DATA SHEET

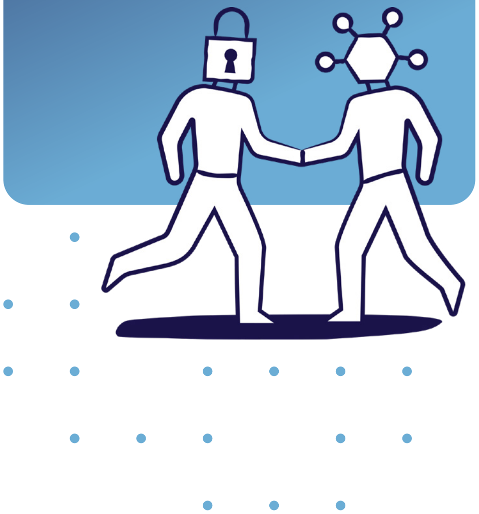
Plixer Scrutinizer

Security benefits

- Reduce security risks
- Support faster time-to-resolution
- Deliver contextual forensics
- Proactive thresholds and alarming

Network benefits

- Enrich data context of network traffic
- Increase efficiency and reduce cost
- Monitor network and application performance
- Achieve fast reporting and massive scale



Plixer Scrutinizer® collects, analyzes, visualizes, and reports on data from every network conversation and digital transaction to deliver security and network intelligence. It provides the insight and historical data needed to manage and optimize business operations while reducing risk by detecting and remediating incidents. Unlike competing solutions that require the addition of many expensive and proprietary appliances, Plixer's implementation collects data that is exported directly from the existing infrastructure (switches, routers, firewalls, packet brokers, etc.). This differentiated approach is frictionless, eases implementation, reduces complexity, and improves ROI.

Plixer Scrutinizer is available as both physical and virtual appliances, as well as through a software-as-a-service cloud-based offering.

Security benefits

Reduce security risks

As a security professional, risk reduction is job one. The decades-long strategy of deploying security products, purchased in the name of prevention, has failed us. Breaches are inevitable. Today, the greatest risk reduction comes from a focus on forensic data and improving time-to-resolution after a breach occurs.

Support faster time-to-resolution

Faster time-to-resolution is accomplished through a faster time-to-know. Remediation can only occur after root cause has been established, and rich contextual data is the enabler. Plixer Scrutinizer gathers flows and metadata from across your entire network infrastructure, providing the visualization and reporting of the forensic details you need for faster time-to-resolution.

Deliver contextual forensics

Access to high volumes of disparate data does not lead to faster response. In fact, it can have the opposite effect. The best context and response come from the correlation of network-related metadata gathered from firewalls, switches, routers, and distributed probes, all stitched together into a single database. Plixer Scrutinizer centrally collects and correlates data from every corner of your existing network, providing the critical information you need.

Proactive thresholds and alarming

IoT, BYOD, and the explosion of virtual machines have all created an unmanageable threat surface. Monitoring network traffic is a highly effective way to identify indicators of compromise. Proactive thresholds, alerting, and open RESTful APIs enable rapid and dynamic event response. Plixer Scrutinizer provides real- time detection of DDoS attacks, whether the attack is volumetric-, application-, or protocol-based.

Network benefits

Enrich data context of network traffic

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

Increase efficiency and reduce cost

Plixer Scrutinizer offers the industry's fastest and most accurate reporting, delivering visibility into bandwidth, application, and user utilization (including the WAN and SD-WAN). When users complain, but your SNMP tool's lights are all green, what do you do? You turn to Plixer Scrutinizer to protect customer satisfaction, productivity, and revenue.

Monitor network and application performance

Network/application optimization and root cause analysis require true end-to-end visibility. Plixer Scrutinizer delivers by collecting, visualizing, and reporting on data that extend 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.

Achieve fast reporting and massive scale

Plixer Scrutinizer's hierarchical design with streamlined and efficient data collection allows you to start small and easily scale to multi-millions of flows per second. Although the network is always blamed, fast and accurate reporting allows the network team to identify root cause and, as is often the case, deliver proof of network innocence.

Complement Plixer Scrutinizer with Plixer Intelligence products

Plixer Security Intelligence

Plixer Security Intelligence consumes and analyzes streamed metadata, in real time, from Plixer Scrutinizer in order to aid resource-strained SecOps teams, dynamically combing massive volumes of machine-generated data and automating the detection and remediation of advanced persistent threats. Plixer Security Intelligence embeds the very latest in machine learning/artificial intelligence (ML/AI) technology and applies a crisp use-case-driven implementation that delivers real, trustworthy results in milliseconds. For more information on the Plixer Security Intelligence product, visit: www.plixer.com/products/security-intelligence

Plixer Network Intelligence

Plixer Network Intelligence, powered by advanced machine learning (ML), is deployed alongside Plixer Scrutinizer. Plixer Scrutinizer streams data in real time to Plixer Network Intelligence, where that data is analyzed with ML. The results of this analysis are sent back to Plixer Scrutinizer, where NetOps staff can visualize and report on it. Plixer Network Intelligence augments NetOps teams by dynamically predicting network capacity requirements, automating network operation functions, improving investigation efficiency, dynamically sharing data with SecOps, streaming data into external data lakes, and streamlining workflows through ServiceNow integration. For more information on the Plixer Network Intelligence product, visit: www.plixer.com/products/network-intelligence

Deployment options

Hardware appliances

Plixer Scrutinizer's appliances are rack-mountable servers with all the capabilities pre-installed.

- Plixer Scrutinizer Collector receives flows and metadata from exporting devices and stores it in a database.
- Plixer Scrutinizer Reporter is the reporting engine of Plixer Scrutinizer.

Hardware appliance specifications are listed in the table below.

Virtual appliances

The Plixer Scrutinizer 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 (defined by VMware).
- 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
- 16 GB DDR3 RAM, 64 GB recommended
- 100 GB SATA drive, 1.5 TB 15K SAS recommended

Hardware appliance specifications

	Collector	**Reporter**
Chassis configuration	2U chassis	1U chassis
Storage	1.8, 3.6, and 7.2 TB capacity options	400 GB capacity
Networking	QP 1 Gb Network Daughter Card (10 Gb available as an option)	Quad port 1Gb LOM
Power	Dual, hot plug, redundant power supply (1+1), 750W	Dual, hot plug, redundant power supply (1+1), 550W
Power cords	NEMA 5-15P to C13 wall plug, 125 volt, 15 amp, 10 ft (3m), power cord, North America	
Weight	72 lbs (32.65 kg)	36.88 lbs (16.73 kg)
Dimensions	26.92" x 17.49" x 3.44" (68.40cm x 44.40cm x 8.73cm)	23.9" x 17.09" x 1.68" 60.70cm x 43.40cm x 4.28cm
Hardware warranty	5 years	
Rails	Sliding ReadyRails with cable management arm	
Heat dissipation	2891 BTU/hr	2107 BTU/hr
Database	PostgreSQL	

Plixer Scrutinizer supported end-system browsers

Desktop browser	Version
Microsoft Edge	Current release
Mozilla Firefox	Current release
Google Chrome	Current release

Plixer Scrutinizer license tiers

	SSRV	SCR-VA/SCR-HDW
Flows collected per second	10K	40K/up to 10+ million
Length of time raw flows are kept	Unlimited	Unlimited
Days of historical flow roll ups	Unlimited	Unlimited
Number of flow exporters supported	Pay per device	Pay per device
Flexible licensing	✓	✓
Advanced Reporting on all vendor-specific exports	✓	✓
Full stitching and deduplication	✓	✓
3rd-party integration (e.g. Splunk, Elasticsearch, etc.)	✓	✓
Support for all versions of NetFlow, IPFIX, sFlow, etc.	✓	✓
Support for all vendor enterprise IPFIX elements	✓	✓
Ability to create filters to narrow in on traffic	✓	✓
All exporters index search for a host	✓	✓
Scheduled email reports (HTML & PDF)	✓	✓
Scheduled email top interfaces	✓	✓
Export data in CSV format	✓	✓

Plixer Scrutinizer license tiers (continued)

	SSRV	SCR-VA/SCR-HDW
Saved reports	✓	✓
Access to API	✓	✓
Report Designer to build new reports from flows	✓	✓
8am – 5pm Eastern Time technical phone support	✓	✓
Create dashboards	✓	✓
Auto DNS resolve hostnames	✓	✓
Configure and trigger notifications	✓	✓
CSV export of tables (e.g. Alarms, Status, etc.)	✓	✓
Flow Hopper to show flow path; hop to hop	✓	✓
Set thresholds in saved reports to monitor	✓	✓
Define IP groups and report	✓	✓
Multi-Tenancy Module—keep selected data private	✓	✓
Threat detection algorithms	✓	✓
Real-time DDoS detection	✓	✓
Business hours-based reporting	✓	✓
ASA ACL descriptions	✓	✓
AWS Kinesis Streaming	✓	✓
Cisco: Sourcefire eStreamer	✓	✓
LDAP, RADIUS, TACACS authentication support	✓	✓
IP address-to-username correlation support	✓	✓

Plixer Scrutinizer license tiers (continued)

	SSRV	SCR-VA/SCR-HDW
Optional 7x24 technical support	✓	✓
Unified distributed collector support		✓
SSO support		✓
SD-WAN support/visibility		✓
Number of login accounts	Unlimited	Unlimited
Number of security groups	Unlimited	Unlimited

Plixer Scrutinizer purchasing options

Plixer Scrutinizer can be purchased in two ways: Subscription license or Software-as-a-Service (SaaS).

Both the Subscription and SaaS Licensing have an ongoing Customer Service Contract as part of the terms of your Subscription or SaaS License.

Subscription license

Subscription licensing is an option that allows the purchase of Plixer Scrutinizer in annual contracts. Users are free to use the software as long as they maintain a contract with Plixer. Product updates and customer support are included as part of the subscription. Hardware and virtual installations can be on-premise or within a customer's instance of private cloud/public cloud.

Software-as-a-Service (SaaS)

The SaaS option of Plixer Scrutinizer allows users to leverage Plixer's cloud infrastructure to collect and report on flow and metadata. Plixer maintains the server and automatically upgrades users to the latest version of the software. Users may continue to collect and report on their flow data as long as they maintain a contract with Plixer. 1-, 2-, and 3-year contracts are available.

Ordering information

Ordering subscription licenses of Plixer Scrutinizer is based on the number of flow-exporting devices that will be sending flow and metadata to a Plixer Scrutinizer collector. Multiple license tiers are available. License cost is determined by the number of flow and metadata exporters. Customized license options are available upon request.

SSRV

SSRV is available as a virtual appliance only and is limited to 10,000 flows per second with unlimited raw flow data collection.

SCR-VA

SCR-VA is the virtual appliance option of SCR. SCR-VA is limited to 40,000 flows per second with unlimited raw flow data collection.

SCR-HDW

SCR-HDW is the hardware appliance option of SCR. SCR-HDW supports up to 100,000 flows per second per collector with unlimited raw flow data collection.

SCR-HDW comes in three options depending on the amount of disk space required to support your given flow collection needs:

- HDW – Collector 1.8 TB
- HDW – Collector 3.6 TB
- HDW – Collector 7.2 TB

Additional external storage arrays are available for purchase as well.

VDR

VDR is a virtual reporter used for distributed environments. Requires SCR-VA or SCR-HDW.

HDR

HDR is a hardware appliance for reporting in distributed environments, and requires SCR-VA or SCR-HDW.

Cloud-SCRT

Cloud-SCRT is a Software-as-a-Service (SaaS) deployment option for Scrutinizer. License cost for Cloud-SCRT is determined by flow collection rates rather than exporter counts.

Key technology integration

Plixer Scrutinizer offers RESTful API integration with key complementary technologies. Some integration examples include Splunk and Elasticsearch for SIEM integration. Active Directory, RADIUS, and TACACS+ integration provides accountability with username-to-IP correlation, and integration with third parties like Endace allows for seamless correlation of flow data with packet capture details. In addition, IPAM integration allows for IP Group details to easily be imported and integrated into the reporting structure. Plixer Scrutinizer boasts technology integration with over 70 leading network and security solutions, protecting existing technology investments.

Warranty

As a customer-centric company, Plixer is committed to providing quality products and solutions. In the event that 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 5-year warranty against manufacturing defects. Software warranties are covered through the Customer Support Contract or through a subscription contract.

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 can be purchased in blocks of two hours and on-site services are available in two-day blocks.

Customer Service Contracts are available as either Tier 1 or Tier 2 Support.

Tier 1: Telephone and live chat support is available from 8am-5pm EST/EDT Monday through Friday. Response time is within 24 business hours of support request.

Tier 2: Live chat support is available from 8am-5pm EST/EDT 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/scrutinizer/

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.