DATA SHEET

Plixer Security Intelligence

Staff augmentation

- Ease resource constraints through automation
- Elevate true positives while suppressing false
- Stream to external data lakes in real time

Advanced threat detection

- Two-phase ML/AI approach increases fidelity
- Precise use-case approach improves detection
- Identify and catch encrypted malware

Any threat intelligence feeds

- STIX/TAXII delivers flexibility and future-proofing
- Correlation of any standard third-party feeds
- Supports customer-created threat feeds

Workflow automation

- Streamline trouble ticket workflows
- Remediate security breaches dynamically
- Improve NetOps and SecOps collaboration

For over 20 years, Plixer has been at the forefront of collecting, visualizing, and reporting on metadata generated from every conversation that crosses the network, from the end user all the way into the cloud. This context-rich metadata is collected directly from the existing multi-vendor infrastructure.

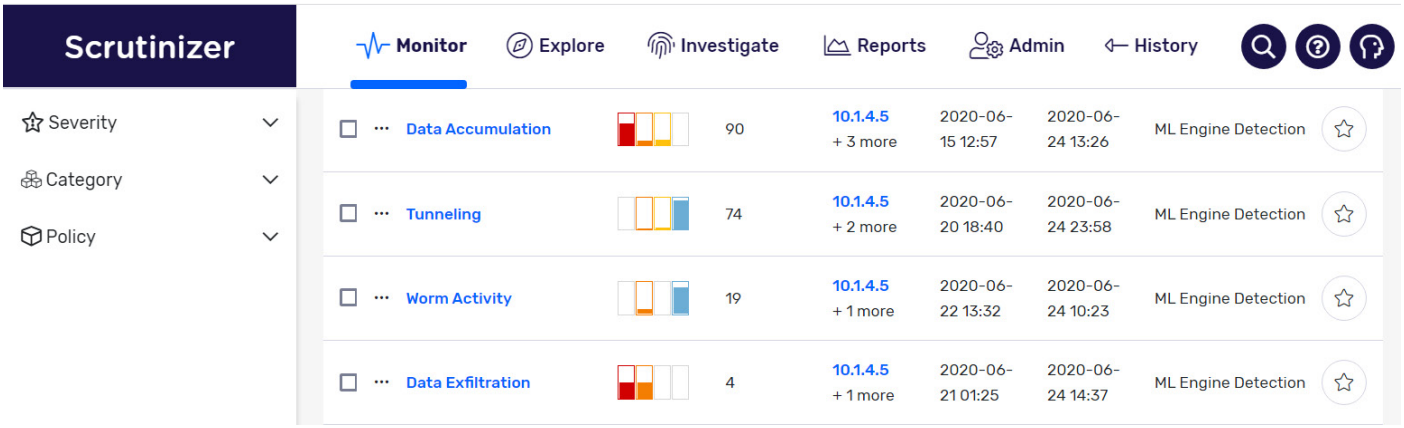
Unlike competing solutions that require the implementation of expensive and proprietary appliances, Plixer's implementation collects data that is exported directly from the existing infrastructure (switches, routers, firewalls, packet brokers, etc.). This differentiated approach is frictionless. It eases implementation, reduces complexity, and improves the ROI of existing infrastructure.

Plixer Security Intelligence consumes and analyzes the 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.

Staff augmentation

Plixer Security Intelligence provides much needed relief to overworked and under-resourced security teams. Analysts are stretched thin trying to reduce risk across a diverse and growing set of threat surfaces. Because most security tools aren't integrated, teams are buried under an avalanche of alarms and false positives, forcing them to constantly react to trouble tickets, struggle to determine what is real, and try to identify what takes priority.

Plixer Security Intelligence bears the load of combing through massive datasets with ML to see patterns that humans can't, and then applies additional AI logic to dynamically eliminate alarms that can be explained. In addition, when Plixer Beacon is also deployed, Plixer



Plixer Security Intelligence applies a two-phase approach to detection. Phase one elevates anomalous network activity or behavior that deviates from what is normal. Phase two then applies AI logic to determine if that anomalous activity or behavior can be explained. Events that are not explainable are presented as alarms to be investigated or dynamically remediated. Alarms are prioritized and ranked by severity, allowing SecOps to focus on what matters most.

Security Intelligence can correlate the business criticality of the associated end device(s) as well as their risk score. This end device insight then influences the severity level of the incident. These advanced capabilities augment the team's ability to identify what is real, helps them know what to work on first, and provides the contextual information needed to resolve the problem quickly.

Advanced threat detection

Many competing network traffic analysis vendors take a "black box of magic approach" that is based on proprietary algorithms, old rulesets, and legacy processing engines. These vendors' solutions have left their customers suffering snail-paced (batched) data processing, excruciatingly long "learning times," and very high false positive rates.

In comparison, Plixer Security Intelligence has been built to include the very latest in machine learning data science, including hundreds of out-of-the-box ML definitions that can also be customized to cover thousands of use cases. Product implementation is fast and easy. Data processing results occur in milliseconds, learning happens quickly and efficiently, and Plixer's two-phase ML/AI detection process delivers leading alarm fidelity.

The most important function of network traffic analysis products is to accurately identify advanced persistent threats buried amongst billions of network conversations. Plixer's two-phase ML/AI detection process was built to filter out false positives and deliver elevated notification for only the real security incidents worthy of action.

In a normal network environment, broadly applying ML across all network traffic will result in many false alarms/alerts. ML works by creating a baseline of what is considered normal and then monitoring network activity for things that fall outside of that "normal." When something deviates from normal patterns, an alarm is generated.

The challenge is that network behavior is a moving target. New applications regularly get deployed, new devices come and go on the network, and the geolocation of traffic changes with the addition of new customers and business partners. With most competing products, these types of normal business changes will trigger false alarms that create hours of work and angst for security teams.

Plixer has taken several steps to alleviate these types of problems. Rather than trying to establish baselines for everything that happens on a network and applying machine learning against all traffic, Plixer takes a use-case-driven approach. We believe that it is extremely important to understand and focus on the types of use cases that are well suited for ML. Things

like protocol and application behaviors, the use of credentials for authentication, the presence of tunneling protocols, ratios of data sent and received, and patterns of lateral movement are just a few examples of metrics that are well suited to ML.

In addition to narrowing the purview of ML to focus on beneficial and appropriate use cases, Plixer has also implemented a two-phase approach to the detection and generation of alarms. In competing products, once a baseline has been established, mathematical algorithms create what is considered an acceptable deviation to that baseline. When activity remains within the standard deviation, all is good. However, when something occurs that places an action outside of what is considered normal, ML will trigger an alarm that goes to a security analyst for investigation.

Plixer believes that this single-step process is flawed and that it is the primary reason for the high number of false positives. Instead, Plixer Security Intelligence takes this process to another level. When an activity deviates from normal and generates an ML alarm, an additional step is taken before the alarm is actually sent to SecOps. Plixer has inserted an AI-driven validation layer that applies additional logic to identify if there is an acceptable reason why this behavior deviation occurred. By applying a second AI-driven step to the process, Plixer Security Intelligence scrubs false positives out and deliver high-fidelity alarms that the SecOps teams can trust.

Real-time data streaming

Many organizations establish centralized data lakes where they consolidate information from all areas of their business. Plixer Network Intelligence allows these organizations to stream network traffic intelligence into them in real-time, using Kafka.

To ensure that data scientists have access to the data they want and can extract value, network teams can configure what data is streamed and how it is aggregated. This capability expands the ROI of the existing network infrastructure and allows the network team to further broaden value to the business.

Security monitoring of TLS/ SSL encrypted traffic

With the goal of protecting data in transit and maintaining privacy, encryption is fundamentally a good thing. But bad actors are using encryption as a way to hide their malicious activity. This means that as the volume of encrypted web traffic rises, risks for organizations rise as well.

Traditional IP and domain threat feeds don't help with encrypted traffic since this information is not transmitted transparently. Organizations often evaluate man-in-the-middle decryption technologies, yet due to the cost and resource intensive nature of the solutions, they often choose not to deploy them.

Users of Plixer Security Intelligence can now leverage JA3/JA3S to identify malicious TLS/SSL encrypted traffic without the need to do man-in-the-middle decryption.

Any threat intelligence feeds

Plixer Security Intelligence supports STIX/TAXII (a threat feed protocol and transport mechanism), which allows users to leverage any third-party IP and domain threat feeds that are STIX/TAXII-compliant. These external feeds can come from other security vendors or from internal security teams who are creating and sharing their own feeds.

In addition to STIX/TAXII support, Plixer Security Intelligence delivers highly scalable, modular, and extensible threat intelligence capabilities. Users can historically identify when, where, and how specific domain and IP details were added into the system. In addition, multiple stream feeds can be supported simultaneously, components within the feeds can be paused or turned off/on, and new intelligence feeds can be imported and evaluated against existing intelligence data. In this way, customers can determine the value of new threat sources and choose whether or not to bring them into the solution.

Workflow automation

Plixer Security Intelligence enables bi-directional integration with ServiceNow, enabling SecOps to streamline the process of trouble ticket creation, In addition, SecOps can share the "collected" network- and end-device-related data that is associated with the incident. This provides context into why the ticket was opened and eliminates the need for duplicate investigative effort. In addition, the NetOps teams can dynamically share security-related data with SecOps for better collaboration, faster time-to-resolution, and data enrichment, which eliminates duplicate investigation.

Plixer Scrutinizer stands out as the market leader in scalable metadata collection, visualization, and reporting. When this metadata is streamed to Plixer Security Intelligence for analysis, SecOps teams' efforts are augmented via automated analysis of machine-generated data to identify and remediate security events in real time.

Plixer Security Intelligence deployment options

The Plixer Security Intelligence product consists of three systems. The core product is deployed on the existing Plixer Scrutinizer instance. The ML (Machine Learning) Engine, which performs the ML processing, is deployed on a separate server. Plixer FlowPro Defender provides additional security capabilities, including JA3 fingerprinting (this is provided as a virtual appliance).

Machine Learning (ML) engine hardware appliances

Plixer ML Engine appliances are rack-mountable servers. Hardware appliance specifications are listed on the following page.

ML engine virtual appliances

The Plixer ML Engine 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
- 3.0 GHz Eight Core CPU, minimum
- 40 GB DDR3 RAM, minimum
- 200 GB SATA drive, minimum

Hardware appliance specifications

	ML engine
Chassis configuration	2U chassis
Storage	3.6 TB capacity
Networking	QP 1 Gb Network Daughter Card (10 Gb available as an option)
Power	Dual, hot plug, redundant power supply (1+1), 750W
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)
Dimensions	26.92" x 17.49" x 3.44" (68.40cm x 44.40cm x 8.73cm)
Hardware warranty	5 years
Rails	Sliding ReadyRails with cable management arm
Heat dissipation	2891 BTU/hr

Plixer Security Intelligence purchasing options

Plixer Security Intelligence is an add-on product to Plixer Scrutinizer and can be purchased as a 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 Security Intelligence in annual contracts. Users are free to use the software as long as they maintain a contract with Plixer and have a licensed Plixer Scrutinizer deployed. 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 Security Intelligence allows users to leverage Plixer's cloud infrastructure to analyze data collected in the cloud-based Plixer Scrutinizer instance. 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.

Ordering information

Ordering subscription licenses of Plixer Security Intelligence software is based on the number of flow-exporting devices. Multiple license tiers are available. License cost is determined by the number of metadata exporters. Customized license options are available upon request.

ML Engine virtual appliances are included in the Plixer Security Intelligence license. Plixer can provide server hardware for these virtual appliances at an additional cost; the number of ML servers required will vary based on details of your environment.