Plixer

WHITE PAPER

Deep network observability for cybersecurity

Unlock the security value of your network

The average dwell time for an attack is 280+ days. That's because threat actors understand that most organizations only monitor the edge and crown jewels (data centers, ingress/egress points, or strategically sensitive areas). As such, our adversaries find ways to compromise a network through approved services and with approved credentials. They hide in an unmonitored corner of the network and move in ways that avoid attention and detection.

Just as your business is reliant upon the network, so are threat actors. Cybercriminals need to use the network to execute their objectives. Each move made by a threat actor can be seen, if you're watching closely enough and have a complete picture of what "normal" looks like.

When properly harnessed, the network can reveal threat actors before they have a chance to do damage. Plixer's Deep Network Observability platform extracts network flow data from your existing devices to detect threats in real time.

Avoid the pitfalls of point-specific observability

The usual response is to load up egress points and data lakes with packet capture infrastructure and packet analysis solutions. While this can help determine exact transaction data if a breach occurs, capturing packets comes with complications, costs, and constraints.

Cost	Complexity
Packet problem: Packet infrastructure is too costly to deploy across the network. **Packet solution**: Capture packets only at high egress points or on critical infrastructure. **The result**: Limited network visibility and blind spots for performance monitoring and diagnostics.	**Packet problem**: In essence, you need to set up a parallel network, or portion of your network. **Packet solution**: Devote personnel to maintain and service packet capture infrastructure. **The result**: Divert team members away from mission-critical activities to service tools that are supposed to help you.

Storage	Encryption
Packet problem: Packet files are very large. **Packet solution**: Rather than storing the payload, process and store only the metadata. **The result**: Payloads from more than a couple of weeks old are no longer accessible, leaving you with data akin to flow data.	**Packet problem**: Most traffic is encrypted, hiding the payload from view. **Packet solution**: Process only the packet headers and decrypt the payload if needed. **The result**: Encrypted packet data is reduced to metadata akin to flow; added storage needs for session keys.

In general, packet-based network threat detection solutions struggle to provide deep observability because they only focus on segments of your network.

Go with the flow

Network flow data provides a low-impact solution for deep network observability to detect, investigate, and respond to threats. Network flow data allows you to monitor all network traffic, understand and visualize network behavior and quickly detect threats.

When most people hear network flow data, they think primarily of NetFlow v5. While NetFlow v5 provides valuable information, it is limited in its view. The advent and innovation provided by IPFIX, though, exploded the visibility value of network flow data.

PLIXER'S IPFIX COVERAGE ACROSS OSI STACK	
Layer	IPFIX information elements leveraged by Plixer
7 - Application	FTP, DNS, RTP, SMTP, VoIP, SIP, HTTP, Application ID, NBAR, NTP, SMB, LDAP
6 - Presentation	SSH, SSL, TLS
5 - Session	SQL, ports (src,dst), RTP
4 - Transport	TCP, UDP, NAT, GTPv1/GTPv2, VPN
3 - Network	IPv4, IPv6, ICMP, GRE, BGP, TTL, RTT, NAT, VLAN tags, SD-WAN
2 – Data Link	MPLS, MAC, RADIUS, IMSI, ISDN, Multicast

PLIXER'S IPFIX COVERAGE OF THE OWASP CYBER DEFENSE MATRIX	
Asset	IPFIX information elements leveraged by Plixer
Devices	OS name, OS version, location, MAC address, Browser info
Applications	Application ID, latency, NBAR, HTTP, SIP, VoIP, SMTP, DNS, FTP, ports, NTP
Network	IPv4, IPv6, TCP, UDP, ICMP, GRE, BGP, MPLS, SD-WAN, VPN, RDP
Data	SQL, SMB, TLS
Users	User, geolocation, RADIUS, LDAP

Network flow data, with the power and flexibility of IPFIX, gives you **wider visibility at a more cost-effective scale**.

Plixer's flow-based platform gives you deep network observability that:

- **Is less costly and complex than packet-based solutions**
  - Flow data is gathered from your existing infrastructure
  - This makes flow easier to deploy and manage
  - You don't need to invest in additional infrastructure to gain network intelligence
- **Gives you the data you need when you need it**
  - Get visibility of every conversation and transaction on your network
  - Long-term historical data for forensics
  - Same encryption visibility as an encrypted packet, but with less overhead

Get deep network observability with Plixer

Surgical use of packet capture technology can be very effective. Packets give you excellent point-specific observability. But a packet-based observability solution will by necessity be limited in its totality. And it comes with cost and complications that can be avoided.

If stopping sophisticated cyberattacks is important to you, Plixer's flow-based platform gives you deep network observability for security intelligence in an easy-to-deploy and cost-effective package.

©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.