WHITE PAPER

Critical context: how Plixer enriches network flow data

Plixer

Complex systems require a different way of thinking. Consider Figure 1. Can you predict which bucket will fill up first? We know it's not bucket 4. And we can probably rule out 1, 2, and 3.

The remaining three are all good contenders. But to make a better guess, we need more information. How fast is the fluid flowing from the faucet? How thick is the fluid? Are the pipes free of friction? Is the faucet even on?

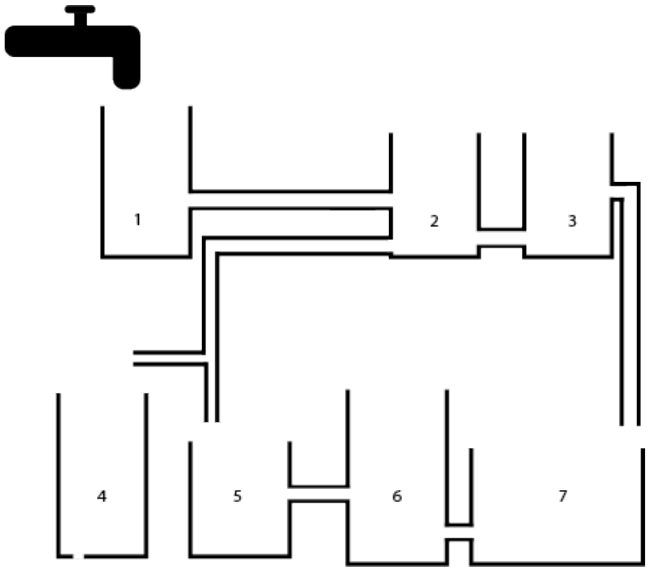


FIGURE 1

Even though we can see the entire system in Figure 1, it's not as easy to deduce how it will function simply by looking at the architecture. To know that you need specific context about the other factors that affect the system—be it the liquid moving through the buckets, the composition of the buckets, the angles, and materials of the pipes, etc.

When you have that information, in addition to the architecture, you can make more informed decisions about how to optimize the system.

This is the difference between visibility and observability. Visibility is your ability to see the architecture of a system. Observability is the actionable insights offered by seeing that system in action. By collecting data on each element, you can see the whole picture and understand how it works, predict issues, detect problems, and know how to respond.

It's all on the network

Figure 1 is an apt analogy for your IT environment. What used to be a fairly simple and controllable system, is now decentralized, abstracted, and dynamic in ways that make understanding your IT environment difficult. Managed and unmanaged devices, cloud/hybrid topologies, and an expanding tech stack that operates in silos all make managing and securing your digital business a steep challenge.

Though our IT environments are more complex than ever, one thing has not changed: our reliance on the network. Because every digital asset, device, and tool touches the network, it remains the only field of vision that spans event space and time. If something happened, the network would see it.

Simply put, our performance and security solutions are built to provide deep network observability. The network tells you critical information about your IT environment and business. By harnessing your network, you can protect your business from sophisticated cybersecurity threats, network slowdowns, outages, and more.

Go with the flow

The data on your network, when properly analyzed, gives you complete visibility of your IT environment. But, more importantly, it gives you the context on how to secure and optimize your digital business. From the network, you can detect, investigate, and respond to threats more efficiently, improve IT operational efficiency with less headcount, and more.

But extracting data from your network can happen in a few ways. Many solution providers will choose some form of edge or crown jewel strategies for data gathering and analysis. For NetOps teams, this might be some form of SNMP and/or Network Fault Management solutions. For SecOps, it may be Deep Packet Inspection on key segments of your network, firewalls, IDSs, and/or EDR solutions. While these solutions are helpful, they don't provide a holistic picture of your network, nor can they properly add context to see the bigger picture of what's happening in your environment. They provide point-specific observability.

Because Plixer's platform uses network flow data as its primary ingestion source—data extracted directly from your network devices switches, routers, firewalls, WAPs, load balancers, etc.—it gives you the complete picture of your IT environment.

When most people think of flow data, they assume we mean NetFlow, Cisco's proprietary flow data protocol. While we do ingest NetFlow, the real power of flow data comes from IPFIX, an open IETF protocol standard and a universal solution for collecting data from the network. The richness of IPFIX (see table below) far exceeds the visibility most people associate with NetFlow.

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

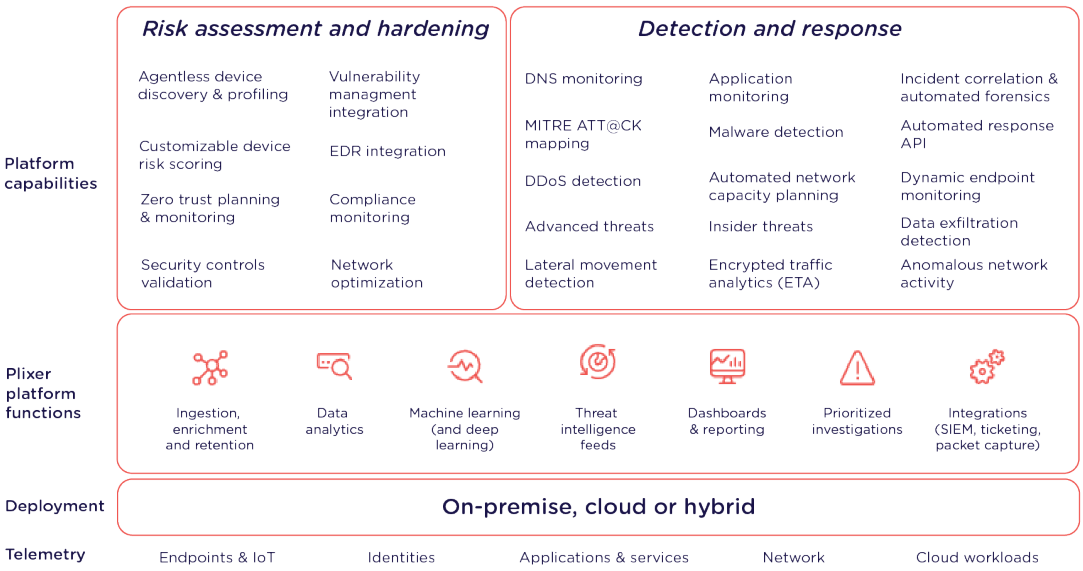
Enriching data for actionable insights

As with Figure 1, gaining visibility into your network is one thing. Knowing how to interpret that data is a whole other challenge. While many other solutions only give you visibility, Plixer takes your newfound visibility and gives it purpose.

From the network, we collect transaction data and enrich it with telemetry data from devices, user IDs, applications and services, and cloud workflows. When analyzing all that data together, we can provide a whole host of context as to why something is behaving a certain way, if it's serious, what's all been affected, and what you can do about it. By enriching our core data collection with additional data sources, we can help you detect, investigate, and respond to threats quickly and predict, plan, and optimize your IT environment.

Endpoint & IoT

Plixer's platform provides agentless device discovery, profiling, and risk scoring for all devices found on the network through Endpoint Analytics. Whether managed or unmanaged, if a device appears on the network, we'll record it and analyze its behavior. With Endpoint Analytics, you can track MAC address, OS, location, last seen date, and more to help you understand if this device is causing issues, represents a vulnerability, or poses a threat to your business.



With Endpoint Analytics, you can see that Bob in accounting has a laptop that is three OS versions out of date. Or that a printer is being used as a staging device by a threat actor. Without endpoint information, the context of the laptop may not have been known and its vulnerability would not have been prioritized. And in the case of the printer, the data collection for that machine may not have been a red flag. Having that data in hand and analyzing it in its proper context allows us to make more sophisticated alert prioritization and enables you to respond with more confidence.

Endpoint data enriches your IT context by giving you device-level detail for performance or security alerts. This data helps you reveal shadow IT, track the security, vulnerability, and activity of all devices (including IoT and OT devices), as well as provide an automated way to manage all your devices.

Identities

Plixer pulls identity data in the form of usernames to help you determine specific users that may create performance or security issues. We're able to pull that information as IPFIX from firewalls or by IP mapping from the active directory infrastructure. In either case, this allows us to enrich the other data being pulled to more accurately pinpoint and diagnose IT issues.

A username will allow you to prioritize and respond to issues, be they security or performance related, more quickly. Take for example Jennifer in engineering,

if you can see that her desktop is choking the network, then when you dig in to see that she is downloading large video files, you know who to talk to—whether it's Jennifer or her supervisor. Or if Jennifer is suddenly trying to access a financial server that she doesn't have credentials for or her desktop without warning has elevated privileges, then you can more quickly respond and be more specific in your investigations to determine the root cause of a compromise (or prove Jennifer is an insider threat).

From an investigation and response perspective, identity data is crucial for a confident understanding of what is happening in your IT environment.

Applications and services

The Plixer platform is also able to extract key application and service data as IPFIX from Application ID data and/or through a sensor. This layer 7 data allows us to detect performance and security issues occurring in applications and services or with a DNS.

Application and service data are essential for providing and ensuring optimal user experience. When a document on SharePoint is slow to open or Lisa in HR cannot get QuickBooks to open, IT gets blamed for having a slow network. In reality, the network may not be the problem at all. But without application latency, jitter, or outage data, you cannot prove your innocence or properly solve the issue.

From a security perspective, knowing which applications or services run on each device is important. This data can help you more quickly root out threats. If apps and services are running on unauthorized, unusual, or unmanaged devices, that information can help you stop an attack in its tracks.

Additionally, application and service data provide critical DNS information to root out threat actors. Take a rogue DNS attack, for example, let's say Jennifer from engineering has a desktop that starts sending out DNS traffic and responses. Endpoint analytics tells us Jennifer's machine is not a DNS server, and the application and services data give visibility and insight into the DNS activity. Both combined tell us immediately that Jennifer's device has been compromised and a quick response is necessary.

Network

As mentioned earlier, the network is the foundation for observability in your IT environment. Everything is on the network and each action leaves a data trail in its wake. By harnessing your existing network infrastructure—servers, hosts, firewalls, etc.—you can extract telemetry data that allow you to build a dynamic baseline of normal traffic. Using AI/ML to construct and analyze this dynamic baseline allows you to spot any kind of behavior anomalies.

When we detect anomalies on the network, be it performance- or security-related, we correlate that anomaly to other related events to show you the bigger picture and provide context to what is happening, where it's happening, and how long it's been happening. This enables you to make better-prioritized decisions, more thorough investigations, and quick responses to protect and enable your business.

Cloud workflows

Extending visibility into the cloud has been a challenge for IT teams. Plixer alleviates that problem by ingesting cloud flow logs without needing to deploy probes or reconfigure cloud networks. This allows you to see traffic entering and leaving cloud environments, as well as intra-cloud activity. When you can apply AI/ML to that data, then you can further protect and enable your business by having a larger context for what is happening.

From cloud flow logs you can learn about how specific devices, users, applications, and services are affecting your cloud performance and security posture. Let's say Sam from IT spins up a temporary DNS server in the cloud and forgets to take it down. That orphaned server could become a performance or a security vulnerability. A threat actor could come across this and use it to continue their attack on your business.

Without cloud visibility, an orphaned asset like that temporary DNS server could go undiscovered, and misconfigurations and unknown vulnerabilities can be exploited. Plixer gathers data from your cloud environment to give you the additional context needed to secure and optimize your IT assets.

Get Deep Network Observability with Plixer

Far beyond just the network, Plixer gives you the widest visibility and context of your IT environment. By harnessing the network, we give you security and performance insights about your entire organization.

Plixer offers the only field of vision that spans the event space & time. We give you a real-time view of your entire environment so you can be more informed and more efficient in your decisions. By enriching that view with data about your devices, users, applications, and more, you have more prioritized alerts to see things sooner and with more clarity.

Don't miss a thing with Plixer.