

**SOLUTION BRIEF**

# Fortinet and Lumu Security Solution

## Comprehensive network detection and response for a proficient cybersecurity operation

### Executive Summary

Continuous Compromise Assessment by Fortinet and Lumu enables organizations to detect and respond to pervasive threats across the network.

### Challenge

Despite billions of dollars invested in cybersecurity, companies continue to be compromised. Current practices focus on defenses and periodic tests, neglecting that the adversary may already be inside the network. Early prevention is most critical. Lumu leverages multiple sources of metadata to get a comprehensive view of an organization's network activity. FortiGate NGFW provides Lumu with real-time detection and response to threats found across the network.

### Joint Solution

Lumu and Fortinet have partnered to deliver an industry-leading security solution to address the pervasive threats inside networks. The integration between Lumu and Fortinet enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers automated attack detection and response across the network.

### Solution Components

Lumu's Continuous Compromise Assessment provides continuous, real-time monitoring to detect malicious activity across the entire network. When an attack is discovered, it's reported to the customer with detailed context to show when an attack took place, who was impacted, and which IoC is associated with the incident.

**FortiGate NGFWs** deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into the hybrid IT architecture and build security-driven networks to achieve: Ultra-fast security, end to end consistent real-time defense with FortiGuard Services, excellent user experience with security processing units, operational efficiency and automated workflows

### Joint Solution Integration

Fortinet FortiGate NGFW and Lumu enable efficient cybersecurity operations through an integrated solution for network detection and response. Lumu continuously collects network metadata from various sources, including Fortinet. When malicious activity is discovered during the data collection process, Lumu triggers an alert to FortiGate NGFW for real-time attack response.

### Solution Components

- Lumu's Continuous Compromise Assessment
- Fortinet's FortiGate NGFW

### Solution Benefits

- Instant attack response, closing the attacker's window of opportunity.
- Enhanced attack detection through metadata collected by FortiGate NGFW
- Continuous network monitoring through Lumu



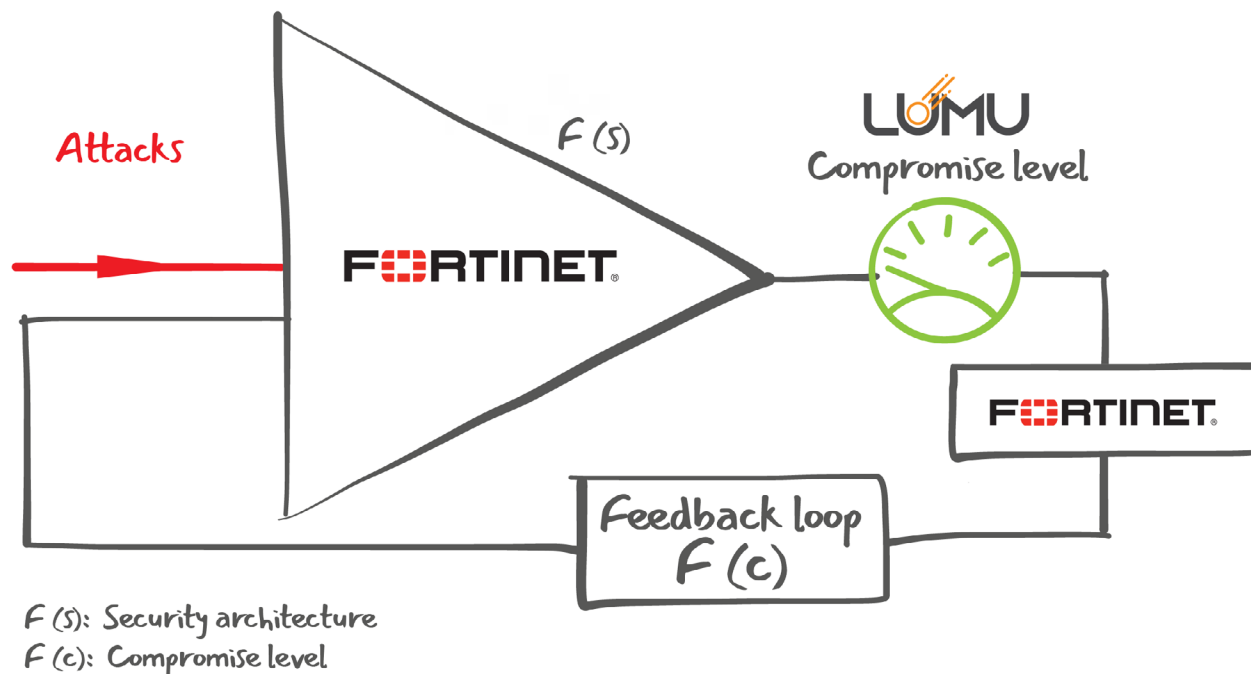


Figure 1: Lumu and Fortinet joint solution

The metadata collected from FortiGate NGFW is also fed into Lumu's Illumination process where data is analyzed for malicious association. If an attack is discovered, Lumu measures the compromise level, does a complete analysis of the IoC, and it runs through FortiGate NGFW to automatically block future connections with this IoC.

## Joint Use Cases

### Use case #1

Fortinet and Lumu offer automated network detection and response. Through one-click integrations, Lumu is able to leverage Fortinet's capabilities for swift action against active threats.

### Use case #2

Secure remote users by offering protection to the entire FortiGate NGFW & Lumu user base.

## About Lumu

Lumu was founded on the belief that organizations, regardless of the size or vertical, should be able to operate cybersecurity proficiently. Continuous Compromise Assessment makes this a reality by monitoring the network to detect malicious activity in real time and providing actionable intelligence.



[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.