Key Features

Use DNS Details to Catch Malware

Detects malware and other applications using DNS for data exfiltration and C2 attacks, as well as discovers misconfigured applications using DNS lookup failures

DNS Query Names

Sees beyond Akamai and Amazon AWS, providing the actual destination domain names for richer context surrounding an event

Application Performance

Build baselines of typical or optimal application performance. When performance suffers, triggered alarms can link you to relevant, helpful reports right away

FlowPro Defender™ Fact Sheet

When network investigations need to take place, security and network professionals depend on solutions that contain the most important communication details. FlowPro Defender™ incorporates Deep Packet Inspection (DPI), which allows it to measure and export metrics beyond the traditional limitations of NetFlow.

Threat Details Matter

Within minutes after installation, FlowPro starts playing a key role in troubleshooting applications. Each gigabit interface is dedicated to a selected portion of your network and sends flows to your collector at line rate with details on all DNS requests.

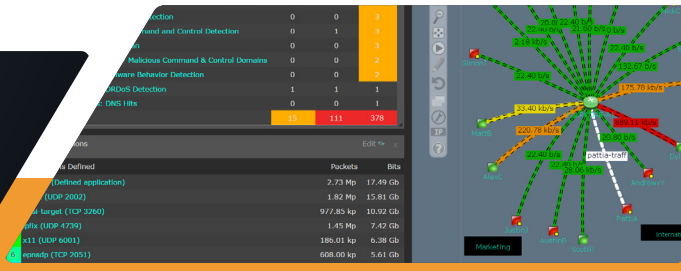
	Client	Responding DNS Svr	DNS Requests
1	dc-1.plixer.local	ns1.oxfordnetworks.net	285
2	dc-2.plixer.local	irdns.pome.myfairpoint.net	215
3	sdcrnl6y1.plixer.local	dc-1.plixer.local	171
4	sd829r942.plixer.local	google-public-dns-a.google.com	153
5	sd82qk942.plixer.local	resolver1.worldpath.net	129
6	192.168.7.81	dc-1.plixer.local	113
7	de27jtc72.plixer.local	dc-1.plixer.local	95

Figure 1. DNS request details

FlowPro Defender keeps an eye on DNS traffic by monitoring DNS lookups, responses, and other types of DNS messages.

1. What malware does it identify?
   - Botnets
   - DNS Command and Control Detection
   - Data Exfiltration
   - Malicious Domain Reputation
   - Malware Behavior Correlation
2. How does it identify malware?
   - FlowPro can identify malware by looking at the DNS lookup failures
   - When a large number of these failures per host are detected, FlowPro triggers an alarm to notify you of the potential malware, including the host and DNS query details

plixer



Destination	Count
ec2-52-54-18-17.compute-1.amazonaws.com	1
204.154.111.113	1
ats1.member.vip.bf1.yahoo.com	1
a172-229-227-246.deploy.static.akamaitechnologies.com	1
a23-219-94-16.deploy.static.akamaitechnologies.com	1

Figure 2. Domain details before implementing FlowPro Defender

Domain	Destination	Count
scss.adobeesc.com.	ec2-52-54-18-17.compute-1.amazonaws.com	1
tps602.doubleverify.com.	204.154.111.113	1
edit.yahoo.com.	ats1.member.vip.bf1.yahoo.com	1
storagetos.datamart.windows.com.	a172-229-227-246.deploy.static.akamaitechnologies.com	1
d14qd3he45186l.cloudfront.net.	a23-219-94-16.deploy.static.akamaitechnologies.com	1

Figure 3. Domain details gained through DNS Query after implementing FlowPro Defender

3. Where is the FlowPro deployed?
   - The FlowPro is deployed in an area of your network where it has visibility into DNS traffic
   - If an organization doesn't have internal DNS, FlowPro can be deployed at the network edge to look for DNS requests and responses crossing the network perimeter
4. More value
   - Discover misconfigured applications using DNS lookup failures
   - Monitor blacklisted domains from a Plixer-maintained database to trigger alarms for violations
   - Providing NetFlow-based visibility into devices or segments of your network that don't natively export flow data

More rich context

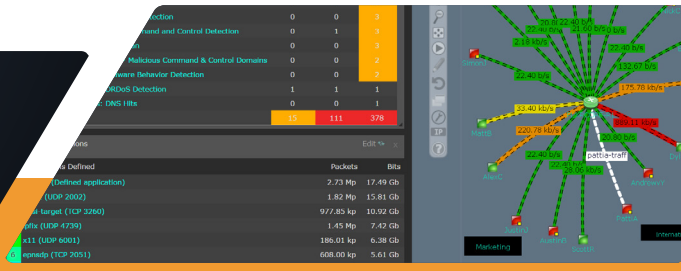
When it isn't being used to uncover malicious activity or guarantee performance, the details FlowPro provides can be cross-reference with metadata from other vendors to complement and pivot between other security platforms like SIEM and packet capture. This results in improved context in all NetFlow, IPFIX, and sFlow exports.

Even when traffic is encrypted, FlowPro gives necessary insight into the sequence of events that led up to a data breach.

Application Performance

Use the FlowPro Defender with your existing flow and metadata collection platform to build a baseline of typical or optimal application performance. When connection performance becomes a problem, alarms can be triggered within your flow collector, which generates reports with additional information. Access to the right details allows the IT team to determine whether the slowdown was caused by the server, the client, or the network.

The FlowPro Defender's details allow the root cause of the issue to be isolated quickly. Since all connections are tracked and sent to the flow collector, network threats (e.g. scans, C&C bots, etc.) are uncovered as well. Correlated with rich contextual details, the FlowPro appliance empowers the IT staff to reduce the Mean Time-To-Know (MTTK) and improve overall operational efficiency.



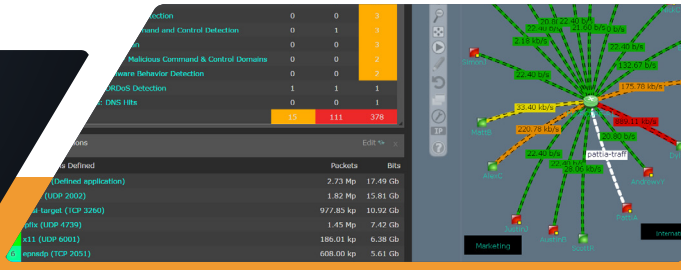
FlowPro Appliance Specifications

	FlowProAPM	FlowPro5-10-APM	FlowPro/FlowPro-DS	FlowPro5-10/ FlowPro5-10-DS
Resources				
CPU	Intel® Xeon® processor (Haswell) 8 core			
Memory	16GB DDR3			
Interfaces				
Management Port	1x RJ45 Copper 1GbE (IPMI optional)			
Monitor Port	3x RJ45 1GbE	5x RJ45 1GbE + 2x SFP 10GbE	3x RJ45 1GbE (expandable to 7x RJ45 1GbE)	5x RJ45 1GbE + 2x SFP 10GbE
Console Port	1x RJ45 standard serial			
Physical				
Hardware Generation	v1.1			
Form Factor	1U			
Height	4.5cm (1.75")			
Width	43cm (16.93")			
Depth	46.8cm (18.43")			
Weight	7 Kg (15.4 lbs)			
Rails	Mounting Ears			
Storage	128GB non-redundant			
Environmental				
Power	Redundant hot swappable 300W PSUs 120~240VAC			
Cooling	CPU: Passive System: 3x cooling fan			
Temperature	System: 0 – 40°C Storage: 0 – 70°C			
Relative Humidity	5 – 90% ambient operating			
Regulatory Compliance				
Please call for a complete list	System: FCC Class A, RoHS, CE Emissions Storage: FCC, UL, TUV, UC, BSMI, VCCI			

**Expansion ports for SFP+ modules to allow for LX and SX Fiber connectibility also included*

The hardware appliance comes with a 1-year warranty against manufacturing defects, and software warranties are covered with a Customer Support Contract. Product evaluations are available upon request. Contact Plixer to learn more.

plixer



207.324.8805