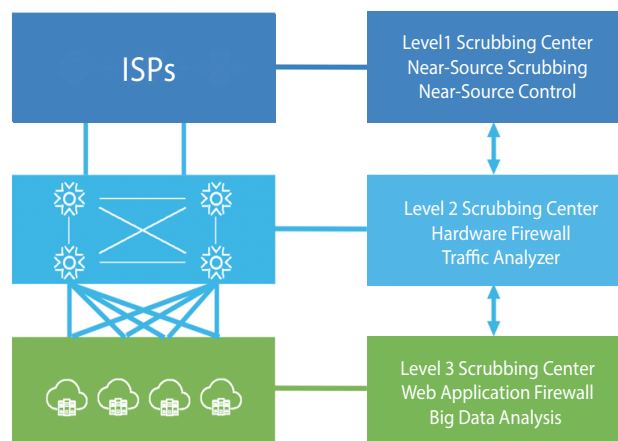
Baishan's Cloud Shield security solution provides broad protection for websites and applications against all types of sophisticated attacks, including DDoS, web application, and direct to origin attacks, leveraging its high-bandwidth, globally distributed network with multiple tiered architectures. It is deployed across Baishan's edge platform, which has more than 450 points-of-presence (PoP) globally across all major continents, so customers do not need to sacrifice performance for protection.

Product Highlights

-  Security at the edge with 30+Tbps capacity globally
-  AI-powered solution to provide up-to-date threat mitigation
-  Tight integration with cloud acceleration service
-  Self-configurable rulesets with real-time logging
-  Dedicated security research team to identify threats

Always-On DDoS Protection

Each PoP in Baishan's globally distributed network is built with proprietary DDoS mitigation technologies. With 30 Terabits-per-second (and growing) capacity, it is a safety net to absorb DDoS attacks on Layer 3 and Layer 4 while allowing the good traffic to pass through. It protects against distributed attacks such as Ping floods, ICMP floods, web sockets attack, transaction floods, resource exhaustion, and UDP abuse. Baishan also works closely with local Internet Service Providers to strategically deploy three-tiered scrubbing centers around the world for more substantial distributed attacks. Each location within the three-tiered scrubbing center can scrub up to 1 Terabits-per-second of DDoS traffic. For application level (Layer 7) attacks, Baishan offers customizable edge rules to protect the network. Our distributed edges will inspect the entire HTTP/HTTPS requests and filter them based on request attributes such as IP addresses, cookies, or headers.



Web Application Firewall at the Edge

Baishan's Cloud Shield WAF protects applications from malicious attacks designed to compromise web servers. It is built on Baishan's globally distributed network with an AI-powered analytical engine to automatically and continuously detect and categorize new threats and vulnerabilities as they emerge (including the zero-day exploits) and to create new WAF rules to mitigate the attack. On top of the rulesets created and maintained by Baishan, this product also incorporates rulesets from open source communities such as OWASP, Common Vulnerabilities and Exposures (CVE), and Chinese National Vulnerability Database (CNVD). The WAF protects against common attacks including injection attacks, cross-site scripting, sensitive data exposure, website tempering, directory traversal attack, and more. Baishan's WAF also offers keyword flagging features, specifically for websites and applications with user-generated content, so customers can detect and replace any keyword to provide necessary content regulation and to avoid censorship. WAF rules can be customized and managed in real-time via Portal or API based on customers' each unique request scenarios. All traffic going through WAF is logged and analyzed for customers to have 100% visibility into their traffic.

Bot Management

Undetected malicious bots can damage a website reputation, steal sensitive information, and negatively impact business revenue. Baishan's Cloud Shield offers comprehensive bot management that built with a machine-learning engine to dynamically detect and block malicious bots. It protects the application against web scrappers, malicious API connections, content tampering, user-specific information stuffing, and more. At the same time, it has a configurable whitelist to allow good bots, such as those belonging to search engines, to pass through to the site. Cloud Shield is built with a sophisticated mechanism to automatically detect malicious bots from the good bots and also allows the customer to customize mechanisms, such as CAPTCHA and JavaScript challenge, to filter away the requests from malicious bots, as an additional layer of protection.

Real-time Logging and Analysis

Baishan's Cloud Shield gives customer full insight into their request profiles, security events, and provide real-time analysis and notifications. Customers can monitor threats and attacks with trend analysis in Portal or consume the statistical data via API to understand the traffic in order to take the most appropriate security measures to protect the websites. Near real-time logging is available and can be pushed to any log analysis platform customer prefers.

24x7 Global Support with Security Monitoring

Baishan's Global Support is available 24x7 to assist customers with mitigating an existing attack or implementing preventative measures for future attacks. Baishan's security experts conduct daily threat monitoring with vulnerability analyses of new threats, monitor industry bulletin boards for new threats and vulnerabilities, and creates new security rules that provide the most up-to-date web application protection.

For more information, please contact: info@us.baishancloud.com.

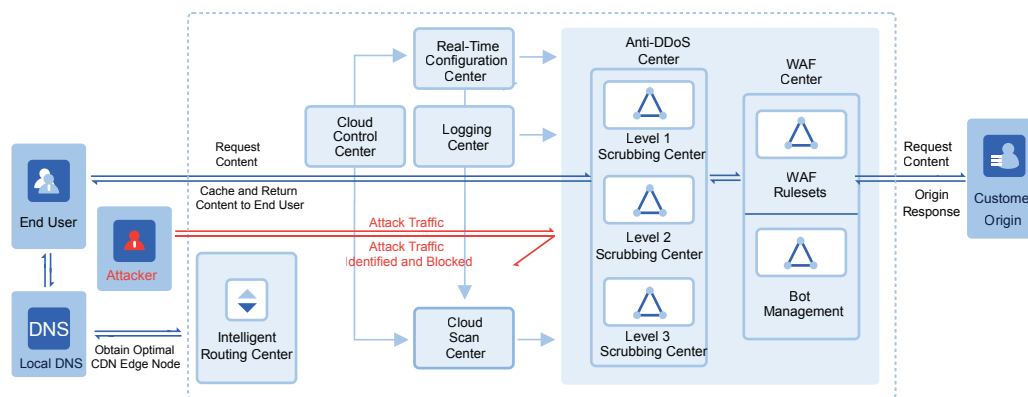


Figure 2 Cloud Security Architecture



NORTH AMERICA OFFICE
777 108th Ave NE,
Suite 2050, Bellevue, WA 98004
Email: info@us.baishancloud.com
Tel: 1-800-260-5186

OFFICES:
Beijing Guian
Shanghai Shenzhen
Xiamen Guangzhou