ManageEngine
Site24x7

What is network observability?

Key elements and use cases

What are we going to cover?

Introduction

With the evolution of networks from simple topologies to dynamic, flexible, and inclusive models that enable users to connect from anywhere in the world, organizations are seeking a solution that can help them transition from traditional monitoring to effortless observability. This growing importance of network observability is transforming the way organizations operate, and makes sure that their employees and customers remain securely connected at all times.

What is network observability?

Network observability is having complete visibility into a network, its components, and related metrics. It enables businesses to gain valuable insights into its networks and detect weak spots that might otherwise go unnoticed. Network observability provides a framework for businesses to monitor and analyze their network performance, identify issues, and troubleshoot them in a timely manner. With its AI-driven insights, organizations can automatically detect traffic, performance, and security anomalies. Network observability helps proactively analyze issues across their entire infrastructure and application stack.

Why is network observability important?

The size and complexity of networks are increasing, and user expectations are also skyrocketing. Organizations need a system that can effectively communicate and state what needs to be fixed. Let's learn about the challenges in today's networks, and see how network observability can help.

- **Blended networks:** Most global organizations own a dedicated on-premises network in addition to several cloud-based networks like Cisco Meraki or VMware NSXs. Even though monitoring tracks availability, traffic patterns, latency, bandwidth, packet loss, and other similar metrics for all the devices, collecting the data requires different methods like SNMP, WMI, or REST API, depending on the device, or the type of network being monitored. This means a network monitoring tool should adapt to monitor blended networks.

- **Interconnected components:** Modern applications often consist of connected components distributed across multiple systems, which adds layers of complexity and increases the likelihood of failures. Continuous monitoring requires collecting metrics to detect anomalies. However, observability makes spotting deviations clearer by aggregating all data on a single pane, making the identification of anomalies easier across a distributed architecture.

- **Increased cyberthreats:** Traditional network monitoring help establish baselines and monitor metrics, but fails to provide the necessary insights to troubleshoot issues. Simply receiving alerts means that existing systems inform you that there's an issue, but they do not provide any warning before a problem arises. In a more serious scenario, a vulnerability in any of the devices might go unnoticed, causing a small issue that could lead to significant downtime, affecting both customers and employees. Furthermore, cybercriminals might exploit vulnerabilities in the system without the network administrator's knowledge. In large and complex systems, a monitoring dashboard might help track issues, but it might not necessarily assist in proactively identifying problems.

- **Insights into network performance:** Basic monitoring of network infrastructure can only provide limited insights into the network's performance. Network observability, on the other hand, goes beyond basic monitoring by collecting and analyzing vast amounts of data from various sources within the network infrastructure. This comprehensive visibility allows organizations to detect proactively and address performance issues, security vulnerabilities, and other network-related challenges before they have any negative impact on their businesses. In other words, network observability provides a big-picture view across network components, applications, and cloud systems, enabling organizations to gain deeper insights and make informed decisions.

- **Monitoring fatigue:** Network monitoring is vital for complete visibility, where network admins establish baseline behavior and receive alerts from monitoring tools if there's any deviation from expected behavior. However, constantly looking at dashboards and metrics can cause network admins to miss some issues due to fatigue, leading to suboptimal network operation over time. Every day, billions of metrics are generated, which is overwhelming, but businesses only need to know if the user flow works as expected without any hitch.

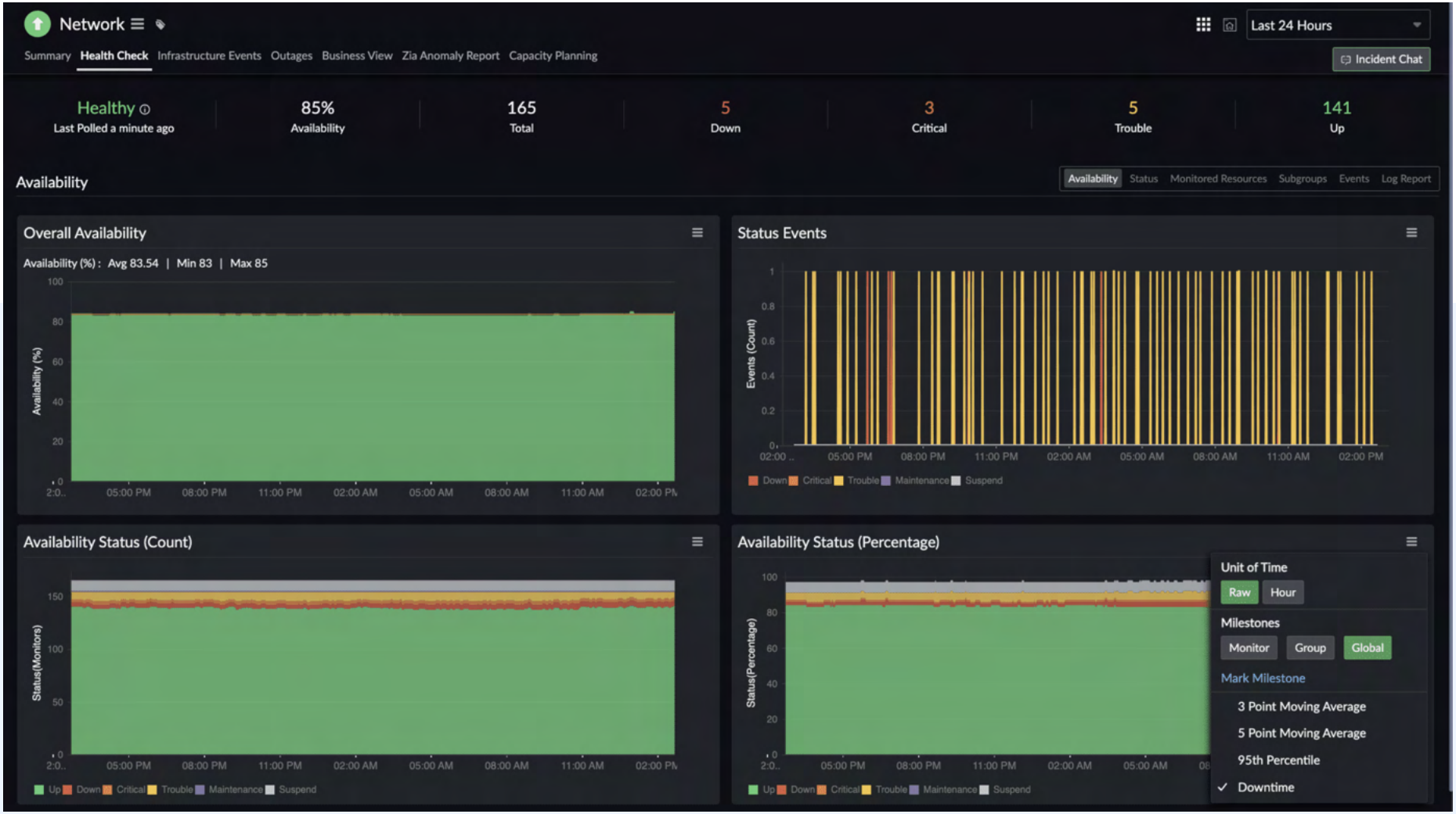
Network observability, on the other hand, focuses on the end-user experience. With an observability solution in place, network admins receive proactive information if any action does not work as intended due to any issue within their network. They can then inform customers beforehand, helping businesses maintain trust and prevent any potential loss of revenue.

Data-driven decision-making: Monitoring a network can be a challenging task for admins, since they have to track scattered metrics from different modules to gain a complete picture of the network's performance. Unfortunately, this process tends to slow down decision-making.

By implementing network observability, administrators can effectively analyze and monitor network performance, which empowers them to make informed decisions about network management and optimization. By analyzing data, they can identify trends, patterns, and performance indicators to improve network efficiency and reduce costs. The actionable insights they get from network observability enable well-informed decision-making, which is crucial for enhancing overall business outcomes.

Network observability vs. network monitoring: What's the difference?

	Network monitoring	Network observability
Data collection	Basics like uptime, bandwidth utilization, and device availability	Comprehensive from various sources like flows, packets, and telemetry
Threshold and alerting	Predefined thresholds	ML and anomaly detection
Incident response	Reactive	Proactive
Application and user performance metrics	Limited visibility	Holistic view
Data analysis	Lacks real-time data analysis	Employs real-time data analysis for quick identification and troubleshooting of issues


Network
Summary
Health Check
Infrastructure Events
Outages
Business View
Zia Anomaly Report
Capacity Planning
Last 24 Hours
Incident Chat
Healthy
Last Polled a minute ago
85%
Availability
165
Total
5
Down
3
Critical
5
Trouble
141
Up
Availability
Availability
Status
Monitored Resources
Subgroups
Events
Log Report
Overall Availability
Availability (%) : Avg 83.54 | Min 83 | Max 85
Availability (%)
Status Events
Events (Count)
Down
Critical
Trouble
Maintenance
Suspend
Availability Status (Count)
Status(Monitors)
Availability Status (Percentage)
Status(Percentage)
Unit of Time
Raw
Hour
Milestones
Monitor
Group
Global
Mark Milestone
3 Point Moving Average
5 Point Moving Average
95th Percentile
Downtime

What are the key elements of network observability?

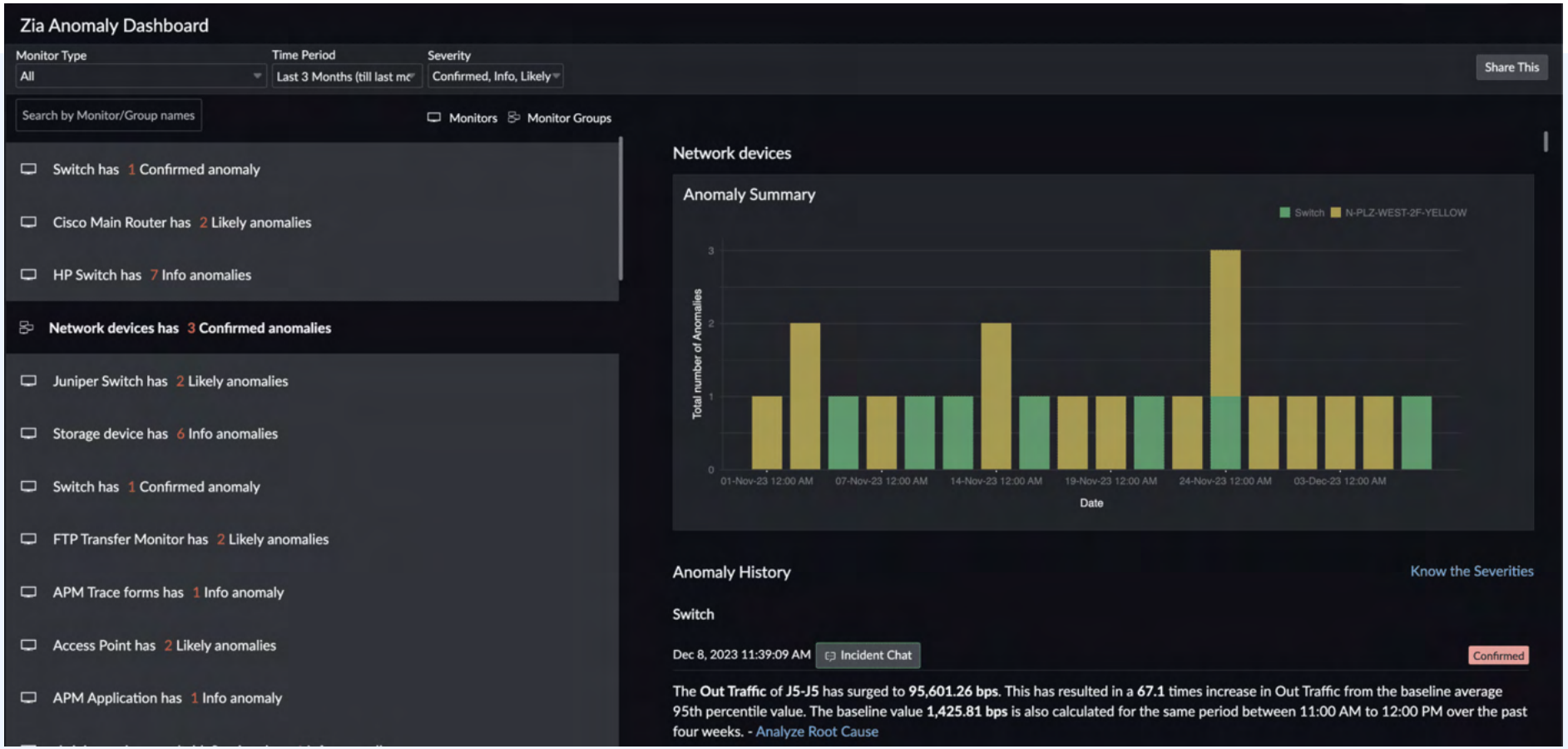
Effective network operations triage requires teams to gather intelligence from various sources like alarms, network flows, performance data, network configurations, and logs. Only with complete operational visibility can teams make quick, intelligent decisions and identify the root cause quickly. Troubleshooting becomes easy when teams gain visibility into the user experience. They can even troubleshoot in the context of a specific network device, interface, or virtual network function. Solutions that collect relevant data formats and data streams enable organizations to focus on what matters, and avoid spending hours searching for the proverbial needle in the haystack in today's networks. Network monitoring software should help administrators by providing them with the necessary tools to quickly identify and resolve issues, instead of adding to the time it takes to triage problems. The goal should be to reduce the need for escalations and empower admins to efficiently manage the network. Missing even a single ingredient of this recipe could mean that the root cause remains hidden for hours or even days, leading to blame games within teams, and a potential compromise to security.

- **Data collection:** By capturing data from different layers of the TCP/IP stack, like network, application, etc., an organization gains a holistic view of its network's behavior and performance.

- **Data analysis:** After data collection, advanced analytics techniques are applied to extract insights.
  - **Machine learning algorithms:** Analyzing network behavior to find patterns and trends, identifying any deviations from normal behavior, and anticipating possible problems.

- **Statistical analysis:** Setting baselines, determining appropriate thresholds, and identifying any deviations from expected performance.

- **Anomaly detection:** Automating the detection of unusual or suspicious network events that could indicate potential security threats, or performance issues.



- **Alerting and notification:** Alerting mechanisms send alarms when specific thresholds are breached, or anomalies are detected. This helps network teams respond proactively to incidents, ultimately reducing the time taken to troubleshoot and resolve network issues, resulting in minimal impact on business operations, ensuring that everything runs smoothly.

What are some network observability use cases?

Consider a banking organization, Zylker, that faces a payment failure. Even one minute of outage could leave thousands of customers in the lurch as they try to complete their transactions. With a monitoring solution in place, the bank staff receives an alert on the system failure which could be because of any network issue like high traffic, poor bandwidth allocation, or a device failure. Here, we will take the case of a router that is not responding as there are incorrect configuration changes.

- **Identify root cause:** With an AI-powered observability solution in place, network admins will view information about any unusual spikes or anomalies in the device's critical performance attributes like response time, CPU usage, or memory utilization. As they drill down, the network admins analyze the reasons for it.

  a. Detect and resolve network bottlenecks, latency issues, or bandwidth constraints before they impact user experience.

  b. Monitor network metrics, such as packet loss, latency, and throughput, to optimize network performance.

- **Detect and respond to security threats:** On the dashboard, the network admins will be able to view that there's an unapproved configuration change. They can then quickly revert the last working configuration file and ensure that the router continues to operate without any glitches. This minimizes the impact, significantly decreases security risks, and eliminates unplanned downtime.

  a. Detect and respond to security threats, such as malware, intrusions, or unauthorized access attempts, in real time.

  b. Monitor network traffic patterns and anomalies to identify potential security breaches or unusual behavior.

- **Generating automated insights about network malfunctioning:** As the solution "learns" about possible cases of network failures, it will generate automated insights and might also provide recommendations. This might include forecasts based on current usage patterns.

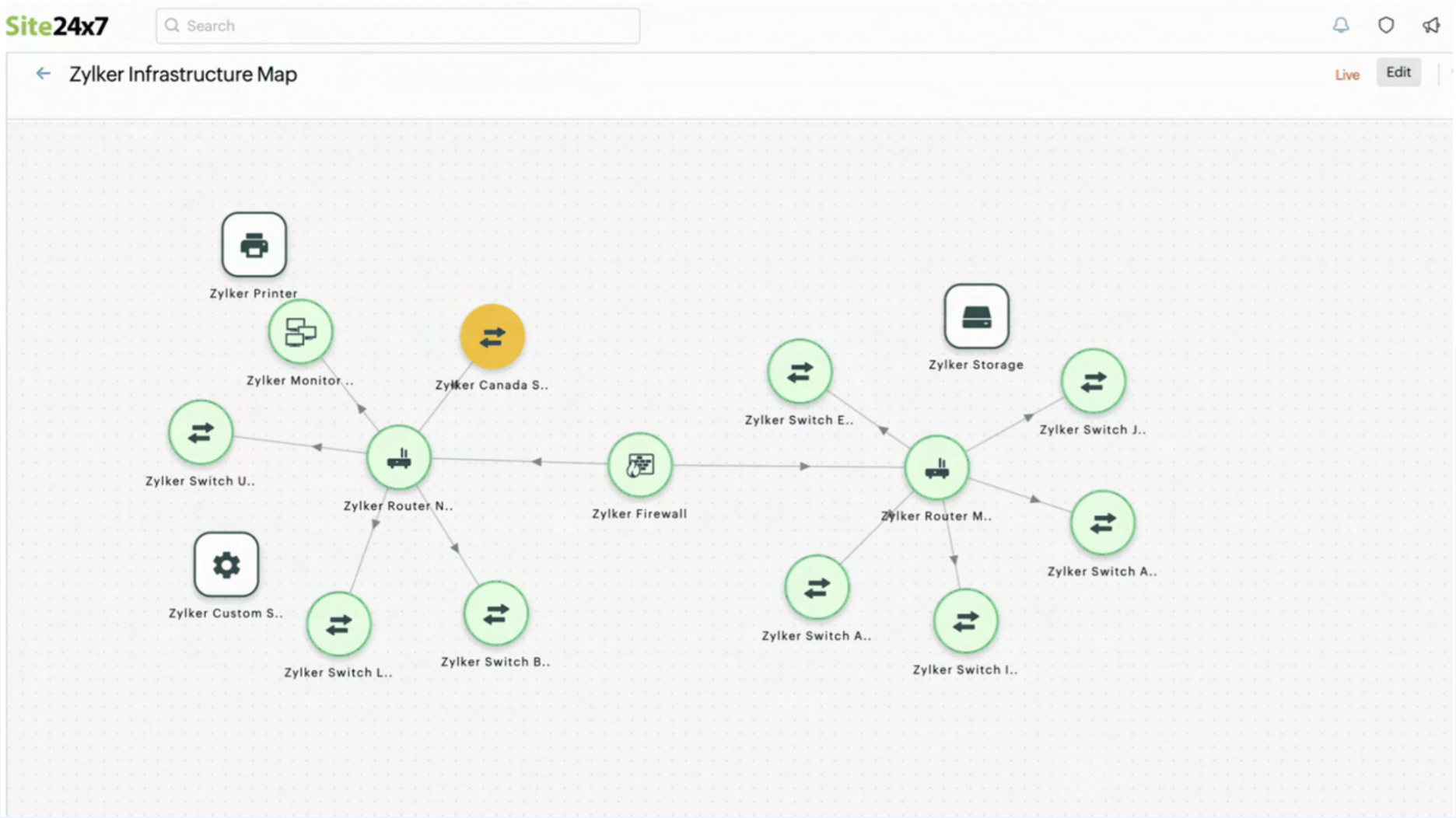
  a. Quickly diagnose and troubleshoot network problems by analyzing real-time data and identifying causes.

  b. Provide recommendations and forecasts that help in capacity planning.

- **Diagnose and troubleshoot network issues:** Network issues could be caused by device hardware, firmware, device configuration, or even improper bandwidth allocation. A holistic view that includes a network map helps network admins understand what fixes must be applied to prevent the same issue from recurring.

  a. Visualize network topology and traffic flows to pinpoint issues, reduce downtime, and minimize service disruptions.

  b. Diagnose the problem to prevent recurrence.


Site24x7
Search
Zylker Infrastructure Map
Live
Edit
Zylker Printer
Zylker Monitor ..
Zylker Canada S..
Zylker Switch U..
Zylker Router N..
Zylker Firewall
Zylker Switch E..
Zylker Storage
Zylker Switch J..
Zylker Router M..
Zylker Switch A..
Zylker Custom S..
Zylker Switch L..
Zylker Switch B..
Zylker Switch A..
Zylker Switch I..

- **Gain insights into application behavior and performance:** An application's slowness might also be caused by a network issue. If Zylker uses only an application monitoring tool but does not monitor networks, it might be impossible to trouble shoot the issue. However, with a network observability solution in place, network admins gain insights into application performance and address issues.

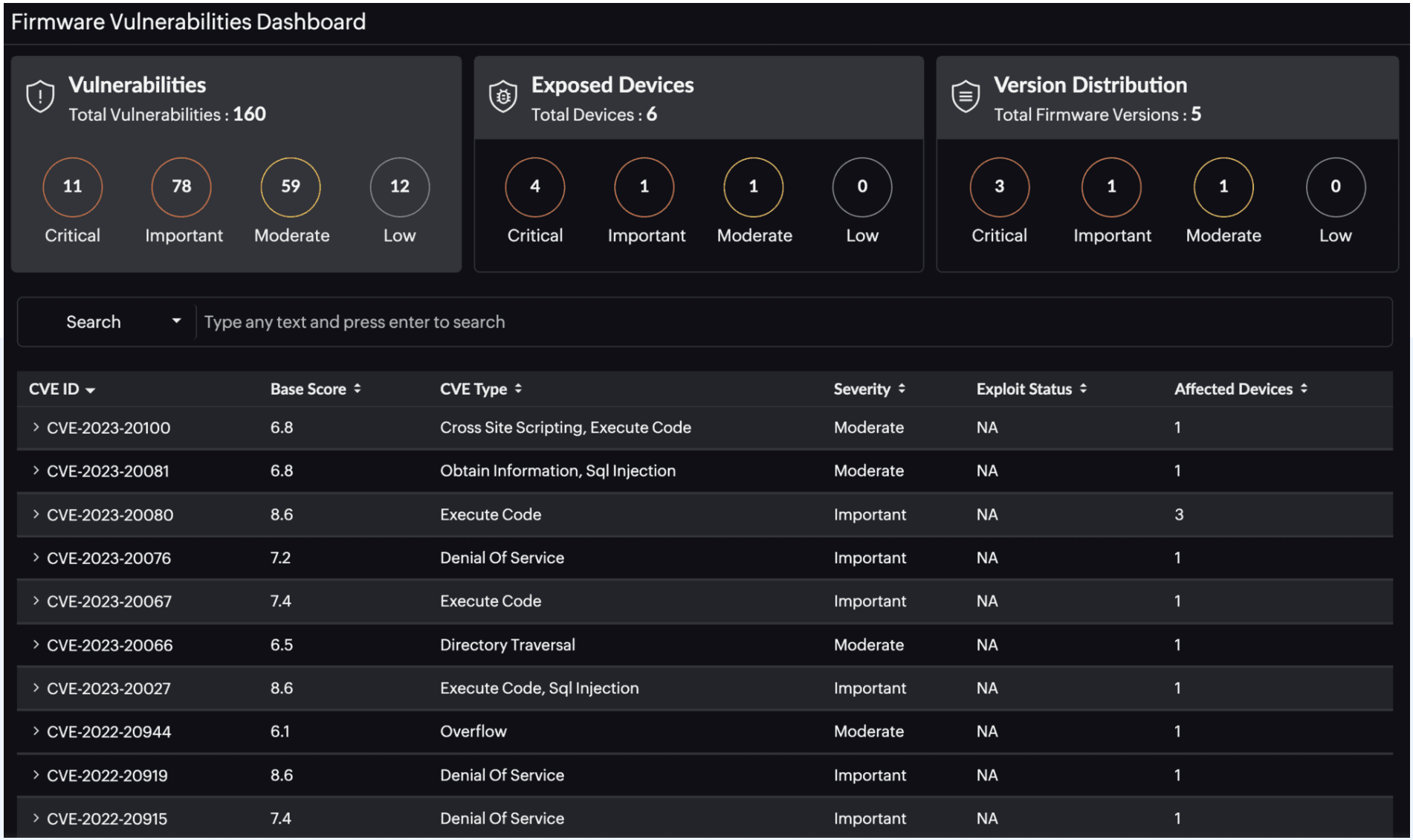
  a. Gain insights into application behavior and performance by monitoring network traffic and application-specific metrics.

  b. Identify and address issues related to application responsiveness, data transfers, or service dependencies.

- **Compliance and Regulatory Requirements:** Every organization needs to ensure that there are rules and policies to defend its networks from potential threats and ensure compliance with industry standards like Cisco IOS, SOX, HIPAA, PCI, or any other custom organizational policies. Failing to do so might result in serious repercussions. The right way to approach this is to have a network observability solution that also includes a compliance module.

  a. Monitor network activity and capture relevant data to ensure compliance with industry regulations and data protection standards.

  b. Maintain audit trails and generate compliance reports for regulatory purposes.



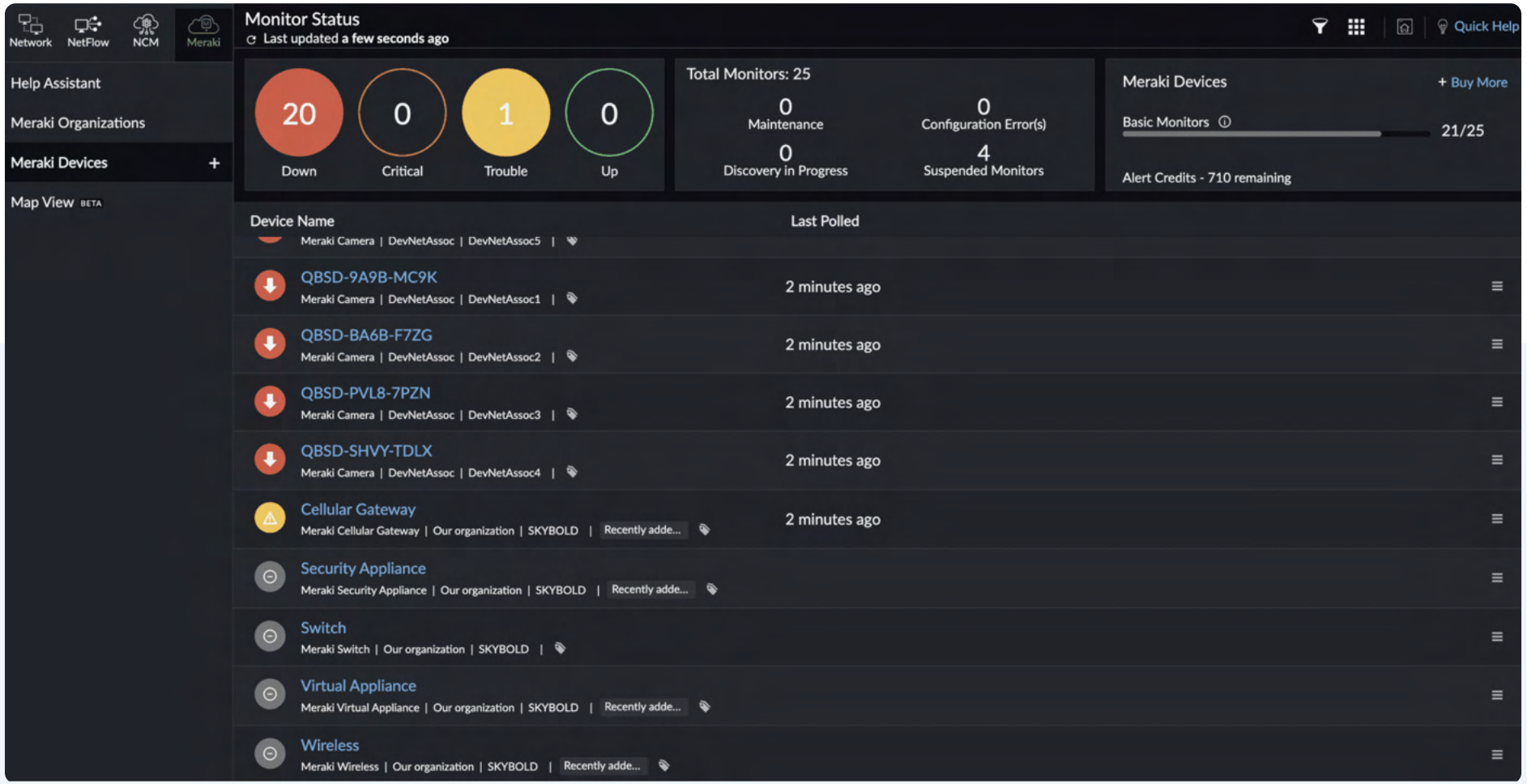
CVE ID	Base Score	CVE Type	Severity	Exploit Status	Affected Devices
CVE-2023-20100	6.8	Cross Site Scripting, Execute Code	Moderate	NA	1
CVE-2023-20081	6.8	Obtain Information, Sql Injection	Moderate	NA	1
CVE-2023-20080	8.6	Execute Code	Important	NA	3
CVE-2023-20076	7.2	Denial Of Service	Important	NA	1
CVE-2023-20067	7.4	Execute Code	Important	NA	1
CVE-2023-20066	6.5	Directory Traversal	Moderate	NA	1
CVE-2023-20027	8.6	Execute Code, Sql Injection	Important	NA	1
CVE-2022-20944	6.1	Overflow	Moderate	NA	1
CVE-2022-20919	8.6	Denial Of Service	Important	NA	1
CVE-2022-20915	7.4	Denial Of Service	Important	NA	1

How can network observability be implemented?

Organizations with a sound network monitoring foundation are better positioned to reinvent, compete, and implement observability solutions with minimal disruption. If an organization doesn't have a monitoring solution yet, implementing a secure, cloud-based network monitoring platform first helps steer it toward network observability easily and achieve more significant growth, efficiency, and resilience.

Here are the steps organizations take to move toward complete observability:

- Identify data sources like network devices, servers, applications, logs, flows, and packets.
- Deploy appropriate data collection mechanisms.
- Establish a centralized repository.
- Implement a network monitoring tool with advanced analytics, which includes ML algorithms, to process and analyze the collected data.
- Employ appropriate alerting and notification profiles according to your organization's needs.


Network
NetFlow
NCM
Meraki
Help Assistant
Meraki Organizations
Meraki Devices
Map View BETA
Monitor Status
Last updated a few seconds ago
Quick Help
20
Down
0
Critical
1
Trouble
0
Up
Total Monitors: 25
0
Maintenance
0
Configuration Error(s)
0
Discovery in Progress
4
Suspended Monitors
Meraki Devices
+ Buy More
Basic Monitors
21/25
Alert Credits - 710 remaining
Device Name
Last Polled
Meraki Camera | DevNetAssoc | DevNetAssoc5 |
QBSD-9A9B-MC9K
Meraki Camera | DevNetAssoc | DevNetAssoc1 |
2 minutes ago
QBSD-BA6B-F7ZG
Meraki Camera | DevNetAssoc | DevNetAssoc2 |
2 minutes ago
QBSD-PVL8-7PZN
Meraki Camera | DevNetAssoc | DevNetAssoc3 |
2 minutes ago
QBSD-SHVY-TDLX
Meraki Camera | DevNetAssoc | DevNetAssoc4 |
2 minutes ago
Cellular Gateway
Meraki Cellular Gateway | Our organization | SKYBOLD | Recently adde...
2 minutes ago
Security Appliance
Meraki Security Appliance | Our organization | SKYBOLD | Recently adde...
Switch
Meraki Switch | Our organization | SKYBOLD |
Virtual Appliance
Meraki Virtual Appliance | Our organization | SKYBOLD | Recently adde...
Wireless
Meraki Wireless | Our organization | SKYBOLD | Recently adde...

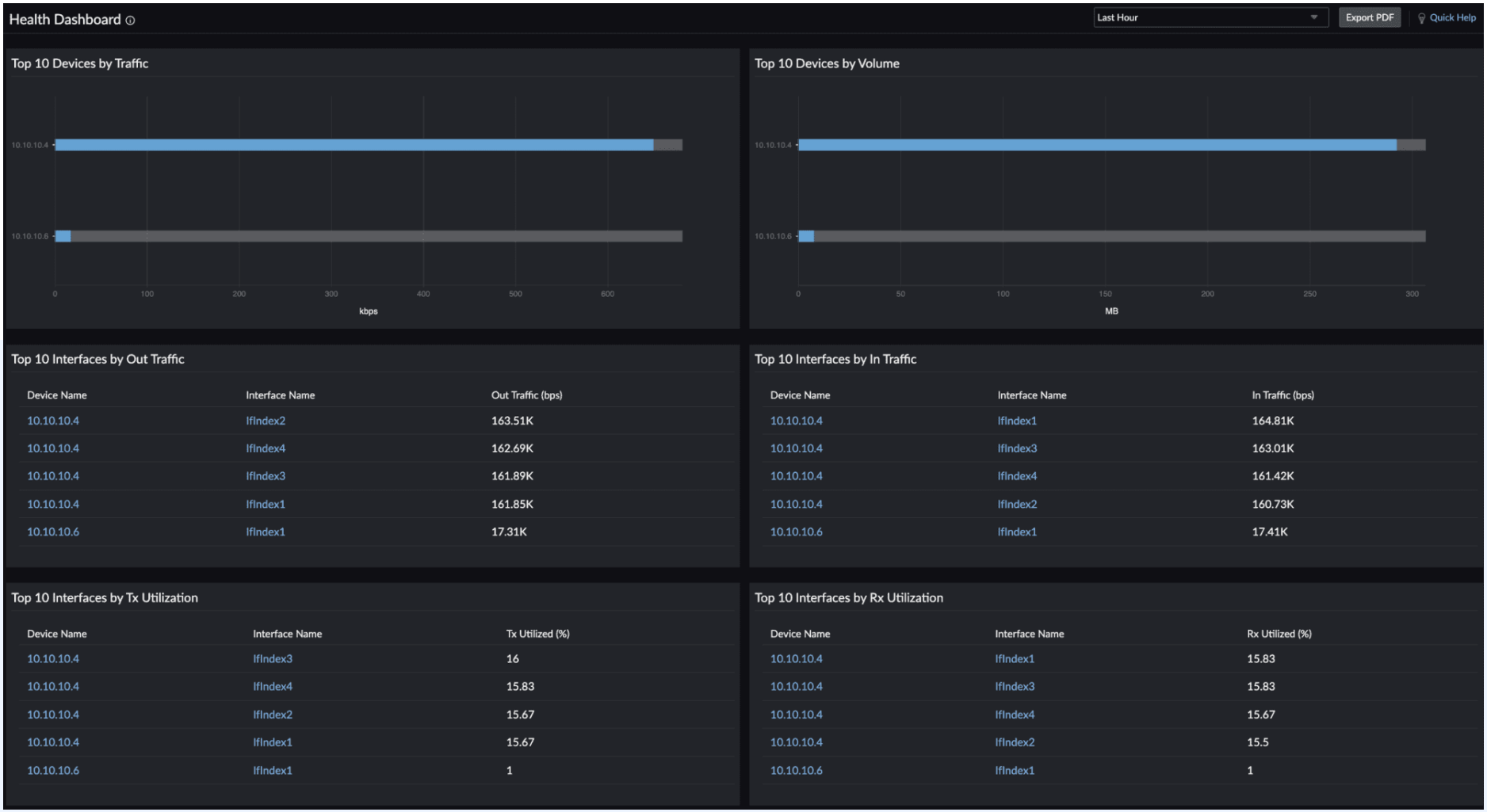
What are the benefits of implementing network observability?

The key benefits for implementing network observability include:

- **No more blame games:** Since you will know exactly where the problem lies in your network, whether it is because of east-west traffic or north-south traffic, you gain complete transparency in operations.

- **Compliant networks:** You can be confident that your networks are compliant with major industry standards, and won't experience problems during an audit.

- **Improved productivity:** Since a major time-consuming task has been automated, employees can work on more productive and cognitive tasks that improve the customer experience and coordination between teams.


Health Dashboard
Last Hour
Export PDF
Quick Help
Top 10 Devices by Traffic
10.10.10.4
10.10.10.6
0
100
200
300
400
500
600
kbps
Top 10 Devices by Volume
10.10.10.4
10.10.10.6
0
50
100
150
200
250
300
MB
Top 10 Interfaces by Out Traffic
Device Name
Interface Name
Out Traffic (bps)
10.10.10.4
IfIndex2
163.51K
10.10.10.4
IfIndex4
162.69K
10.10.10.4
IfIndex3
161.89K
10.10.10.4
IfIndex1
161.85K
10.10.10.6
IfIndex1
17.31K
Top 10 Interfaces by In Traffic
Device Name
Interface Name
In Traffic (bps)
10.10.10.4
IfIndex1
164.81K
10.10.10.4
IfIndex3
163.01K
10.10.10.4
IfIndex4
161.42K
10.10.10.4
IfIndex2
160.73K
10.10.10.6
IfIndex1
17.41K
Top 10 Interfaces by Tx Utilization
Device Name
Interface Name
Tx Utilized (%)
10.10.10.4
IfIndex3
16
10.10.10.4
IfIndex4
15.83
10.10.10.4
IfIndex2
15.67
10.10.10.4
IfIndex1
15.67
10.10.10.6
IfIndex1
1
Top 10 Interfaces by Rx Utilization
Device Name
Interface Name
Rx Utilized (%)
10.10.10.4
IfIndex1
15.83
10.10.10.4
IfIndex3
15.83
10.10.10.4
IfIndex4
15.67
10.10.10.4
IfIndex2
15.5
10.10.10.6
IfIndex1
1

How does Site24x7 help you implement network observability?

As organizations move towards implementing digital transformation, they must provide reliable services that are not impacted by natural disasters or cyberthreats. To deliver reliable services that garner trust and provide exceptional user experience, the organization should ensure that its networks are observable, which requires an observability solution.

An observability solution requires metrics that need constant monitoring. Observability and monitoring complement each other, where monitoring is a part of observability, and observability cannot be achieved without monitoring. If a system is observable, it can be easily monitored.

- Digital transformation necessitates reliability.
- Delivering reliable services requires resilient networks.
- To build resilience, you need observability.
- To implement observability, you need metrics.
- Metrics are derived from constant monitoring.

About ManageEngine Site24x7

ManageEngine Site24x7 is an AI-powered observability platform for DevOps and IT operations. The cloud-based platform's broad capabilities help predict, analyze, and troubleshoot problems with end-user experience, applications, microservices, servers, containers, multi-cloud, and network infrastructure, all from a single console. For more information about Site24x7, please visit www.site24x7.com.

Get Quote Request Demo