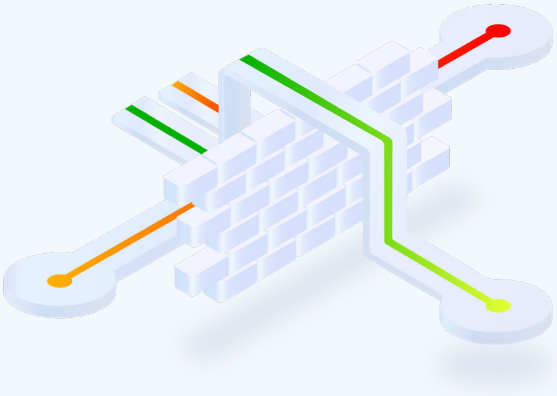

Web Application Firewall

Mission-critical applications must function continuously to ensure business success. Attacked applications can lead to loss of revenue, reputation and brand. Customer facing applications, e-commerce carts and trading platforms must be protected from existing threats and new vulnerabilities, as they emerge.

Web application firewall (WAF) stops threats, attacks and exploitations, where weaknesses exist and provides real-time analysis and reporting on attempted attacks.

Web application attacks

The number of attacks against applications continues to rise and they are rapidly becoming more automated. Common vulnerabilities and exposures, SQL injection and cross site scripting (XSS) attacks are designed to access sensitive and confidential content. As the interconnectivity of business and applications grows, the use of APIs has also increased the attack surface area.

Key Benefits

- Mission-critical applications are protected against evolving threats
- Business critical data leakage can be prevented
- Advanced detection and protection can be automated
- Legitimate traffic and e-commerce are not affected
- Monitor threats in real-time and receive reports

How we combat web application attacks

We provide a unique combination of analytics and threat intelligence to deliver comprehensive web application protection, against all known, severe and new evolving threats. We also help clients expand their mitigation with solutions adapted to specific application needs.

Backed by machine learning and automated policies that update over time, we protect all types of Web and Rest/SOAP API applications to ensure that no harmful requests reach clients' web servers.

The data leakage detection ensures clients' applications do not leak sensitive information, such as credit card numbers and social security numbers.

We offer protection from new attacks via our attack-level insight into the emerging threat landscape which delivers actionable intelligence fed directly into our Threat Protection Platform.

Key features

- OWASP Top 10 policies
- User Behavior Analysis
- Application Behavior Analysis
- Supports HTTP(S), HTTP/2 and WebSocket
- HTTP Protocol security
- Protocol convergence, (HTTP 2.0, SPDY)
- Server load balancing, (advanced SLB methods to monitor CPU, memory usage on SLB members)
- Automated key and certificate management for SSL and TLS
- Proxy mode

Threat Protection Centers™ (TPC)

Amsterdam, New York, Los Angeles, Singapore, Stockholm, Frankfurt, Dubai, Tokyo (2019), London (2019), Miami (2019)

RiverView Portal™

Our RiverView™ portal monitors attacks in real-time. It provides statistics on all traffic and attempted attacks and a comprehensive reporting function allows clients to create daily, weekly and monthly reports.

You receive the best possible protection from fresh attacks with our Security Operation Center which monitors the constantly evolving threat landscape around the clock.

Regardless of where your assets are located – on premises, in cloud-based platforms, third party hosts – our Threat Protection Platform is equipped to provide multi-vector threat protection to all deployed assets.

Baffin Bay Networks AB | Regeringsgatan 65, 111 56 Stockholm, Sweden
info@baffinbaynetworks.com | baffinbaynetworks.com