ESG Lab Review

Sophos Security Heartbeat

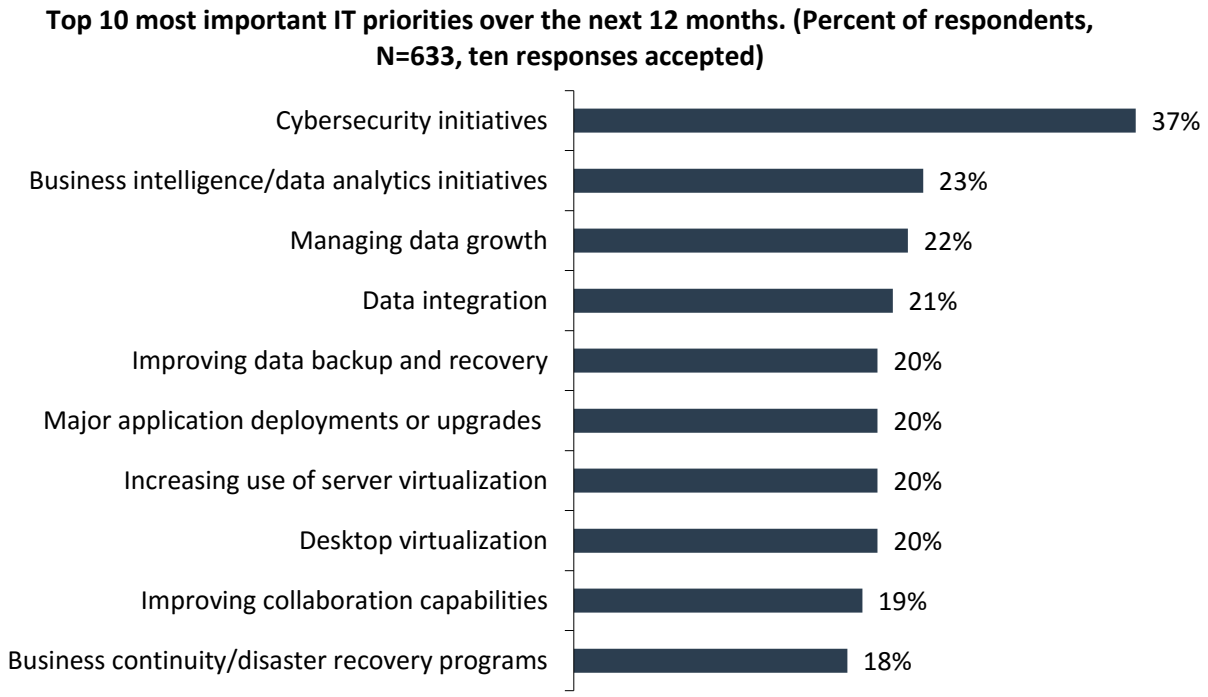
Date: January 2016 **Author:** Tony Palmer, Sr. ESG Lab Analyst; and Jack Poller, ESG Lab Analyst

Abstract: *This report examines 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 automatically prevent, detect, and respond to threats throughout the organization's infrastructure in real time.*

The Challenges

ESG asked 633 IT professionals and managers to identify their most important IT priorities, and more than one-third (37%) flagged cybersecurity initiatives, making it the most-often cited response by a wide margin, as shown in Figure 1. In addition, 46% of respondents indicated that they believe their organization has a problematic lack of information security skills, the number one response for the third year running.[1]

Figure 1. Top Ten Most Important IT Priorities over the Next 12 Months



Source: Enterprise Strategy Group, 2016.

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.

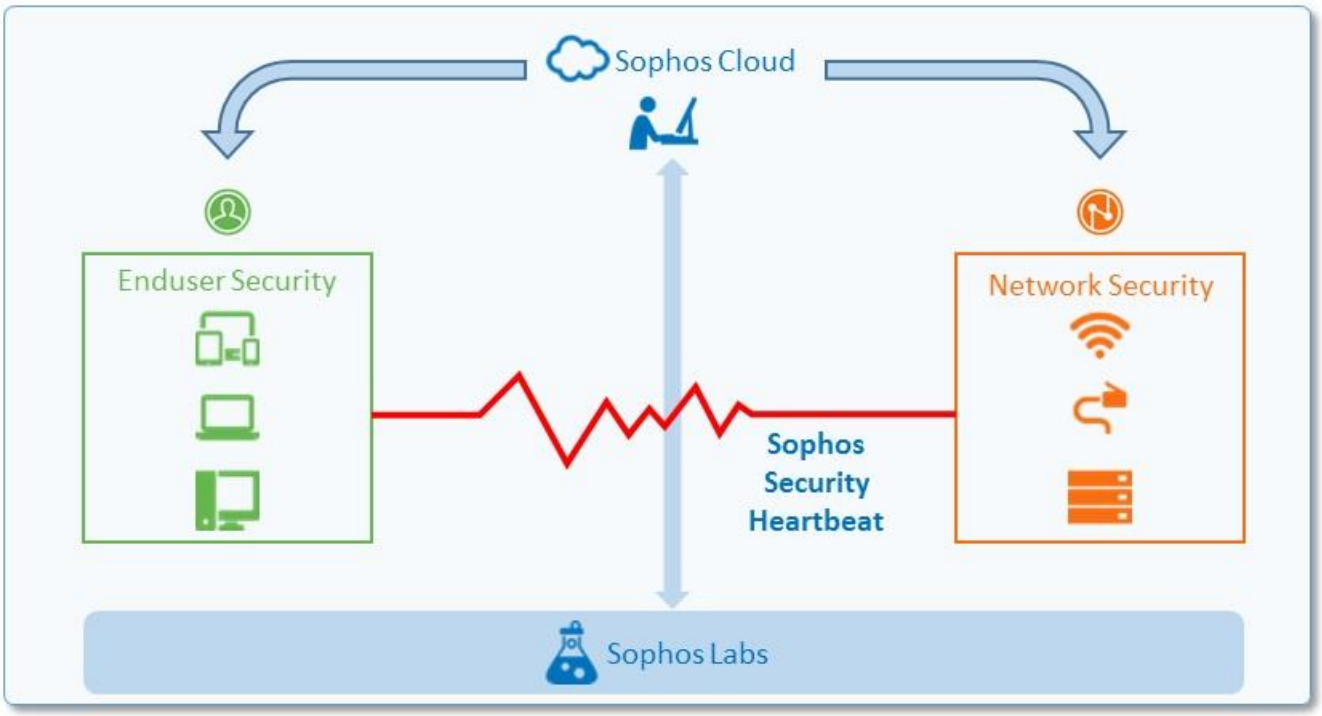
[1] Source: ESG Research Report, 2016 IT Spending Intentions Survey, January 2016.

IT infrastructure security is commonly deployed with point solutions, where antivirus directly protects laptops and desktops, and firewalls and intrusion protection devices protect endpoints and other hosts from attack via 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. However, none of the constituent components of traditional UTM or SIEM solutions communicate with each other. As a result, these solutions are resource intensive, requiring complex analysis of events in order to identify threats and attacks. Incident response in these solutions requires manual remediation.

The Solution: Sophos Synchronized Security

Sophos synchronized security is designed to help customers prevent, detect, and remediate advanced attacks across the IT infrastructure. As shown in Figure 2, Sophos synchronized security employs a Security Heartbeat which enables direct sharing of intelligence between Sophos next-generation end-user protection (NGEP) and Sophos next-generation firewall (NGFW) solutions. This synchronization provides automated correlation, accelerated threat discovery, automated incident response, simple unified management, and faster decision making.

Figure 2. Synchronized Security with Sophos Security Heartbeat



Sophos XG Firewall is a next generation firewall integrating advanced threat protection, intrusion protection, and risky user behavior detection technology with traditional firewall features. Sophos Endpoint Protection is a next generation endpoint protection solution providing advanced threat protection, web filtering, anti-virus, and policy enforcement. The Security Heartbeat provides real-time communication of threat, health, and security intelligence between the firewall and the endpoint protection.

Upon initialization, Sophos Endpoint Protection and the Sophos XG Firewall 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 firewall and the endpoint protection are “in sync” and have complete knowledge of the threat and precisely who or what is impacted.

Whereas traditional security solutions log events, create alerts, and require manual intervention, the synchronization of intelligence with the Security Heartbeat enables policy driven automation to handle threats and attacks. 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.

ESG Lab Tested

ESG Lab performed hands-on testing of Sophos synchronized security with a focus on how synchronization enables rapid detection, prevention, and remediation of threats. Testing began with a look at the Sophos Network Security Control Center, which provided a comprehensive view of insights collected across the network, users, applications, and devices. The objects in this view are all active and clickable, giving an IT security administrator a summary view of issues that need immediate attention, and enabling deeper analysis as needed.

As shown in Figure 3, the center of the dashboard provides insights into network traffic. At the top is a graph showing network activity over time. Below that are summary statistics about allowed and prohibited activity. Prohibited activity includes reconnaissance attacks, and attacks targeted at web browsers, operating systems, and specific applications. The bottom of the dashboard contains links to reports providing details on the risky apps, objectionable websites, and intrusion attacks observed in the preceding day.

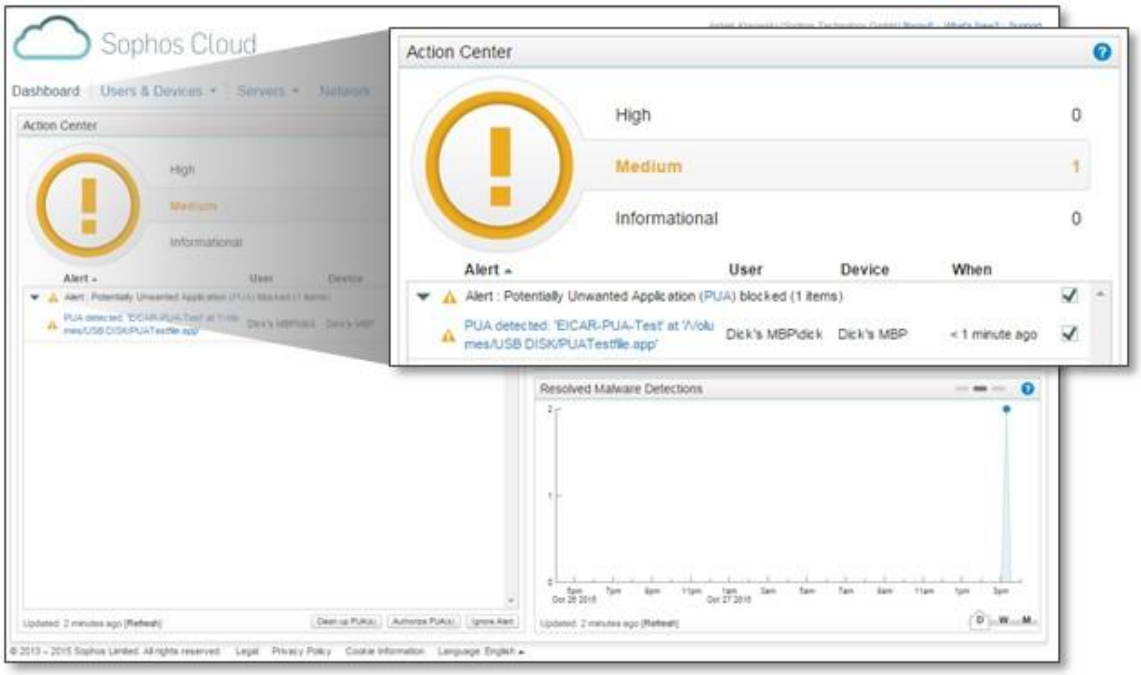
The right hand side of the dashboard provides insights into the security "health" of users and devices. The Security Heartbeat section shows that there are two endpoints with a healthy security heartbeat connected to the firewall. Sophos colors healthy, normally operating systems green to indicate that there are no security issues with those systems.

The Advanced Threat Protection section shows that Sophos has identified one endpoint that has a security issue. Sophos colors this metric red to indicate that these endpoints are suffering from malware or other security threats.

Figure 3. The Sophos Network Security Control Center

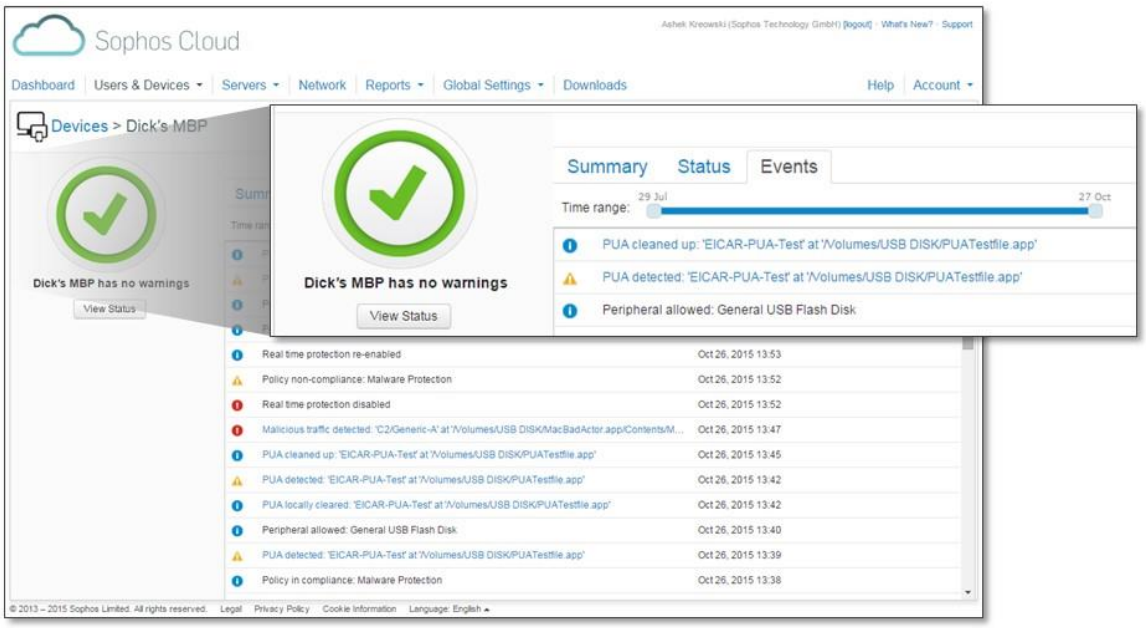
ESG Lab next looked at a use case where a user runs a potentially unwanted application (PUA). As shown in Figure 4, Sophos Endpoint Protection automatically detected the execution of the PUA, alerted the user, and changed the health status of the endpoint to yellow nearly instantly. Sophos colors the health status yellow to indicate that the endpoint has a security issue that needs remediation, but the issue is not severe enough to be considered malware.

Figure 4. Potentially Unwanted App Detected at the Endpoint



Using the Security Heartbeat, Sophos Endpoint Protection automatically notified the firewall of the endpoint's change in health status, and the firewall applied policies—customizable to match the needs of each organization—to isolate the endpoint from critical resources. When the PUA was removed, the endpoint protection updated the endpoint health status to healthy, displayed as a green checkmark. The firewall automatically applied policies to re-enable endpoint access based on the change of the health status.

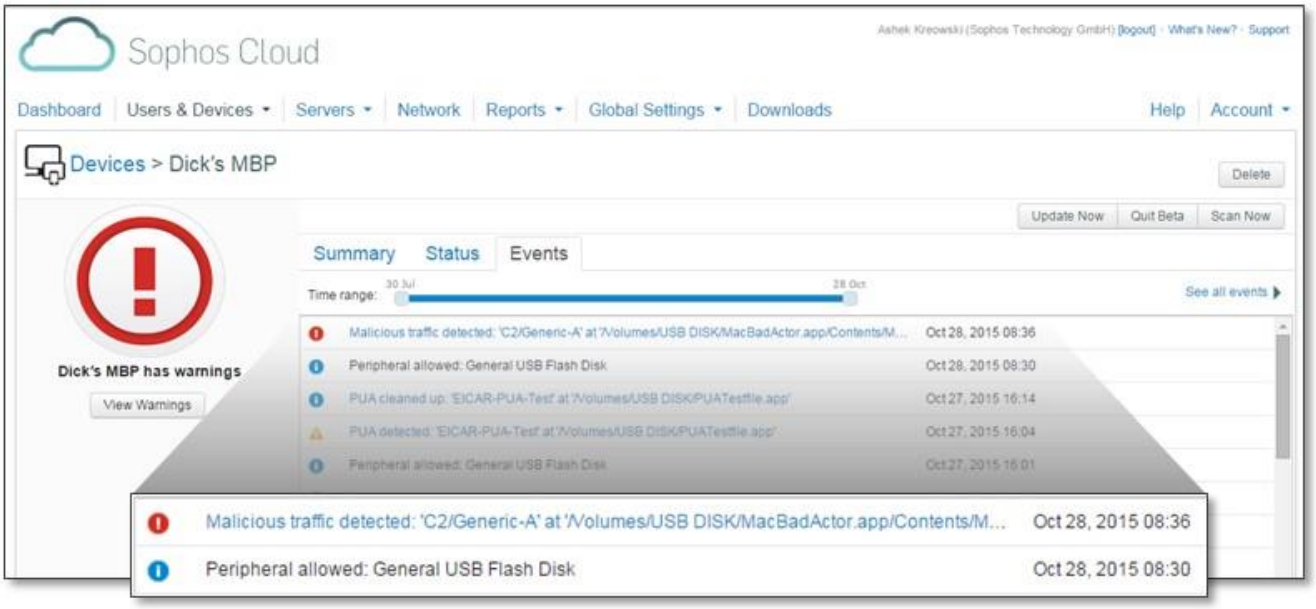
Figure 5. Potentially Unwanted App Removed



Next, ESG Lab simulated the all too common occurrence of malware introduced into a system through an infected USB drive. As shown in Figure 6, Sophos next generation endpoint protection automatically detected and remediated the threat in seconds. While this was happening, the endpoint changed its health status to red, indicating that the endpoint was infected with malware. The Security Heartbeat automatically notified the firewall of the endpoint's change in health status.

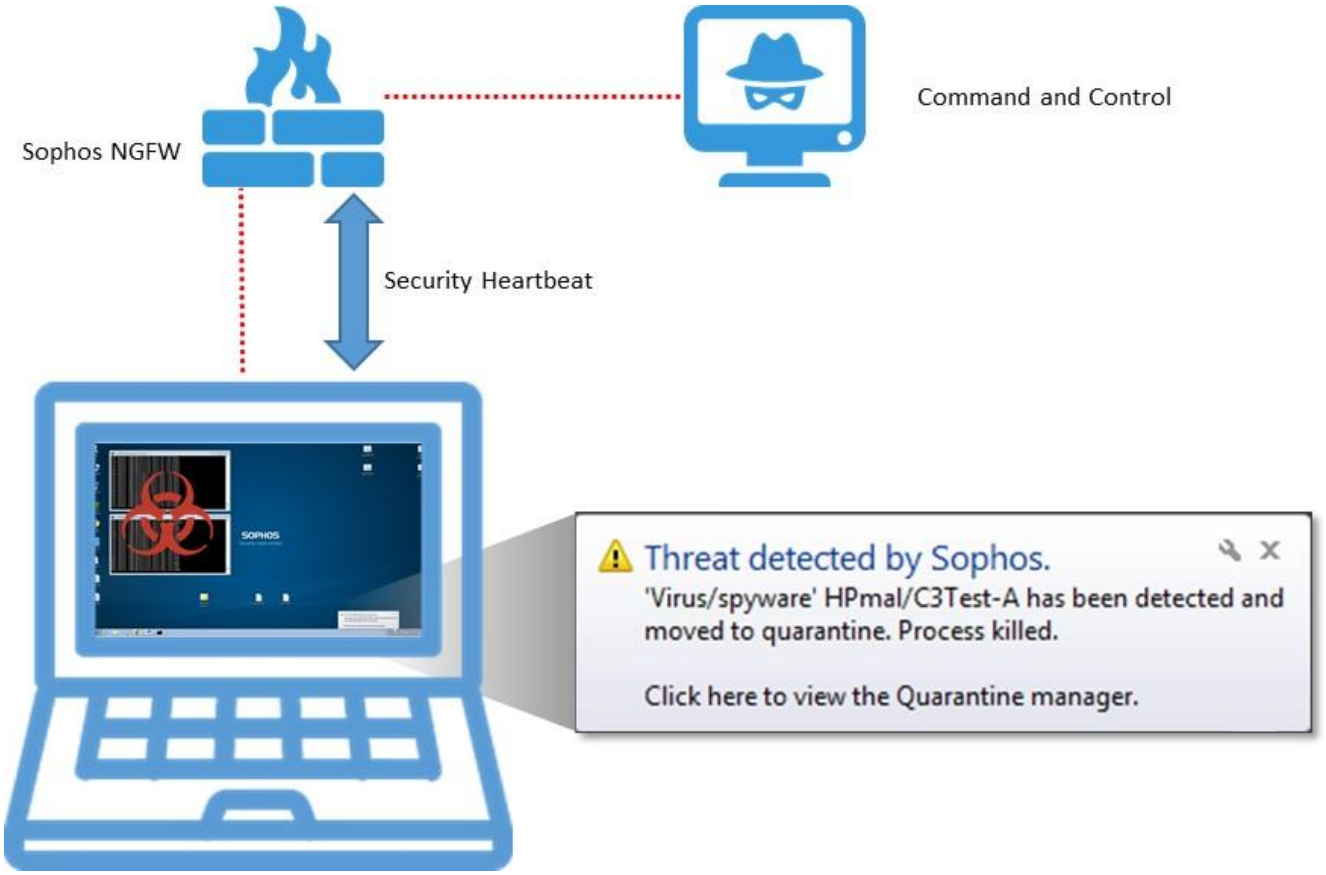
Triggered by the change in health status, the firewall automatically applied policies to isolate the endpoint from both the internal network and the external network. After the threat was removed, the endpoint health status reverted to green, and Sophos endpoint protection notified the firewall of the change in health status. Again, the firewall automatically applied policies to restore network connectivity to the endpoint. These firewall policies are customizable by the administrator.

Figure 6. Malware Detected at the Endpoint



Finally, ESG Lab looked at the scenario where an endpoint is infected by malware as yet undetected by endpoint software, as in zero-day attacks, where no methods of detecting the new malware have been introduced. In this test, software running on the endpoint simulated the behavior of unknown malware by attempting to communicate to a command and control server.

Figure 7. Malware Detected by Network Behavior



When the firewall detected this traffic and identified unknown malware by network behavior, the firewall not only blocked network access, it was able to use information provided by the Security Heartbeat to identify the endpoint, the user, and the application. The firewall automatically alerted Sophos NGEP running on the user's machine within a second of detection and the endpoint changed its health state to red. The endpoint then attempted to stop and remove the malware and notified the user with a popup message.

Traditional security solutions send alerts to the IT administrator when they detect the aberrant behavior of the unknown malware. The administrator then faces a long and complex process to address the issue, first identifying the affected endpoint, then determining which process caused the alert, and finally manually removing the malware.

Leveraging the Security Heartbeat to communicate intelligence between the firewall and the endpoint protection, Sophos automated the the entire process to identify and remediate the issue. No administrator intervention was required, and the entire process was completed in about eight seconds. In conversation with security professionals, ESG Lab learned that manually uncovering the context of the type of events tested here typically takes hours and involves multiple IT resources. When remote sites or BYOD devices are involved, this can stretch to days or longer.

Why This Matters

31% of organizations surveyed by ESG Research identify new malware threats as the issue having the most significant influence on their future endpoint security strategy.[2] A major contributor to the increasingly dangerous threat landscape are unknown threats that are undetectable by traditional methods. In the same survey, when asked to identify their biggest endpoint security challenges, 29% of the organizations stated that endpoint security is based upon too many manual processes making it difficult for the administrators to keep up. Automation of detection, prevention, and mitigation of these attacks before, during and after they occur, wherever they occur in an organizations' environment is critical.

ESG has confirmed that Sophos' Security Heartbeat provided nearly instantaneous communication between Sophos' Endpoint Protection and Sophos XG Firewall solutions and enabled them to work together, providing enhanced detection, source identification, and automated incident response.

Through our hands-on testing, ESG Lab validated that Sophos' integrated approach—providing bi-directional communication and control between network and endpoint security solutions—enables organizations to implement policies to enable or restrict access to critical resources based on endpoint health. This level of automation can be extremely valuable, enabling already overburdened IT administrators to keep up with the ever-increasing pace of threats and attacks and reducing time to response from hours to seconds.

[2] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.

The Bigger Truth

Security breaches have become increasingly ubiquitous in modern IT environments. Bad actors are targeting smartphones, tablets, desktops, and application servers. Organizations relying on independent, standalone security devices can potentially find themselves vulnerable to an attack that bypasses any single 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.

ESG research has found that 80% of the security professionals surveyed agree that managing endpoint security processes and technologies has become more difficult over the last two years. Almost two-thirds of security professionals believe that no single endpoint security product suite is capable of meeting all of their organizations' endpoint security requirements on its own, an indicator that there are gaps in traditional endpoint security solutions.[3] Intensifying this situation is the the rise of targeted attacks, and the frequency of publicly disclosed data breaches. Integration of next-generation perimeter defenses with endpoint protection is no longer just nice to have; it is a necessity. Sophos' Security Heartbeat provides continuous bi-directional communication and automated incident response. Based on our testing, ESG Lab believes that this type of synchronized solution can be much more effective than standalone systems for protecting enterprises against today's increasingly dangerous threats.

[3] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.