

# Leverage AI for Continuous Detection and Optimization Across IT Operations With FortiAIOps

## Executive Summary

Rapid digital transformation (DX) has greatly increased network complexity, making management more challenging for IT teams. As a result, more visibility and better analysis when things go wrong are needed. At the same time, organizations are more focused on application use and user experience. Software-as-a-Service (SaaS) applications and Internet-of-Things (IoT) devices are now being heavily relied upon, and must remain available and at peak performance at all times. Network operations center (NOC) teams rely on the insights produced by various technologies in order to track availability, performance, trends, and more. However, all these tools generate extensive amounts of data for NOC teams to sift through.

FortiAIOps, artificial intelligence for IT operations (AIOps), empowers organizations to leverage AI and machine learning (ML) to systematically consume the extensive amount of data being produced by the network. This enables IT teams to become proactive, instead of focusing on extensive post-incident debugging tasks. The Fortinet AI-powered approach makes it possible for teams to predict potential issues before they impact users, receive recommended actions, and automate tasks—at machine speed.

## Fragmented Network Operations Overburdens IT Teams

NOC teams struggle to address the size, volume, and disparity of tools utilized for operations. The attempt to monitor and execute tasks for various operational aspects makes it increasingly difficult to consolidate the products they use. This results in fragmented operational efforts, such as repetitive manual workflows, decentralized operations, and lack of streamlined team collaboration. As these teams confront each operational aspect, they must complete a number of manual configurations layered with extensive workflows, that lead to an ever-increasing workload. These are all key factors that further limit overall visibility within the network. In addition, the likelihood of human error, misconfigurations, and network downtime increases.

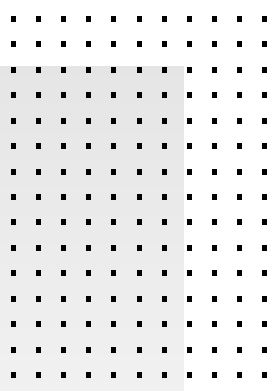
## Reduce Mean Time To Identify With Machine Learning

FortiAIOps enables teams to ingest high data volume and automate IT operations processes, thanks to machine learning. Teams are able to correlate events, detect anomalies, and optimize overall operations. As a result, organizations can reduce their mean time to identify (MTTI). This is achieved with:

### Triaging

IT practitioners face the impossible challenge of ingesting unmanageably high volumes of data from throughout their IT infrastructure. This includes extensive numbers of screens calling for their attention, producing operator fatigue.

FortiAIOps provides a remedy to the overwhelming nature of alerts by filtering and correlating actionable information automatically. As a result, data that reflects similarity are grouped together, allowing teams to not only address high-value issues but also reduce operational problems created by human error. This accelerates understanding of the information populated throughout the environment and remediation process. In addition, teams are able to identify issues in real time and prioritize key activities, optimizing operations.



**80% of network operation tickets could be positively impacted through the implementation of AI/ML to incidents.**

– Fortinet internal research

## Root cause analysis

With modern architectures producing vast data, even the most experienced team member will have trouble identifying what is causing an issue when LAN and WAN are both in play. This is why network operations teams require a multitude of segmented expert staff members and technology solutions, which makes it increasingly difficult to achieve nimble operations. During a root cause analysis (RCA), IT practitioners are required to context-switch across multiple tools, in an effort to identify pertinent information. This causes key insights to be missed. The consequence is the tendency to wrongfully classify issues that produce user complaints that may then snowball into more problematic outcomes or widespread outages.

FortiAIOps leverages ML to support teams in quickly capturing insights that zero-in on the causes within infrastructure and devices that produce the vast majority of outages and incidents. This enables teams to find the exact root cause of an incident immediately. Furthermore, AI leverages the process as a learning opportunity, to help predict potential future incidents, and stores the historical data. With FortiAIOps, organizations can stop an issue in its tracks and build a proactive posture, enhancing the elasticity of the team.

## End-to-end visibility with AI and ML

It is vital for IT teams to have comprehensive visibility into the digital branch and to understand key operational issues that relate to connectivity and productivity. Similar to practitioners struggling with the process of analyzing the root cause of an incident, there is an abundance of technologies utilized to track and manage each aspect of operations. These continuously monitor and analyze what might impact the business. In turn, there is no singular console to manage from, which clouds visibility as practitioners traditionally use multiple interfaces. Organizations that leverage a patchwork approach require further specialized expertise in each product area. The combination of various tools and talent organizations to invest in, greatly increases costs, while adding to further complexity.

To maximize efficiency, reduce overhead, and improve operations, Fortinet offers broad coverage across device, local-area network (LAN), and wide-area network (WAN). Comprehensive coverage helps organizations understand the anomalies in user-to-application access with simplified monitoring using a single console. This includes deployments such as wireless, switch, network firewall, extender, and software-defined WAN (SD-WAN). As a result, FortiAIOps provides organizations with full performance visibility into their network, along with AI and ML. The combination greatly reduces the need to hire extensive specialized staff. Furthermore, FortiAIOps can gather all the data from networking equipment collected by FortiGate, and create a NetOps rating. It does this by analyzing data across 23,000 different network log types. This enables early identification of anomalies and a simple-to-digest approach.

## Accelerate Network Maturity With a Complete NOC

The modern-day NOC commonly has complex layers of technologies used to retain a strong network posture. However, as an environment becomes more comprehensive, it also becomes more challenging to manage. Identifying what solutions are needed for various points in an organization's infrastructure evolution determines the success of the IT operator.

Fortinet provides easy-to-use NOC tools to best support teams in identifying the right technologies at the right time. With this model, IT teams can identify what capabilities in the Fortinet Security Fabric they require based upon their existing investment in people and processes.

Fortinet offers a range of components to improve efficiency at each stage of an organization's deployment of a Fortinet Secure Connectivity solution. Fortinet solutions such as FortiManager, FortiAIOps, and FortiMonitor fit into the framework to provide the solutions required to solve the challenges faced at every stage of deployment. This ultimately supports the acceleration of an organization's network maturity, while assuring reduced MTTI and mean time to respond (MTTR).

**FortiMonitor.** In early phases of a deployment, there may be a prolonged period of additional vendor equipment making up part of the IT-owned network footprint. FortiMonitor allows for visibility and analysis of all equipment with a focus on Digital Experience Management (DEM).

**FortiManager.** As the Fortinet network footprint grows, the need for central management and configuration with zero-touch deployment capabilities also grows. FortiManager offers direct control and provisioning of the full Fortinet Connectivity solution, from security, to SD-WAN, to switching and Wi-Fi.



**FortiAIOps.** As a full Fortinet Network Connectivity solution that leverages Fortinet for WLAN, LAN, SD-WAN, and 5G/LTE Gateway becomes the predominant equipment, a need for simplified management and troubleshooting arises. FortiAIOps integrates with other Fortinet NOC products to provide triaging of events, speedy root cause analysis, and enhanced visibility across a wide and complex network to save IT time and energy.

## FortiAIOps Solves NOC Complexity

IT operations teams cannot counter the overwhelming, dynamic workload without machine support:

- The data ingested has become too vast.
- The tools leveraged for support lack integration and cohesive coordination.
- The processes to address incidents are too lengthy.

In order to shift away from a reactive approach, the modern NOC needs a force multiplier that delivers comprehensive visibility and cohesion throughout every area of the IT infrastructure. FortiAIOps provides this much-needed support, enabling teams to stop problematic occurrences before they ever happen, respond swiftly when they do, and see what's happening throughout their environment.

Network operations leaders can use the Fortinet Network Connectivity Solution maturity model to find their current level of maturity and the steps that they must take to reach the next level, maximizing visibility, efficiency, and investment.



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2022 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.