O2 business

CYBERSECURITY EVOLVED:

THE SOPHOS BUSINESS IMPACT

Quantifying the real-life protection and efficiency benefits of the Sophos cybersecurity system via five customer case studies.

We're pleased to share this research report conducted and written by our partner, Sophos

A Sophos white paper July 2020

Telefónica

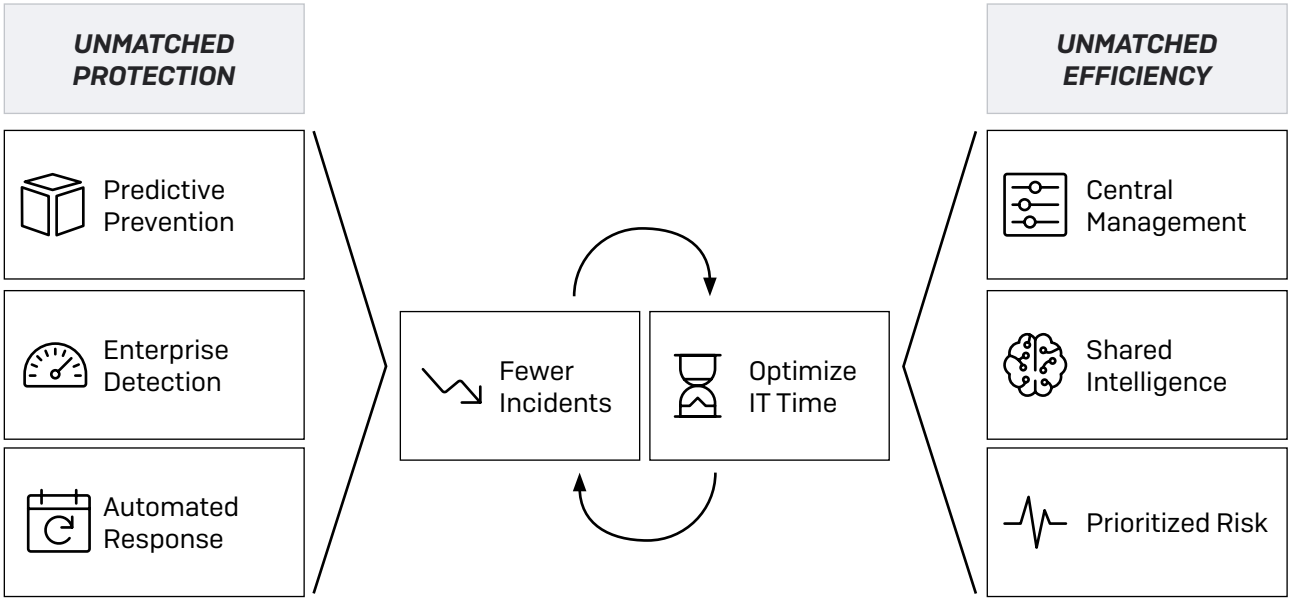
SOPHOS

Introduction

When you choose Sophos for your threat protection, you benefit from the world's first – and best – cybersecurity system:

- **Complete portfolio of next-gen products and services.** We can help with all your cybersecurity needs: endpoint, mobile, and server protection; EDR; next-gen firewall; email; unified endpoint management; and more. Whether you're running a full cloud, hybrid, or on-premises deployment, we've got you covered.
- **Unparalleled protection.** Benefit from both the very latest technology as well as the expertise of our world-renowned data science, threat hunting and SophosLabs teams. Enterprise-level detection blocks today's advanced attacks while AI-powered deep learning neural networks predictively stop never-before-seen threats. Sophos products also work together in real time to further elevate your protection. They share threat health and security information and respond automatically to incidents.
- **Single management platform.** Manage all your Sophos protection through Sophos Central, our cloud-based management platform. It uses shared intelligence to deliver prioritized risk information, while guided investigations give you recommended actions for each scenario.

The Sophos cybersecurity system **elevates your protection** while **lowering your total cost of ownership (TCO)**. It does this by creating a virtuous circle where unmatched protection and unmatched efficiency continually reinforce each other.



This virtuous circle enables you to significantly increase the efficiency of your IT team and reduce your exposure to threats – all without adding headcount.

Customer Impact

To measure that impact of the Sophos cybersecurity system in live customer environments, we interviewed five Sophos customers across North America, Europe, and Asia. Each customer scenario was different, with varying organizational structures, challenges, and business requirements. However, one major finding was common to all:

*Customers said that they would need to **double** their security headcount to maintain the same level of protection if they didn't have a Sophos next-gen cybersecurity system.*

They also told us that they experience fewer security incidents, and can identify and respond quicker to issues that do occur. Results from using Sophos include:

- 50% reduction in IT security headcount overhead
- 90%+ reduction in time spent on day-to-day cybersecurity administration
- 90%+ reduction in time to identify issues
- 85% reduction in the number of security incidents
- Significant reduction in the downtime on the overall organization

Customer A: Healthcare Provider, U.S.

- 4,500 employees
- 80 IT staff, of which three are dedicated to cybersecurity
- Sophos products: Intercept X Advanced with EDR, XG Firewall, Intercept X for Server Protection (Windows, Linux, and virtual machines)

Customer A is a regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.

Business impact

- **50% reduction in IT security resource requirements**
  The customer currently employs three dedicated cybersecurity heads. They calculated they would need to employ three additional full-time security analysts solely to cover incident response if they didn't use Sophos.

  Prior to Sophos, the team had to do a lot of manual work to identify what was happening on their network and a significant part of their time was spent identifying incidents. Sophos now proactively identifies the issues for them and automatically resolves the situation in 95% of cases. As a result, the team can focus on remediation for the 5% of issues that need human involvement.

- **90%+ reduction in day-to-day security administration**
  The IT security manager spends 30 minutes each day reviewing logs and investigating anything of concern. Prior to Sophos, it used to take him an entire day to get the same level of information and confidence. With Sophos, all data is consolidated in a single management platform and presented in a consistent format, making it easy to identify and respond to issues. This removes the onerous daily task of mapping data across multiple sources to try to identify suspicious vs. malicious vs. benign.

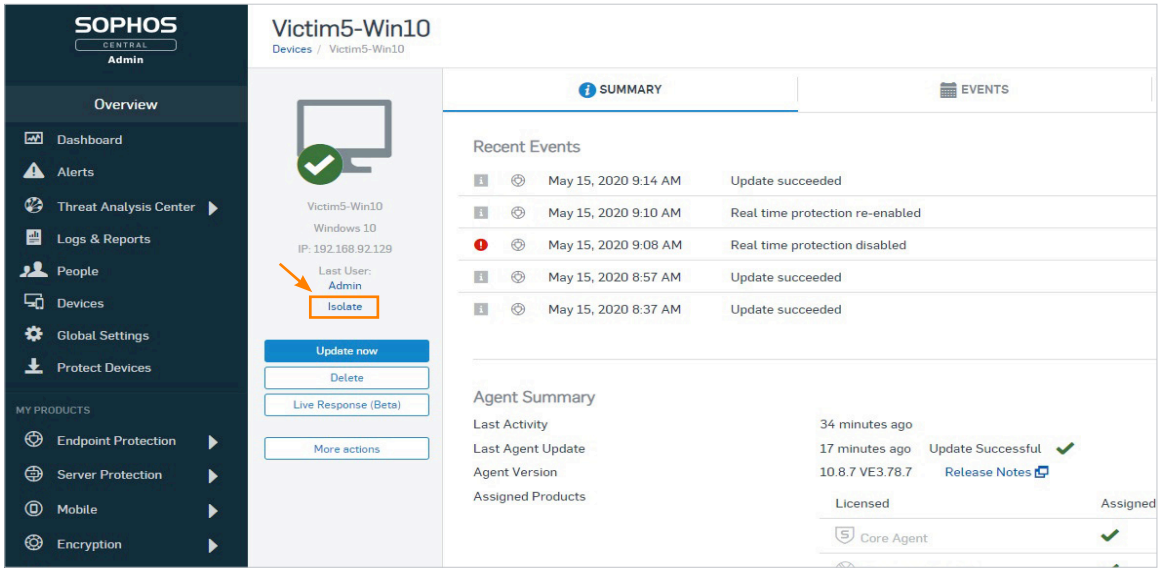
- **85% reduction in security incidents**
  As a hospital they hold large quantities of sensitive Personally Identifiable Information (PII), as well as payment information, making them a target for cybercriminals. Prior to Sophos, they experienced on average three incidents each day that were worthy of further investigation. With Sophos this has dropped to an average of one every three days.

- **90%+ reduction in time to investigate an incident**
  Prior to Sophos, conducting a thorough investigation into an incident would take around three hours, which included getting local access to the affected computer. Now it takes a maximum of 15 minutes with everything done remotely via the Sophos Central platform.

  Previously the team would need to disable the network adapter and then physically get to the device to investigate and resolve the issue before manually reconnecting. They would also need to accommodate their users' workflows; for example, waiting until a doctor wasn't treating a patient before gaining access to that system for remediation. The ability to isolate the device via the Sophos Central console enables the team to investigate the issue remotely without impacting user and system availability.

  The reduced investigation time and ability to manage everything remotely also significantly reduces disruption to other users within the hospital.

- **Continuous protection during investigations**
  Previously devices would be removed from the network for manual investigation and wouldn't get protection updates while they were offline. With Sophos, when the IT team isolates a device to investigate an issue it remains online and continues to receive protection updates.



Customer B: Education Services Provider, India

- 700 employees
- Head office in Bangalore, plus local managers on site across India and the wider Southeast Asia region
- Sophos products: Intercept X Advanced with EDR, Intercept X Advanced for Server, XG Firewall

Customer B provides educational services to colleges and universities across India and the wider Southeast Asia area. They secure tens of thousands of students via a centralized IT team based out of their head office in Bangalore, together with a team of local IT managers on site.

Business impact

- **50% reduction in resource required for day-to-day security management**
  Previously, they employed four engineers to manage day-to-day security. Since moving to Sophos, they have only needed two engineers to cover security across the company.
- **94% reduction in time to identify high-risk areas that require investigation**
  Prior to Sophos it took the customer three to four hours to identify critical issues they needed to focus on for further investigation. Now it takes just ten to fifteen minutes, to identify the security priorities across the organization in Sophos Central.
- **98% reduction in time to identify the source of bad traffic on the network**
  The previous network security implementation would take two days (and sometimes longer) to identify which device on the network was causing performance or security issues. Now it takes just 15 minutes to pinpoint the issue and start addressing it.
- **95% reduction in time spent managing firmware updates**
  The previous network security implementation also created availability and risk issues as each software update would take between three and four hours. Now, with Sophos, it takes just ten minutes per update. With 20 to 25 updates a year, this equates to a savings of 75 hours a year for updates (the equivalent of two full working weeks).

Customer C: Clinical Trials Provider, U.S.

- 150 employees across four locations
- Two IT staff, covering all areas including cybersecurity
- Sophos products: Intercept X Advanced with EDR, XG Firewall, Central Device Encryption

Customer C is a private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications. Due to the nature of their business, they hold large amounts of sensitive personal information.

Business impact

- **50% reduction in IT resource requirements**
  This customer has a small team of just two people to manage all aspects of IT. Currently they spend one hour a day reviewing logs and investigating anything of concern. If they moved away from Sophos they advise that they would need to hire one or two more security engineers just to manage the logs.

- **33% reduction in time to deal with a potential issue**
  Previously, when they had a security issue with a device, their solution was to reimage the machine, which took between 90 minutes and two hours. Now they can conduct a deep investigation from system isolation and thorough threat hunting to full security scan and final remediation in approximately one hour with no reimaging. An additional benefit they are realizing with the Sophos approach is that the user can start being productive as soon as the investigation is over, whereas with reimaging they would also lose time resetting configuration and customizations on their machine.
- **88% reduction in threat risk as they can identify issues much faster**
  With the Sophos cybersecurity system, the IT team can identify new issues that need to be investigated within minutes of a suspicious event arriving. Prior to Sophos, it took a full day to go through the logs to find the issues that needed investigation. This reduction in response time significantly reduces threat exposure.
- **Improved user behavior**
  With Sophos, users now know the IT team can quickly address issues and incidents without causing them downtime or extra work. As a result, the IT team reports users are now far more willing to report issues or concerns (e.g. they clicked on a potentially malicious link in an email).

Customer D: Public Service Provider, Serbia

- 300 employees
- 10 IT staff, of which four are focused on cybersecurity
- Sophos products: Intercept X Advanced, Intercept X Advanced for Server, XG Firewall, Sophos Email, Sophos Mobile

Customer D is a public sector organization that covers the Serbian capital Belgrade. This long-term Sophos customer has migrated to our next-generation products that are managed through Sophos Central.

Business impact

- **50% reduction in time spent on day-to-day security management**
  They now spend 30 minutes a day on security administration, reviewing the alerts, logs, users, devices, traffic, and applications in the Sophos Central management console, to make sure everything is okay. This day-to-day management of security was previously taking at least twice as long to determine high-priority issues to address, and what actions to take.
- **90%+ reduction in time spent on day-to-day security management vs. other vendors**
  The customer estimates that, based on prior experience, day-to-day security management would take a full day with other vendors, compared to just 30 minutes with Sophos.
- **Zero major security incidents**
  The customer has been using Sophos for many years and has not had a major security issue in the last 8-10 years. That's not to say that they don't get threats; rather their Sophos products resolve them quickly and quietly in the background without the user being aware.

Customer E: Regulatory Approval Body, Slovenia

- 150 employees, of which one third work remotely and two thirds are based in the head office
- Two IT staff, covering all areas including cybersecurity, plus external provider support for major projects
- Sophos products: Sophos Endpoint Protection, Intercept X Advanced for Server, XG Firewall, Sophos Mobile, Sophos Device Encryption

Customer E is a public sector organization responsible for ensuring products meet required standards. This long-term Sophos customer has migrated to our next-generation products that are managed through Sophos Central.

Business impact

- **50% reduction in time spent on day-to-day security management**
  They spend 15-30 minutes each day on security administration: checking the firewall, looking at alerts, cleaning up the email quarantine etc. Previously, they would have spent at least twice as long. This increased efficiency is a result of being able to manage all their security products in one place, and not needing to switch between applications and servers.
- **Zero major security incidents**
  The customer cannot remember a single major security incident since using Sophos.

Conclusion

As the customer testimonies demonstrate, Sophos' approach to cybersecurity delivers real protection and efficiency savings. It enables you to significantly increase the efficiency of your IT team and reduce your exposure to threats – all without adding headcount.

While our customers' business environments, resources, and challenges vary from organization to organization, they consistently report a 50% reduction in IT security workload from running a Sophos cybersecurity system. Customers enjoy a 90%+ reduction in time spent on day-to-day cybersecurity administration, as well as an 85% reduction in the number of security incidents.

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

200612 WPEN (NP)

SOPHOS

O2 business

Telefónica

SOPHOS

Published in June 2020. All information is correct at time of publication. Telefónica UK Limited Registered in England no.1743099.
Registered Office: 260 Bath Road, Slough, SL1 4DX