PLIXER

5 STEPS TO UNCOVERING SECRETS IN YOUR NETWORK

BUSINESS ARTICLE

Every network holds hidden insights—whether it's security vulnerabilities, performance bottlenecks, or unauthorized access attempts. Here are five steps you can take to uncover these network secrets.

1 Conduct a Network Audit

To uncover unknown issues, first establish a baseline of normal activity with a comprehensive network audit. This will also help identify weak points in your infrastructure.

- **Implement an observability platform**: Aggregate data from network devices, cloud environments, and endpoints into a single view.
- **Use packet analysis and flow data together**: NetFlow reveals traffic patterns, while DPI uncovers application behavior and security threats.
- **Leverage real-time telemetry**: Collect and analyze real-time network telemetry to gain insight into latency, packet loss, and performance deviations.
- **Enable continuous discovery**: Use automated tools to dynamically map devices, applications, and traffic flows as the network evolves.
- **Staying Compliant**: An audit helps ensure compliance with regulatory frameworks by identifying unauthorized assets and tracking data flows.

2 Look for Anomalies with AI-Driven Contextual Insights

Network observability enables teams not only to uncover suspicious activity that bypasses threshold monitoring, but also to investigate and understand the "why" behind them.

Teams leveraging AI can use deep learning models to analyze data, metrics, behaviors, intelligence, and insights from multiple places in a variety of ways.

- **AI-driven analysis beyond simple metrics**: Identify deviations from normal patterns, such as spikes, unusual port activity, and excessive data transfers.
- **Correlate security and performance data**: Combine network traffic insights with endpoint security data to determine whether anomalies indicate a cyberattack, a benign change in user process or workflow, or a performance issue.
- **Root cause analysis**: Use contextual analysis to determine whether an issue stems from a misconfiguration, external attack, or application failure.
- **Threat discovery**: Employ MITRE tactics to identify security risks before they escalate into full-blown cyberattacks.

3 Track & Attribute Resource Consumption

Understanding who and what is consuming network resources can help pinpoint inefficiencies and security risks. For example, a school district recently discovered that student devices were consuming 40% of network bandwidth due to unauthorized streaming applications.

- **Monitor application traffic**: Identify applications using excessive bandwidth or experiencing high latency.
- **Track user activity**: Determine if any users are accessing data or systems outside their normal behavior. Look for shadow IT and unsanctioned applications consuming network resources.
- **Gain visibility into cloud and hybrid environments**: Track communications between on-premises infrastructure, SaaS applications, and multi-cloud networks.
- **Assess device performance**: Ensure that network infrastructure, such as routers and switches, is operating optimally and not overburdened.

4 Identify Trends & Predict Issues Before They Escalate

Rather than just reacting to issues after they occur, network observability helps predict and prevent issues before they affect users or security posture.

- **Analyze historical patterns**: Use machine learning models to detect early warning signs of failures, breaches, or performance degradation.
- **Establish dynamic baselines**: Rather than relying on static thresholds, observability solutions adapt baselines based on evolving network behavior.
- **Predict capacity and demand**: Identify when network infrastructure is approaching its limits and proactively allocate resources.
- **Proactively mitigate security threats**: Detect stealthy threats, such as low-and-slow data exfiltration or lateral movement within the network.

5 Automate Alerts & Investigations

Traditional monitoring generates too many false positives, requiring manual correlation to identify real issues. Observability reduces noise by applying AI-driven insights, helping organizations reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

- **Use AI-driven anomaly detection**: Reduce reliance on static alert rules by using AI to detect true deviations from normal network behavior.
- **Automate root cause analysis**: Observability solutions can correlate flow data, metrics, and traces to pinpoint issues quickly and provide actionable information.
- **Cross-validate alerts**: If using our Plixer One platform, NetOps teams can use its ML engine to check the validity of alerts from other sources.

Conclusion

By following these five steps, NetOps teams can uncover hidden risks, optimize performance, and improve security posture. A proactive approach to network observability ensures that threats and inefficiencies are addressed before they become major issues. Start implementing these strategies today to gain full visibility and control over your network.

plixer.com
sales@plixer.com