WHITEPAPER

How Plixer maximizes network investments

Imagine a platform so effective you can't afford ***not*** *to have it*

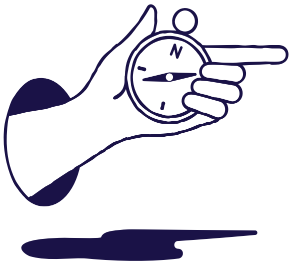
Plixer

The advent of modern corporate networks brought great possibility—and great headaches for those responsible for the performance and security of those networks. Cloud environments, a diverse ecosystem of endpoints, and porous networks offer incredible flexibility and are responsible for a boom in productivity and scalability. The result, however, is a network that is more difficult to manage and secure. That's due, in no small part, to the difficulty in achieving complete visibility across such a diverse network.

And while many solutions exist to solve this problem, none are more nimble or cost-effective than those that leverage network flow data.

Plixer and the power of network telemetry

Your network flow data provides a wealth of information. It tells you who is talking to whom, when, which applications are involved, as well as how much data is moving through your network and (with integration) even layer 7 detail.



Because network flow data comes from your existing network monitoring and security infrastructure, there's no expensive collection equipment to deploy. This means there's no upfront investment or recurring hardware to replace, no lengthy deployment or upgrade project to manage, no delay in your visibility, and no need to prioritize certain portions of your network over others. Instead, you get near-instant visibility across your entire network.

By leveraging the metadata that already exists within your network, Plixer provides valuable platforms to address both Network Performance Monitoring and Detection (NPMD) and Network Detection and Response (NDR)—improving the efficacy and efficiency of both your NetOps and SecOps teams. With the added power of our machine learning and detection algorithms, Plixer can easily separate the normal from the suspicious behavior or identify degradations in network performance.

Business continuity is your business

Ensuring your business continues to run, regardless of what the world may throw at you, has never been more critical. From policy enforcement to business continuity to compliance, keeping your network running properly is mission critical. With Plixer, you have the contextualized visibility and tools needed to validate your network and policy configurations. Our platforms alert you of compromises and issues as they occur on your network so your team can investigate and respond before business operations can be disrupted.

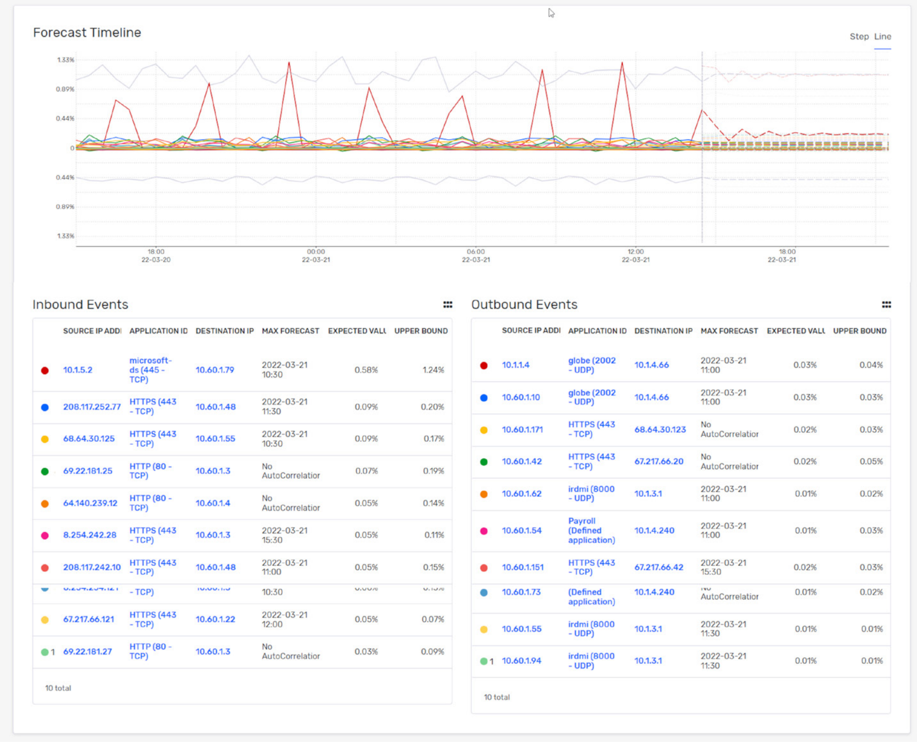
Today, a Zero Trust architecture is a foundational network policy that provides you with a reduced attack surface and data exposure risk—as well as enforcing corporate and regulatory requirements. With your NGFW, you can create perimeters around finely scoped portions of your network to constrain access to individual applications. Plixer allows you to create groups and define them for monitoring. Once you've established these microsegmented groups and their acceptable behaviors—your Zero Trust policy—you'll immediately be notified of any policy violations.

Similarly, you can use Plixer's real-time monitoring and alerting, as well as our comprehensive audit trail, to monitor other security and compliance policies.

The value of network monitoring and capacity planning

Resource planning has become a full-time job with your infrastructure spread out over so many disparate locations and platforms. And without good insight into your consumption of network resources, you'll lack predictability into your compute and storage needs. This can be a costly mistake—whether you're over-resourced and paying for unused capacity, or under-resourced and forced to pay expediting charges and suffer performance impacts.

Plixer monitors network consumption across your network resources, including your cloud environments, and can alert you as you approach capacity thresholds. Moreover, with our machine learning capabilities, you can account for seasonality changes, providing predictive capacity requirements.



Inbound Events

	SOURCE IP ADDI	APPLICATION ID	DESTINATION IP	MAX FORECAST	EXPECTED VALU	UPPER BOUND
●	10.1.5.2	microsoft-ds (445 - TCP)	10.60.1.79	2022-03-21 10:30	0.58%	1.24%
●	208.117.252.77	HTTPS (443 - TCP)	10.60.1.48	2022-03-21 11:30	0.09%	0.20%
●	68.64.30.125	HTTPS (443 - TCP)	10.60.1.55	2022-03-21 10:30	0.09%	0.17%
●	69.22.181.25	HTTP (80 - TCP)	10.60.1.3	No AutoCorrelatior	0.07%	0.19%
●	64.140.239.12	HTTP (80 - TCP)	10.60.1.4	No AutoCorrelatior	0.05%	0.14%
●	8.254.242.28	HTTPS (443 - TCP)	10.60.1.3	2022-03-21 15:30	0.05%	0.11%
●	208.117.242.10	HTTPS (443 - TCP)	10.60.1.48	2022-03-21 11:00	0.05%	0.15%
●	[illegible]	- TCP)	[illegible]	10:30	[illegible]	[illegible]
●	67.217.66.121	HTTPS (443 - TCP)	10.60.1.22	2022-03-21 12:00	0.05%	0.07%
● 1	69.22.181.27	HTTP (80 - TCP)	10.60.1.3	No AutoCorrelatior	0.03%	0.09%

10 total

Outbound Events

	SOURCE IP ADDI	APPLICATION ID	DESTINATION IP	MAX FORECAST	EXPECTED VALU	UPPER BOUND
●	10.1.1.4	globe (2002 - UDP)	10.1.4.66	2022-03-21 11:00	0.03%	0.04%
●	10.60.1.10	globe (2002 - UDP)	10.1.4.66	2022-03-21 11:00	0.03%	0.03%
●	10.60.1.171	HTTPS (443 - TCP)	68.64.30.123	No AutoCorrelatior	0.02%	0.03%
●	10.60.1.42	HTTPS (443 - TCP)	67.217.66.20	No AutoCorrelatior	0.02%	0.05%
●	10.60.1.62	irdmi (8000 - UDP)	10.1.3.1	2022-03-21 11:00	0.01%	0.02%
●	10.60.1.54	Payroll (Defined application)	10.1.4.240	2022-03-21 11:00	0.01%	0.03%
●	10.60.1.151	HTTPS (443 - TCP)	67.217.66.42	2022-03-21 15:30	0.02%	0.03%
●	10.60.1.73	(Defined application)	10.1.4.240	AutoCorrelatior	0.01%	0.02%
●	10.60.1.55	irdmi (8000 - UDP)	10.1.3.1	2022-03-21 11:30	0.01%	0.01%
● 1	10.60.1.94	irdmi (8000 - UDP)	10.1.3.1	2022-03-21 11:30	0.01%	0.01%

10 total

The dotted lines on the right side of the graph show the forecasted capacity consumption, providing you with advanced warning of increased capacity needs.

Automating service levels for improved vendor management

Chances are pretty good that if a vendor is critical to your overall business or network performance, there's a heavily-negotiated service level agreement attached to that service. But today's complex networks—and overtaxed teams—make monitoring those agreements difficult. With Plixer, you can easily establish thresholds for alerts, so you'll never miss a performance degradation. Moreover, you'll be well equipped to take that information back to your vendor with our comprehensive reports. Plixer can help ensure you get the quality service you are paying for by automating your vendor management.

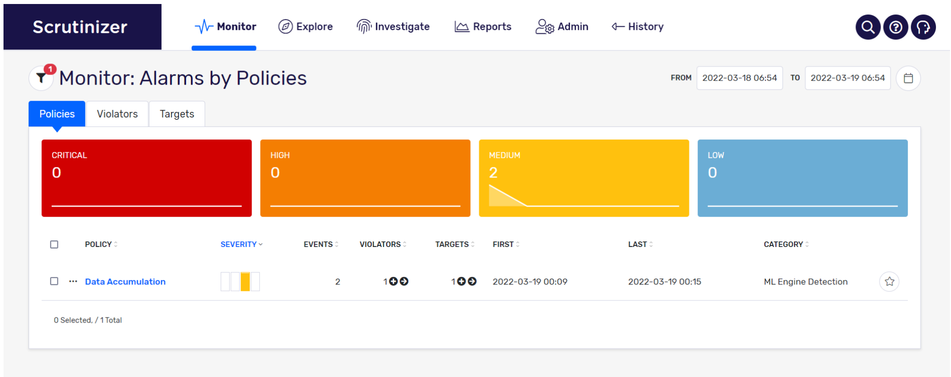
Network and application performance monitoring

Latency, packet loss, and jitter can degrade an application's performance, especially sensitive, real-time applications. These degradations can negatively impact user experience and consume valuable hours of your network team's time as they determine the root cause.

Plixer provides performance monitoring to easily identify the source of the problem. By starting with a baseline of known good traffic, anomalies are easily spotted. Our advanced machine learning provides predictive consumption information, identifying problems before they cause a problem.

Maximizing your security team

With security teams stretched thin and suffering from alert fatigue, anything that can improve their efficiency can have significant returns—both in your overall security and in your team's productivity. With Plixer's ability to baseline your traffic and identify abnormal behavior using our advanced machine learning engines, you'll be alerted to suspicious activity like lateral movement and data staging before your critical assets walk out the door. And with our intelligent correlation that looks for the tactics, techniques, and procedures that a threat actor must take to identify your critical assets, your team will get the right alerts when they need them—not a bunch of false positives.



Monitor: Alarms by Policies

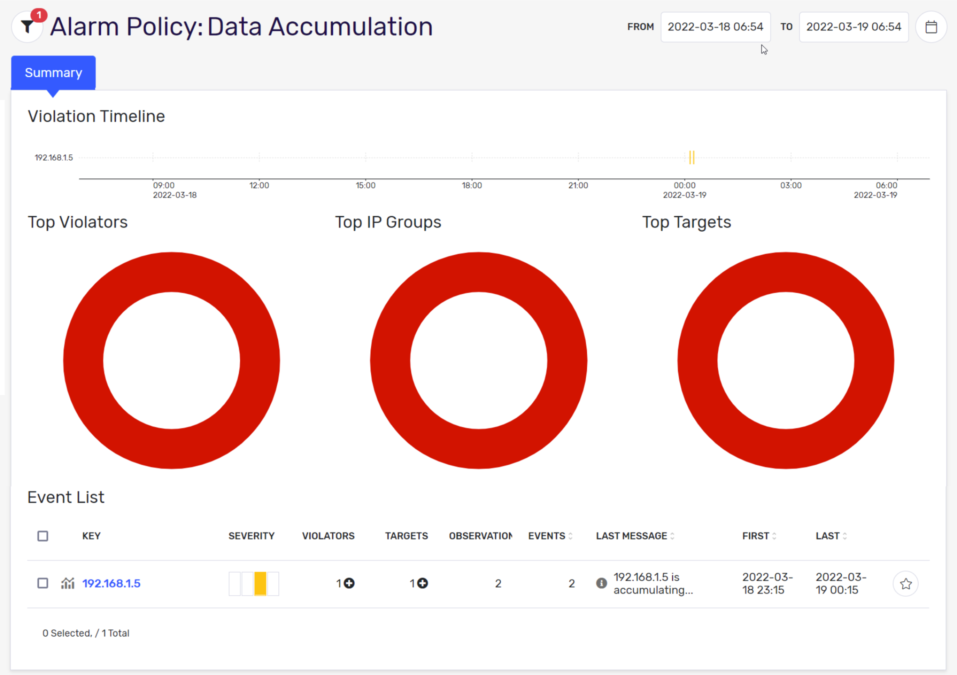
FROM 2022-03-18 06:54 TO 2022-03-19 06:54

CRITICAL	HIGH	MEDIUM	LOW
0	0	2	0

□	POLICY	SEVERITY	EVENTS	VIOLATORS	TARGETS	FIRST	LAST	CATEGORY
□	Data Accumulation		2	1	1	2022-03-19 00:09	2022-03-19 00:15	ML Engine Detection

0 Selected, / 1 Total

Plixer's dashboard alerts you to any abnormal activity. Clicking on the 'Data Accumulation' policy will allow you to drill down into the specifics of the violation.


Alarm Policy: Data Accumulation

FROM 2022-03-18 06:54 TO 2022-03-19 06:54

Event List

□	KEY	SEVERITY	VIOLATORS	TARGETS	OBSERVATION	EVENTS	LAST MESSAGE	FIRST	LAST	
□	192.168.1.5		1	1	2	2	192.168.1.5 is accumulating...	2022-03-18 23:15	2022-03-19 00:15	☆

0 Selected, / 1 Total

Here you can see the events list with the policy violators, including specifics around the policy violation.

Of course, metadata does have its limitations. It can't see into the payload of the packet—the details of the traffic itself. For that, you'll need to deploy packet capture capabilities to store copies of the packet for future needs. Deploying that capability can be expensive, requiring significant investment in sensors, storage, and management overhead. That cost typically means that PCAP capabilities are concentrated at high-value resources or network egress points.

While packets are crucial for understanding the packet payload, a necessary component of any detailed forensics investigation, they aren't a good tool for early detection of security issues. For that, it's hard to beat the efficiency and cost-effectiveness of network flow data.

And once an issue is identified, Plixer integrates with your existing workflow, including your PCAP infrastructure, to help automate your response and remediation. All of this means that your SecOps team is more efficient, allowing you to stay one step ahead of the threats.

One platform, multiple teams

One of the biggest advantages of Plixer's technology is the ability for both NetOps and SecOps teams to leverage the same tool. Unlike most competitive solutions that require discrete tools to be deployed and managed, Plixer's multipurpose engine means reduced upfront costs and platform management overhead.

By relying on network flow data monitored by Plixer's network performance and network detection capabilities, enterprises can maximize their investment in their existing network monitoring and security tools. With the addition of our advanced machine learning capabilities for NPMD and NDR, you'll get industry-leading functionality out of a consolidated architecture

With complete network visibility, Plixer helps you avoid being inundated with alerts by correlating activity and presenting you with a holistic picture of what's happening on your network, while still retaining all the low-level detail you'll need to assist in your forensic investigations.

About Plixer

Plixer provides a single platform for network security and monitoring. As a leader in Network Detection and Response & Network Performance Monitoring and Diagnostics, Plixer provides the intelligence needed to analyze, evaluate, and visualize conversations across the entire network. Plixer identifies anomalous behavior and provides historical data to investigate and remediate threats and issues faster.

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.