SOLUTION BRIEF

Digital Experience and Network Performance Monitoring With FortiMonitor

Executive Summary

Today, organizations are accelerating their digital transformation initiatives. Digital transformation is driven by the user experience instead of feeds and speeds, and because the user experience can determine the success or failure of applications, 100% uptime is critical. According to Gartner, by 2023 the use of NetOps 2.0 principles will grow by 40%, and those embracing NetOps can reduce application delivery times by 25%.[1]

FortiMonitor is a cloud-based solution that delivers a complete picture of every service, network device, and application in any deployment, whether it is containers, cloud, on-premises, or hybrid. But it does more than just inventory and monitor hardware and services; it also tracks the availability of the entire user experience from end to end. FortiMonitor extends network monitoring beyond the Fortinet Security Fabric, to encompass context from third-party network, infrastructure, applications, and cloud for comprehensive digital experience monitoring (DEM). With FortiMonitor, operations center teams can record user interactions with applications, whether it's a sign-up form or an order for goods and services. Teams then can play back the recording to make sure that everything is working as it should and users have positive experiences.

Fortinet Security Fabric FortiMonitor Solution

- **Digital experience monitoring.** Get insight into the quality of a user's experience with apps and services
- **Single source of truth for operations.** Reduce alert fatigue, tool sprawl, and resolution times
- **Automated remediation.** Use automated diagnosis and remediation for hybrid infrastructures

Network Performance Is Key

Given that most IT environments are increasingly complex and distributed, organizations need a high-performance, secure network to successfully achieve their digital business initiatives. The availability, performance, security, and quality of an application and its components all affect the end-user experience.

Being able to ingest at scale, and more importantly, trust the log and event data from every piece of infrastructure in the stack is mission critical. Teams need to be alerted with the data they need to correlate and respond to security threats. In addition to security data, teams need information on availability, performance, security, and service quality of the network, applications and overall infrastructure, including secure access service edge (SASE) services, email, security analytics, virtual private networks (VPNs), and web application firewalls.

FortiMonitor analyzes both network health metrics and application performance to identify potential problem areas that can affect user access, and provides network visibility and agile remediation for hybrid environments, including edge and cloud networks, to achieve greater security and business efficiency.

Monitor the Network

FortiMonitor is a holistic, scalable, Software-as-a-Service (SaaS)-based digital experience and network performance monitoring solution. It consolidates monitoring, network incident management, automation, and network configuration management into a single source of truth, providing visibility into every service, network device, and application in any deployment, whether containers, cloud, on-premises, or hybrid.

Digital experience monitoring

FortiMonitor provides end-to-end application visibility for digital experience monitoring.

- Simple Network Management Protocol (SNMP) is used to monitor infrastructure devices from the FortiMonitor collector.
- Agent software monitors operating system (OS), application, and container metrics.
- Public probes and collectors perform HTTP(S) and browser synthetic monitoring.
- Application programming interfaces (APIs) are used to monitor additional services such as VMware ESX and a range of cloud services.

The metrics gathered by agents, collectors, and probes are displayed on the device's instance page, which also shows device details, associated incidents, monitoring configuration, and availability and performance metrics.

Single source of truth

After a performance issue is detected, it must be fixed. FortiMonitor extends traditional performance monitoring features with incident response tools. It provides a single platform that can detect and respond to performance incidents quickly and efficiently. In addition to performance monitoring, FortiMonitor also provides flexible alerting, extensive incident management features, and automated response tools.

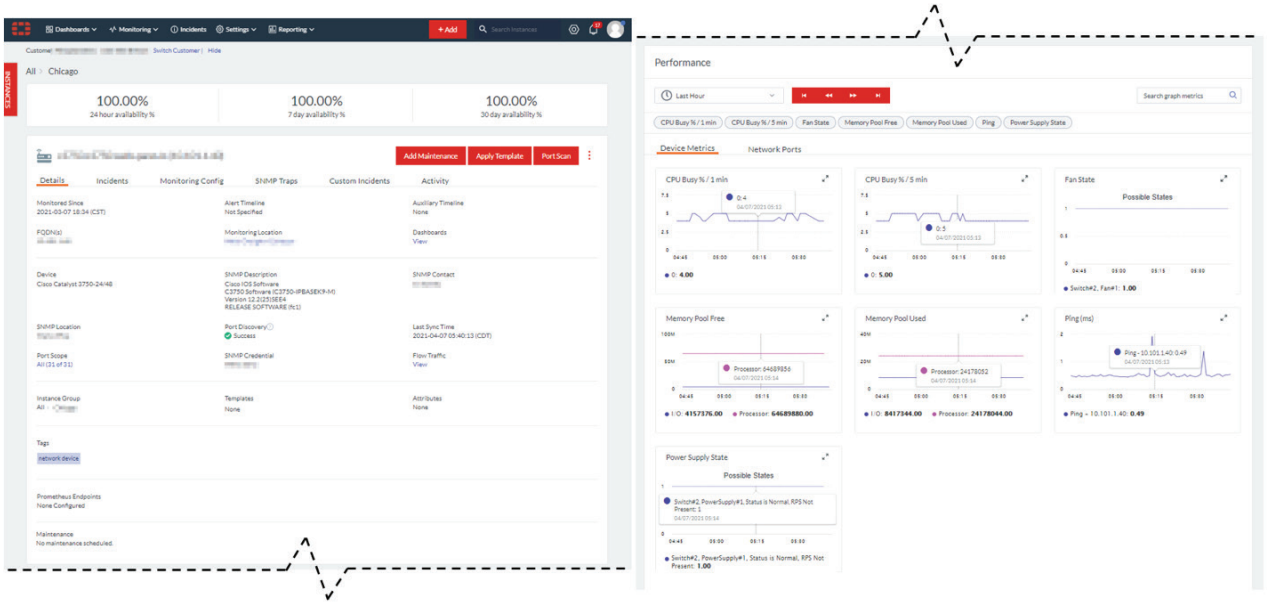
With a single view of all incidents, teams can quickly assess top-level incident status, acknowledge an incident, and assign an incident lead. Selecting an incident displays the incident detail view, which shows:

- The incident title, status, lead, start time, and end time
- The cause of the incident (for example central processing unit [CPU] usage threshold breach)
- Performance metrics that provide additional contextual information from within the incident view
- The incident timeline and messages

The system posts action messages in the timeline and teams can enter messages and updates as an action log or for collaboration with other team members.

Automate remediation

The agent countermeasures in FortiMonitor provide configurable automated actions to help quickly gather additional information or perform remediation actions in response to an incident. Countermeasures are automatically triggered by FortiMonitor in response to an incident and run on the agent that was the incident source.



Scalable and Easy To Use

FortiMonitor is easy to use and easy to manage. It uses the Fortinet Security Fabric to provide complete network visibility and replaces existing siloed performance monitoring systems with integrated incident response and automation features.

For supported device types, FortiMonitor also offers guidance through the device onboarding process. Policy workflow sequences can be configured to automatically apply templates and settings to discovered devices, which help simplify the onboarding process in larger environments.

The flexible, widget-based monitoring dashboards in FortiMonitor provide information on connected systems. It includes a set of preconfigured, customizable system dashboards that are enabled as the associated device types are configured. You can choose from a range of graphs, charts, metrics, and tables to customize a system dashboard, or build your own custom dashboards from scratch.

Because FortiMonitor is a SaaS platform, it can seamlessly scale as you grow. Onboarding is a smooth and easy process with no physical equipment, so teams can start monitoring the network quickly.

Quickly Fix Issues

The combination of SaaS architecture and tool consolidation in FortiMonitor provide greater availability, reduced complexity, and greater response efficiency. With FortiMonitor, teams can quickly identify, manage, and fix customer experience performance issues before they affect the business.

Enterprise IT teams are increasingly reliant on platforms that prioritize both customers' and employees' experience. If services fail or become degraded, FortiMonitor can automatically provide detailed, actionable diagnostics about those incidents to operations teams. By contextualizing alerts and using automated remediation through FortiMonitor, professionals can significantly reduce mean time to detection and mean time to repair. And if issues do arise, Automated Runbooks can be deployed to resolve issues without a team member having to step in, as well as run important diagnostics as soon as an event is detected.

[1] Josh Chessman, et al., "NetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext," Gartner, October 9, 2019.

June 3, 2021 7:26 AM

1034819-0-0-EN