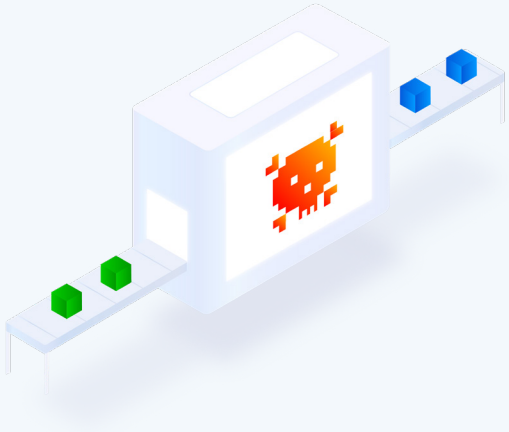

Intrusion Prevention System

Intrusion Prevention examines and inspects network traffic flows to identify potential threats and stop exploit attempts in real time. It provides wide-ranging mitigation against a range of severe and evolving threats, including malware (malicious software) and exploit code, minimizing risk of downtime or system compromise.

Constantly evolving threats

We typically define threats as either malware or exploit code. Malware includes viruses, worms, Trojan Horses, and spyware. Exploit code is code or commands that exploit specific bugs or vulnerabilities in software or hardware. This is also known as “zero-days” when weaknesses are not public knowledge.

Key Benefits

- Combats malware and exploit code
- Continuous, real-time threat monitoring
- Automated signature generation minimizes manual tuning
- Detailed event information for further analysis
- Seamless integration with other modules irrespective of deployment type
- Prevents compromises
- Protects servers against application and OS vulnerabilities

Delivering comprehensive intrusion prevention

We ensure clients are safe from known and unknown malware and exploit code threats. Our Threat Protection Centers™ (TPC™) control potential threats in a safe environment (sandboxing). To do this, we extract files from the data stream, if the Threat Policy allows it, and send them to a caged operating system image platform – the function supports all the most widely used operating systems – where we replicate how files would have been used on the endpoint.

We monitor everything a potential threat does, for example whether it makes dependency calls to external files or Internet resources, or if it tries to retrieve other malware or exploit code. When a threat has been identified, a new signature is generated and pushed back to the data path of the TPC™, where further mitigation is carried out. All this happens in real-time.

We use 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.

Intrusion Prevention offers seamless integration with other modules irrespective of deployment type.

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 convergence, (HTTP 2.0, SPDY)
- Server load balancing, (advanced SLB methods to monitor CPU, memory usage on SLB members)
- Proxy and/or routed mode

Threat Protection Centers™ (TPC)

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

RiverView™

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