Besecure Managed WAF Service

Besecure Managed WAF Service is a web application firewall (WAF) service that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations. Using machine learning to model each application, Besecure Managed WAF Service defends applications from known vulnerabilities and from zero-day threats. High performance physical, virtual appliances and containers deploy on-site or in the public cloud to serve any size of the organization — from small businesses to service providers, carriers, and large enterprises.

Web Application Protection

Using an advanced multi-layered and correlated approach, Besecure Managed WAF Service provides complete security for your web-based applications from the OWASP Top 10 and many other threats. First layer of defense uses traditional WAF detection engines (e.g. attack signatures, IP address reputation, protocol validation, and more) to identify and block malicious traffic, powered by intelligence from industry leading security research labs. Machine learning detection engine then examines traffic that passes this first layer, using a continuously updated model of your application to identify malicious anomalies and block them as well.

API Discovery & Protection

Fueling the digital transformation APIs have become increasingly popular, providing the backbone for mobile applications, automated business to business operations and ease of management across applications. However, with their popularity they also increase the attack surface with additional exposed application surfaces that organizations must secure. Besecure's Managed WAF Service provides the right tools to address threats to APIs. API Discovery and Protection uses machine learning algorithms to automatically discover APIs by continuously evaluating application traffic. Discovery is an integral role for establishing a positive security model and protects your critical APIs based on your profiled API inventory. Our WAF Service can also integrate out of the box policies together with an automatically generated positive security model policy that is based on your organization's schema specification (OpenAPI, XML and generic JSON are supported schemas) to protect against API exploits. Schema validation can be integrated into the CI/CD pipeline, automatically generating an updated positive security model policy once the API is updated.

Web Security

- Web Security
- AI-based Machine Learning
- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP address reputation
- IP address geolocation
- HTTP RFC compliance
- Native support for HTTP/2
- Web Socket protection and signature enforcement
- Man in the Browser (MiTB) protection

Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

besecure
Managed E-Business Security™

besecure
Managed E-Business Security™

Bot Mitigation

Besecure Managed WAF Service protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing and other automated attacks to protect your web assets, mobile APIs, applications, users and sensitive data. Combining machine learning with policies such as threshold based detection, Bot deception and Biometrics based detection with superior good bot identification Besecure Managed WAF is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques Besecure Managed WAF can differentiate between humans, automated requests and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required.

Machine Learning Improves Detection and Drives Operational Efficiency

Besecure Managed WAF's multi-layer approach provides two key benefits: superior threat detection and improved operational efficiency.

Our service's ability to detect anomalous behavior relative to the specific application being protected enables the solution to block unknown, never-before-seen exploits, providing your best protection against zero-day attacks targeting your application.

Operationally, the machine learning feature relieves you of time-consuming tasks such as remediating false positives or manually tuning WAF rules. Besecure Managed WAF service continually updates the model as your application evolves, so there is no need to manually update rules every time you update your application.

Our service enables you to get your code into production faster, eliminating the need for time-consuming manual WAF rules tuning and troubleshooting the false positives that plague less advanced WAFs

Solving the Challenge of False Threat Detections

False positive threat detections can be very disruptive and force many administrators to loosen security rules on their web application firewalls to the point where many often become a monitoring tool rather than a trusted threat avoidance platform. The integration might be a matter of minutes, however fine-tuning can take days, or even weeks. Even after setup, the service can require regular checkups and tweaks as applications and the environment change.

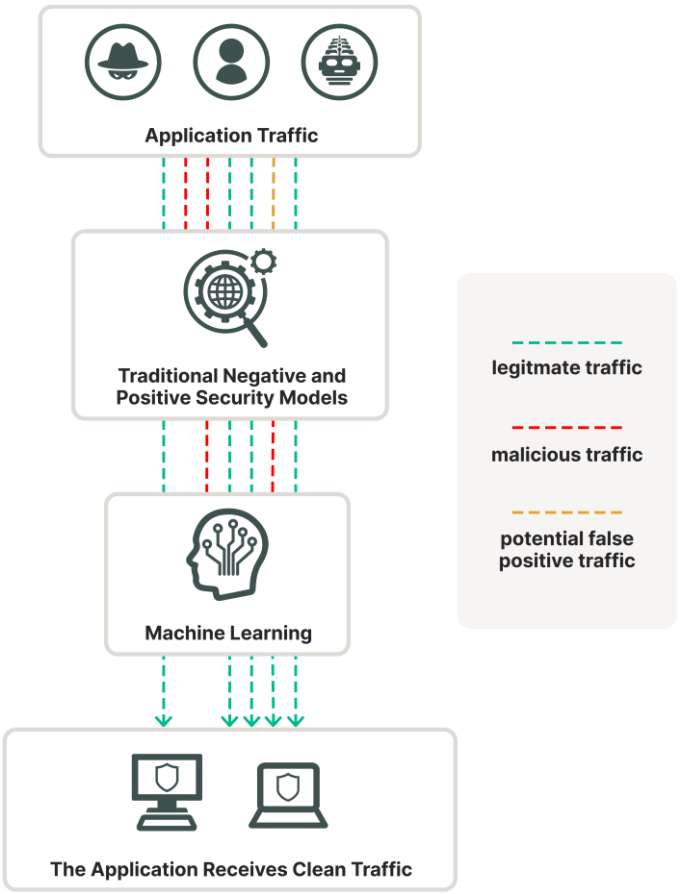
Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)
- File upload scanning with AV and sandbox

Security Services

- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi and XSS detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall § DoS prevention Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

Besecure Managed WAF's AI-based machine learning addresses false positive and negative threat detections without the need to tediously manage whitelists and fine-tune threat detection policies. With near 100% accuracy, the dual layer machine learning engines detect anomalies and then determine if they are threats unlike other methods that block all anomalies regardless of their intent. When combined with other tools, including user tracking, session tracking, and threat weighting, Besecure Managed WAF virtually eliminates all false detection scenarios.



Authentication

- Active and passive authentication
- Site Publishing and SSO § RSA Access for 2-factor authentication
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

Management and Reporting

- Web user interface
- Command line interface
- Graphical analysis and reporting tools
- REST API
- Detailed logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics
- SNMP, Syslog and Email Logging/ Monitoring
- Administrative Domains with full RBAC

Advanced Graphical Analysis and Reporting

Besecure Managed WAF service gives administrators the ability to visualize and drill-down into key elements such as server/IP configurations, attack and traffic logs, attack maps, OWASP Top 10 attack categorization, and user activity. Besecure Managed WAF service lets administrators quickly identify suspicious activity in real time and address critical use cases such as origin of threats, common violations, and client/ device risks.

www.besecuregroup.com

Greece, Southeast Europe
19, Syngrou Ave., 117 43,
Athens, Greece
Tel. +30 210 330 7 440, Fax +30 210 330 7 441

Cyprus, Middle East
133B Fraglin Roosevelt Ave, 3011,
Limassol,Cyprus
Tel. +357 250 29 300, Fax +357 250 29 301

Belgium, Western Europe
Place Rouppe 27,
1000, Brussels, Belgium
Tel. +32 25 88 4470, Fax +32 25 88 4471