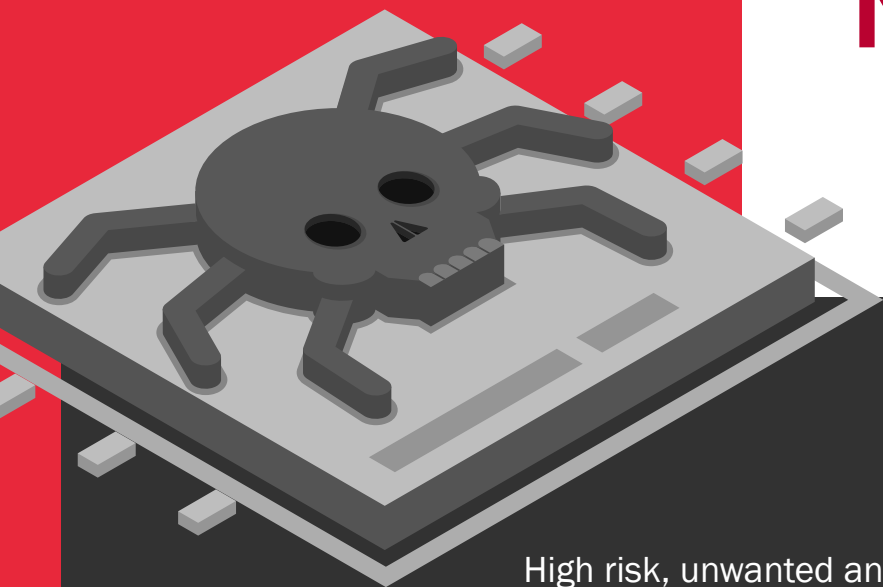# SOPHOS

STOP THE PARASITES ON YOUR NETWORK

High risk, unwanted and even malicious applications are hiding like parasites on many organizations' networks. That's because most next-gen firewalls are failing to do their job. They can't identify specific applications and at best are only able to identify the protocol such as HTTP, HTTPS/SLL, UDP or TCP. Which is of no use to a network admin trying to see what security, compliance and productivity risks are present on their network.

What are these parasitic applications? Why can't next-gen firewalls see them? And what can you do to make sure you identify every single app on your network?
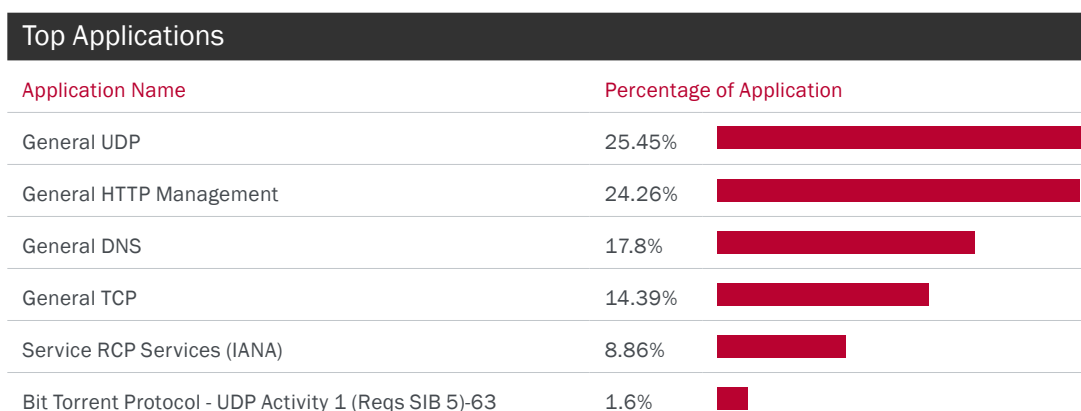
How Big Is the Parasite Problem?

"45% of network traffic goes unidentified on the average corporate network."

In other words, the average organization can't identify or classify almost half of the applications running on its network. For a small or medium sized organization that could mean tens or hundreds of unknown applications running on the network.

The applications don't need to be actively malicious to pose a problem for your network. Many of them will put additional strain on valuable network bandwidth, but not actively seek to cause harm, while others can open security holes by using unsanctioned connections.

And for a quarter of organizations this picture is even worse – 70% of their network traffic is going unidentified.

The image below shows what a typical firewall dashboard looks like in regard to information on applications. Most likely you have seen something similar in your current or previous firewalls.

Top Applications

Application Name	Percentage of Application	
General UDP	25.45%	
General HTTP Management	24.26%	
General DNS	17.8%	
General TCP	14.39%	
Service RCP Services (IANA)	8.86%	
Bit Torrent Protocol - UDP Activity 1 (Reqs SIB 5)-63	1.6%	

Conventional firewall dashboard showing categories that could not be identified.

In this example roughly 90% of network traffic cannot be identified beyond broad categories, which is of no use to those looking for more detail to prioritize mission-critical applications and restrict unwanted ones.

So why can't your firewall identify these applications?

The vast majority of modern firewalls use signatures to detect applications (similar to traditional antivirus products) which has an obvious downside – if the application doesn't match a known signature then the firewall can't tell you what it is. Some applications use clever techniques to constantly change their traffic patterns and the manner in which they connect outside your organization to evade detection. Other applications use encryption to avoid detection or pretend to be a common web browser so they can pass through the firewall freely. Finally, there are applications that have recently changed, are bespoke or just too obscure to be identified.

Whatever the reason, these hidden applications pose a threat to the performance of your network, legitimate applications and in some cases can also create security or compliance risks for the wider corporate network.

Why Admins Are Worried

"84% of IT managers agree lack of app visibility is a serious security concern."

It should come as no surprise that the vast majority of IT managers are worried about these hidden applications running on their organization's network.

- They may represent a security concern either as a direct threat or malicious app, or enable unsanctioned Shadow IT putting data at risk or creating other security risks

- They may be adversely impacting the performance of your network, utilizing bandwidth and host resources

- They may represent a compliance, productivity, or liability issue if users are using these apps for illegal, inappropriate, or unsanctioned activity

- They may be important mission critical applications that you are unable to properly prioritize with QoS (Quality of Service) and traffic shaping to ensure top performance

IT managers also cite further concerns in addition to security worries caused by lack of network visibility:

"52% are worried about loss of productivity as a result of unknown network traffic."

Users accessing social media apps or playing games on the corporate network causes an obvious productivity loss for the perpetrators, in addition to the additional strain on bandwidth.

"42% are concerned about legal liability or compliance issues due to potentially illegal or inappropriate content."

Users streaming or downloading copyrighted and illegal content could have wider implications for the organization.

Common Network Parasites to Watch Out For

"4 in 10 IT managers worry they can't account for their bandwidth consumption."

Now we've seen why these hidden applications can put your network at risk, let's take a look at the more common types of application and specific examples for each.

Instant Messaging (IM) and conference apps

e.g. Skype, TeamViewer

IM and conferencing apps are notoriously evasive to ensure they can punch through most firewalls unconstrained. Of course, every organization now depends heavily on some form of IM and conferencing application suite as part of day-to-day business, so being able to identify and prioritize VoIP and screen sharing for these applications is important. At the same time, unsanctioned IMs not only run the risk of productivity loss, but can also represent a Shadow IT security or compliance risk as users are able to connect with and transfer files to people outside of your organization with little or no oversight.

Peer-to-peer clients

e.g. BitTorrent, uTorrent

Peer-to-Peer (P2P) clients are most often utilized to share illegal or copyrighted content, and are carefully designed to mask their traffic and activity. In addition, these applications can easily hoover up significant amounts of bandwidth. This category of unseen applications represents an enormous compliance and liability risk, productivity and resource challenge, and a significant security risk if compromised downloads are entering your network through these tools.

Proxy and Tunnel Clients

e.g. Ultrasurf, Hotspot Shield

Encrypted cloud proxy servers are designed to mask a user's identity, location, and activity. Many people take advantage of these services to bypass geo-location restrictions e.g. watching Netflix shows only available in the US despite your physical location being in Europe. They are also frequently utilized by rogue users to bypass your firewall which is often blind to the encrypted traffic, enabling them to freely access inappropriate or illegal content.

Gaming Platforms

e.g. Steam, Origin

Gaming platforms give users access to thousands of games posing an obvious risk to productivity as well as bandwidth strain for streaming-based games or multiplayer-focused games.
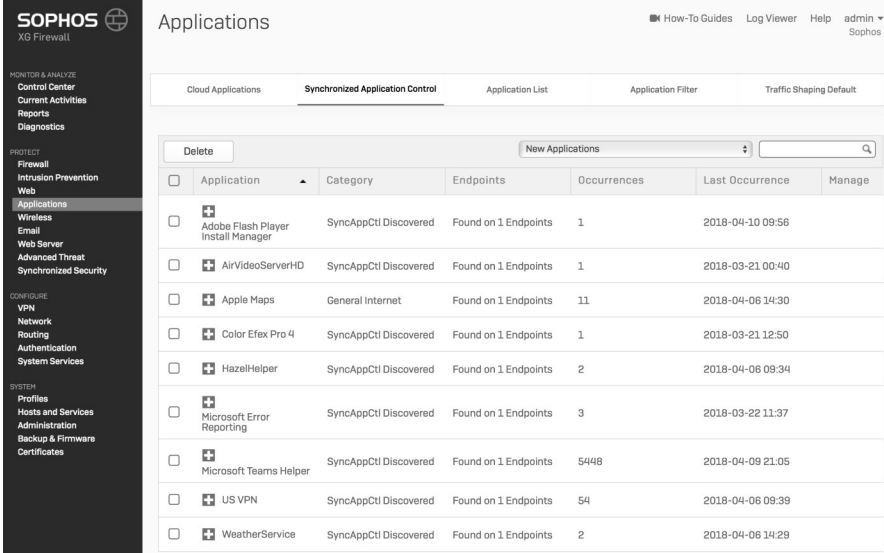
These are just a few examples of applications that can't be identified, intentionally or not and can have a negative effect on your organization's network.

Solving the Visibility Problem

"67% of Sophos customers have discovered over 100 unwanted applications." [1]

While next-gen firewalls need to rely on deep packet inspection, pattern matching, and signatures to try and identify applications as they traverse the network, the endpoint is in the unique position where it inherently knows with absolute clarity exactly what executables are generating all network traffic. Hence the solution, a rather obvious matter of connecting the endpoint with the firewall to share this valuable information. Fortunately, at Sophos, we have the technology in place to simply and effectively enable this: Synchronized Security.

Sophos Synchronized Security is a revolutionary new approach to IT security that enables security products to share information and work together to provide real-time insights, unparalleled protection, and automated incident response.
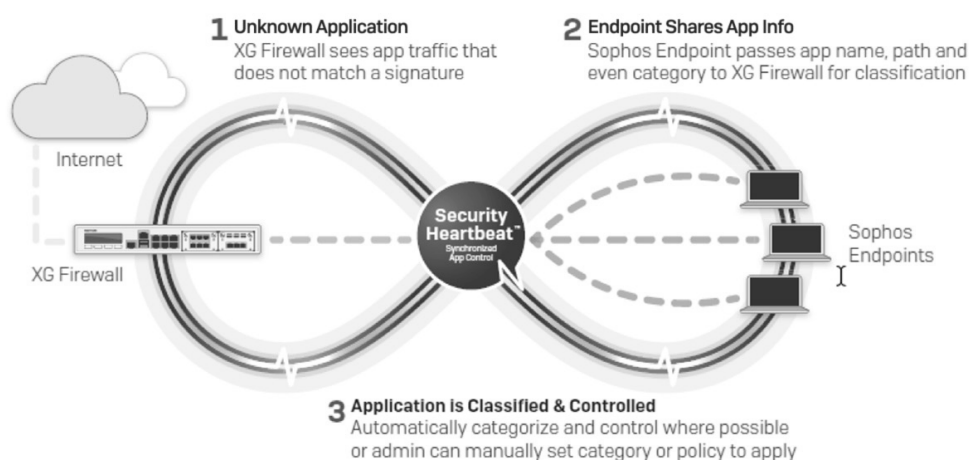

Sophos Synchronized App Control displaying all network applications

One of the first Synchronized Security innovations, Security Heartbeat™, connects Sophos Central managed endpoints with Sophos XG Firewall to share endpoint health status, enabling instant identification of systems at risk. When a compromise is detected at either the endpoint or the firewall, traffic light style indicators and alerts are issued in real-time, immediately identifying the computer, user, and process involved. And perhaps the most important benefit of Security Heartbeat, is that the firewall can include endpoint health status in firewall rules, enabling automated response, either limiting access or completely isolating the compromised system until it can be cleaned up. This has reduced response time from hours to seconds and helps reduce the risk of infections spreading to other parts of the network.

---

[1] Sophos customers using XG Firewall and Sophos Endpoint with Synchronized App Control enabled.

Another Synchronized Security innovation is Synchronized App Control. As the name implies, Synchronized App Control leverages Sophos' unique Synchronized Security ecosystem to effectively and elegantly solve the problem with identifying unknown, evasive or custom application traffic on the network. Synchronized App Control leverages its information sharing ability with the Endpoint to determine the source of unidentified app traffic on the network, effectively removing this thick veil covering networks today.

Synchronized App Control in Action

1 Unknown Application
XG Firewall sees app traffic that does not match a signature

2 Endpoint Shares App Info
Sophos Endpoint passes app name, path and even category to XG Firewall for classification

3 Application is Classified & Controlled
Automatically categorize and control where possible or admin can manually set category or policy to apply

It's the first major breakthrough in network application visibility and control since the next-gen firewall was conceived.

When a Sophos Central managed endpoint connects to a network with an associated XG Firewall, it will establish a Security Heartbeat™ connection to share health and security status and telemetry. In addition, the endpoint will now also use this connection to share the identity of all network applications with the firewall.

Where the firewall can't confirm the identity of the application using traditional signature techniques because the application is evasive, custom, new or using a generic connection, the app information provided by the endpoint will be utilized to identify, classify and control it. Where possible, the applications shared by the endpoint will be automatically classified into an appropriate category. This will automatically subject the newly identified and classified application to any app control policies that are already being enforced on the firewall.

For example, an evasive BitTorrent client will be automatically assigned to the Peer-to-Peer application category. And if the firewall has an app control policy in effect to block Peer-to- Peer apps, the new BitTorrent traffic will be automatically blocked – without any intervention by the network administrator.

The Benefits

"90% of Sophos customers say they now have greater control over their network traffic." [2]

Identify Unknown Apps

Synchronized App Control reveals all the apps that are currently going unseen on the network including all new apps as well as tunneling, proxy and VPN applications that often use encryption to bypass firewall control – creating an enormous blind-spot as well as a variety of compliance, performance, and security risks. If there are existing policies in place to block or traffic shape these types of applications, the newly identified applications falling into this category will be subject to the same policies automatically. In addition, the users and hosts involved will be easily identified enabling intervention and education where appropriate.

Prioritize Custom Apps

Synchronized App Control will immediately identify custom business applications that are completely invisible to your current firewall such as finance, CRM, ERP, manufacturing and other networked applications that are important to your organization. For the first time, Synchronized App Control provides an opportunity to apply traffic shaping and QoS policies to ensure these mission-critical applications are getting appropriate priority and optimal performance.

Control Evasive Apps

Synchronized App Control will automatically discover all evasive applications that are continuously changing the way they connect and communicate in order to evade detection and control. In effect, Synchronized App Control puts an end to these tactics once and for all. Regardless of how evasive these apps try to be, they will be completely unable to evade Synchronized App Control.

[2] Sophos customers using XG Firewall and Sophos Endpoint with Synchronized App Control enabled.

Summary

Next-gen firewalls are failing to detect parasite applications that are hiding on organizations' networks. Which opens these organizations up to potential compliance violations and legal issues, as well as putting security at risk and causing bandwidth wastage.

Sophos turns on the spotlight so the applications have nowhere to hide – you get 100% visibility of the applications running on your network, so you can prioritize, assign and block applications as needed. It's a major breakthrough in network visibility and control that leaves other next-gen firewalls lost in the fog.

"No other company is close to delivering this type of communication between endpoint and network security products."

Chris Christianson
Vice President of security programs at IDC

LOC **LES OLSON I.T.**
COMPANY

SOPHOS