DATA SHEET

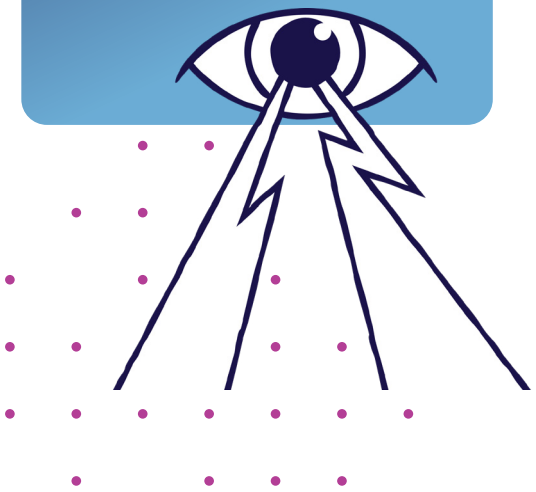
Plixer FlowPro

Security benefits

- Detect abnormal behavior and security threats
- Monitor DNS traffic to catch malware and botnets
- Identify malware that uses C2 communications
- Visualize encrypted web traffic destinations

Network benefits

- Increase visibility where metadata is not exported
- Monitor performance with Layer 7 precision
- Achieve faster fault isolation and MTTR
- Visualize traffic and apps across your entire network



Complete visibility of network traffic is key to managing your network, protecting your assets, and investigating security incidents. While Scrutinizer collects network traffic data directly from a wide variety of infrastructure devices, there are many situations where Plixer FlowPro can be deployed to deliver additional, valuable network and security insights. Plixer FlowPro provides deep packet inspection, application fingerprinting, application performance, and visibility from Layer 2 through Layer 7. It also gives you the ability to monitor domain name system (DNS) traffic to identify the fully qualified domain names for encrypted web traffic, protocol anomalies, and malicious activity.

This single platform enables network operations to efficiently manage and optimize the network, while simultaneously enabling security operations to lower risk, gain data context, and respond quickly to security incidents. Whether you need to monitor traffic in remote offices, an isolated data closet, or a full data center, Plixer FlowPro provides the information you need to perform root-cause analysis of both network performance and security events.

Security benefits

By installing Plixer FlowPro Defender where it can observe your entire network DNS traffic, you gain details about what is entering and leaving your network over DNS.

Ninety-one percent of malware today uses DNS in its attacks. Specifically, malware creators abuse DNS to bypass your firewall and use your DNS servers (internal or external) to communicate directly with assets within your network.

One technique encodes information such as credit card numbers into the fully qualified domain name (FQDN) sent to the DNS server. When the DNS server looks it up, it finds that the domain name does not exist. The local DNS server then forwards the request out of your network with your data, where it makes its way to an

authoritative DNS server controlled by the malware creator. The malware creator can simply decode the FQDN forwarded by your DNS server and store your stolen information for later resale on the black market. Malware creators can also use the DNS reply to send an encoded response back to your asset, providing additional instructions to the malware. Using a combination of deep packet inspection (DPI) and behavioral analytics, Plixer FlowPro Defender quickly identifies and alerts on assets compromised by malware that has leveraged various forms of DNS abuse for data exfiltration or C2.

Network benefits

Cloud-hosted applications such as CRM systems, backups, and email services put your business performance at the mercy of the internet. Resolving issues around poor connection times is often more involved than merely reviewing a bandwidth utilization trend. Packet loss, retransmits, and round-trip time can all be major contributors to a poor application experience. The physical location of the end user can also be a significant factor. Is the problem isolated to a specific end system, an end user, a subnet, or the entire organization?

Plixer FlowPro Application Performance Monitor (APM) empowers network administrators to find the root cause. By leveraging DPI to monitor critical application traffic, both internal and cloud-bound, it provides detailed visibility into each connection to help ensure that the end-user experience remains optimized.

Beyond performance information, Plixer FlowPro APM provides insight into potential configuration issues as well. VoIP quality of service is often measured with MOS score, ToS, packet loss, and jitter; however, phone calls can also be affected by the wrong codec and the network path a call takes. Plixer FlowPro APM exports these factors in a way that makes troubleshooting easier, reducing Mean Time to Resolution.

Deployment options

Plixer FlowPro appliances are rack-mountable servers with all the capabilities pre-installed. Traffic to be monitored is sent to Plixer FlowPro through one of several interfaces on the device. This data is mirrored traffic from routers, switches, or firewalls in your environment that may not otherwise be able to export native flow and metadata.

Hardware appliance specifications are listed on the following page.

Virtual appliances

The Plixer FlowPro virtual appliance is available for deployment on a VMware, Hyper-V, or KVM server.

- The VMware virtual engines are packaged in the .OVA file format.
- The Hyper-V virtual engines are packaged in the .ZIP file format.
- The KVM virtual engines are packaged in the .TAR.GZ file format.

The virtual appliance minimum system specifications are:

- Network connection; Gigabit Ethernet recommended
- VMware ESXi 5.5 and above, Hyper-V 2012, or KVM 14 and above
- 2.0 GHz Quad Core CPU, minimum
- 4 GB DDR3 RAM
- 20 GB SATA drive

Hardware appliance specifications

	Plixer FlowPro 1GbE	Plixer FlowPro 10GbE
Chassis configuration	1U Chassis	
Processor	1 x Intel Xeon° E3-1275 v3 3.5Ghz (4 cores) 95 Watts	
Memory	16 GB	
Storage	128 GB	
Networking	8x RJ45 1GbE	2x 10GbE Interfaces
Power	Dual, Hot Plug, Redundant Power Supply (1+1), 300W	
Power Cords	NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 Amp, 10 Feet (3m), Power Cord, North America	
Weight	15.43 lbs. (7 kg)	
Dimensions	16.9" x 1.73" x 18.42" (431mm x 44mm x 468mm) (WxHxD)	
Environmental	**Storage:** Temperature: -20°C to 70°C (-4°F to 158°F) Humidity: 5% to 95% **Operating:** Temperature: 0°C to 40°C (32°F to 104°F) Humidity: 5% to 90%	
Hardware Warranty	1 Year	

Plixer FlowPro purchasing options

Plixer FlowPro is purchased as a subscription license. The subscription has an ongoing Subscription Agreement as part of the terms of your subscription license. Product updates and customer support are included as part of the subscription.

	Plixer FlowPro	Plixer FlowPro APM	Plixer FlowPro Defender	Plixer FlowPro APM - Defender
Obtain traffic visibility from all network locations	✓	✓	✓	✓
Monitor network traffic	✓	✓	✓	✓
Virtual appliance available	✓	✓	✓	✓
Physical appliance (with up to 7 monitor ports) available	✓	✓	✓	✓
Monitors via SPAN, mirror port, or ethernet tap	✓	✓	✓	✓
ERSPAN support	✓	✓	✓	✓

	Plixer FlowPro	Plixer FlowPro APM	Plixer FlowPro Defender	Plixer FlowPro APM - Defender
Troubleshoot latency issues		✓		✓
Measure application round trip time		✓		✓
Packet-level performance metrics		✓		✓
Resolve network performance issues		✓		✓
Identify Layer 7 applications		✓		✓
Monitor latency for Layer 7 applications		✓		✓
Monitor latency for clients/ servers		✓		✓
Monitor VoIP performance		✓		✓
Detect malware DNS data exfiltration			✓	✓
Detect malware DNS Command and Control			✓	✓
Detect compromised assets using DGAS			✓	✓
Alert on DNS lookup to known malware C2 sites			✓	✓
Alert on DNS lookup to user-defined domains			✓	✓
FQDN reporting			✓	✓
DNS performance visibility			✓	✓

Ordering information

Multiple Plixer FlowPro license options and support tiers (see details in Service and Support below) are available. License costs are determined by a number of factors, including the functionality needed, mirror ports required, and the term length of the agreement.

Hardware appliance: 1 GbE interfaces

The 1 GbE hardware appliance comes with 8x1GbE interfaces. By default, 1 management interface and 3x1GbE monitoring interfaces are enabled. Additional interfaces may be enabled for a maximum of 1 management interface and 7x1GbE monitoring interfaces per appliance.

Hardware appliance: 10 GbE interfaces

The 10 GbE hardware appliance comes with 2x10GbE interfaces and 1x1GbE management interface. By default, the management interface and both 2x10GbE monitoring interfaces are enabled.

Virtual appliance

The virtual appliance supports one management interface and one monitoring interface. Additional monitoring interfaces can be accomplished through the purchase of additional licenses and increasing system resources.

Warranty

As a customer-centric company, Plixer is committed to providing quality products and solutions. If one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your product repaired or media replaced as soon as possible.

The hardware appliance comes with a 1-year warranty against manufacturing defects. Software warranties are covered through the Subscription Agreement.

Service and support

Plixer provides a comprehensive set of professional service offerings. Plixer can design, deploy, and optimize your implementation as well as deliver customized training. Remote services and on-site services are available.

Tier 1 or Tier 2 Support options are available in Subscription Agreements.

Tier 1

Telephone and live chat support is available from 8am-5pm ET Monday through Friday. Response time is within 24 business hours of support request.

Tier 2

Live chat support is available from 8am-5pm ET Monday through Friday. Telephone support is available 24 hours a day, every day of the week. Response time is within 1 hour of support request.

Please contact your Plixer account executive for more information about Plixer service and support.

Additional information

For additional technical information, please visit: https://www.plixer.com/products/flowpro/