SOLUTION BRIEF

Fortinet and LinkShadow Security Solution

Next-generation Behavioral Analytics With Proactive Defense

Executive Summary

LinkShadow empowers security teams with cutting-edge threat anticipation with Proactive Incident Response, in turn providing rapid insight into the effectiveness of the existing security investments. Organizations benefit from a highly automated, complex incident response, which allows for faster remediation and facilitates an adaptive defense against sophisticated and unknown attacks.

Challenge

New and unknown attacks occur every day and attackers could destroy your business overnight. Security teams need to be fortified against such attacks and empowered with full visibility to guarantee optimum protection against planted seeds by bad actors. With the sheer number of security tools in the security operations center (SOC) and the complexity of those tools, it takes the security analyst a considerable amount of time to investigate an anomaly and respond to it, which leads to an inefficient investigation and slow response. In the modern SOC, the security analyst should be able to investigate and respond to an anomaly rapidly and use the minimal number of dashboards and clicks possible to come up with an informed decision.

Joint Solution

LinkShadow and Fortinet have partnered to deliver an industry-leading security solution to address the challenges. The integration of LinkShadow Cybersecurity Analytics Platform and Fortinet FortiGate, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, provides unparalleled detection of the most sophisticated threats to enhance an organization's defense against advanced cyberattacks, zero-day malware, and ransomware.

Organizations get advanced protection against unknown attacks and malicious insiders. The Fortinet and LinkShadow joint solution enables hunting for internal and external cyberattacks using cutting-edge threat hunting that is empowered with threat-intelligence feeds from top security leaders in the market.

The LinkShadow Platform completes the full cycle of user and entity behavior analytics (UEBA), threat hunting, and threat detection and shares it with Fortinet FortiGate Next-Generation Firewalls (NGFWs) for optimal benefits from the Security Fabric platform.

Joint Solution Components

Fortinet FortiGate NGFW

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 deliver ultrafast security end to end, enable consistent real-time defense with artificial intelligence (AI)/machine learning (ML)-powered FortiGuard services, achieve seamless user experience with security processing units (SPUs), and improve operational efficiency and automate workflows.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall
- LinkShadow Cybersecurity Analytics Platform

Joint Solution Benefits

- Seamless integration to automate the incident response
- High-level insights into security investments
- Proactive prevention against behavioral anomalies
- Defense against unknown attacks in early stages

FORTINET FABRIC-READY

LinkShadow Cybersecurity Analytics Platform

The LinkShadow Cybersecurity Analytics Platform monitors full network traffic passively, providing high-end visibility and a birds-eye view on all activities, and empowers your defense system with UEBA and threat hunting use cases that help to detect and identify attacks not only at early stages but the second it becomes suspicious.

Joint Solution Integration

LinkShadow gets full visibility from the Core Switch and analyzes the behavior of the network traffic to detect anomalies and threats using the advance ML crafted by LinkShadow engineers. Leveraging the integration with Fortinet FortiGate NGFWs, the security analyst can send an action to the firewall directly from LinkShadow. The integration allows the security analyst to respond to threats rapidly and more efficiently.

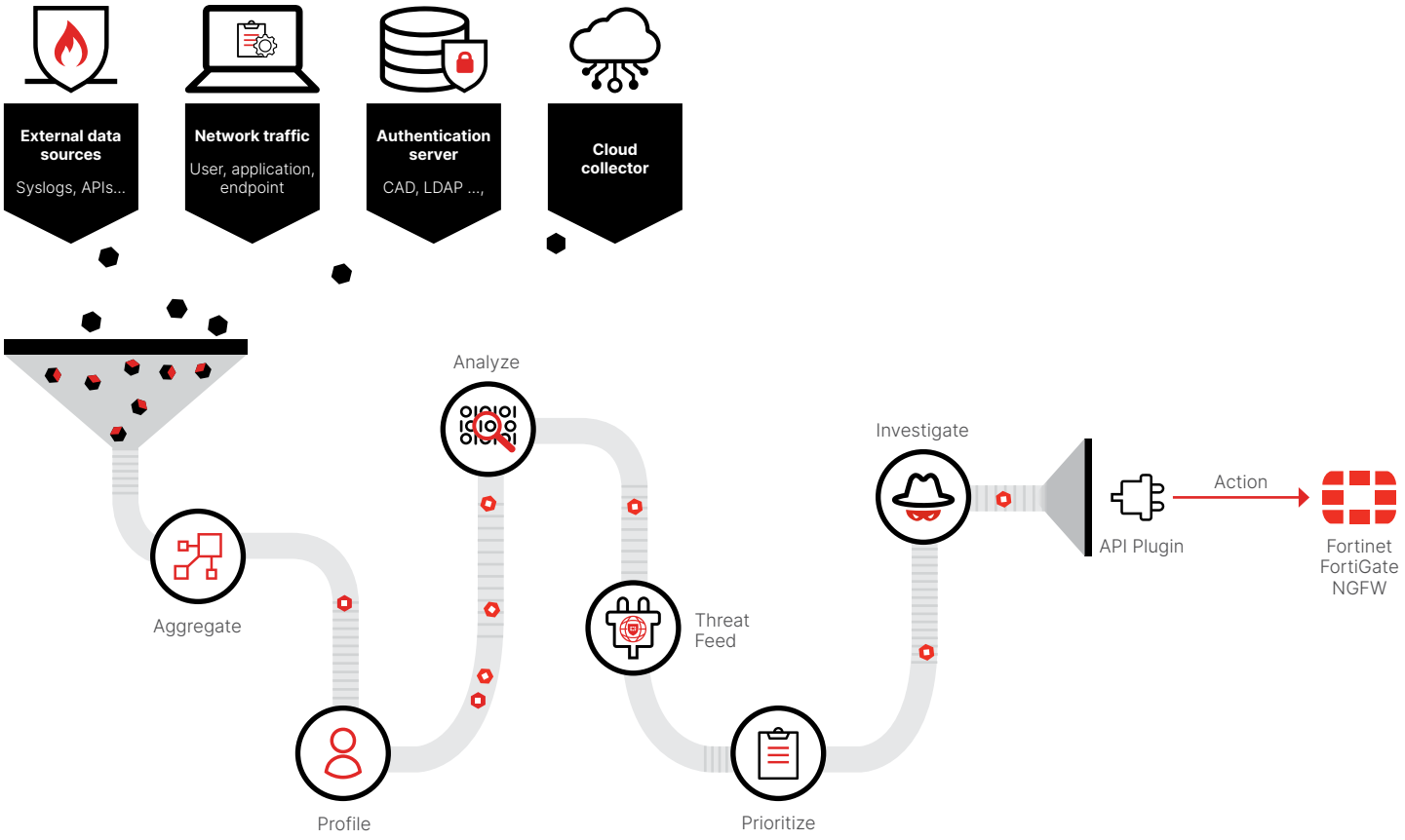


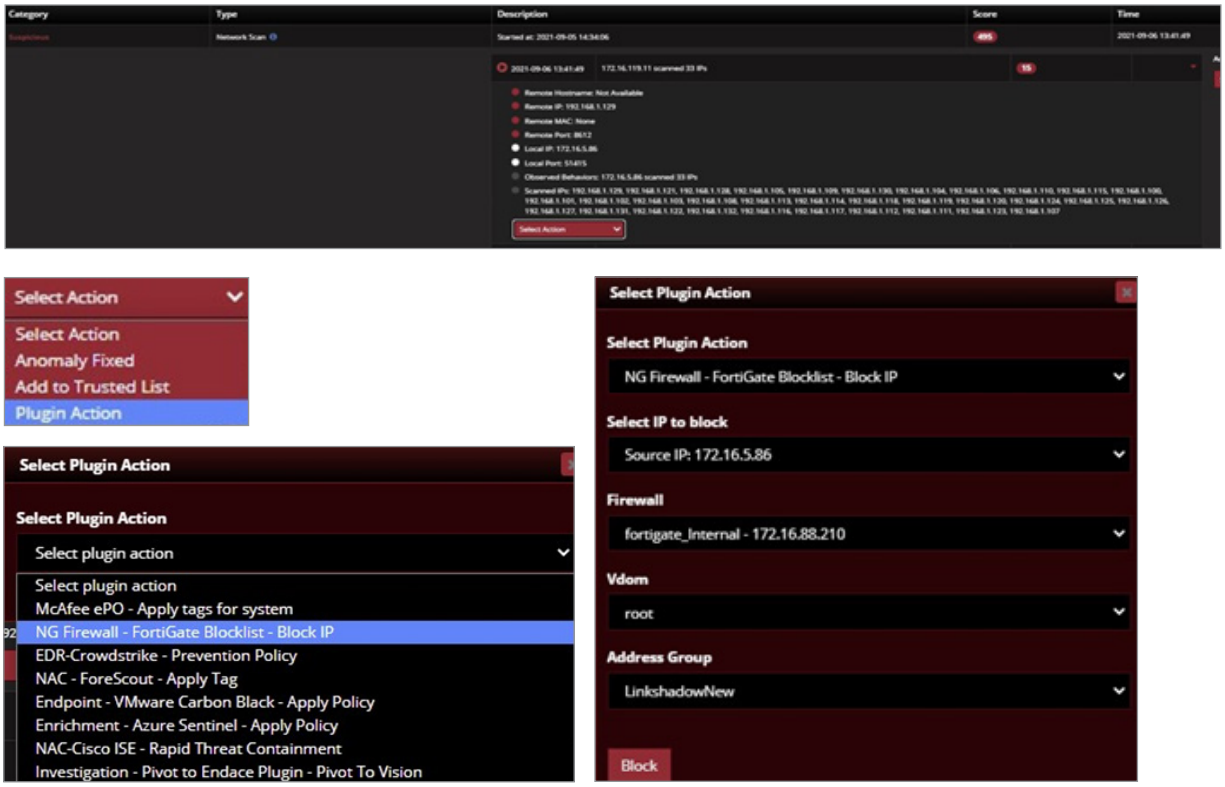
Figure 1: How the plugin works.

Once an anomaly is detected, the security analyst clicks on the device name to bring up the Entity Inspector page. The security analyst then scrolls down to the bottom to get to the anomalies section and expands the anomaly in question and clicks on "Select Action." Using the API plugin, the security analyst can choose the Fortinet FortiGate NGFW option and send an action to FortiGate.

Security analysts can then view the blocked IPs in the plugin store and unblock them when required.

Joint Use Cases

Early detection and response of compromised system – Instead of sleeping on an anomaly until it poses a real threat, LinkShadow monitors the connections to the external network for each profile individually. LinkShadow has full visibility up to the application layers, which allows it to monitor unusual or abnormal connections and data exfiltration. It communicates with FortiGate which then proactively stops the anomaly before it becomes a real threat.



About LinkShadow, Inc.

LinkShadow, the next-generation cybersecurity analytics was created by a team of highly skilled experts, solution architects, product specialists, and programmers to formulate a next-generation cybersecurity solution that provides unparalleled detection of even the most sophisticated threats. LinkShadow was built with the vision of enhancing organizations' defenses against advanced cyber-attacks, zero-day malware, and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.

October 20, 2021 3:52 AM
1316224-0-0-EN