Sophos' Heartbeat puts the pressure on midmarket security vendors

NOVEMBER 23 2015
BY ERIC OGREN (/BIOGRAPHY?EID=907)

How many times does security find out about an infection only after a user calls the service desk with poor performance complaints and a job ticket is created for a security investigation? Sophos is seeking to address this issue with new product releases featuring regular health-status communications (what it calls a 'heartbeat') between endpoints, network devices and cloud-based management consoles, enabling real-time automated responses to security incidents. With the Security Heartbeat innovation, medium-sized businesses, especially those without dedicated security teams to respond to alerts and job tickets, can worry less about synchronizing individual silos of security technologies.

The 451 Take

Regular proactive communications between major security elements is an incident-response concept that we believe is long overdue. We expect security technologies on the endpoint and in the network to effectively block and clean up discovered attacks. We also recognize the difficulty of non-integrated security products to effectively react to indicators of compromise resulting from unrecognized attacks. While it's self-evident (to us, anyway) that security technologies across endpoints, networks, applications and data should collectively participate in detecting and responding to a new infection, relatively few vendors have effectively addressed the need. In most organizations, security teams would have to step in to analyze a compromise or attack indicator to determine if there is
indeed a breach, and then manually initiate a security reaction. However, midsized
organizations may not have qualified security staff at all, and security teams at larger
organizations may be chronically understaffed. The industry needs an automated
response capability to protect the business from attacks that exploit the gaps in visibility
and response arising from technology silos. We think Sophos is onto something good with
its regular heartbeat checks between endpoint, network and management software at 15-
second intervals, in a move that demonstrates where synchronized security infrastructure
needs to go.

Context

Defense in depth through best-of-breed security products is a strategy that should be filed in
the buzzword-bingo closet for security teams. Enterprises investing in the best security
products they can find create operating stovepipes, making responses to the inevitable
breaches an experience both exhausting and far too often fruitless. The traditional security
industry offers endpoint security, network security, application security and single pane of
glass management, but little in the way of coordination across all of these disciplines.

Into that breach steps Sophos, a publicly held security vendor headquartered in Oxford, UK.
Sophos is particularly well positioned to capitalize on the opportunity to integrate an
operational heartbeat across its portfolio based on its medium-sized customer profile and
balanced product mix:

- Roughly 56% of Sophos' sales are to medium-sized businesses of between 100 and 5,000
  employees. Relatively few of Sophos' midmarket customers have dedicated security
  practitioners in IT. Marketing to medium-sized businesses requires Sophos to create
  security products that are easy to manage by administrators with little expertise in the
detailed analysis of threats and vulnerabilities and that can respond to incidents without
requiring direction from a security expert.
- Sophos' product mix shows an approach to protecting medium-sized organizations from
cyber-threats balanced between network devices and endpoint software. In the first half
of 2015, the company announced 51% of its revenue came from networking, 43% from
endpoint and the remaining 6% was classified as other. Sophos has the expertise to coordinate the three critical network, endpoint and management elements of a security infrastructure. The strength of its synchronized product approach is reflected in its 8.9% Y/Y revenue increase.

We see Sophos as having the engineering expertise across networking devices and endpoint software, as well as the administration appeal of its cloud-based management, to make security easier for midmarket enterprises to administer and deploy. The introduction of a heartbeat-based coordination across its products represents an evolutionary next-generation step for Sophos.

Products

The regular 15-second Security Heartbeat is the star feature of the Sophos XG Firewall and UTM releases. The bidirectional communication between network and endpoint security elements is unique, with security and operational benefits to enterprises. The regular Heartbeat offering promises multiple benefits to enterprises, including:

- Endpoints identify themselves to the security fabric as they connect to the network. IT always has an accurate representation of exactly which devices are operating on the network at any moment.
- Sophos XG appliances can automatically isolate endpoints reporting a decline in health, even without knowing details of the attack. This helps midmarket firms impede the rapid spread of an attack to co-workers.
- Information of discovered attacks, such as the context of questionable applications and files, can be spread to other endpoints, enhancing their resistance to new threats.
- Incident response is accelerated due to endpoints reporting information such as device identity, user name and infected process information. IT has the basic pieces to proceed directly to mitigation actions.
- Automated communications reduce the workload of IT security administrators, allowing a heightened focus on supporting the business.
While we have seen messaging between under-duress endpoints and firewalls, and periodic scanning of endpoints for operating status, we have not seen a continuous flow of information between fundamental security elements. We consider Sophos XG appliances and Sophos Heartbeat software to be a significant innovation that can raise security performance standards for medium-sized organizations.

Two aspects beyond the heartbeat are significant to Sophos gaining market share with the XG Firewall and Heartbeat:

- The new XG functionality runs on existing Sophos SG appliances, enticing organizations to become a complete Sophos anti-malware shop. Enterprises with non-Sophos endpoint software deployments may be displaced to achieve enhanced security and the operational benefits of one less security vendor to manage without forklift upgrades in their network.
- Sophos Cloud management may energize MSSPs to sell and support Sophos-based security services. Organizations with little security experience and no desire for on-premises management can defer to outsourced security services.

**Strategy**

We all know that the very best network and endpoint security is not going to catch all attacks. To be clear, security products are very adept at detecting and blocking damage from recognized attacks. It is the unidentified attack that causes detection and incident response problems – and far too often, the attributes of such attacks are known to some other aspect of security technology in the enterprise, but because these technologies seldom inform each other automatically, the threat is missed. The next generation of security infrastructure has to be more effective in cooperating between network and endpoints in limiting the damage once an endpoint detects failing health or threat intelligence identifies an impending attack.

Many vendors can send a signal to a firewall to isolate an endpoint, or update a high-priority attack signature list. Sophos elevates the requirements by synchronizing communications and actions between endpoint, network and management security elements to enhance detection and response to security incidents and to reduce the IT workload.
Medium-sized organizations offer unique challenges for security vendors – there are no security practitioners to fill in gaps between product features; there is a fair amount of complexity in endpoint, network and management performance requirements; and they prefer fewer vendors. Sophos believes the optimal approach for protecting medium-sized businesses requires real-time coordinated actions between endpoints, network and management.

**Competition**

To be sure, Sophos is not the first security vendor to connect endpoint, network and cloud management security products. The natural inclination is to signal a firewall to quarantine an infected endpoint, to communicate new threats to endpoint protection software via updated signatures and to orchestrate the security dance via management consoles.

High-availability options for firewalls and network devices have deployed a heartbeat as an operational tactic for seamless and transparent failover. Sophos has taken the concept further as a strategic approach to enterprise security.

We believe Sophos' midmarket competition starts with network security vendors that condense multiple security features into easier-to-manage UTM devices. The network security vendors we believe will be most competitive for Sophos include Cisco, Fortinet and Palo Alto:

- **Cisco Advanced Malware Protection** products feature an AMP for Networks and an AMP for Endpoints. However, administrators have to manually respond to alerts sent to the management console because incident response actions are not automated.
- **Fortinet** favors a network-centric approach headlined by its FortiGate UTM appliance. While Fortinet does offer FortiClient endpoint software coordinating with network devices, the company is best known for integrating security into high-performance network appliances.
- **Palo Alto Networks** complements its PA line of next-generation firewall and WildFire sandbox with Advanced Endpoint Protection software and the Endpoint Security Manager. The next-generation approach needs to coexist with existing endpoint security reactions to suspicious behavior instead of relying on signatures.
We see Trend Micro leading the competition among the endpoint software-oriented security vendors with Deep Security on endpoints and Deep Discovery in the network. While there is some overlap in target markets, Trend Micro tends to approach a profile of larger organizations with virtual datacenters and cloud-based application requirements.

Of the traditional vendors, Kaspersky is a rising force among medium-sized EMEA firms, while McAfee (Intel), Microsoft and Symantec divvy up the Americas market. We feel the greatest competition for Sophos may be the traditional mindset prevalent in medium-sized businesses with minimal security expertise of treating network security, endpoint security and security management as three distinct disciplines and products. Sophos would have to displace the entire security infrastructure of firewalls and endpoint software for the customers to reap the benefits of its synchronized Security Heartbeat, a process that could take a few quarters.

We do find that Sophos is ahead of the pack with its regular Heartbeat. Not only does this provide vibrant systemic security, it also provides Sophos a path for potentially enhancing its protocol for data-driven real-time security and operations intelligence for analytic processing.

**SWOT Analysis**

**Strengths**

Medium-sized organizations will appreciate the automated security of Sophos' coordinated endpoint, network and management features. The Heartbeat provides rapid detection of infected endpoints, allowing IT to expeditiously respond to incidents without becoming dedicated security experts.

**Weaknesses**

The Sophos sales channel will have to displace incumbent endpoint software and/or network security devices to get the full benefit of synchronized security. That may be viewed as too disruptive to the business for new prospects to take the plunge, and limit the appeal of the Heartbeat to deeper penetration of the installed base.

**Opportunities**

There is a very significant opportunity for Sophos to enhance the content of its Heartbeat datagram with operational endpoint data to facilitate real-time security analytics, configuration control, and integrated security operations. We can also envision an enhanced partnership program to make it easier to capture new accounts and to protect the security investments of larger enterprises wishing to embrace Heartbeat.

**Threats**

The prevalence of cloud-based applications may weaken the demand for deploying a new security infrastructure. Prospects may choose to shift security to cloud vendors instead of investing in coordinated security.

**Eric Ogren (/biography?eid=907)**
Senior Analyst
basic_acquirers=McAfee+Inc [fka Network Associates])
Microsoft Corporation (145) (https://makb.the451group.com/results?basic_acquirers=Microsoft+Corporation)
Sophos Plc (8) (https://makb.the451group.com/results?basic_acquirers=Sophos+Plc)
Symantec Corporation (43) (https://makb.the451group.com/results?basic_acquirers=Symantec+Corporation)

Figures shown indicate number of transactions

COMPANY MENTIONS (PRIMARY)
Sophos (/search?company=Sophos)

COMPANY MENTIONS (OTHER)

CHANNELS
Information Security (/dashboard?view=channel&channel=5)

SECTORS
All / Security / Anti-Malware / Anti-malware suites (/search?sector=401)
All / Security / Endpoint integrity assurance (/search?sector=410)