SOLUTION BRIEF

Fortinet and TriagingX Security Solution

Automated Endpoint Forensic Investigation Solution

Executive Summary

The integration of TriagingX TXHunter with Fortinet FortiGate and FortiSIEM products enables customers to perform automated endpoint forensic investigation. This reduces investigation time, provides deeper insights into alerts and events, and enables detection of advanced attacks to prevent catastrophic security breaches.

Security and risk management leaders are struggling with two key challenges: Firstly, they often have too many alerts and events that they need to investigate, to ensure thatthey are not missing any early opportunities to detect new attacks to prevent catastrophic security breaches; Secondly, they often do not have enough resources and experts to perform the investigation process, due to the complexity involved in the forensic investigation process.

TriagingX and Fortinet recently established a technology partnership to address the above challenges by providing automation of endpoint forensics investigation by leveraging the Fortinet platform, while not requiring additional specialized personnel and expertise.

Joint Solution Description

Alerts from FortiSIEM and the Fortinet FortiGate firewall are automatically fed into TXHunter, and based on the criticality level or the user's configuration, forensic investigation is automatically launched on the alerted endpoint. The results of the investigation are fed back to FortiSIEM, and the user can view and act on the investigation results or set it to automatically remediate the issue.

The functionality of the joint solution is summarized in the illustration below.

Diagram of Joint Solution

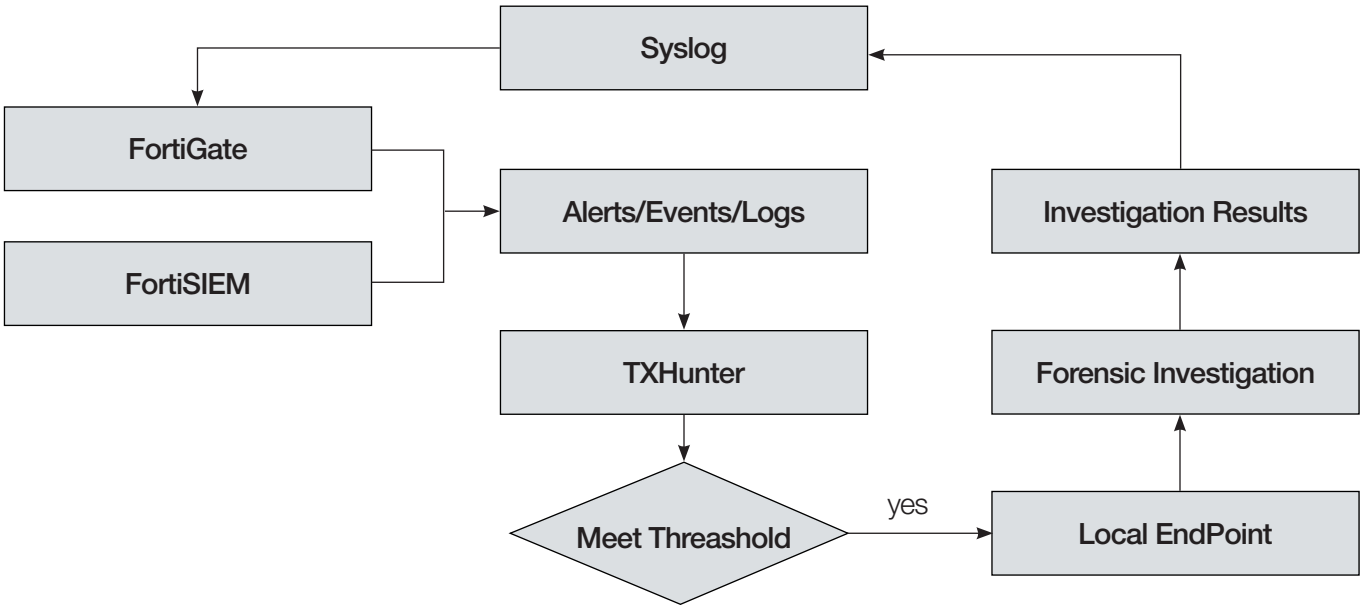

Figure 1: TriagingX-Fortinet solution.

Joint Solution Benefits

- Perform fully automated endpoint forensic investigation with the joint solution
- Investigate alerts and events directly from FortiSIEM by leveraging the integration
- Reduce investigation time from hours to minutes
- Obtain deeper insights on alerts and events
- Reduce or eliminate manual intervention with automated forensic investigation
- Enable detection of advanced attacks and potential risks at the earliest possible time, to prevent catastrophic security breaches

FORTINET Fabric-Ready

TriagingX's TXHunter is a fully automated endpoint forensic investigation solution. Its machine-assisted behavioral-based forensic analytic engine goes beyond static IOC queries to detect hidden and advanced threats. It detects reverse shell attacks, APTs, ransomware, malicious network connections, malicious emails, and cryptocurrency mining malware attacks. It is fast, consistent, efficient, and effective.

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.

As the number of endpoints, IoT, infrastructure, security tools, applications, VMs, and cloud components in a deployment grows constantly, security management can be a challenge. FortiSIEM—the Fortinet multivendor security information and event management solution—brings it all together, providing visibility, correlation, automated response, and remediation in a single, scalable solution. Using a business services view, the complexity of managing network and security operations is reduced, freeing resources and improving breach detection. FortiSIEM provides cross-correlation and applies machine learning and UEBA to improve response, and to stop breaches before they occur.

An Example Use Case

Managed security service providers (MSSPs) are continuously searching out technologies that will improve their service offerings. TriagingX enables MSSPs to greatly enhance their threat hunting and incident response capabilities, not only in efficiency and speed but more importantly in visibility of granular details of the actual attacks that clients are experiencing. Coupled with advanced visibility, correlation, and SIEM provided by FortiSIEM, customers can readily perform fully automated endpoint forensic investigation.

About TriagingX

TriagingX is headquartered in Silicon Valley. Our team successfully created the first-generation malware sandbox that is being used by many Fortune 500 companies for daily malware analysis. We are targeting one of security's fundamental challenges by targeting the asymmetric advantage enjoyed by attackers, where they often only need to compromise one weakness, while defenders scramble to prioritize and fix scores of vulnerabilities. We have moved beyond signatures or static IOCs and instead focus on the attack techniques and anomalies in order to significantly reduce the time to investigate suspect events in a simple to understand format and often in under 10 minutes. Our philosophy is to minimize the security computing load on the endpoint or server, keep core data inside the enterprise and leverage advanced analytics to reduce the time to detect and respond. Learn more at www.triagingx.com.

June 23, 2020 1:56 AM

707902-0-0-EN

sb-FA-triagingX-6182020