

### Network Benefits

Enrich data context of network traffic

Increase efficiency and reduce cost

Monitor network and application performance

Achieve fast reporting and massive scale

### Security Benefits

Reduce security risks

Support faster time-to-resolution

Deliver contextual forensics

Advanced security analytics

## Scrutinizer: Data Sheet

Scrutinizer® is the foundation for Plixer's network traffic analytics system. It stands out in the industry by offering the most scalable solution on the market, delivering the fastest reporting, and providing the richest data context available anywhere. Role-based access automatically presents the network and security teams with the data they need to support fast, efficient network and security incident response.

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

### 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. 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

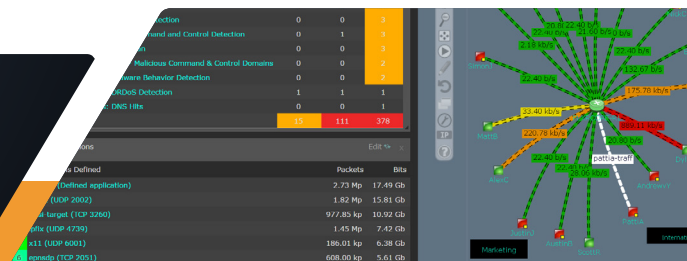
Scrutinizer offers the industry's fastest and most accurate reporting, delivering visibility into bandwidth, application, and user utilization (including the WAN). When users complain, but your SNMP tool's lights are all green, what do you do? You turn to Scrutinizer to protect customer satisfaction,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

#### Monitor Network and Application Performance

Network/application optimization and root cause analysis require true end-to-end visibility. Scrutinizer delivers by collecting, visualizing, and reporting on data that extend all the way from the user, through the Wi-Fi, into the wired edge and distribution closets, across the data center, and into the cloud.

#### Achieve Fast Reporting and Massive Scale

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.

207.324.8805

## 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. 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. Scrutinizer centrally collects and correlates data from every corner of your existing network, providing the critical information you need.

### Advanced Security Analytics

IoT, BYOD, and the explosion of virtual machines has created an unmanageable threat surface. Monitoring for anomalous activity and device behavior with network traffic analytics is the most effective indicator of compromise. Advanced analytics with proactive thresholds, alerting, and open RESTful APIs enable rapid and dynamic event response.

## Deployment Options

### Hardware Appliances

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

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

Hardware appliance specifications are listed on the following page.

### Virtual Appliances

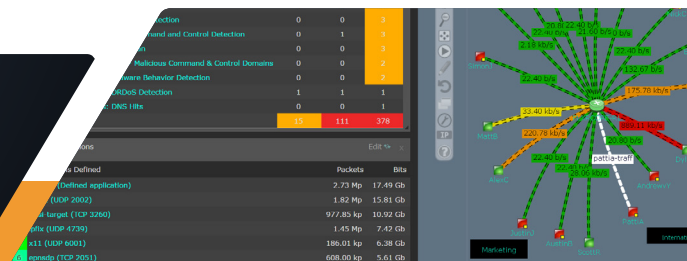
The Scrutinizer virtual appliance is available for deployment on a VMware, Hyper-V, or KVM server.

- 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

# plexer



207.324.8805

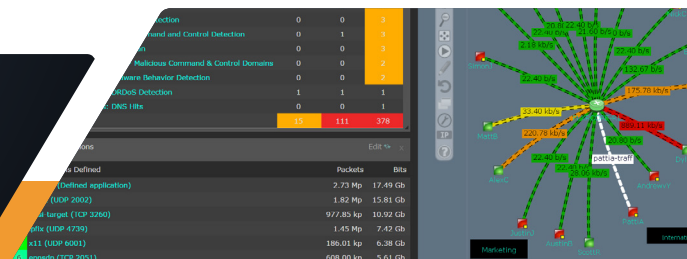
## Hardware Appliance Specifications

	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 (10Gb 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 Feet (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	

## Scrutinizer-Supported End-System Browsers

Desktop Browser	Version
Microsoft Edge	Current release
Microsoft Internet Explorer	Current release
Mozilla Firefox	Current release
Google Chrome	Current release

# plexer

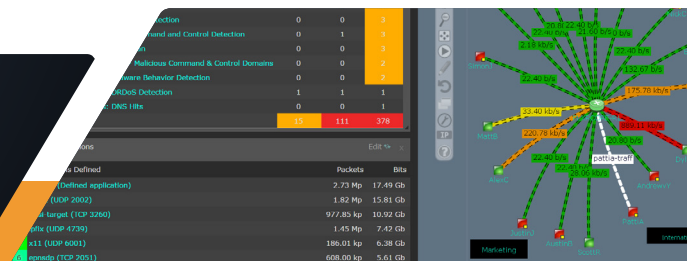


207.324.8805

## Scrutinizer License Tiers

	Free	MDX	SSRV	SCR-VA/SCR-HDW
Flows Collected Per Second	10K	10K	10K	40K/Up to 10+ million
Length of time raw flows are kept	5 hours	24 hours	Unlimited	Unlimited
Days of historical flow roll ups	1 week	Unlimited	Unlimited	Unlimited
Number of flow exporters supported	Unlimited	Pay by device	Pay by device	Pay by device
Flexible Licensing	Limited	✓	✓	✓
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	✗	✓	✓	✓
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 host names	✗	✓	✓	✓

# plexer

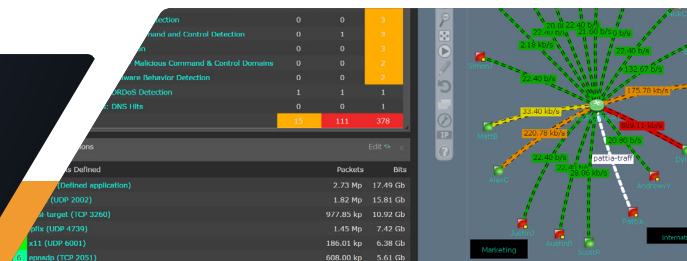


207.324.8805

## Scrutinizer License Tiers (continued)

	Free	MDX	SSRV	SCR-VA/SCR-HDW
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 traffic	✗	✗	✓	✓
Define IP groups and report	✗	✗	✓	✓
Multi-Tenancy Module – keep selected data private	✗	✗	✓	✓
Threat detection algorithms	✗	✗	✓	✓
Business hours-based reporting	✗	✗	✓	✓
ASA ACL descriptions	✗	✗	✓	✓
AWS Kinesis Streaming	✗	✗	✓	✓
Cisco: Sourcefire eStreamer	✗	✗	✓	✓
LDAP, RADIUS, TACACS authentication support	✗	✗	✓	✓
Number of login accounts	2	5	Unlimited	Unlimited
Number of security groups	2	5	Unlimited	Unlimited
IP address-to-username correlation support	✗	✗	✓	✓
Optional 7x24 technical support	✗	✗	✓	✓
Unified distributed collector support	✗	✗	✗	✓

**plexer**



207.324.8805

## Scrutinizer Purchasing Options

Scrutinizer can be purchased in three ways: Perpetual license, Subscription license, or Software-as-a-Service (SaaS).

When purchasing a perpetual license, the first year of the Customer Service Contract is free. At the end of the first year, the Customer Service contract can be renewed in blocks of 1-4 years.

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

### Perpetual License

Perpetual licensing is an option that allows the purchase of Scrutinizer outright with a non-expiring license. Users may continue to use the version of Scrutinizer they have purchased without additional cost. Upgrades are supported through the Customer Service Contract. Hardware and virtual installations can be on-premise or within a customer's instance of private cloud/public cloud.

### Subscription License

Subscription licensing is an option that allows the purchase of 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 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

Multiple Scrutinizer license options (see below) and tiers are available. Perpetual and subscription license costs are determined by the number of flow exporters. SaaS license cost is determined by flow collection rates. In addition, customized license options are available upon request.

### MDX

MDX is available as a virtual appliance only and is limited to 10,000 flows per second and 24 hours of raw flow data.

### 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:

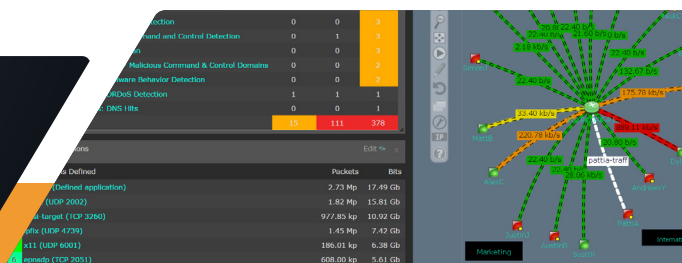
- HDW – Collector 1.8 TB
- HDW – Collector 3.6 TB
- HDW – Collector 7.2 TB

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.

# plixer



207.324.8805



## 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

Scrutinizer is a network traffic analytics platform that 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. 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.

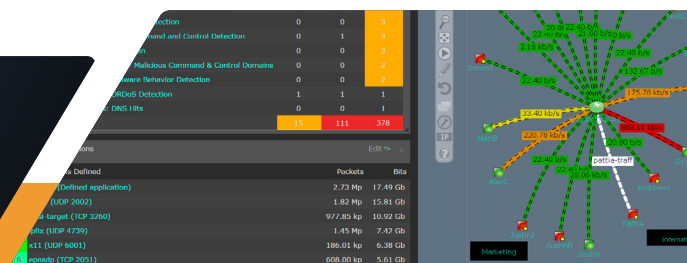
Please contact your Plixer account executive for more information about Plixer service and support.

## Additional Information

For additional technical information, please visit:

<https://www.plixer.com/products/scrutinizer/>

# plixer



207.324.8805