Sophos Security Heartbeat

Date: November 2015 **Author:** Tony Palmer, Sr. ESG Lab Analyst; and Jack Poller, ESG Lab Analyst

Abstract: *This report provides a first look at the key attributes of Sophos synchronized security with a focus on how synchronization between endpoint and network security using Sophos Security Heartbeat can enable a business to prevent, detect, and respond to threats throughout the organization's infrastructure automatically, and in real time.*

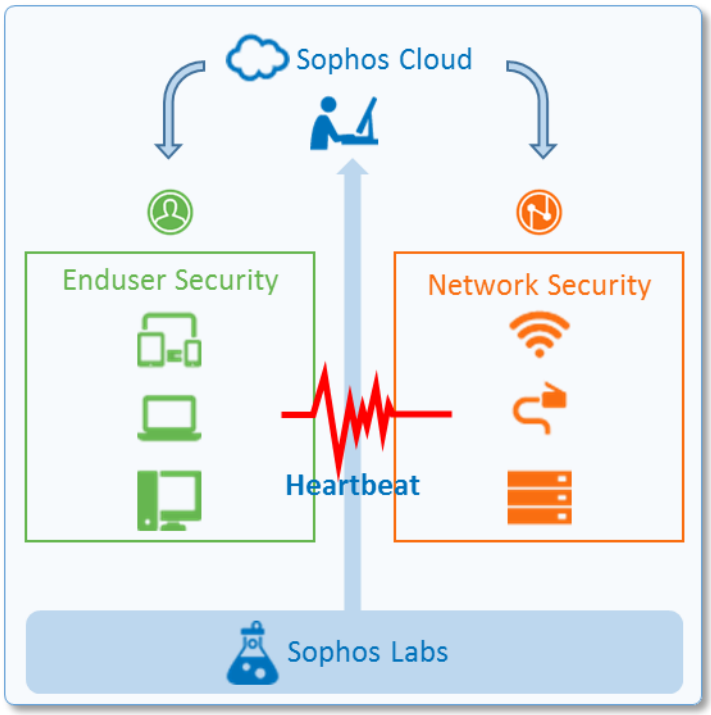
According to ESG Research:[1]

1/3 Of respondent organizations believe ***Information Security*** is one of the most important IT priorities within their organization in 2015.

28% Percentage of respondents who believe their organization has a ***problematic lack of information security skills.***

Sophos' Vision for Synchronized Security

Advanced malware attacks can cause tremendous damage to an organization, from data loss through compromised identities to operations shutdowns. The cyber-criminals perpetrating these attacks are sophisticated, continuously adapting the latest exploits, and creating new and insidious methods of infiltration and attack. These attacks are far more difficult to detect and prevent than they have ever been before, especially for point security products focused on just one aspect of the security ecosystem. Sophos designed synchronized security to help customers detect, prevent, and remediate advanced attacks across the IT infrastructure.



Early IT infrastructure security deployed point solutions, where antivirus protected Windows PCs, and firewalls and intrusion protection devices protected the network. Unified threat management (UTM) solutions are integrated versions of these point solutions, and their main advantages are simplicity, streamlined installation and use, and the ability to perform concurrent updates of all security functions. Security information and event management (SIEM) systems represent a different level of integration, combining the logs and threat alerts from a variety of point solutions into a single user interface for managing all threats and security incidents.

Sophos synchronized security is designed to be the next generation of IT infrastructure security, and employs a Security Heartbeat to synchronize endpoint and network security systems. Synchronization provides system-level intelligence, automated correlation, accelerated threat discovery, automated incident response, simple unified management, and faster decision making.

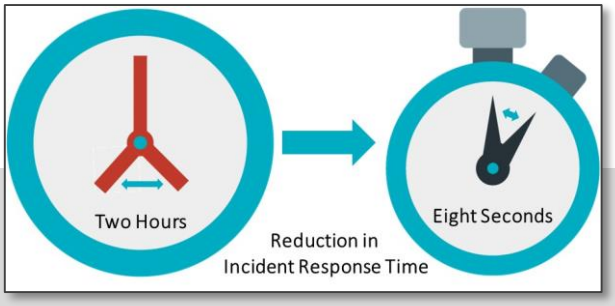
The Security Heartbeat provides real time communication between Sophos next-generation end-user protection (NGEP) and Sophos next-generation firewall (NGFW) solutions. Upon initialization, the NGEP and the NGFW register with Sophos Cloud, which sends certificate and security information to both. Every 15 seconds, the Security Heartbeat exchanges red/yellow/green health information between the endpoints and the firewall. When a compromise is detected, user, machine, and process information are shared so that the NGFW and NGEP are "in sync" and have complete knowledge of the threat and precisely who or what is impacted. This heartbeat enables active source identification and automated incident response. Administrators can also implement policies to enable or restrict access to critical resources based on endpoint health. This level of automation can provide cross domain information and context to free up security resources for more strategic and proactive activities, like deep analysis of incidents affecting groups of systems or users.

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

ESG Lab Demo Highlights

ESG Lab had the opportunity to get hands-on experience with Sophos synchronized security with a focus on how synchronization enables rapid detection, prevention, and remediation of threats.

- Sophos NGEP automatically detected and remediated locally introduced well-known threats in seconds. The endpoint changed its health status to red, and after the threat was removed, the health status reverted to green. The Security Heartbeat automatically notified the NGFW of the endpoint's change in health status, and during the time the endpoint was in the red state, the firewall applied policies to isolate the endpoint from the network.
- Sophos NGEP automatically detected the execution of potentially unwanted applications (PUA), alerted the user, and changed the health status to yellow nearly instantly. The Security Heartbeat automatically notified the NGFW of the endpoint's change in health status, and the firewall applied policies to isolate the endpoint from critical resources. When the security administrator approved or stopped the PUA, NGEP updated the health status, and the NGFW applied policies to re-enable endpoint access.
- When the NGFW identified unknown malware by network behavior, the NGFW not only blocked the network access, it was able to use information provided by the Security Heartbeat to identify the endpoint, the user, and the application. The NGFW notified the user of the issue within a second of detecting it and the endpoint changed its health state to red. The endpoint also attempted to stop and remove the malware. The entire process took about 8 seconds and required no administrator intervention.



First Impressions

Security breaches have become increasingly ubiquitous in modern IT environments. Bad actors are targeting smartphones and tablets, Windows desktops, and application servers. Organizations relying on independent, standalone security devices can potentially find themselves vulnerable to an attack that only needs to be missed by one device. The consequences of these attacks can be devastating financially, operationally, and to an organization's reputation. The costs may include resuming operations, closing security gaps, legal liability, and regulatory fines.

ESG Lab interviewed an Information Security manager at an organization with about 2,500 users, and confirmed the observation that manually uncovering the context of the type of events tested here takes on average two hours and involves multiple IT resources. When remote sites or BYOD devices are involved, this can stretch to days or longer.

Sophos is focused on synchronizing endpoint and network security systems to provide automated correlation, threat discovery, and incident response in seconds, simplifying management, and enabling faster decision making. ESG Lab was impressed with the tight integration of Sophos NGEP and NGFW using the Security Heartbeat. Sophos NGEP was able to detect and remediate threats while NGFW automatically applied policies to isolate endpoints until remediation was complete. Sophos was also able to alert endpoints of malware infections detected by network behavior, all in seconds, and all without administrator intervention.