SOLUTION BRIEF

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

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

– Fortinet internal research

Rapid digital transformation (DX) has greatly expanded the attack surface. This results in an increased need for more security controls to stop the sophisticated attacks targeting more and more vectors. At the same time, organizations are more focused on application use and user experience. Multi-cloud networks, Software-as-a-Service (SaaS) applications, telework, and Internet of Things (IoT) are now being relied upon, and must remain available and secure at all times.

Network operations center (NOC) teams rely on the insights produced by various technologies in order to track availability, performance, security, 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 siloed tools. At the same time, repetitive tasks are automated. This enables IT teams to become proactive, instead of focusing on extensive debugging tasks. The Fortinet AI-powered approach makes it possible for teams to predict potential issues before they happen, receive recommended actions, and automate tasks such as fixes—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 vulnerabilities—leading to a successful breach—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:

Alerting

IT practitioners face the impossible challenge of ingesting unmanageably high volumes of data from throughout their IT infrastructure. This includes extensive numbers of alerts, producing operator fatigue. FortiAIOps provides a remedy to the overwhelming nature of alerts by filtering and correlating actionable information automatically. As a result, alerts that reflect similarity are grouped together, allowing teams to not only address high-value alerts but also reduce vulnerabilities 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.

Root cause analysis

With modern architectures producing vast data, even the most experienced team member will have trouble identifying configuration outliers. 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 an outage or minor environmental issue that may then snowball into more problematic outcomes.

FortiAIOps leverages ML to support teams in quickly capturing insights that zero in on fluctuations with infrastructures and applications 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. It also stores the historical data. This allows organizations to 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 such as connectivity. 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 do not have a patchwork approach require further specialized expertise. The combination of various tools and talent organizations 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), wide-area network (WAN), and cloud. 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, software-defined WAN (SD-WAN), and secure access service edge (SASE). 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. A natural language interface expands performance insights into an organization's environment. Furthermore, FortiAIOps can gather all the data from wireless collected by FortiGate, and create a NetOps rating. It does this by analyzing multiple FortiGates across 23,000 different network log types. This enables early identification of anomalies and a simple-to-digest approach.

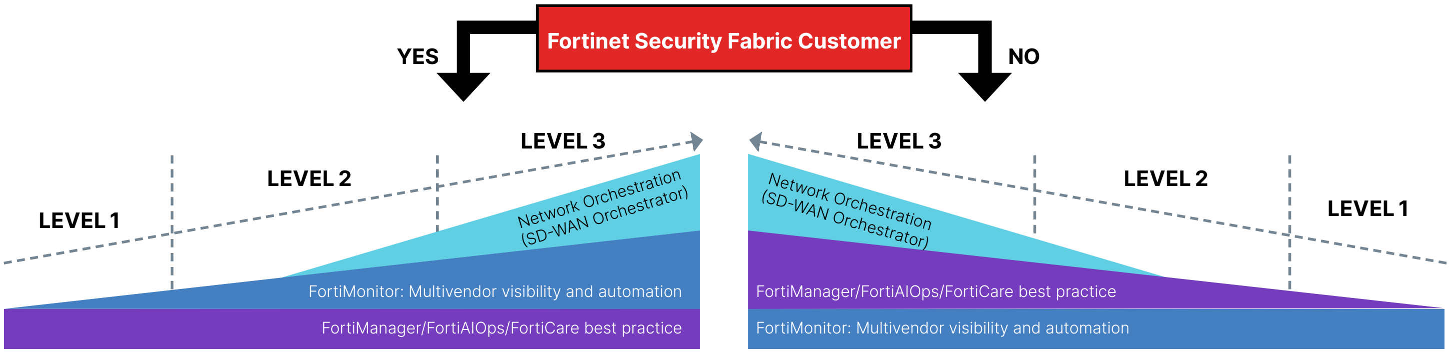
Accelerate Network Maturity With the NOC Maturity Model

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 an easy-to-use NOC maturity model 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 maturity. Because of varied staffing levels and organizational structures, NOCs at each of these levels have different requirements. 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 maturity. This ultimately supports the acceleration of an organization's network maturity, while assuring reduced MTTI and mean time to respond (MTTR).

NOC Maturity Model


Fortinet Security Fabric Customer
YES
NO
LEVEL 1
LEVEL 2
LEVEL 3
Network Orchestration (SD-WAN Orchestrator)
FortiMonitor: Multivendor visibility and automation
FortiManager/FortiAIOps/FortiCare best practice
LEVEL 3
LEVEL 2
LEVEL 1
Network Orchestration (SD-WAN Orchestrator)
FortiManager/FortiAIOps/FortiCare best practice
FortiMonitor: Multivendor visibility and automation

The typical roles and responsibilities of the NOC include:

- **Level 1:** Most commonly, network engineers at this level should be responding to monitoring-tool detected anomalies and declared incidents requiring resolution. They also need tools to respond to other monitoring events that require other actions (such as threshold-crossing alerts).
  - Tools: FortiManager, FortiAnalyzer, FortiMonitor, Best Practice Service
- **Level 2:** Typically, these engineers are more highly skilled than those at Level 1. They respond to and resolve networking incidents that are unable to be resolved at Level 1 and are escalated. They use additional tools, knowledge, and insights to improve incident diagnosis and recovery.
  - Tools: FortiMonitor, FortiAIOps
- **Level 3:** These typically make up the smallest team focused on the most complex incidents and problems. This level is also commonly the interface step to an application support engineering team.
  - Tools: FortiMonitor, FortiAIOps
- **NOC manager:** This role is responsible for continuous operations of the NOC as well as human resources and workforce management.
  - Tools: FortiMonitor (NOC Dashboard)

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 NOC 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.

FORTINET®

www.fortinet.com

June 3, 2021 8:29 AM
1070901-0-0-EN