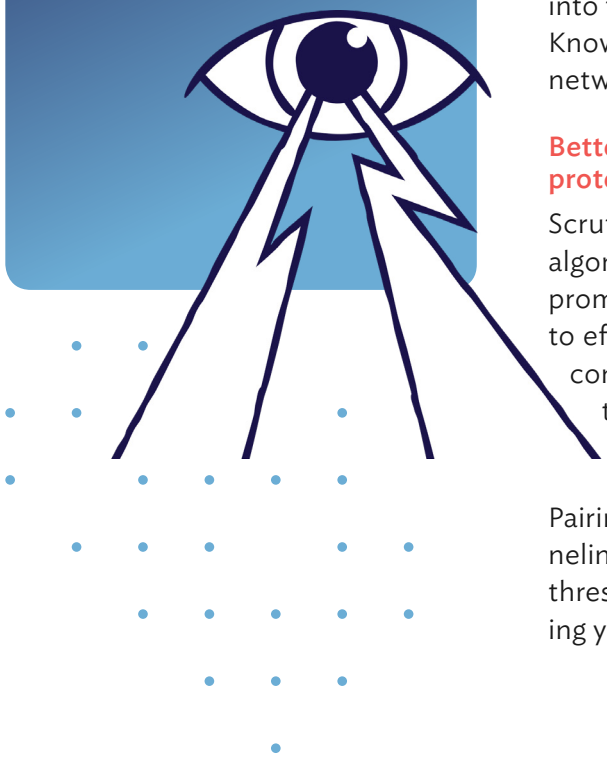
BROCHURE

Network traffic analysis for better management & security

Scrutinizer benefits & capabilities

- Incident response
- Rich context
- SIEM integration
- Scalability
- Virtualization



Contextual forensic data for fast and effective incident response

Scrutinizer is a distributed and highly scalable network traffic analytics system. It leverages the existing network as a sensor by collecting all types of flows (such as NetFlow, sFlow, J-Flow, IPFIX, etc.) and metadata. It provides thorough insight into 100% of all communications from every wired and wireless device that accesses the network.

Increased network operations efficiency

Scrutinizer's award-winning network usage reports provide insight into users, applications, and network devices. With the deepest insight available, Scrutinizer allows administrators to peer deep into the network to see how it is being used, reducing Mean Time to Know (MTTK) and streamlining IT's Mean Time To Repair (MTTR) network-related events.

Better security with advanced threat protection and behavior analysis

Scrutinizer's Flow Analytics use dozens of behavior-based security algorithms that baseline and monitor traffic for indicators of compromise. The distributed collection architecture allows Scrutinizer to effectively shrink the attack surface and expedite the process of containing a threat. Maintaining constant control while identifying the entire attack continuum is part of what makes Scrutinizer ideal for confronting advanced threats head-on.

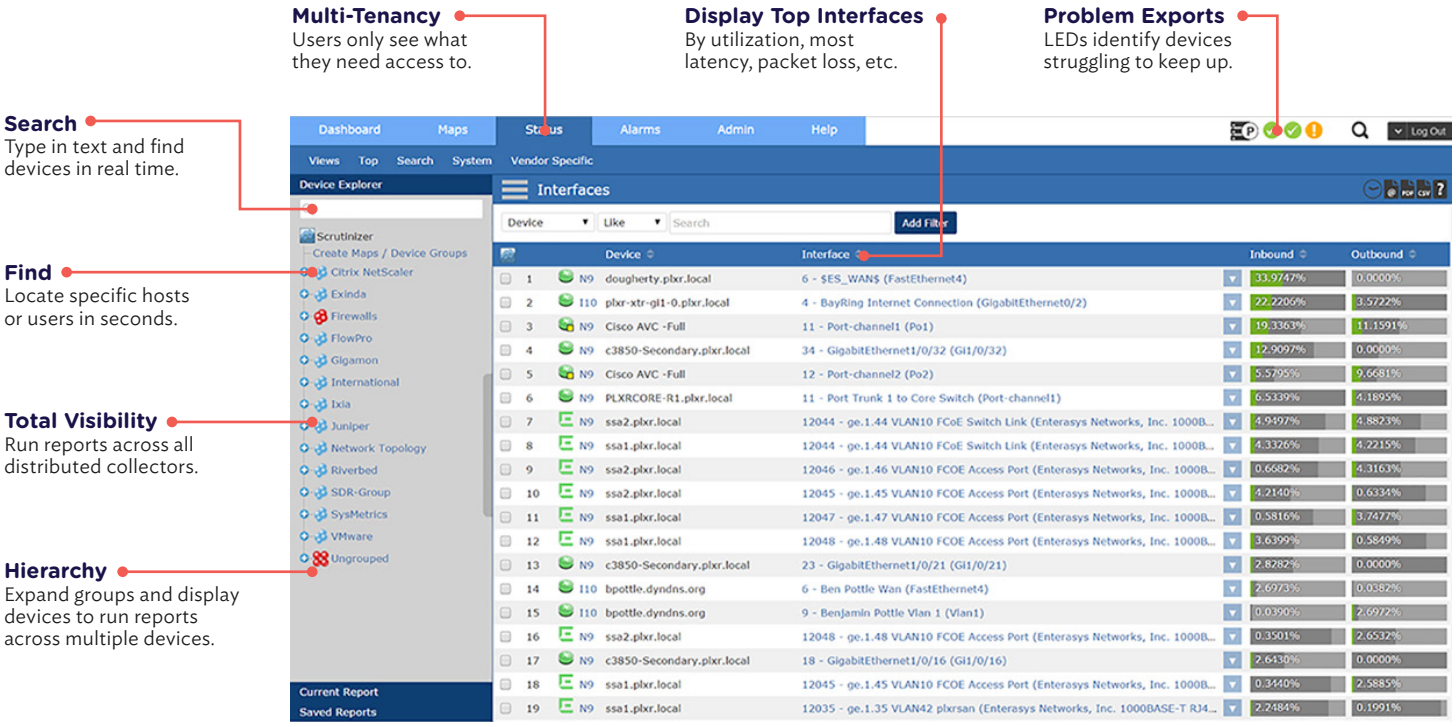
Pairing with FlowPro Defender allows for detection of DNS tunneling, botnets, and low-and-slow data thefts. Custom behavior thresholds can be used to monitor the unique applications supporting your business.

Features and benefits

- Enjoy 100% support for *all* flow technologies (e.g. NetFlow, J-Flow, sFlow, IPFIX, and derivatives), eliminating additional investments in “less open” tools
- No vendor left behind: all companies supported, inclusive of their unique exports, leading to fewer in-house scrips to report on vendor-proprietary exports
- Archive raw flows for years to meet HIPAA, PCI, and other compliance demands
- One architecture, one interface, and one place for reporting: easily scalable from small environments to billions of flows per day
- Protect existing investments through technology integration with Cisco ISE, ASA with FirePOWER, and SD-WAN, as well as Splunk, Palo Alto Networks firewalls, Gigamon, Ixia, Endace, and many others
- Baseline traffic and trigger alerts based on irregular behavior and odd patterns
- Monitor homegrown and customized application profiles, eliminating the need for separate tools
- Identify the undetected. Proactively discover low-and-slow data theft and contagions by uncovering bot communications and DNS tunneling
- Flexible data visualization options (e.g. trends, bars, pie charts, matrix, Sankey, etc.) provide clarity for all audiences
- The exporter provides proactive notification, so if flow data is being lost, IT can investigate and fix the problem

A single interface with fast searching

When security and network incidents occur, time is money and the clock starts ticking immediately. Reporting speed and data accuracy are paramount to quick resolution. Scrutinizer has been purpose-built to deliver the fastest reporting in the industry. When time-to-know matters, Scrutinizer is the system of choice.



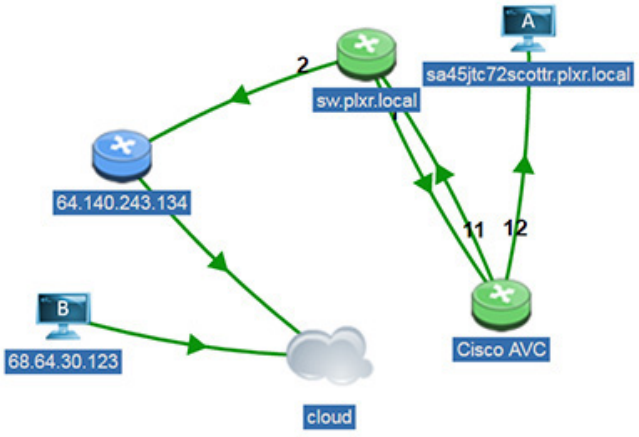
For the sake of efficiency, Scrutinizer collectors are deployed hierarchically. The exporting devices (e.g. switches, routers, firewalls, etc.) send flow and metadata to the collectors, where it is stored locally. From the web interface, administrators can run queries and report on data relating to an IP address, hostname, username, and more. The reporting engine reaches out to distributed collectors, gathers the related data, and then correlates and displays the data within seconds.

When the security team wants to find out where an IP address has ever been seen on the network, including when and where it connected, that information is available in seconds through host indexing. Simply click on the router, report on the data, and observe all the context—fast.

Flow path, even across collectors

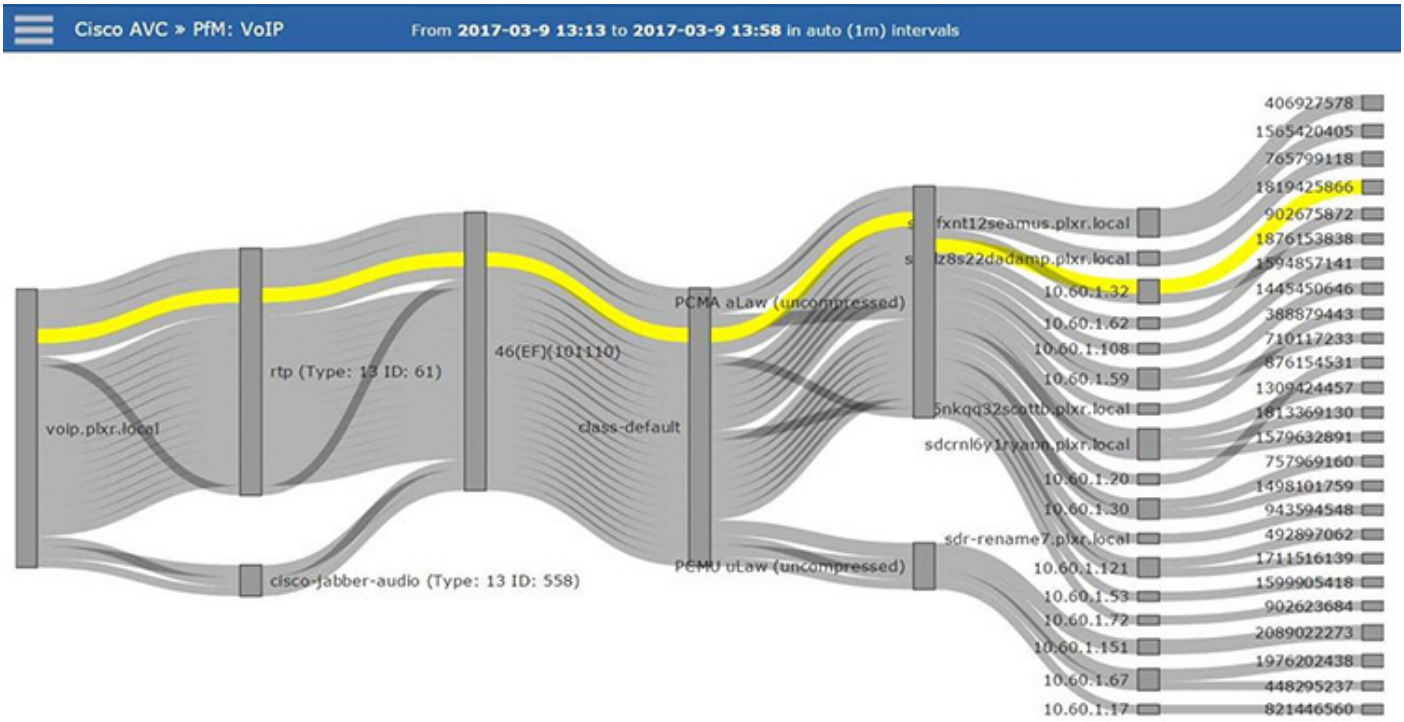
When flow path is in question, click a button and watch as Scrutinizer's Flow Hopper builds out the end-to-end, hop-by-hop path of the traffic at the time of the event.

To do this, Scrutinizer leverages its knowledge of the topology combined with the details found across most flow-exporting vendors. Even when the return path goes through routers exporting flows to different collectors, Flow Hopper will stitch together the entire connection, giving security and application teams the end-to-end picture.



Flow Deduplication and Stitching

NetFlow deduplication happens when multiple routers or switches export the same flows for two hosts communicating with one another. If a flow (e.g. A to B) with a matching tuple is generated by three routers, the reporting engine will identify this and serve up a single result.



Scrutinizer never drops any of the flows that are deduplicated, as this can result in lost information and prevent the system from determining details such as end-to-end flow path. Even with deduplication enabled, all original flows are saved and archived for future reference.

NetFlow stitching is the process of looking at certain protocols (e.g. TCP) and assuming that a return flow occurred. Even if the return path is going through a router exporting flows to a different flow collector, Scrutinizer will stitch flows across collectors. This unique list-identify-select navigation ensures total visibility of the flow path even when the returning connection is through routers that export to an entirely different collector.

Don't be limited to utilization

Why be confined to a list of interfaces ordered by utilization? If Cisco AVC performance metrics are being exported, list interfaces by flows with the most latency, packet loss, jitter, or retransmitted packets.

If an interface is suffering from excessively high round trip times, drill in to list the interfaces and identify the flows. Select Flow Hopper to highlight where in the path the latency is being introduced and why. Determine if it was caused by bandwidth consumption, queue drops, or incorrect DSCP values and do it all with flow data.

A10 Networks	Check Point	Fatpipe	Open vSwitch	Sophos
Adtran	Cisco	Fortinet	Palo Alto Networks	Stormshield
Alcatel	Citrix	Gigamon	pfSense	Talari
APCON	Dell	HPE	Plixer	Telesoft
Arista	Ecessa	IBM	Procera	Ubiquiti
Aruba	Embrane	Ixia	Riverbed	VMware
Astaro	Endace	Juniper	Saisei	Vyatta
Avaya	Ericsson	Meraki	SilverPeak	Xirrus
Barracuda	Exinda	MikroTik	Solera	YAF
Big Switch	Extreme Networks	nProbe	SonicWALL	Ziften
Blue Coat	F5			

List of vendors whose unique NetFlow and IPFIX exports are supported by Scrutinizer

Third-party vendor integration and support

No other vendor can match the extensive reporting and threat detection provided by Scrutinizer for every flow-exporting vendor in the world.

Better context through metadata enrichment

Beyond the data found in flows, 3rd-party integration delivers vastly greater contextual details. Usernames, operating systems, wireless access points, physical location (e.g. building, floor), MAC addresses, and more can all be gathered from authentication systems to enrich the data being requested.

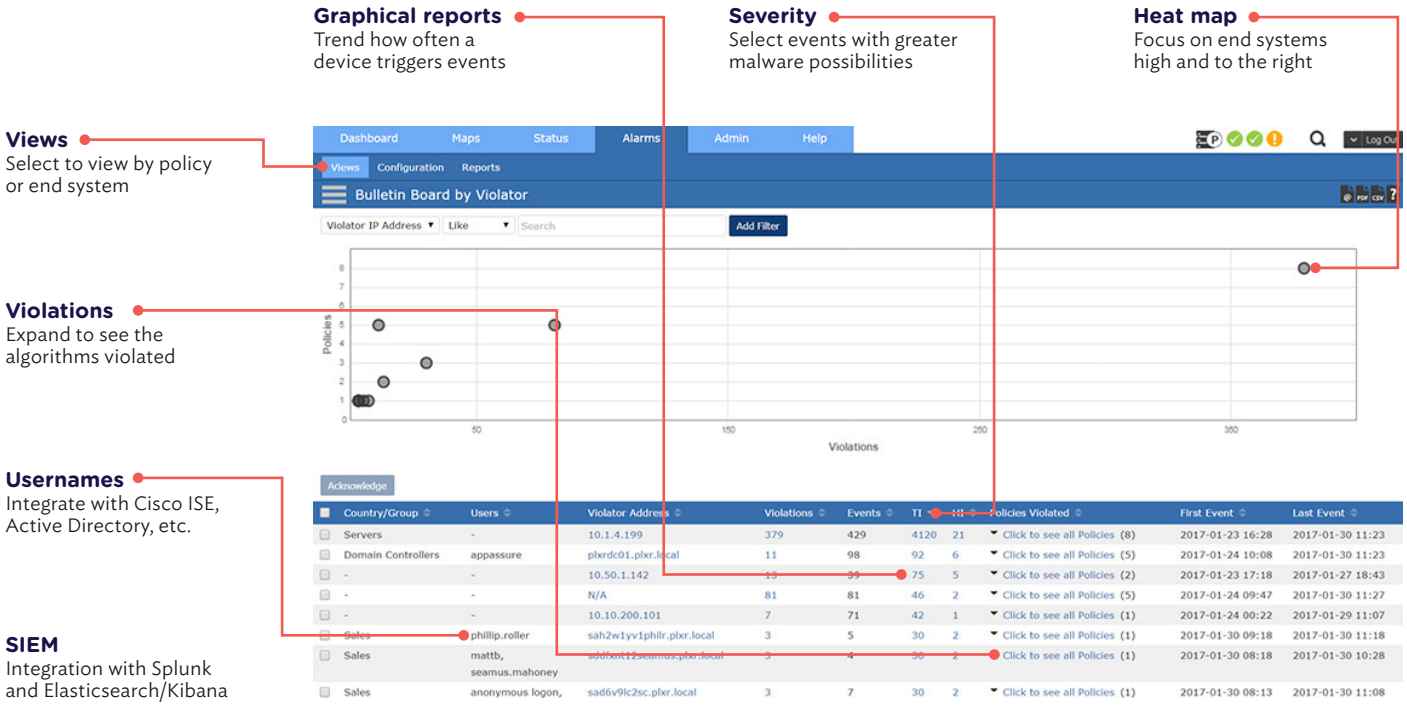
Next-generation details

Next-generation collection and reporting need to include next-generation metadata. Scrutinizer archives unique flow exports, such as Cisco's Application Visibility and Control (AVC), Network-Based Application Recognition (NBAR), Network Secure Event Logging (NSEL), High Speed Logging (HSL), and SD-WAN by Viptela, providing security and network teams the deepest and broadest visibility ever seen in the industry. Furthermore, Scrutinizer gathers data from numerous vendors that are exporting details on domains, URLs, Uniform Resource Identifiers (URIs), round trip time, retransmitted packets, TCP window size, jitter, packet loss, VoIP payload, and caller ID. When the IT team needs to respond quickly, these details provde the greatest amount of insight without requiring that organizations deploy additional probes.

> "NetFlow will provide 80% of the network visibility needed, whereas probe-based technologies should be used in the core 20% of the network infrastructure."
>
> —Debra Curtis, Jonah Kowall
> *Gartner, When is NetFlow Good Enough?*

Greater situational awareness for better threat detection and faster incident response

Situational context drives more efficient incident response and faster time to resolution. Scrutinizer integrates with dozens of leading technologies to consume, visualize, and report on vast amounts of metadata to complement flow-related information.



The integration of Scrutinizer with Cisco ISE, ForeScout CounterACT, and Microsoft Active Directory enables the association of an IP address with usernames, countries, and groups, saving hours of manual effort and providing immediate accountability. Integration of Cisco ASA with FirePOWER, Palo Alto Networks, Gigamon, Ixia, and others delivers insight into the applications and domains end users are accessing. This includes details such as the exact URL visited or telephone number called.

In addition, DNS-related metadata provides the ability to discover botnets, Domain Generation Algorithms (DGAs), and data exfiltration. DNS metadata also provides insight into the vast amount of encrypted web traffic associated with cloud-based applications and Content Deliver Networks (CDNs). Integration with AWS enables Scrutinizer to deliver visibility not only into your network, but into cloud applications as well.

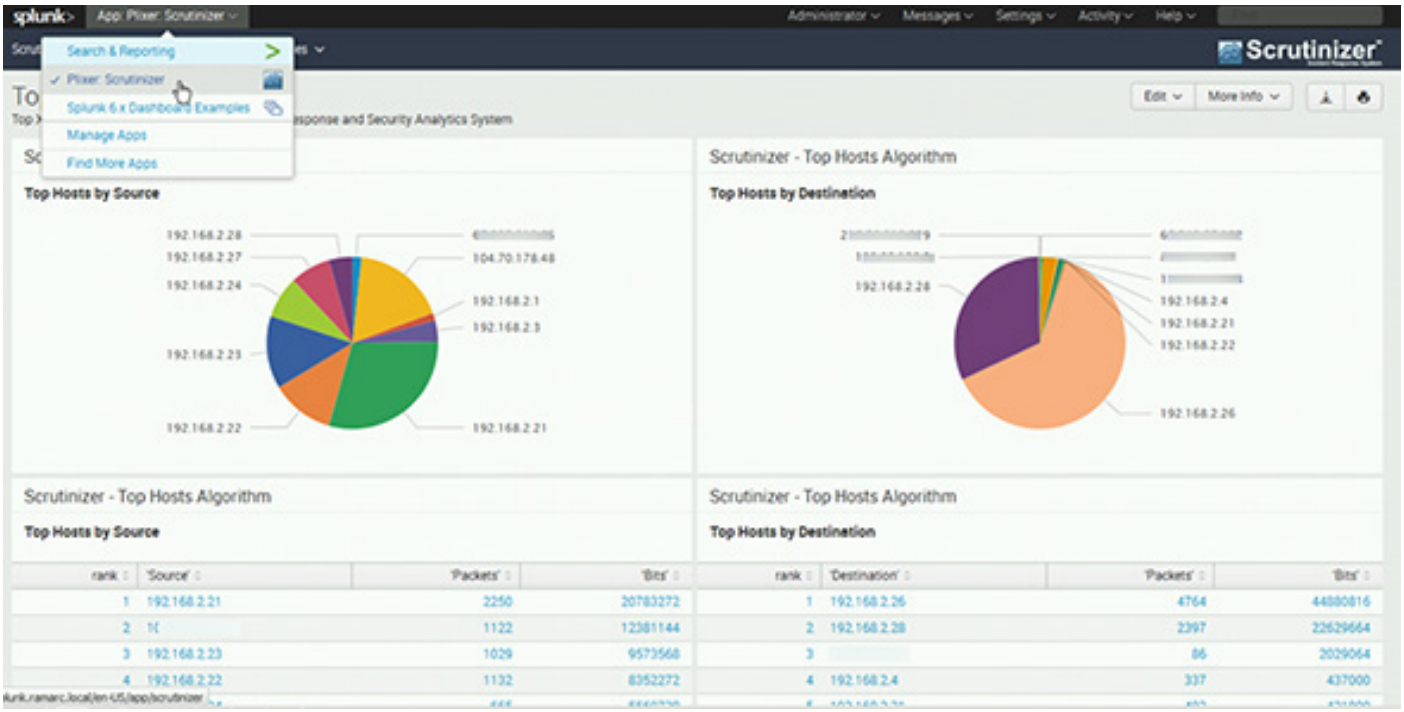
Integration with Deep Packet Inspection (DPI) from Endace and Syslog data from Security Information and Event Management (SIEM) tools like Splunk and Elastic Search/Kibana provides the ability to rapidly correlate packet-level and log data. Scrutinizer becomes the single source of truth, eliminating the need to jump to different investigation tools to complete the discovery process.

Context is key; point security solutions cannot provide all of the details. Simple-to-implement integration via an open API ensures that IT maximizes their investment in existing security systems.

SIEM integration

Scrutinizer is a best-of-breed solution that performs flow analysis and reporting, complementing SIEM tools very well. Support for Splunk and Elasticsearch/Kibana is built into the core of Scrutinizer.

SIEMs are typically used as log aggregators for many existing security products, like firewalls and instrusion prevention systems. They are good at correlating log events across multiple platforms. Scrutinizer delivers added value by complementing log information from the SIEM with contextual flow and metadata, delivering deep insight into incidents.



For example, when the flow data is displayed in the Splunk dashboard, drill in on IP addresses and start filtering by including and excluding details until the root cause of the problem becomes clear. If more than summarized flow information is required, select Scrutinizer in the Splunk menu.

Scrutinizer's powerful filtering and logic operators (if, and, else, greater than, less than, etc.) provide a mechanism to drill down to the specific details needed to conclusively identify the root cause of the problem.

As flow and metadata volumes grow, scalability becomes essential

Achieve massive collection rates

A single Scrutinizer collector is capable of collecting, processing, storing, and rolling up over 100K flows per second.

When distributed collectors are deployed, collection rates reach into the millions of flows per second. Customers needing

to archive tens of billions of flows per day can achieve those rates with Scrutinizer.

Flow collection volumes are rapidly expanding

The need for the ability to scale collection volumes makes sense. NetFlow, IPFIX, and to some extent sFlow are great visibility technologies and are available from every corner of the network. Collected flows give security, network, and application performance teams historical insight into every connection on the network on a hop-by-hop basis.

Flow export volumes are expanding rapidly. Cisco AVC, which delivers a rich set of metadata, can increase the volume of exported flows by as much as 200%. Companies like Gigamon and Ixia are exporting NetFlow data for every packet, as well as offering metadata exports on layer 7 information. Factor in that four times as many vendors today are exporting flows compared to three years ago, and it becomes easy to understand why unscalable legacy collection systems will fail.

Visibility into virtual environments

The introduction of virtualization and virtual networking does not have to mean compromised threat detection or murkier traffic visibility. With Scrutinizer monitoring the virtual environment, IT can ensure that virtual- and software-defined networks are maintaining the highest performance possible. Data can be gathered and correlated across both the physical and virtual environments.

Because NetFlow and IPFIX are native to the VMware operating systems, every virtual appliance deployed can export details about the traffic they support.

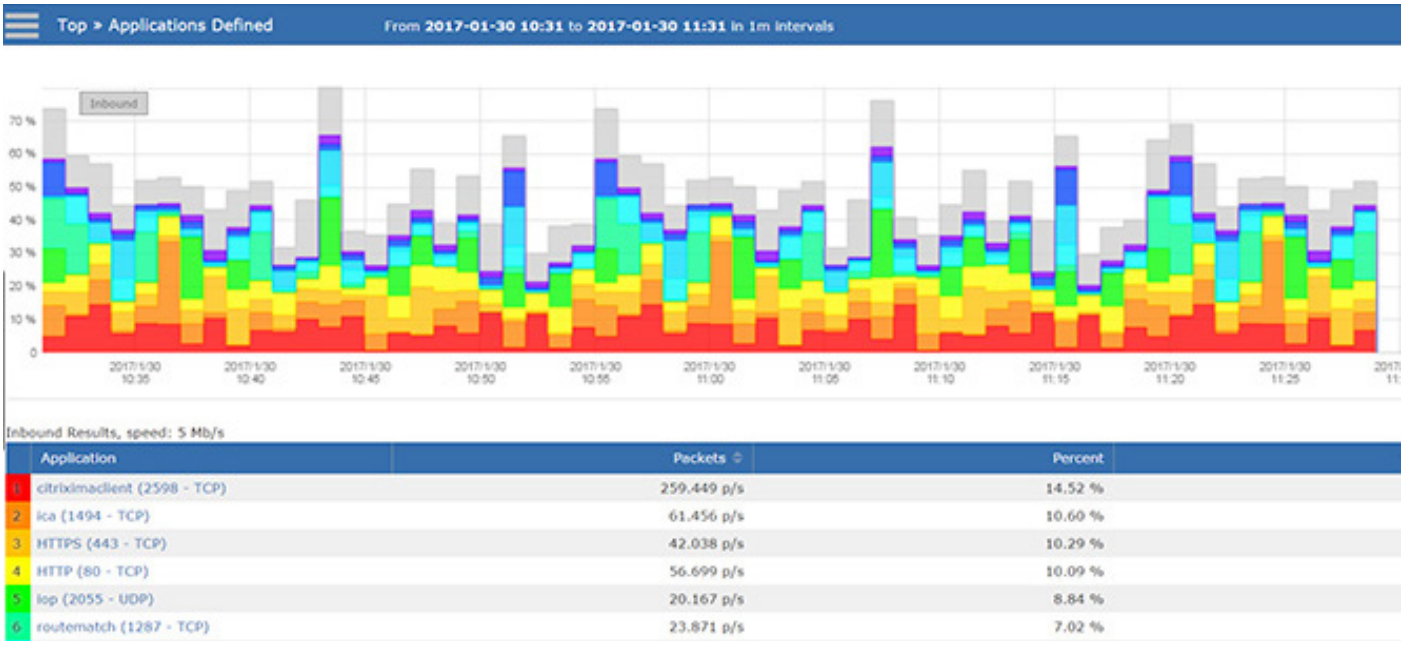
Several VMware products export flows:

- VDS
- DFW (NSX)
- ESX
- VXLAN

Features and benefits

- Verify that network provisioning times are reduced from days to seconds
- Ensure that operational efficiency is gained through VMware's automation
- Confirm that workloads are moved correctly and independently of physical topology
- Integrates with available VMware APIs to gain additional context on the flows received
- Total visibility that automatically follows configuration changes—even those triggered by vMotion

Total visibility should result in comprehensive security and threat detection with the same benefits that are possible in a physical network. This not only means anomaly detection and traffic insight on each virtual machine, but also on the traffic between virtual machines on the same server hardware.



Summary

Scrutinizer is built on a strong foundation of total visibility, informational accuracy, and flexibility. With the industry's fastest reporting, it provides the source-of-truth for rapid and efficient network and security incident response. It fits into your unique network topology and works alongside the industry's most prominent vendors and technologies to deliver detailed and accurate context into your network traffic.

With the ability to achieve massive collection rates, Scrutinizer's flow analysis capabilities are poised to scale as your organization does. Greater situational awareness is mere seconds away, letting your team stay on top of threats and network incidents.

"Plixer is one of the industry's premier thought leaders. It is clear to me that the team at Plixer is passionate when it comes to anything NetFlow- and IPFIX-related."

Aamer Akhter
Technical Leader & Architect for Network Management Solutions
Cisco Systems

"I am very impressed with the product that Plixer has developed and I'm looking forward to many deployments together. We are partnering with Plixer to come up with a world-class user interface."

Pritam Shah
Manager, Performance Monitoring
Cisco Systems

"With the advent of BYOD and the proliferation of mobile applications – it's become ever important to have visibility into your wireless network using deep packet inspection...The canned reports within Scrutinizer focus on wireless downstream traffic, wireless upstream traffic, traffic per SSID and additional reports with a focus on the client."

Jameson Blandford
Technical Marketing Manager
Cisco Systems

Devices supported

Cisco series routers (not a complete list)

- 800, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 7200, 7600, ASR 1000, CSR 100V
- All IOS versions capable of exporting NetFlow, sFlow, or IPFIX
- Cisco routers running IOS 12.2 will support flow exports

Cisco series switches (not a complete list)

- All Catalyst series capable of exporting flows (e.g. 2960, 2960-X, 3560, 3750, 3850, 4500, and 6500)
- All Nexus series capable of exporting flows (e.g. 7000)
- All IOS versions capable of exporting NetFlow, sFlow, or IPFIX

Cisco security devices (not a complete list)

- All ASA series
- All ASR series (e.g. 1000 Zone-Based Firewall High Speed Logging)

Cisco other (not a complete list)

- Network Generation Appliance (NGA)

Non-Cisco devices

- 100% of all hardware and software vendors
- 100% of all flow derivatives (e.g. all NetFlow versions, IPFIX, sFlow, J-Flow, NetStream, AppFlow, ZFlow, Cascade Flow)

For a full list of technology partners, visit:
plixer.com/partners/alliance-partners/

Deployment options

- Hardware appliance
- VMware
- Hyper-V 2012
- KVM
- Software-as-a-service (SaaS)

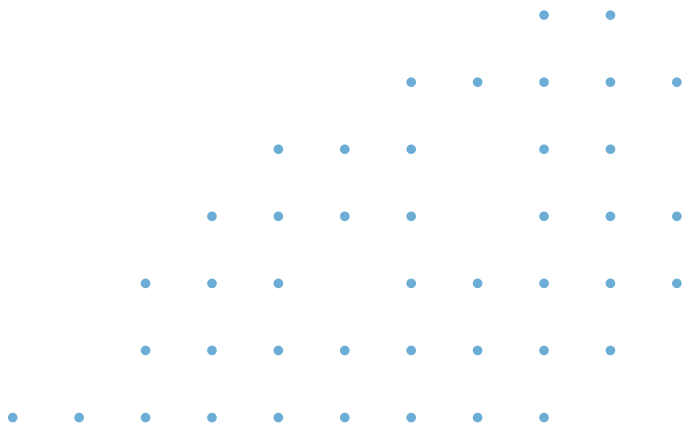
Virtual appliance & SSRV requirements

- Network connection; Gigabit Ethernet recommended
- VMware ESXi 5.5, 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

Contact Plixer

68 Main Street, Suite 4
Kennebunk, Maine 04043

Phone: +1.207.324.8805
Fax: +1.207.324.8683
Website: www.plixer.com



©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

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.