SOLUTION BRIEF

# Fortinet and FlowMon Security Solution

## Executive Summary

The spread of the zero-trust mindset testifies to how common unknown and insider threats have become. What is more, some assets find themselves outside the protected boundary due to the trend of cloud migration. Modern cybersecurity calls for a combined security model—an airtight perimeter and an intelligent system for rooting out network-borne threats, focusing on the following key aspects:

- Multilayered security
- Early threat detection
- Automated incident response

The Fortinet and Flowmon solution provides an automated, multilayered protection system against unknown and insider threats.

## The Solution

Fortinet FortiGate next-generation firewalls (NGFWs) enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks. They draw on continuous threat-intelligence updates to protect against a wide variety of known and unknown threats and can easily integrate with third-party security solutions and co-create a shared threat-intelligence pool.

Flowmon combines Network Performance Monitoring and Diagnostics (NPMD) and Network Traffic Analysis (NTA) in one solution dedicated to ensuring stable and secure digital environments. Its artificial intelligence (AI)-powered engine analyzes network telemetry in real time, detecting anomalies hidden in the traffic. Using a combination of analytical methods, it is able to automatically identify multitudes of threats, ranging from data breaches to compromised hosts through to ransomware attempting to establish persistence.

FortiGate and Flowmon work together to create an impervious, multilayered cybersecurity system. FortiGate watches the perimeter and protects against external threats, while Flowmon analyzes traffic in the network to detect unknown and insider threats that originate from within.

When Flowmon detects a sign of a threat (e.g., reconnaissance or lateral movement of an attacker), it sends a message to FortiGate, which in turn blocks the communication on the perimeter.

## Joint Solution Components

- Fortinet FortiGate Next-generation Firewalls (NGFWs)
- Flowmon Platform

## Joint Solution Benefits

- Automated and multilayered protection solution
- Identify a wide variety of threats via Flowmon traffic and performance analysis automatically, including unknown and insider threats
- Leverage the award- winning FortiGate firewall for security policy enforcement and unparalleled security protection

FORTINET FABRIC-READY

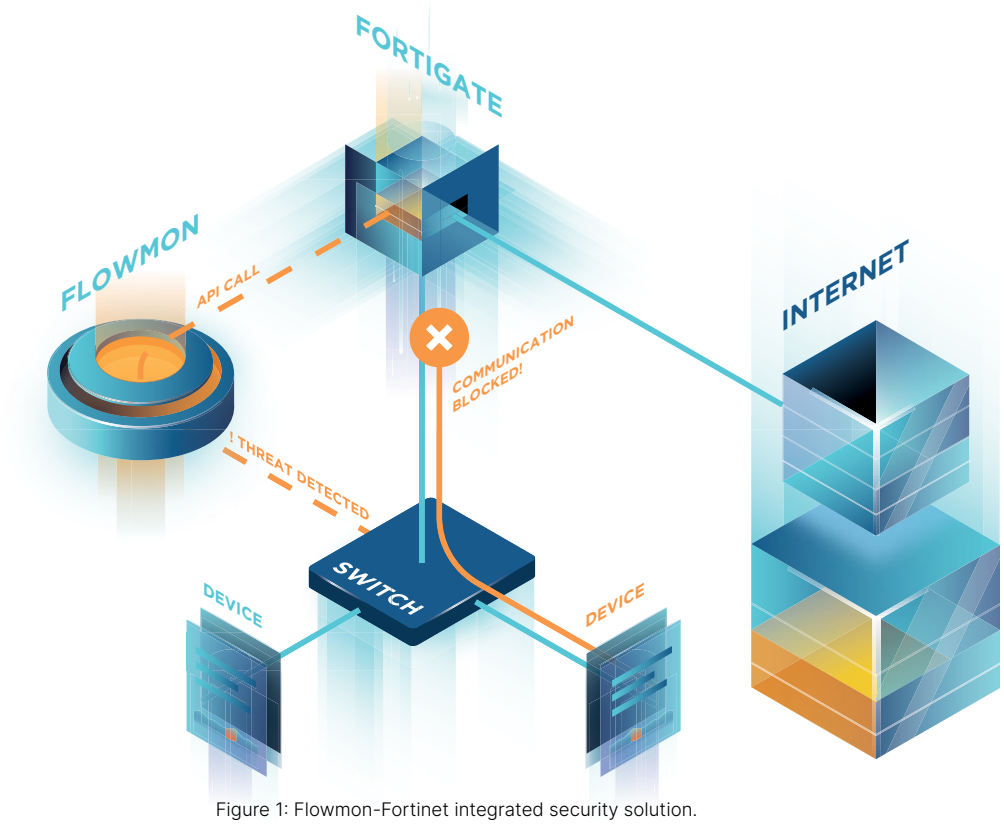


Figure 1: Flowmon-Fortinet integrated security solution.

## More Than a Sum of Its Parts

The integrated solution creates an automated system of threat detection and response, which, thanks to the simultaneous deployment of several detection techniques at once, covers a far wider spectrum of threats and makes life much easier for security administrators. Threats remain blocked for weeks, leaving plenty of time for investigation and remediation.

The symbiotic combination of Fortinet and Flowmon is the ideal protection in a world of increasingly fluid and elusive threats. It combines high performance with unmatched scalability and will seamlessly integrate into any security matrix.

## About Flowmon

Flowmon develops an actionable network intelligence solution that enables businesses to ensure their services are running well and securely, and their workforce is productive. Learn more at https://www.flowmon.com/en.





September 30, 2021 1:58 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 4:sb-FA-fortinet-and-flowmon-092021:sb-FA-fortinet-and-flowmon-092021

628618-0-0-EN