BAFFIN BAY NETWORKS

Web Application Protection
DATA SHEET

We provide protection against all OWASP Top 10 attacks.

Backed by advanced deep learning and machine learning, we protect all types of Web and Rest / SOAP API applications.

The web application threat

Companies and organizations use web applications such as banking, ecommerce and trading platforms to enhance the scope and functionality of their businesses.

Some of those applications may be developed in-house and some may be purchased externally. Organizations' IT security functions also face the challenge of keeping pace with a rapidly evolving threat landscape as new vulnerabilities are disclosed daily.

Baffin Bay Networks prevents attackers from exploiting these vulnerabilities, and provides real-time logging, reporting, and statistics on attempted attacks.

Web application attacks

Web applications are the targets of increasingly sophisticated attacks that seek to expose sensitive and confidential content. Typical attacks include:

- Injection (e.g. SQL)
- Session management
- Cross-site scripting (XSS)
- Cross-site Request Forgery
- Sensitive Data Exposure

How we combat web application attacks

Baffin Bay Networks operates the world's largest Threat Protection Network™ (TPN), ensuring that we provide protection against all OWASP Top 10 attacks. We also enable customers to extend mitigation with solutions tailored for specific application needs.

Backed by machine learning, signatures, user and application behavior analysis, we protect all types of Web and Rest / SOAP API applications to ensure that no harmful request makes it through to your web servers.

Data leakage detection is an important function used to ensure that your application is not leaking sensitive information like credit card numbers or social security numbers.

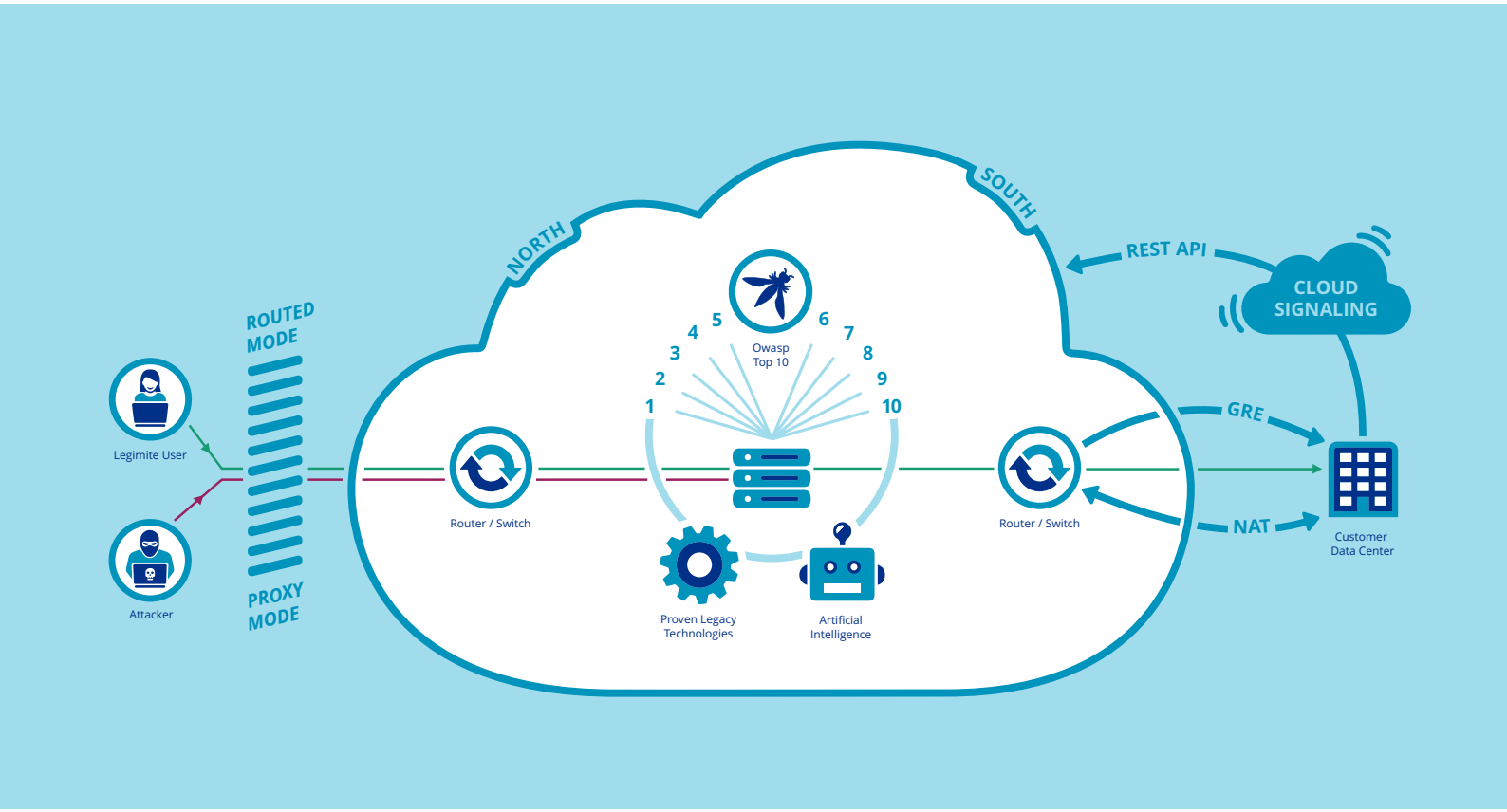
We also ensure that our customers meet all relevant regulatory requirements, for example supporting PCI compliancy. The importance of regulatory frameworks and compliance is set to grow rapidly in the years ahead – an area where Baffin Bay Networks is well equipped to support its customers.

Key features

- Bot-protection
- OWASP Top 10 policies
- User Behavior Analysis
- Application Behavior Analysis
- Supports HTTP(S), HTTP/2 and Web-Socket
- HTTP Protocol security
- Protocol optimization for all major protocols (compression and HTTP pipelining)
- Protocol convergence (HTTP 2.0, SPDY)
- Server load balancing (advanced SLB methods to monitor CPU, memory usage on SLB members)
- Free and automated key and certificate management for SSL and TLS
- Proxy mode

All attacks can be monitored as they occur in real-time through our RiverView™ portal. Statistics on all traffic is available, and a comprehensive reporting engine allows you to manage daily, weekly and monthly reports.

Our Security Operation Center continuously monitors the dynamic threat landscape to offer the best possible protection for new attacks.



MARCH 8, 2017 - REV 1.0.1 EN

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