DATA SHEET

Plixer Beacon

IT operations benefits

- Improve inventory management
- Reduce manual, resource-intensive processes
- Gain real-time visibility into device identity, location, and behavioral information
- Automated device discovery and onboarding
- Protect investments and streamline adoption with 3rd-part integrations
- Ensure high scalability and availability
- Accelerate time-to-value with vast device profile library

SecOps & NetOps benefits

- Automatically detect & mitigatie rogue devices
- Authenticate devices, segment networks, and institute granular network access controls
- Improve compliance with data privacy regulations
- Intelligently assess and quantify endpoint vulnerabilities (requires optional Plixer Risk Intelligence add-on)
- Correlate endpoint events with network and security incidents (requires optional Plixer Scrutinizer)

Plixer Beacon gives IT, network, and security operations teams deep visibility and tight control over network endpoints (PCs, mobile devices, VMs, IoT endpoints, etc.). With Beacon, organizations gain real-time insights into device identity, location, and behavioral data, as well as the ability to automatically identify and remediate threats. This helps organizations track assets, strengthen security and compliance, and mitigate risk.

Designed for massive scalability, the product supports up to 1.5 million devices and provides single pane-of-glass management for ultra-efficient administration. The optional Plixer Risk Intelligence add-on helps organizations easily evaluate endpoint risks and isolate vulnerable devices, providing a collective risk score for the entire network and individual scores for specific endpoints.

Plixer Beacon tightly integrates with Plixer Scrutinizer, which enables operations teams to correlate endpoint alarms and events with network performance and security incidents. The product also integrates with Plixer Network Intelligence and Plixer Security Intelligence products, so organizations can also leverage machine learning and artificial intelligence for additional insights.

Components and scalability

Plixer Beacon is based on a distributed architecture with a server component and one or more collector components. Collectors gather and analyze endpoint data. The server maintains the endpoint database, supports system management functions, and provides a web UI for administrators.

Collectors are deployed in an incremental fashion for cost-effective scalability. In smaller environments, the server and collector can be deployed as a single physical or virtualized appliance.

Server-to-collector connections can be initiated in either direction and over any TCP port. This allows for easy deployment in nearly any network, regardless of firewall and security policies.

High availability and disaster recovery

Plixer Beacon supports redundant configurations, disaster recovery options, and non-disruptive data updates to ensure high availability for critical operations.

The product can be deployed in a redundant fashion to enable continuous availability in the event of equipment failures or catastrophes. The high availability pair includes an active primary appliance and a passive (hot standby) backup appliance, managed as a shared virtual IP address. The high availability pair can be collocated to protect against hardware failures or deployed in different sites for geo-redundancy.

The disaster recovery option provides additional resiliency by administratively transitioning active service roles to an alternative site in the event of a catastrophe such as a site-level outage. The product supports multiple recovery sites.

Finally, administrators can update key Plixer Beacon application data (OS risk data, device profiles, etc.) without performing a software upgrade or disrupting operations.

ServiceNow integration

ServiceNow integration lets operations teams easily incorporate Plixer Beacon into established helpdesk workflows. Endpoint events (rogue endpoint detection, anomalous endpoint behavior, etc.) can be forwarded to ServiceNow to automatically create tickets, streamlining operations.

Data collection

Plixer Beacon uses device profiles to categorize and track endpoints with similar functional capabilities or characteristics. The product passively and actively gathers rich contextual data from a variety of sources (DNS, DHCP, SNMP polling, SNMP traps, NetFlow/J-Flow/sFlow, Active Directory, RADIUS Accounting, port mirroring, etc.). It uses machine learning and artificial intelligence to identify detailed inventory and configuration information (make, model, operating system, physical location, IP address, VLAN address, etc.) for network endpoints.

Control and segmentation

Plixer Beacon provides granular network security by auto-authenticating all endpoints—even those that don't have a supplicant or aren't supported by traditional 802.1X systems. The product can be deployed independently or in conjunction with a traditional 802.1X NAC system for ultimate flexibility.

Plixer Beacon intelligently detects anomalous events (duplicate MAC addresses, irregular behaviors, etc.) and automatically takes corrective actions (quarantine, re-authenticate, port blocking, etc.) to isolate suspicious devices and mitigate risks.

Data and system security

Plixer Beacon appliances come hardened with only the necessary ports and services enabled. All component-to-component communications, including high availability and reporting server replication traffic, is secured using strong, modern, standards-based, AES encryption.

On-premises deployment and collection models keep all data within an organization's enterprise security perimeter. Furthermore, server and profile updates support airgap deployments—with no external connection needed.

Plixer Beacon requires only read-only credentials for network data collection. Administrative access to network components is not required.

In addition, the product only retains device identity and behavior attributes. It does not collect personally identifiable information with regulatory compliance implications (HIPAA, GDPR, PCI, etc.)

Deployment and usability

Simple to deploy and scale, Plixer Beacon helps organizations accelerate time-to-value and simplify operations. The solution requires no supplicant or client software and is easy to roll out, administer, and support. Rapid device addition and deletion capabilities let administrators manage endpoints quickly and easily. Administrators can efficiently edit thousands of device profiles and maintain full control over data. Downloadable import templates make it simple to add or update information about network infrastructure devices used for data collection.

An easy-to-use rules editor further streamlines operations by allowing administrators to clone existing profiles, update profiles, and use factory profiles to gain additional data like device and OS views. A profile management wizard enables mass editing of profiles. Plixer Beacon data can be exported to CSV or XML for easy integration with external reporting tools and applications.

Plixer Beacon customers can upload anonymized endpoint data to Plixer Customer Support to share information and improve knowledge. Plixer aggregates and warehouses the data, using the power of crowdsourcing to expand and improve its device profile library and keep pace with change.

Open APIs and interfaces

Plixer Beacon supports open APIs and other interfaces for easy integration with external applications and systems. The Plixer Beacon web UI supports a JSON-RPC API as well as a REST API to enable bidirectional communications with other commercial or internally developed applications. In addition, organizations can forward Plixer Beacon events to external systems such as SIEM solutions or IT operations solutions for enterprise-wide monitoring and management.

Plixer Beacon also supports a data connector that lets organizations automatically ingest device attributes from static sources or from platforms that don't support network-based data collection mechanisms.

The product includes a centrally managed, distributed LDAP device database and RADIUS authentication platform that can serve as a stand-alone authentication/segmentation solution or can be used to augment legacy 802.1X NAC solutions.