DATA SHEET

Plixer Replicator

Reduce Infrastructure Resources

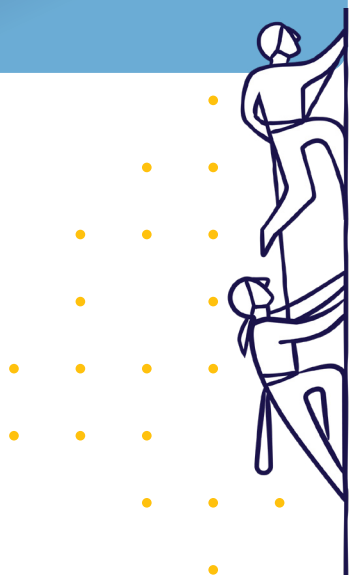
- Forward, duplicate, and load balance data for analysis
- Protect the CPUs of the infrastructure
- Greater flexibility to use infrastructure data

Future-Proof Configuration

- Configuring new devices is a one-time effort
- Improved productivity
- Easy to add new devices as needed

Ensure Data Integrity

- Thwart bad actors trying to cover their tracks
- Ability to back up system messages to multiple locations



Organizations of all sizes are actively striving to leverage data intelligence so they can make better business decisions and protect themselves against security threats. Much of this data currently exists within their existing network infrastructure, but exporting it to all the places, products, and tools where it delivers value can be a challenge. Plixer Replicator is an important piece of the puzzle to ensure that every organization can make the best use of their network traffic flows and metadata.

Plixer Replicator ingests flows and other metadata from your existing infrastructure. It can then duplicate, forward, and load balance this data to Plixer Scrutinizer or forward it to any of your other management and analytics tools.

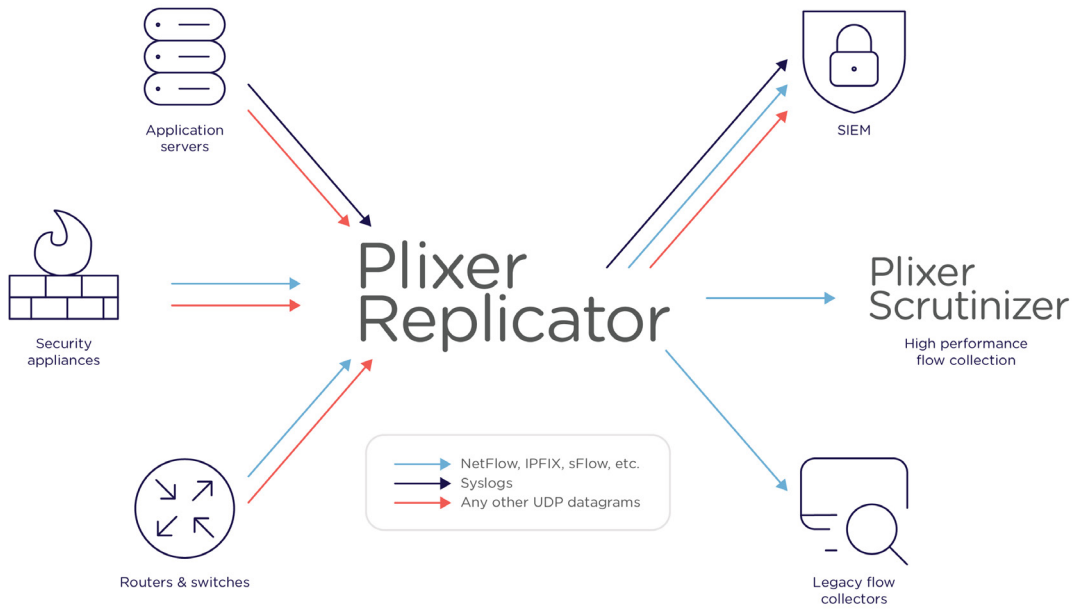
Reduce infrastructure resources

Network infrastructure equipment like routers, switches, firewalls, etc. are natively capable of exporting network traffic-related metadata as NetFlow or IPFIX. These network infrastructure devices are typically limited to exporting one or two streams of this data to external locations. This is done to reduce CPU utilization; however, it limits your ability to get that data to multiple locations for analysis..

To combat this, Plixer Replicator centrally collects data from the infrastructure, duplicates it, and forwards it to multiple locations for analysis. This protects the CPUs of the network infrastructure while providing the greatest flexibility to use that data for better decision-making and business intelligence.

Improve resiliency and future-proof configuration

When you configure network devices to export their data to Plixer Replicator, configuration becomes a one-time effort. Security and network teams regularly introduce new products and tools into their environment. Any changes made to these collection and analytics tools becomes a breeze. Instead of touching every network device again, simply update Plixer Replicator to forward data wherever you



want it—be it to a SIEM, flow collector, big data platform, or analytics application.

By leveraging Plixer Replicator's robust forwarding capabilities, IT teams significantly reduce configuration time as new data sources are deployed on the network. This improves productivity and makes it easier to add new devices as needed.

Ensure data integrity

As a proactive effort to thwart cybercriminals in their attempt to delete data and cover their tracks, Replicator sends data to many different locations. A transparent "bump-in-the-wire," Plixer Replicator does not store information, but rather transparently collects, duplicates, and forwards it to disparate locations. By distributing millions of flow and metadata records to different products and locations, it becomes impossible for bad actors to hack all of these databases and cover their tracks.

Plixer Replicator gives companies with compliance requirements a way to back up system messages and notifications to multiple locations so when an audit takes place, they can be certain they have the data.

Plixer Replicator and Plixer Scrutinizer

By pairing Plixer Replicator with Plixer Scrutinizer, the flow and metadata exports from hundreds or thousands of devices can be analyzed to detect a wide range of network threats, including APTs, employee misuse, DDoS attacks, and data leaks. Additionally, security audit trails of all network traffic enable rapid response to network incidents.

From Plixer Replicator to Plixer Scrutinizer, better context is achieved by correlating traffic flows and metadata, collected from all corners of the network into a single database. Rapid filtering and reporting from this rich data deliver deep insight to answer the questions: who, what, where, when, why, and how.

Network and application optimization, as well as root cause analysis require true end-to-end visibility. Plixer Scrutinizer delivers by collecting, visualizing, and reporting on data forwarded by Plixer Replicator that extends all the way from the user through to the cloud. It also provides real-time detection of DDoS attacks, minimizing disruption and loss of revenue.

System specifications (hardware appliance)

Category	Description
Chassis configuration	1U
Processor	1 x Intel Xeon° E-2124 3.3Ghz (4 cores) 71 Watts
Memory	8GB
Storage	2 x 600GB (RAID 1)
Networking standard	Dual port 10/100/1000Base-T Gigabit Ethernet
Replication rate	Engine capable of 82,000 packets per second (pps) and 82,000 pps output
Hardware warranty	5 years (60 months)
Power supply	Redundant 350W power supplies
Management port	Yes
Weight	29.98 lb (13.6 kg)
Dimensions	23.45" x 17.08" x 1.68" (59.56cm x 43.40cm x 4.28cm)
Environmental	**Storage:** Temperature: -40°C to 65°C (-40°F to 149°F) Humidity: 5% to 95% **Operating:** Temperature: 10°C to 35°C (50°F to 95°F) Humidity: 10% to 80%
Compliance	US CFR Title 47, FCC Part 2, 15 ANSI C63 2009 Canadian ICES-3(A)/NMB-3(A), Issue 5 UL 60950-1 UL 60950-1 (Information Technology Equipment - Safety - Part 1: General Requirements) CSA C22.2 No. 60950-1-07 (Information Technology Equipment - Safety - Part 1: General Requirements) IEC 60950-1 (ed.2);am1

System specifications (virtual appliance)

Category	Description
Hypervisor	VMware, Hyper-V 2012, KVM
OS	Fully self-managed operating system and database included
RAM	2GB
Disks	20GB
Processor	1 CPU 1 Core
Replication rate	Engine capable of 82,000 packets per second (pps) and 82,000 pps output