BROCHURE

Reduce risk, gain context, and speed up time-to-resolution

Reduce risk

- Flow analytics for detection
- Proactive thresholding and alerting
- User accountability

Faster time-to-resolution

- Metadata correlation
- Flexible and rapid reporting
- User accountablility

Contextual forensics

- Visualize every conversation from layers 2-7
- Maintain historical data for as long as you want
- Report and filter on any data element

Proactive thresholds and alarming

- User your network as a sensor
- Deliver dynamic notification when thresholds are exceeded
- Proactive notification via RESTful APIs

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.

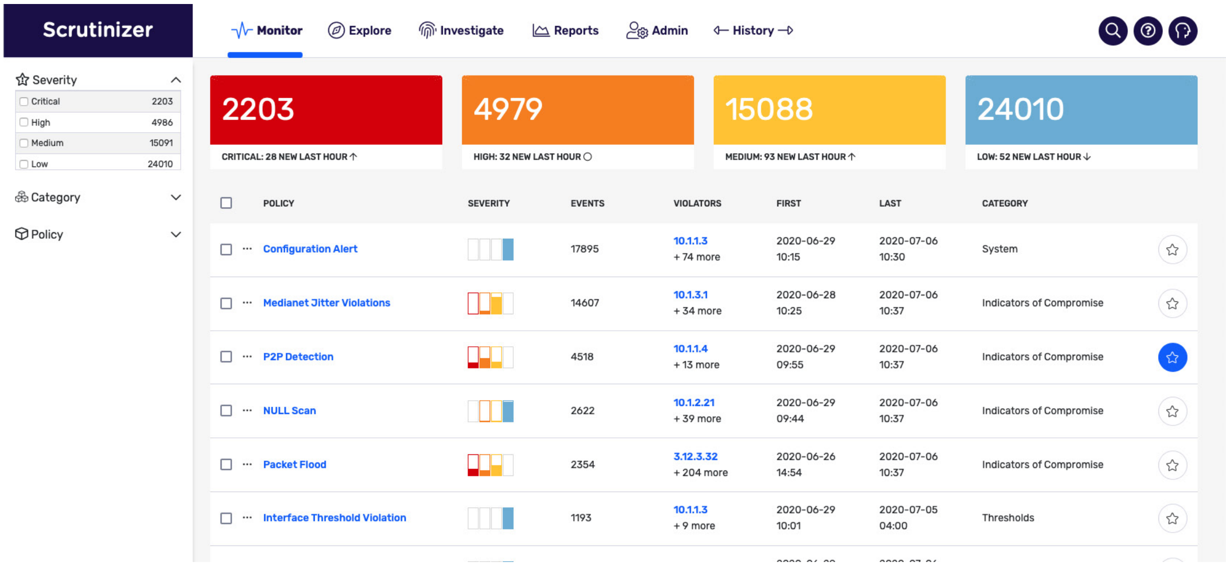
Reduce risk

The primary security objective for organizations of all sizes is to reduce risk. Products aimed at prevention will continue to be part of the equation, but in today's threat environment, the greatest risk reduction occurs from a focus on improving time to resolution after a breach.

Bad things will happen; it is inevitable. In order to reduce risk, you must have a combination of strong forensic data, detailed context, powerful reporting and the ability to hold users accountable. Together these capabilities enable faster 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.



□ Critical	2203
□ High	4986
□ Medium	15091
□ Low	24010

2203 — CRITICAL: 28 NEW LAST HOUR ↑

4979 — HIGH: 32 NEW LAST HOUR ○

15088 — MEDIUM: 93 NEW LAST HOUR ↑

24010 — LOW: 52 NEW LAST HOUR ↓

□	POLICY	SEVERITY	EVENTS	VIOLATORS	FIRST	LAST	CATEGORY	
□	Configuration Alert		17895	10.1.1.3 + 74 more	2020-06-29 10:15	2020-07-06 10:30	System	☆
□	Medianet Jitter Violations		14607	10.1.3.1 + 34 more	2020-06-28 10:25	2020-07-06 10:37	Indicators of Compromise	☆
□	P2P Detection		4518	10.1.1.4 + 13 more	2020-06-29 09:55	2020-07-06 10:37	Indicators of Compromise	★
□	NULL Scan		2622	10.1.2.21 + 39 more	2020-06-29 09:44	2020-07-06 10:37	Indicators of Compromise	☆
□	Packet Flood		2354	3.12.3.32 + 204 more	2020-06-26 14:54	2020-07-06 10:37	Indicators of Compromise	☆
□	Interface Threshold Violation		1193	10.1.1.3 + 9 more	2020-06-29 10:01	2020-07-05 04:00	Thresholds	☆

FIG.1—*The Alarms Tab displays a list of events, indicating severity, and enabling rapid investigation and response.*

Deliver contextual forensics

Access to high volumes of raw data does not lead to faster response. In fact, it can have the opposite effect, increasing complexity and slowing response times. What is needed is context and data correlation.

Many systems on the market gather lots of data points, but don't provide context to make the data useful. If you have, for example, a list of Tor connections on your network, but don't know which users accessed those nodes, how useful is the data?

The best context comes from the correlation of network-related data with metadata from point security products like firewalls, IDS/IPS, SIEM, and distributed probes. Everything that runs your business flows across the network. It passes all traffic between users and the applications they need in order to be productive and drive revenue. Root cause analysis is best derived when you can instantly stitch together the user, device, location, protocol, and application data (including URL and URI) for every flow on the network.

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 method 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.

Extend security capabilities even further

As an add-on to Plixer Scrutinizer, Plixer Security Intelligence consumes and analyzes streamed metadata from Plixer Scrutinizer 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.

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.