SOPHOS
Security made simple.

ControlScan
Unified Security + Compliance

Switching to Next-Gen Endpoint Security

By **Marty Ward**, VP Product Marketing, Sophos

Threats are becoming increasingly dynamic and industrialized which is forcing organizations to defend against new advanced attacks as well as traditional malware. As a result, more and more organizations are making the switch to next-gen endpoint protection from Sophos to get the proven, innovative defense they need. This solution brief shows how Sophos Next-Gen Endpoint Protection delivers the protection, usability and support required to stay ahead of the constantly evolving threat landscape.

“Smarter, faster hackers cause huge spike in cyber attacks.”[1]

Another day, another headline. High profile data breaches. Alarming new statistics. The cyber threat environment is more dynamic than ever. Information from the Verizon 2015 Data Breach Investigations Report[2] paints a disturbing picture of a threat environment that continues to grow in terms of the volume of attacks as well as their speed and sophistication.

- In 2014, there was a 26% increase in security incidents and a massive 55% increase in confirmed data losses.
- In 60% of cases, attackers are able to compromise an organization within minutes.
- 70 to 90% of malware samples are unique to a single organization.

In addition, both public and boardroom awareness of cyber threats has continued to grow. Again, from the Verizon report: “The New York Times [devoted] more than 700 articles related to data breaches, versus fewer than 125 the previous year.” Similarly, awareness of cyber threats within organizations is on the rise with both the broader employee population and boardroom executives.

Increased security spending, with some regrets

With increasing public and boardroom awareness, it shouldn’t come as a surprise that organizations continue to increase IT security spending. According to the Ponemon 2015 Global Study on IT Security Spending & Investments[3], 46% of organizations increased their security spending over the past two years, and 50% expect to increase IT security spending over the next two years.

However, the Ponemon study also raises questions about how well those security investments have been working: “Companies admit they have been disappointed with some of their technology purchases. In the past 2 years, respondents say on average 37% of all investments in enabling security technologies fell below their expectations.”

Asked why they regret those security investments, the top five issues cited by organizations in the Ponemon study were categorized into 3 main areas.

1. Protection (System Effectiveness)
2. Usability (System complexity, Personnel and lack of in-house expertise, Installation costs)
3. Support (Vendor Support)

At Sophos, we ask our new endpoint protection customers what prompted them to change endpoint security solutions, and the answers mirror many of the top issues raised in the Ponemon study. Primarily they are frustrated with continued malware outbreaks that got past their previous solution, slow performance, multiple agents, product complexity, poor customer support, and difficulties integrating a wide range of integrated defenses.

Evolution of threats

The problems arising above are the result of the continued evolution of threats while customers continue to try to defend with legacy endpoint solutions. Traditional endpoint security was built to address viruses, Trojans, and worms whereas threats have advanced to exploiting vulnerabilities, ransomware, and in-memory attacks. There are changes to both the type of threats we see today as well as the targets.

In Figure 1 below we highlight some key trends including the fact that the majority of threats are now unknown, zero-day attacks. They have also moved from simple malware to industrialized attacks which are very coordinated, often including multiple attack techniques and communication mechanisms. Given that traditional endpoint security has done a good job preventing malware, hackers have moved on to compromising credentials in order to move around within systems as a legitimate user or admin. Legacy endpoint security was not designed for this.

Figure 1. Evolutionary Threat Trends

Threats	Targets
Known to Unknown 75% of malware inside an organization is unique to that organization (Source: Sophos Labs)	**Large to Small Business** 70% of all organizations reported a compromise in the last 12 months. (Source: Sophos Labs)
Simple to Industrialized As Malware-as-a-Service platforms evolve, payloads are being monetized on the Dark Web with the same market pressures we see govern any industry (Source: FBI / InfoSec London)	**Volume to Targeted** Exploit kits cause over 90% of all data breaches (Source: NSS Labs)
Malware to Hacking 63% of data breaches involve stolen credentials (Source: Verizon DBIR)	**Everyone to Weakest** Average time to fix vulnerabilities is 193 days (Source: WhiteHat Security)

In addition, the targets of the attacks have changed. Rather than going after large enterprises only, hackers have realized that small and medium sized businesses have equally valuable data and often partner with large enterprises, so that data is shared everywhere which makes it easy to move between companies to get the data they want.

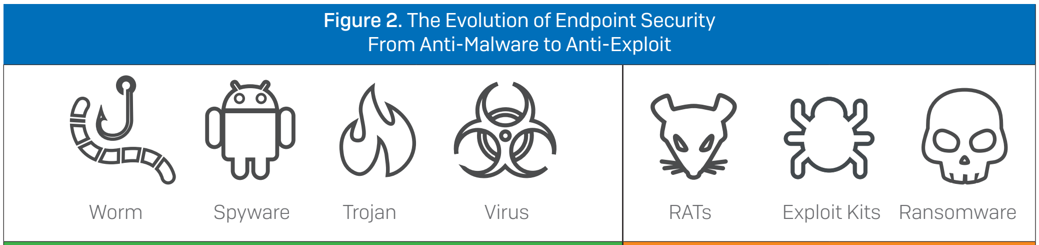
Exploit kits, which are “hacking as a service” tools that anyone can use, now account for 90% of all data breaches. They enable hackers to get very targeted in their attacks, pinpointing the demographics they desire in order to maximize effectiveness of their actions. Furthermore, since companies still tend to take half a year to patch known vulnerabilities, hackers are moving their approach from “spray and pray” to focusing on exploiting this lack of diligence.

Evolution of Endpoint Security

The good news is the security industry has continued innovating as well. In this multi-decade chess match between hackers and vendors, every move is met with a counter move, with each side hoping to leapfrog the other. The security industry has always been fascinated with the concept of a silver bullet, and as such there are more than 1000 security technologies companies in the world today, many of them with a single technology they believe is the solution to all your problems. Unfortunately, we all know that is not the answer.

Just like there are multiple pieces in a chess match, there are multiple technologies required to fully protect your endpoints. The traditional security options listed in Figure 2 like exposure prevention, pre-execution analytics, and file scanning are still necessary ingredients to block all the noise of traditional malware. Chet Wisniewski, Principal Research Scientist at Sophos like to say, "Burning down the haystack makes it a lot easier to find the needle."

Figure 2. The Evolution of Endpoint Security
From Anti-Malware to Anti-Exploit



Traditional Security			Advanced Security	
Exposure Prevention	Pre-Exec Analytics	File Scanning	Run-Time	Exploit Detection
URL Blocking Web/App/Dev Ctrl Download Rep	Generic Matching Heuristics Core Rules	Known Malware Malware Bits	Behavior Analytics Runtime Behavior	Technique Identification

That needle is likely to show up in the form of an advanced in-memory attack or exploit, which is why you need run-time detection and prevention as well as exploit detection in your endpoint solution. These advanced (and signature-less) prevention technologies look for exploit techniques and behaviors that will block unknown advanced attacks.

While we believe "defense in depth" is still a good strategy, the silver bullet of security is the integration of these technologies to work as a coordinated security system, one that's even more sophisticated than the advanced attacks targeting businesses these days.

Transforming endpoint protection with Sophos

To make real headway against today's threats, it is essential to invest in the most effective IT security solutions that can be put into use with the staff and expertise available. Sophos Next-Gen Endpoint Protection not only integrates a wide range of advanced security technologies. It is also intelligently designed and backed by world-class support to get them working in your organization.

Innovative Protection

Sophos combines the latest advanced threat defenses with proven anti-malware technology:

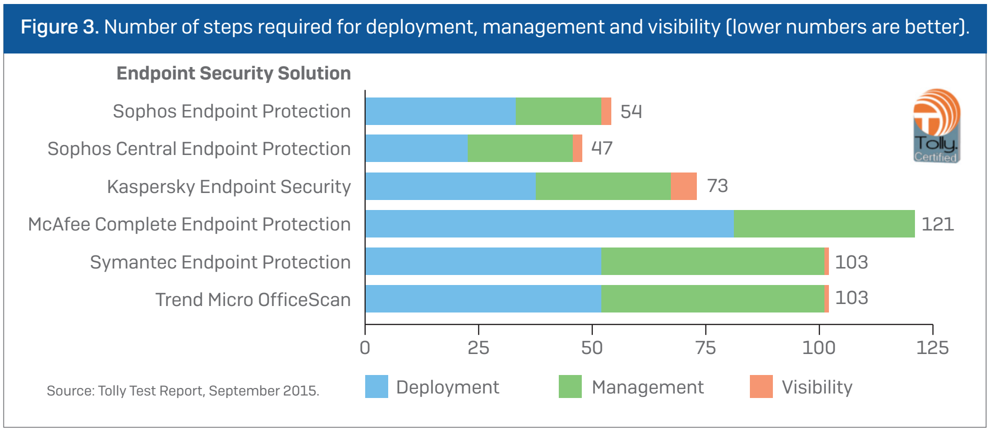
PREVENT		DETECT	RESPOND
Before It Reaches Device	Before It Runs on Device	Stop Running Threat	Investigate and Remove
Web Security Blocks malicious scripts and redirects used to deliver threats. **Download Reputation** Uses multiple variables to warn users about files that, although not confirmed malicious, may not be worthy of trust. **Web Control** Category-based web filtering enforced on and off the corporate network. **Device Control (e.g. USB)** Manages access to removable media and mobile devices and prevents data loss using prebuilt or custom rules. **Application Control** Point-and-click blocking of applications by category or name. **Browser Exploit Prevention** Identifies and blocks attempts to take advantage of exploits that could be used to compromise the web browser.	**Anti-Malware File Scanning** Actively runs on an endpoint to identify known malware and suspicious files, then prevents them from being launched. **Live Protection** Communicates in real time with SophosLabs to match signatures of suspicious files, query URL and download reputation and submit highly suspect files to the Labs for further sandbox analysis. **Pre-execution Behavior Analysis / HIPS** Leverages Sophos Behavioral Genotype Protection to block would-be malicious computer code before it is executed. **Potentially Unwanted Application (PUA) Blocking** Blocks programs that aren't necessarily malicious but that are generally considered unsuitable for most business networks. **Exploit Prevention** Identifies and blocks attempts to take advantage of application or operating system vulnerabilities.	**Runtime Behavior Analysis / HIPS** Dynamically analyzes the behavior of programs running on the system in order to detect and block activity that appears to be malicious. **Malicious Traffic Detection (MTD)** Identifies and alerts you in real time when malware tries to communicate with command and control servers. **CryptoGuard Ransomware Protection** Detects the malicious spontaneous encryption of files, stops the attack, and then rolls affected files back to their safe states.	**Automated Malware Removal** Removes malware from endpoints without admin interaction, only issuing an alert if manual attention is required. **Synchronized Security** Endpoints and firewall communicate using an advanced Security Heartbeat™ to accelerate threat discovery and automate incident response. **Root-Cause Analysis** Traces the history of an attack, from the application used to deliver the attack to the point where the attack was convicted. Also provides remediation advice and best practices guidance. **Sophos Clean** Deep forensic cleaning for advanced attacks exterminates malware including affected remnant files and registry keys.

Sophisticated Simplicity

To get these defenses working in your organization, they are designed with ease of configuration, deployment and management firmly in mind. Sensible default policies and point-and-click functionality help you quickly deploy protection, and an intuitive, easy to use dashboard provides great visibility of your environment and quick access to routine administrative tasks.

Independent usability testing by Tolly[4] confirms that Sophos is significantly easier to use than other endpoint security solutions (Figure 3).

Figure 3. Number of steps required for deployment, management and visibility (lower numbers are better).



Source: Tolly Test Report, September 2015.

Sophos Central Endpoint Protection was formerly known as Sophos Cloud Endpoint Protection.

Expert Support

No matter how usable a solution is, there will be times when outside help is needed. Sophos maintains a 100% in-sourced, global team of technical experts who are available 24 hours a day, seven days a week. Most importantly, the Sophos support team delivers consistently delivers high customer satisfaction scores to keep customers coming back if help is needed to take advantage of the additional security capabilities in Sophos Endpoint Protection.

> "Almost overnight, we went from minimal protection and poor support to a solution that's not only effective and easy to manage, but is backed by outstanding support."
>
> ROBERT TALLEY
> IT Director, Lassen County Office of Educaton

> "We had a Symantec product and I deployed Sophos in two hours to about 800 machines. Awesome!"
>
> STEVE
> Network Manager, Gaming Industry

Migrating to Sophos Next-Gen Endpoint – a five-step process

For most organizations, the most significant barrier to migrating to next-gen endpoint security is the perceived pain of switching. At Sophos we've worked with thousands of customers over the years to fine tune the migration process. In many cases, this process can be accomplished in a matter of hours or days.

1. Select and Install management console

Sophos offers both on premise and cloud-based management options.

- **Sophos Central** offers the fastest path to a fully operational management console. After activating a Sophos Central account, it can be setup and deployed in less than five minutes.
- For customers who prefer a traditional on premise management console, install and configure the **Sophos Enterprise Console** and any related management components.

2. Prepare Endpoint Deployment Package

The Sophos deployment package includes a competitive software removal tool that can be customized to completely remove the specific endpoint software being used in your environment. Following the removal of legacy endpoint security software, the Sophos Endpoint Protection installation package completes the deployment of the Sophos Endpoint Protection software. The process includes options for interactive or silent installation. The latter option makes the deployment process transparent to minimize the impact on your end users.

3. Configure Sophos Endpoint Protection Policies

Sophos Endpoint Protection includes a range of endpoint security capabilities, which may or may not be available in your legacy endpoint security solution. Start by configuring endpoint protection policies for any security capabilities that were enabled in your previous solution, like endpoint anti-virus.

You can choose to enable new security capabilities in Sophos Endpoint Protection, like malicious traffic detection, application control and web control, when you initially deploy Sophos Endpoint Protection or phase in these new security capabilities over time.

4. Start Rollout

A best practice for any new endpoint software rollout, including Sophos Endpoint Protection, is to start by deploying new software to a limited number of endpoints to test the deployment process and verify operation of the new endpoint security software. Select test endpoints that are easily accessible and being actively used to quickly test deployment and verify proper operation.

5. Complete Rollout Across Organization

After the initial test rollout, you are ready to complete the rollout of Sophos Endpoint Protection across your organization. For larger organizations, this can be further broken down into phases based on geography, organizational unit or another method appropriate to your organization.

Like any new technology deployment, there is some learning curve to come up to speed with Sophos Endpoint Protection. However, most find our solution so easy to use that the up-front time investment is paid back many times over with later savings on administration as well as with the ability to get more security capabilities working at the endpoint.

Conclusion

With cyber threats moving at a rapid pace, organizations must continue to seek ways to optimize their IT security investments. To avoid buyer's remorse and ensure you have the most effective solution for your organization, there are three key factors to consider when selecting an endpoint product:

1. **Protection** – does it give you the full breadth of security capabilities you need to prevent, detect, and respond to today's threats?
2. **Usability** – can you deploy and manage the solution successfully, given the staffing and skill levels of your IT security team?
3. **Support** – will you get high quality help whenever you need it from security experts?

For many organizations Sophos Next-Gen Endpoint has provided the path forward to get the protection, usability and support that they need. If you are not completely satisfied with your current vendor, perhaps it's time to join the thousands of customers that have switched to Sophos.

To learn more about Sophos Next-Gen Endpoint Protection or request a free trial, please visit **www.controlscan.com/security/advanced-endpoint-security**.

References

1. "Smarter, faster hackers cause huge spike in cyberattacks", USA Today, 15 April 2015.
2. 2015 Data Breach Investigations Report, Verizon Enterprise Solutions, April 2015.
3. 2015 Global Study on IT Security Spending & Investments, Ponemon Institute LLC, May 2015.
4. Tolly Test Report, September 2015.

ControlScan
Unified Security + Compliance
800.825.3301 x 2
controlscan.com

Oxford, UK

SOPHOS