SOPHOS
Security made simple.

CYGNUS SYSTEMS, INC.
Keeping IT Real

# Synchronized Security:

## Best-of-breed defense that's more coordinated than attacks

Today, many organizations deploy multiple layers of disparate security products across their networks and endpoints: host- and network-based firewalls, content inspectors, malware analyzers, event managers, and much more. This "defense-in-depth" strategy is meant to help protect against both known and emerging threats, with the idea being that somewhere – anywhere – along the attack chain, one of these products will be able to neutralize a malicious onslaught.

While various point products deserve merit in their own rights, there are a few fundamental downsides to such a "siloing" strategy. For starters, these products often work in isolation from one another rather than sharing information in any rapid, meaningful manner. As such, on the most basic level, there's an obvious opportunity for firewalls and endpoints to share contextual network and process-level data with each other in real time in order to isolate and neutralize infections.

Second, the deeper and wider an organization's defense-in-depth strategy, the more cumbersome it becomes to manage. This results in added staffing costs to manually correlate alerts, manage multiple user interfaces, and monitor events. It can also affect performance thanks to multiple software agents jostling for system resources.

Third, while security information and event management (SIEM) tools have been developed to try to bridge the communications gaps between multiple point products, their purpose is mainly to collate data into a single sensible view. Their ability to extract actionable information is generally weak, after-the-fact, and must be analyzed thoroughly by senior-level staffers first.

To illustrate the current situation faced by most of today's organizations, imagine posting security guards inside and outside of your building, but not giving them two-way radios to communicate with each other. Instead, they would be told to send all communication one way to a centralized system, at which point a human would need to remain vigilant for any information that might be meaningful to one of the other guards and, if found, would need to be delivered to the guard by hand. Now imagine multiple buildings with multiple perimeter guards outside, a guard in every room inside, and all of these guards sending data to this central system – a system that can't coherently discern which guard is sending which message. Add to this a constant barrage by intruders who challenge this patchwork defense with new, innovative, and increasingly-stealthy techniques.

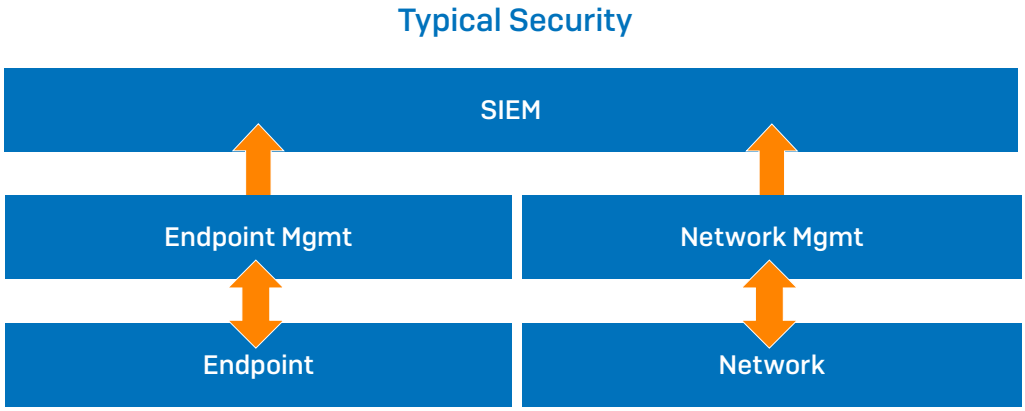



Figure 1: Typical solutions try to correlate and make sense of data and require headcount and scarce expertise

## Yesterday's Defenses vs. Today's Attacks

While motivation behind the early days of cyberattacks might have been a combination of curiosity and a desire for mayhem, today's attacks are more sophisticated and coordinated than ever. Attacks are motivated by money, secrecy, and political causes, and are carried out by crime syndicates, nation-states, and hacktivists. They bend end users to their will by parlaying well-crafted phishing attacks into credential theft, privilege escalation, and data exfiltration. They exploit buggy software almost as quickly as it's patched. They infiltrate networks with memory-based malware and move laterally in the blink of an eye, infecting other systems along the way.

As the security industry struggles to catch up, today's cyber criminals stay one step ahead thanks to underground communications, shared techniques and code, anonymous currencies, intelligently morphing malware, and readily-leveraged networks of pre-infected devices. There are even fully-functioning, sophisticated, cloud-based attack services that can be leveraged by just about anyone – app stores for crime, in other words – complete with revenue splits that funnel back to the coders each time a successful attack lands a windfall.

Meanwhile, end users move more and more data to the public cloud, load their personal devices up with company assets, and expect to be able to seamlessly work from outside the corporate perimeter – whether from home, across town, or the other side of the globe.

Dealing with today's threats has caused nearly insurmountable challenges for even the world's largest and most forward-thinking organizations. Attacks keep getting more complex and coordinated, while point products meant to defend against them often work in isolation. Attack surfaces keep expanding as end users leverage smartphones, cloud applications, and multiple portable devices while budgets for IT departments fail to grow to scale with ever-increasing demands. According to Ponemon Institute, 74% of data breaches go undiscovered for more than six months. And according to ESG Group, 46% of organizations believe they have a problematic shortage of cybersecurity skills.

**74%**
of data breaches go undiscovered for 6+ months.

**46%**
of organizations have a problematic shortage of cybersecurity skills.

## Synchronized Security – a Simple Solution to a Complex Problem

For the first time, endpoint and network protection can operate as one integrated security system comprised of best-of-breed products that share a common interface and bi-directionally exchange real-time information in order to respond automatically to threats.

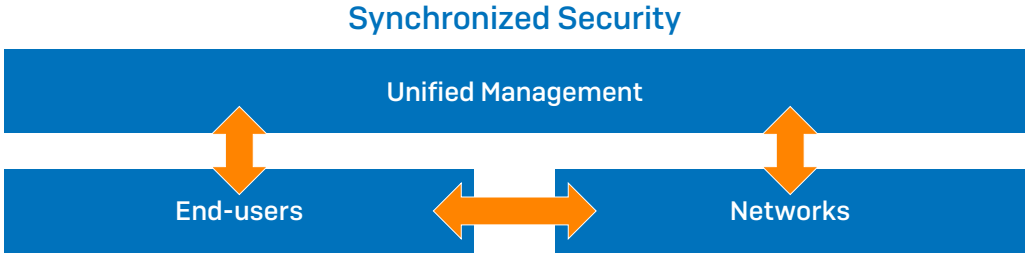


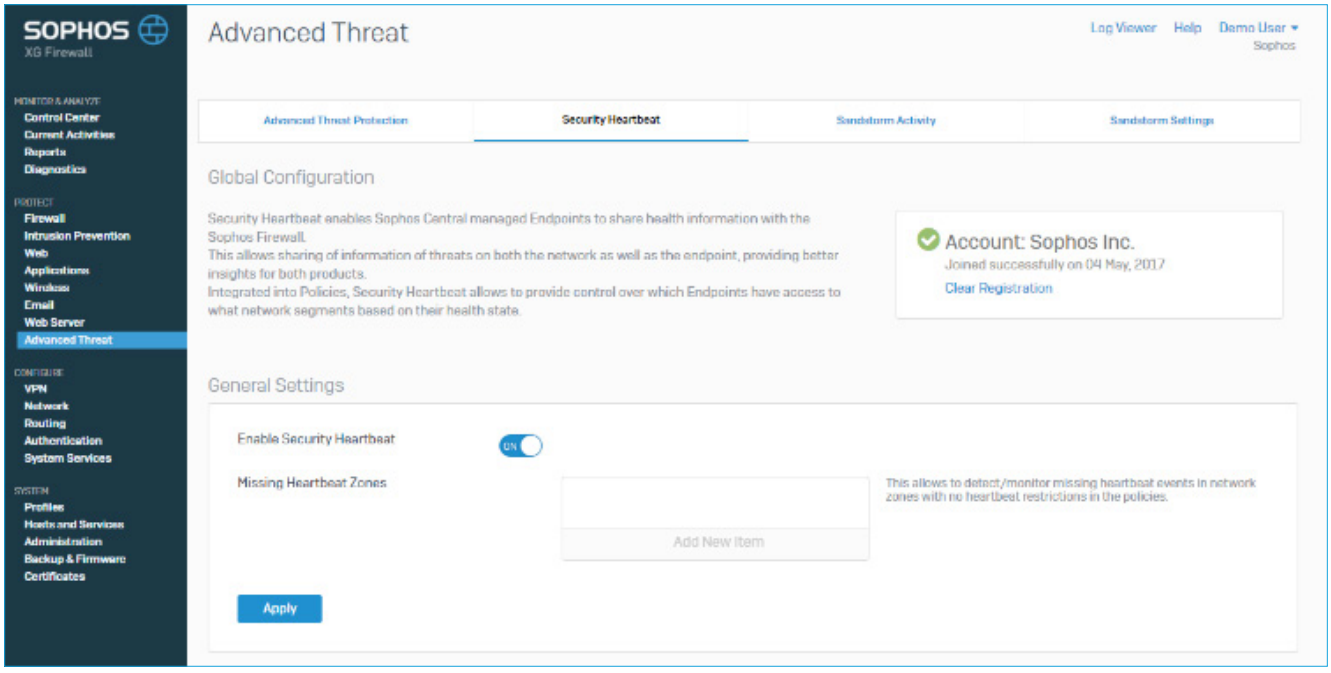

Figure 2: Synchronized Security simplifies and unifies communication and management

Simplified management makes the framework easy to set up and manage without additional analysts and event managers, while automated detection, isolation, and remediation results in attacks being neutralized in mere seconds – not hours or days. It's better protection that's also more cost effective and time efficient.

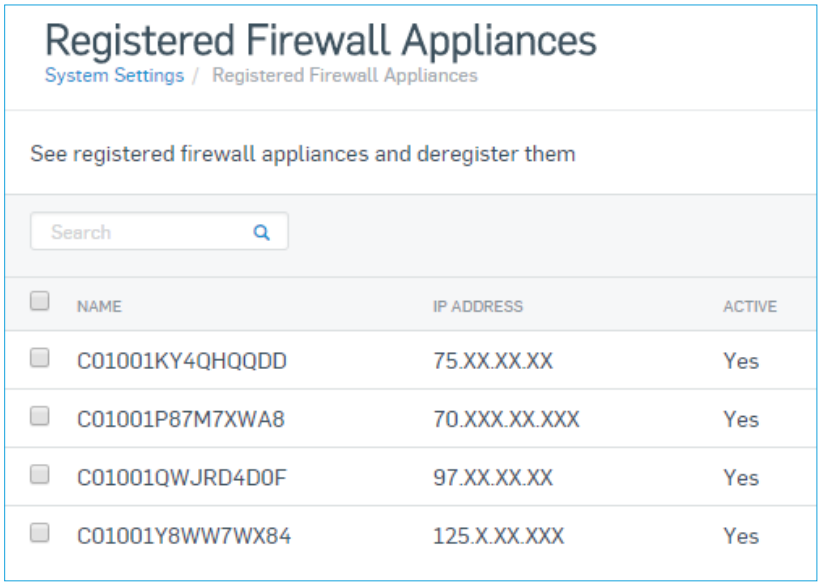
| | Synchronized Security | Typical Security |
|---|---|---|
| Intelligence | Shared | Isolated |
| Correlation | Automated | Manual and partially automated |
| Unknown Threat Discovery | Contextually assisted | Unassisted |
| Incident Response | Highly targeted | Imprecise |
| Additional Product and Headcount Investment | None | Significant |
| Management | Simple and unified | Complex and siloed |

Table 1: Characteristics of Synchronized vs. Typical Security

Communication between firewalls and endpoints is facilitated by the Sophos Security Heartbeat, an easy-to-deploy feature that creates a secure, two-way channel guided by the cloud-based Sophos Central management console.




Setup consists simply of entering your Sophos Central admin credentials into the Security Heartbeat section of the Sophos XG Firewall interface. Once that's been taken care of, the firewall will become visible in Sophos Central, any computers managed via Sophos Central will begin sending a heartbeat connection to connected firewalls, and connected firewalls will send a heartbeat back to the computers.



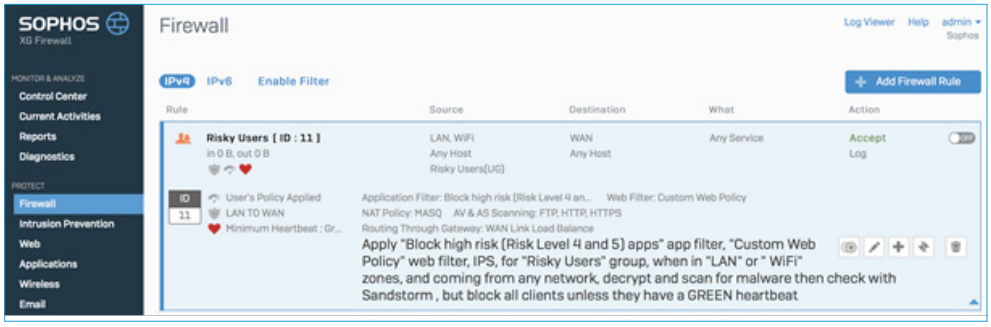

Computers will automatically connect to the nearest firewall, while firewalls will check incoming connection requests from computers to ensure they're secured via Sophos Central. In turn, computers validate the firewall as well by checking that its security information matches up with Sophos Central. It all happens automatically: no complex rules, configurations, or updates.

## Synchronized Security in Action: The Basics

With the firewall and endpoint clients connected, system health information begins to flow from the endpoints to the firewall via Sophos Central. On the XG Firewall dashboard, the Sophos Security Heartbeat widget indicates the health status of all your Sophos Central-managed endpoints. If any systems are running unwanted applications or are infected, they'll show here as yellow or red. Red indicators should be dealt with immediately, while yellow indicates risk but not urgency.


Sophos Security Heartbeat widget shown on XG Firewall dashboard

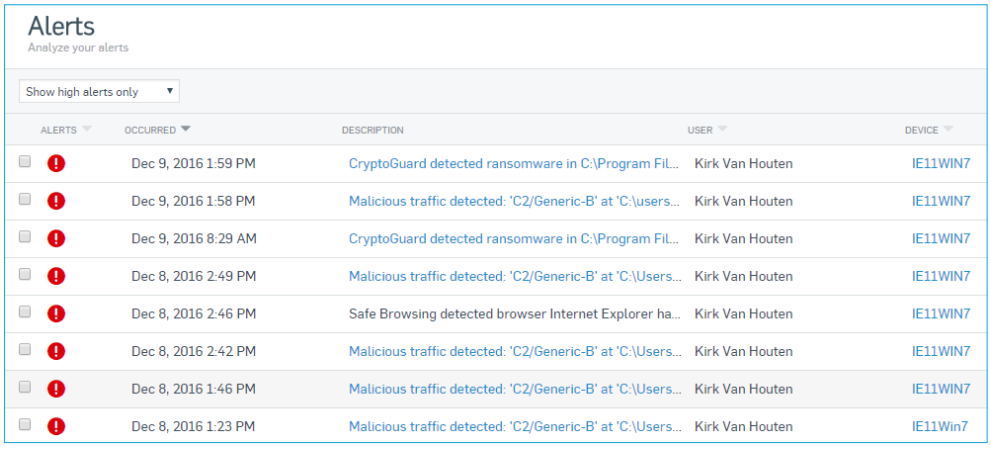
Firewall rules can be created to leverage changes in security status. For example, you could allow computers in yellow states to access the internet in general but block these machines from accessing sites that may contain sensitive company information, such as Salesforce or Dropbox. In red states, you could block internet access to these machines altogether and, if you've licensed our SafeGuard file encryption product, revoke file encryption keys until the affected computers return to a green state. At that point, internet access would automatically be restored and file encryption keys re-issued.




Firewall rule in XG Firewall interface blocks risky users from network access unless they're in a safe state

Sophos XG Firewall is also able to detect if a previously-healthy endpoint is generating network traffic without sending a heartbeat. This could be an indication that the endpoint's malware protection has been tampered with or disabled by an intruder. In an instance such as this, the endpoint would be isolated from the rest of the network until it can be cleaned up and its heartbeat restored.

Thanks to Security Heartbeat, affected machines are clearly identified inside both the XG Firewall interface and the Sophos Central Admin interface. Machine name, logged-in user, and the process name that triggers an alert are all shared, which greatly reduces time spent investigating, detecting, and remediating threats. This could take hours or days of manual labor in traditional, protection-siloed environments where the investigator only has the transient IP network address to identify the source of the problem.




Alerts page showing red alerts in Sophos Central Admin

## Synchronized Security Means Stronger Servers

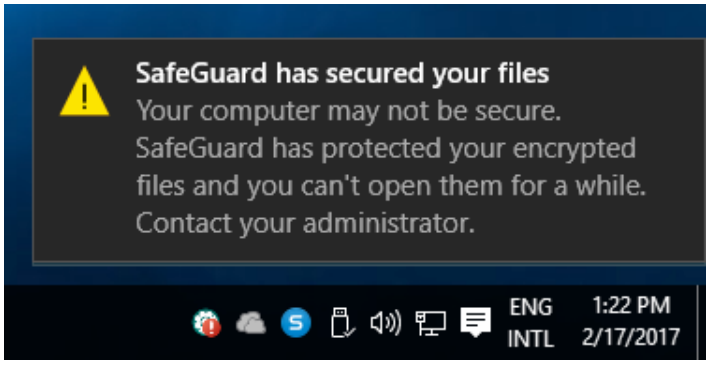
Servers almost invariably contain an organization's most valuable data and, as such, make highly sought-after targets for malware authors. It's important to protect servers against direct attacks, of course, but it's also imperative to fend off lateral movement from end-user computers that are connected to your servers.

In the case of an attack, Sophos Server Protection can notify the XG Firewall of a change in health state, at which point the firewall can isolate the server both from the Internet and from other machines on the network in order to prevent data exfiltration and the possible spread of infection. Known as Destination Heartbeat, inbound connections to the server will be rejected by the firewall and the server will be hidden from other devices on the network as well. Once remediated, network access and server visibility can be restored automatically.

With two-way communication between firewalls, servers, and endpoints, Sophos Synchronized Security ensures immediate coordination to thwart the most sophisticated attacks. And automated identification and isolation of servers based on Sophos Security Heartbeat means less time spent responding to incidents. Combined with regular heartbeat policy enforcement, this can effectively isolate a compromised system completely - both inbound and outbound.

## A New Prescription: Synchronized Encryption

File encryption is traditionally a cumbersome process for admins to set up and for end users to work with. However, Sophos SafeGuard Encryption employs a novel approach to an organization's security strategy: by default, all files are encrypted and then validated against the user, application, and security state of the device for decryption. Only applications deemed safe are allowed to see unencrypted data, which means malware can't access sensitive data at all. The entire process is transparent to the end user, with content being encrypted as soon as it's created, remaining encrypted when shared across the organization or uploaded to cloud sites, and optionally password-protected with a single click when shared externally.



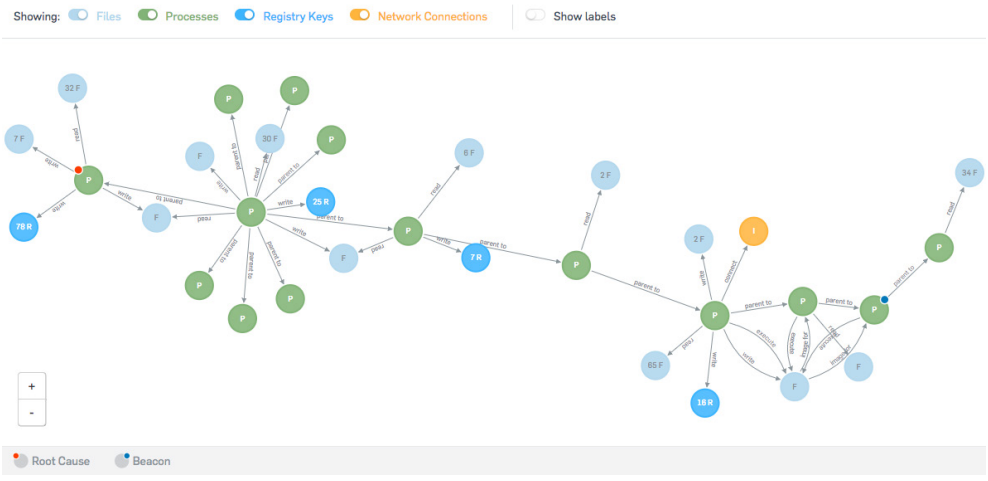

Message that SafeGuard has revoked file encryption keys during an attack

Sophos SafeGuard Encryption is Synchronized Security-ready as well. If a Sophos-protected endpoint communicates to the XG Firewall that it's been attacked, the firewall will not only isolate the endpoint from the network, but will also remove the SafeGuard file encryption keys on that machine. That way, any data that gets exfiltrated will be unusable by attackers. Once the endpoint is returned to a safe state, it's allowed back on the network and encryption keys are re-issued. The entire process – from isolation to cleanup to restoration – happens automatically and within mere seconds, not hours or days as it could with an attack against a patchwork of point products.

# Getting to the Root of an Attack

Of course, while the automated isolation, remediation, and restoration afforded by Synchronized Security and its bi-directional Security Heartbeat is a true game-changer in the security industry, easily-digestible analysis of past attacks is paramount when it comes to fortifying against future ones.

The root cause analysis feature found in Sophos Intercept X offers detailed, forensic-level playback of an attack's infection path – complete with information about affected files, processes, and registry keys, and followed by prescriptive remediation guidance.



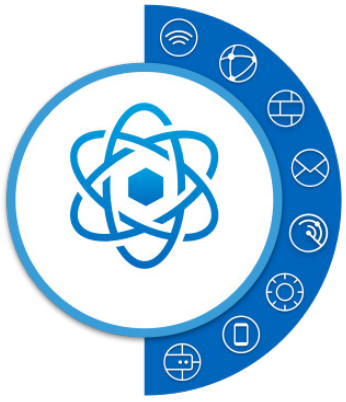

The Visualize tab of the root cause analysis feature found in Sophos Intercept X

You'll be able to see how malware got into your system in the first place, what it did before it was convicted and removed, make sure it's completely cleaned up, and take steps to avoid similar attacks down the road.

# Synchronized Security is Simply Better Security

Synchronized Security is a best-of-breed security system that enables your defenses to be as coordinated as the attacks they protect against. It combines an intuitive security platform with award-winning products that actively work together to block advanced threats, giving you unparalleled protection, automated incident response, and real-time insight and control.

Unlike disparate point products that breed complexity with each additional layer, the more Sophos solutions you have, the more you benefit from Synchronized Security.



Learn more and try for yourself at

**www.sophos.com/synchronized**

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com



2017-05 WP-NA (NP)

CYGNUS SYSTEMS, INC. Keeping IT Real

SOPHOS