BAFFIN BAY NETWORKS

Threat Protection
DATA SHEET

We ensure our customers are safe from today's known and unknown threats.

We provide comprehensive mitigation against a range of severe and continually evolving threats.

Threat Protection

Baffin Bay Networks provides comprehensive mitigation against a range of severe and continually evolving threats, including Malware and Exploit Code. We provide a unique combination of technical expertise and exceptional capacity and technology to ensure that our customers always maintain safe and efficient online functionality.

Constantly evolving threats

Although the threat picture is constantly changing, Baffin Bay Networks classifies threats under the following two broad categories: Malware and Exploit Code. Malware, (malicious software), is an umbrella term that includes threats such as viruses, worms, Trojan Horses, and spyware. Exploit Code is code or commands that exploit specific bugs or vulnerabilities in software or hardware, also known as zero-days when vulnerabilities are not public knowledge.

How Baffin Bay Networks ensures comprehensive threat protection

Baffin Bay Networks ensures its customers are safe from currently known and unknown threats. Our Security Operation Center continuously monitors the dynamic threat landscape to offer the best possible protection for new attacks.

Our Threat Protection Center™ (TPC) operates a highly-sophisticated Threat Cloud, and executes all potential threats in a safe environment, (sandboxing). We extract files from the data stream, if the Threat Policy is configured to allow this, and send them to a caged operating system image platform – we support all commonly used operating systems – where we emulate how files would be used on the endpoint.

We monitor everything that a potential threat does, for example whether it makes dependency calls to external files or Internet resources, or whether it attempts to retrieve other malicious software or Exploit Code.

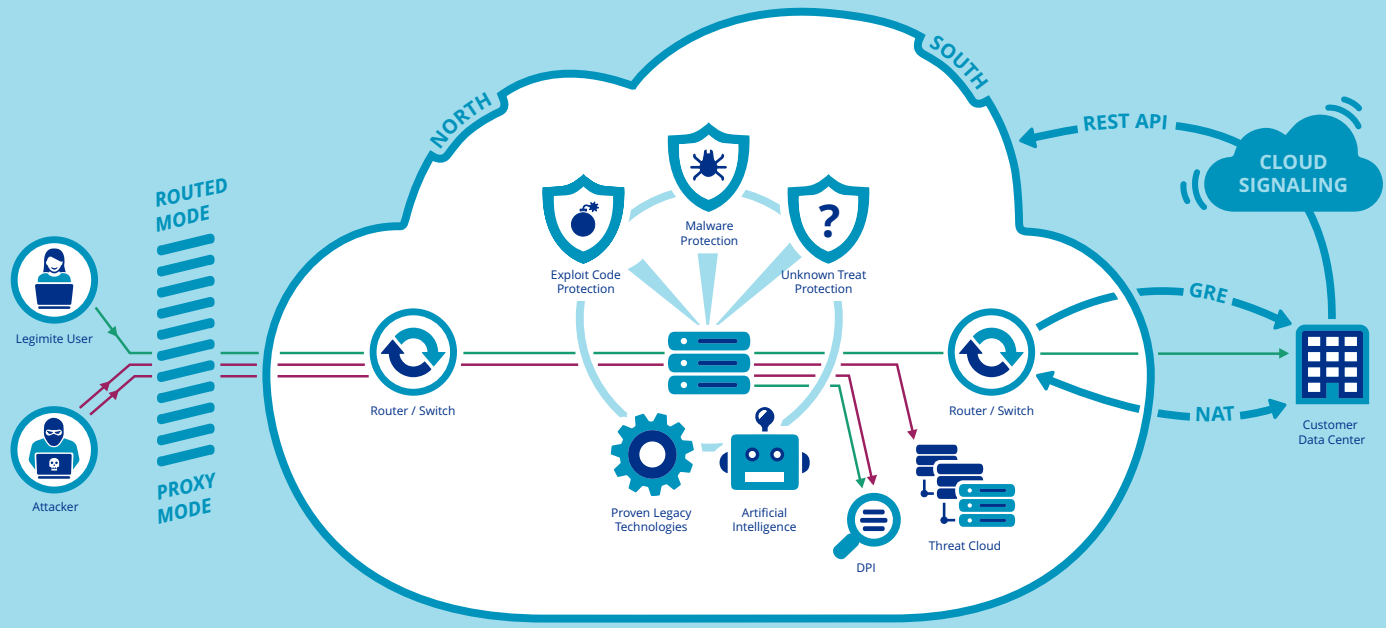
Once a new threat has been identified, we automatically create a new signature that is pushed back to the data path of the TPC, where further mitigation is carried out in real-time.

We rely on advanced static and dynamic analysis of potential threats. Looking at the state of memory prior to, during and after a threat has been executed reveals potential heap spray-based attacks that seek to exploit potential vulnerabilities on the endpoint.

We provide customers with detailed information on all attempted attacks. Customers are also able to upload their own files to the Threat Protection Center™ (TPC) through an API to perform analysis of non-internet based threats that reach customers via external storage functions such as USB flash-drives.

Key features

- Malware protection
- Exploit Code protection
- Protect against unknown threats (Zero-days)
- IP-based Threat Intelligence
- Support for all major protocols
- Protocol security, (HTTP, SMTP, FTP, DNS, SSH)
- 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 traffic
- Proxy and/or routed 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.

Threat Protection Centers ™ (TPC)

Amsterdam, East and west coast US, Singapore, Stockholm and Tokyo

Internet Exchange Points

Amsterdam, Copenhagen, Dubai, Frankfurt, Gothenburg, Helsingfors, Prague, London, Oslo and Stockholm

MARCH 8, 2017 - REV 1.0.1 EN

Baffin Bay Networks AB

Regeringsgatan 65, 111 56 Stockholm, Sweden
info@baffinbaynetworks.com
baffinbaynetworks.com