SOLUTION BRIEF

FortiMonitor Healthcare Digital Experience Monitoring Solution

Executive Summary

Most healthcare IT environments are increasingly complex and distributed. Organizations need a high-performance, secure network to deliver excellent employee experiences and patient care. Availability, performance, security, and quality of applications and their components are all factors that must be managed effectively to reach these experience and patient care goals.

FortiMonitor delivers cloud-based full stack visibility of the security and network health combined with automated remediation. It ensures an application in any deployment, whether containers, cloud, on-premises, or hybrid, is meeting user expectations. By analyzing network and security health, potential problem areas can be identified and remediated before they affect the healthcare organization.

> *"IT operations teams are constantly looking for ways to simplify the way they collect, analyze and respond to increasing amounts of data. Fortinet's new offerings enable these overburdened teams to have better visibility and insights into highly distributed data to make better decisions on what actions need to be automated. Ultimately, this drives operational efficiencies by eliminating manual operations and optimizes users' digital experiences."*[1]
>
> – Bob Laliberte, Sr. Analyst and Practice Director, ESG

The Drivers of Change in Healthcare

Today, healthcare organizations are accelerating their digital transformation initiatives with virtual visit platforms, hybrid cloud, and connected medical devices. These initiatives are driven by the clinical user experience. Because the user experience can determine the success or failure of applications, 100% uptime is critical. Substandard application performance and lack of application availability can result in increased clinical errors and potentially missed patient encounters.

Network and infrastructure teams need to have comprehensive visibility into networks and applications because they are tasked with ensuring the quality of user experience. As healthcare IT infrastructures become increasingly complex and diverse, network operations center (NOC) teams inevitably use a multitude of solutions to gain deep insights into the health of their network and quality of application services. However, disjointed tools for local-area networking (LAN), wide-area networking (WAN), cloud performance, and security monitoring can impede holistic end-to-end user to application visibility and add operational complexity.

Standard monitoring tools focus on individual elements and metrics such as server CPU utilization, disk performance, interface statistics, and network traffic flows. While these metrics are important, they don't give a comprehensive picture of application and network health. This traditional monitoring strategy leads to the development of fragmented and high-maintenance multivendor environments with solutions that often do not coordinate or integrate well. The ongoing proliferation of monitoring and diagnostic tools introduces operational friction, context switching, and the manual implementation of monotonous repetitive tasks. Predictably, this inefficiency overwhelms teams and limits their ability to work efficiently.

Multilayered, distributed, and complex networks make it difficult to perform root cause analysis (RCA) to resolve user experience issues. Because they have to perform manual operations and processes to implement network changes, operators take longer to remediate user experience issues.

Full Stack Visibility and Automated Remediation

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 synthetic transaction-based monitoring.
- Application programming interfaces (APIs) are used to monitor a range of cloud services and additional legacy on-premises 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.

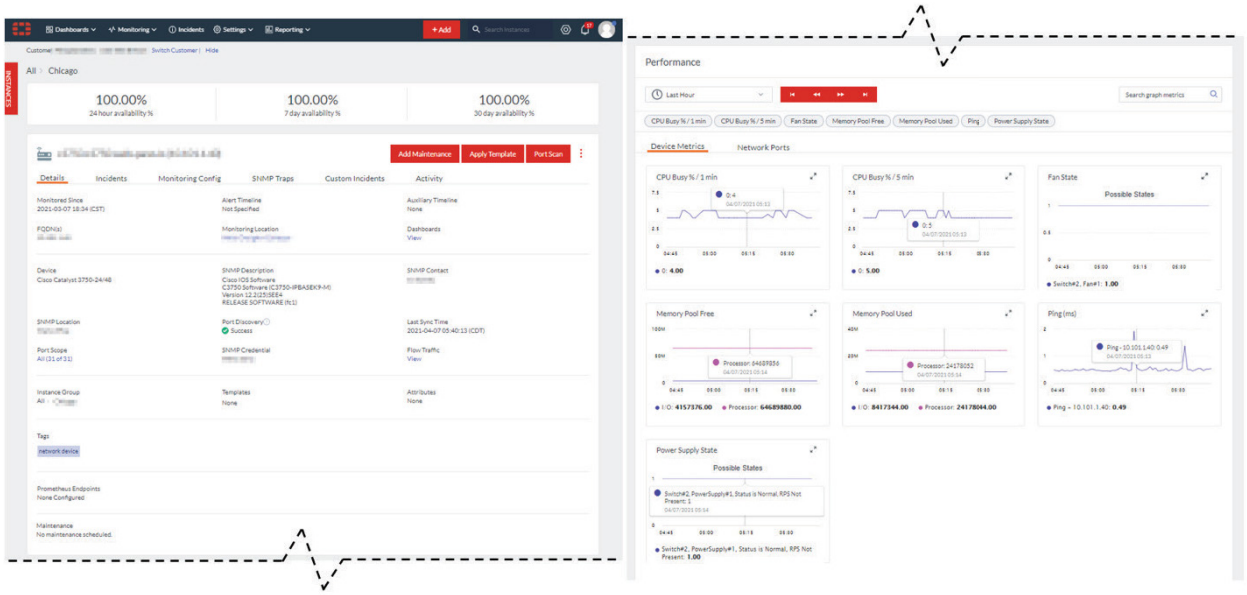
With a single view of all incidents, teams can quickly assess top-level incident status, acknowledge an incident, and assign an incident lead. Selecting an incident displays the incident detail view, which shows:

- The incident title, status, lead, start time, and end time
- The cause of the incident, for example, a central processing unit 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.

Automated 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. FortiMonitor can be configured to automatically solve issues that normally might require intervention by operations staff.



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 Identify, Manage, and Fix Issues

FortiMonitor is also quick and simple to deploy because it is a SaaS platform and replaces a variety of tools that provide only a fraction of information FortiMonitor provides. Operations teams have a consolidated view of what's going on with the network and applications, which helps ensure that the applications clinicians rely on every day are available and running at top performance levels.

Contact your Fortinet healthcare security expert to learn more: healthcare@fortinet.com.

[1] "Fortinet Simplifies Network Operations by Enhancing Security Fabric with Digital Experience Monitoring," NASDAQ, June 8, 2021.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 29, 2021 8:57 PM
1329255-0-0-EN