

SOPHOS

Security made simple.



Simple Security Is Better Security

How small and medium-sized businesses can benefit from cloud-based security

By **Tsailing Merrem**, Senior Product Marketing Manager

Most vendors seem to assume that small and medium-sized businesses (SMBs or SMEs) have the expertise and full-time staff of a large enterprise to manage IT security. Too often for SMBs, this one-size-fits-all approach results in higher costs, lower productivity and more risk.

In this paper we examine the inherent complexity of enterprise-class security products and the very different needs of SMBs. Then we look at a simpler alternative: cloud-based endpoint security.

Complexity in IT security

It's no secret in the IT security community that SMBs are poorly served by the industry's flagship vendors and products. The big companies that dominate the market design their offerings for enterprise customers with well-staffed IT organizations and dedicated security teams.

Unfortunately, a product that perfectly meets the needs of a trained security professional can potentially have the opposite effect and increase the vulnerability of a small business where security administration is handled by an IT generalist—or the business users themselves.

One source of complexity in IT security products is historical. The largest vendors built out their portfolios through decades of acquisition, folding one product into another. The result is a hodgepodge of technologies managed by a shared console, bringing all the coordination and configuration challenges to one busy interface.

A second root of complexity is vendor bias to the skilled user. A security specialist with a large environment to protect may prefer to have granular control of every feature, capability and configuration setting. But for the SMB administrator, this can be a recipe for information overload and paralysis.

Making simple products that small businesses can use is costly, which is why most vendors merely repackage their enterprise offering for the SMB market.

Small businesses are a big target

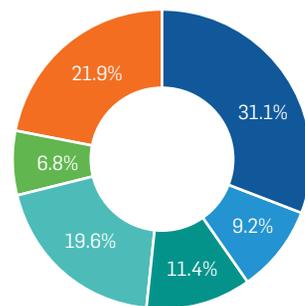
Even if vendors seem to ignore the needs of small businesses, SMBs present a huge opportunity for cybercriminals. Out of the nearly six million employers in the United States,¹ the vast majority of them have fewer than 100 employees. According to the 2013 Verizon Data Breach Report, 40% of 621 data theft incidents confirmed in 2012 affected organizations with fewer than 1,000 employees.²

Recent studies point to less rigorous security at smaller firms. In a Sophos-sponsored Ponemon Institute survey of IT managers at small to mid-sized companies, the average self-assessment score of security posture (ability to mitigate risks, vulnerabilities and attacks) was a 6 on a scale of 10. Respondents reported, on average, fewer than three full-time workers fully dedicated to IT security. And respondents reported a wide range of challenges including insufficient budgets, personnel and in-house expertise.

You might think this would present large security vendors with a huge market opportunity. But most vendors find that selling to large customers is easier and more profitable.

1. <http://www.census.gov/econ/smallbus.html>
2. <http://www.verizonenterprise.com/DBIR/2013/>

Data Breaches by Company Size



Company size	# of data breaches
1-100	193
101-1,000	57
1,001-10,000	71
10,001-100,000	122
More than 100,000	42
Unknown	136
Total data breaches:	621

Source: Verizon

The cost of complexity

Small organizations that deploy enterprise-grade security products without the specialists necessary to manage them are exposed to a wide range of risks and costs.

- An IT generalist may struggle to manually configure a host intrusion prevention system (HIPS) with hundreds of rules, deciding instead to turn off most of the product's functionality. Only 10% of businesses use all the security features and functions they pay for.
- An improperly configured firewall or IPS can leave open security holes, or generate false positives and lock down users. That hurts the productivity of IT personnel and the organization at large.
- Different web security policies on network and endpoint filters can create interference and confusion, slowing or locking down legitimate traffic.
- Third-party integration services and maintenance contracts can dramatically increase security costs.
- Keeping IT generalists trained on complex security solutions often requires annual, multi-day courses, adding to costs and taking the IT person away from the office.

None of this is inevitable or unavoidable. IT security products aren't complicated because it's impossible to make them user-friendly for non-specialists. It simply requires that vendors build some of the specialist's knowledge and experience into the products themselves.

Sophos simplicity helps MSQ Partners slash security admin costs

"Previously we worked long hours every day, trying to manage a number of different solutions across the world. It was difficult to get to the root of the challenges we faced. With Sophos, it takes just two days a month."

GORDON O'BRIEN
Group IT Manager, MSQ Partners

How the cloud can simplify security

The growing movement to cloud-based, cloud-managed security-as-a-service gives you an opportunity to improve user experience, reduce complexity and enhance security. Today's cloud-based IT security solutions are perfect for SMBs because they're easy to install, configure and manage, and should provide automatic, real-time protection from most threats.

Cloud-based security products could easily offer simple features such as:

- **Unified security management** – knowledgeable workers use multiple devices to get their work done. Effective security solutions should provide unified management that protects Windows, Mac and mobile devices
- **User-centric management, reporting and licensing** – Secure your end users regardless of which devices they use. User-based policy is set once and will automatically be enforced across devices. IT admins also get a single pane of glass view of the security status of the organization and can drill down per-user or per-device
- **Pre-configured settings** – IT security suites can be preconfigured to simplify set-up of features like HIPS, web security and web filtering that previously required specialized skills to deploy and manage
- **Built-in web security filtering** – Since 90% of attacks come from the web, Sophos has incorporated web security filtering into every security product. Access to malicious or infected websites is automatically blocked and malicious files are intercepted before they infect your organization.
- **Coordinated web content filtering policy** – Cloud-managed and endpoint-enforced web filtering capabilities offer consistent protection and policy enforcement no matter where users log on. When a remote user opens an Internet connection, the PC security client automatically enforces content and connection policies with no need to backhaul traffic. The predefined policy lets you easily set policies to address security and compliance requirements. Once set, it automatically works on both Windows and Mac. You can also set time-based policies to limit non-business web browsing during business hours.
- **Quick deployment and maintenance-free, with no server to set up.** Cloud-based security services are easy and quick to set up. With no server to install, deployment takes just a few minutes. It's simple to manage and maintenance-free with automatic software upgrades and threat updates, and real-time policy refreshes.

Sophos Cloud allows a single IT resource to manage 17 government departments effectively.

"Sophos Cloud is a perfect fit for me, as a one-person IT shop. It's the easiest antivirus solution I've ever deployed."

JOEL ROHNE
IT/GIS Director, Worth County



Sophos Cloud

With our latest release, Sophos Cloud is the only integrated security solution for Windows, Mac and mobile devices. It's ideal for organizations of all sizes, but specifically SMBs that may have limited resources, remote locations and roaming workers. Sophos Cloud provides complete coverage everywhere and deploys instantly to deliver complete endpoint protection, web filtering and mobile device management without complexity.

It is effortless to deploy, manage and maintain and gives you the following benefits:

- A cloud-based management console hosted by Sophos, so there's no server to install
- Built-in best practices to optimize protection and minimize effort
- Industry-first user-based management and reporting that follows users across systems, providing a single pane of glass view for admins
- A clean, intuitive management dashboard that provides insight into actionable events to streamline administration
- Automatic upgrades and updates and unlimited scalability

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs—a global network of threat intelligence centers. Read more at www.sophos.com/products.

Sophos Cloud

Visit Sophos.com/cloud for a 30-day free trial

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