SOPHOS
Security made simple.

Enhancing Office 365 Security – What You Need to Know

The attraction of Office 365 is clear. Why set up your own Exchange Server, or manage and maintain Office software, when Microsoft can take care of it all for you?

Consider, however that when you hosted your Microsoft infrastructure in your own datacenter, you supplemented it with security technology from other suppliers to reduce the risks of malware threats and guard against service outages. These risks haven't disappeared in your new cloud and Office 365 world.

This paper discusses why businesses are making the switch to Office 365 and examines some of the key IT security challenges that arise in doing so. It then looks at the critical security technologies that businesses should have in place alongside their Office 365 deployment.

Adoption of Office 365 is growing fast

Uptake of Office 365 continues at a rapid pace. A recent Gartner report (ref: Implementing Office 365: Gartner Survey Results and Analysis, 2016 Published: 4 May 2016), estimated that 78% of enterprises use, or plan to use Office 365 within the next six months, up 13% from a previous survey taken in 2014.

It's easy to see why Office 365 is an attractive proposition for businesses of all sizes. It gives them access to the de-facto standard in communication and collaboration tools without any of the up-front or ongoing maintenance costs of managing the hardware and software required to run these services in-house. Deploying Office 365 means no upgrades, new servers, or additional on-site security systems to protect this infrastructure when new cyber-attacks threaten. It's easy to decrease your usage by turning off redundant accounts or provide staff with new accounts as your business grows.

Effectively, you are outsourcing the responsibility of the maintenance of your Exchange servers and business applications to Microsoft. This, in turn, reduces the workload of your IT staff and frees up time for them to work on other IT projects.

Concerns around Office 365 security remain

While Office 365 is a fantastic tool for business productivity and Microsoft provides robust security for customer data held in the cloud, there are many more security factors to consider. In fact Gartner suggests that today 40% of Office 365 users are securing their deployment with third party security solutions to fill the gaps in security. Your users, workstations, servers, and data outside of the cloud all need additional security. There are a number of areas that need to be considered:

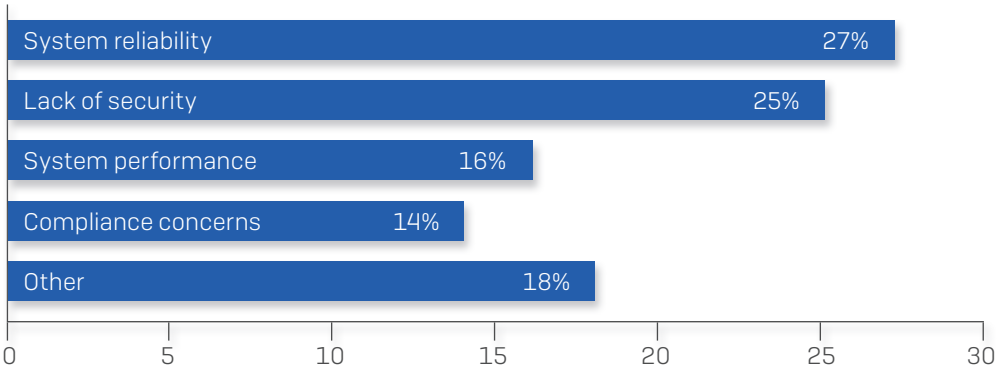
Firewall and Web Security: Office 365 doesn't provide a secure web gateway to protect and control end user internet access or a firewall to secure the organization perimeter.

Email Security and Continuity: Although Microsoft offers add-on subscriptions to deliver Email Security features many customers report issues with spam and malware getting through and as a result prefer to put their security in the hands of security specialists. And recent and fairly frequent Office 365 outages have meant that email continuity services are required, for example Email Spooling and Emergency Inbox for users to access mail when the service is down. Microsoft Exchange Online (included in the E1, E3 and E5 Office 365 plans) doesn't provide the critical email continuity features you may have deployed on your premises.

Next-Gen Endpoint Security: Office 365 doesn't provide defenses on endpoint devices against dangerous malware threats such as ransomware.

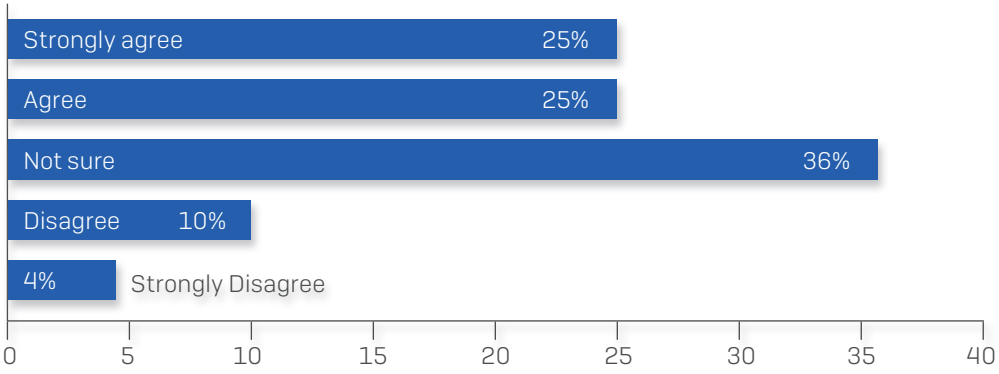
These concerns are being felt by organizations out in the real world. Recent Sophos surveys identified 'system reliability' and 'lack of security' as the biggest concerns for organizations using Office 365 as their email platform.

What are your biggest concerns with using Office 365 as your email platform?



And 50% of respondents agreed or strongly agreed that third-party security solutions are essential to extend inadequate Office 365 security.

Third-party security solutions are essential to extend inadequate Office 365 security



So it comes as no surprise that most organizations are choosing to supplement their Office 365 implementation with security and continuity solutions from other vendors. In fact, the same Gartner report (ref: Implementing Office 365: Gartner Survey Results and Analysis, 2016 Published: 4 May 2016), states that when asked to explain the main reason your organization does not use and has not considered using Office 365, 23% cited legal or business concerns about information security.

Email continuity

Email is a critical business application in the vast majority of organizations and is also the top reason that businesses are adopting Office 365. The recent survey by Gartner (Implementing Office 365: Gartner Survey Results and Analysis, 2016 Published: 4 May 2016), states that 70% of respondents ranked Exchange Online in the top three most important Office 365 capabilities to use.

Office 365 is generally reliable providing a 99.9% SLA, but just 0.1% of downtime translates into more than 8¾ hours per year. Furthermore, Osterman (Microsoft® Office 365® for the Enterprise: How to Strengthen Security, Compliance and Control Published March 2014) research has calculated that:

"For the typical organization, the cost of user productivity loss during email outages is 20 cents per user per minute. This means that a single, 30-minute outage for a 500-seat organization will be $3,000."

Microsoft will credit 100% of your monthly fee if uptime falls below 95%. But using Osterman's figures, 5% downtime will cost a 500 user business $216,000 in one month – well in excess of the subscription cost.

And outages do happen. There have been some well publicized recent news stories where Office 365 outages cased problems both in the United States (http://www.theregister.co.uk/2016/06/30/office_365_down_in_nyc/) and in Europe (http://www.computing.co.uk/ctg/news/2447946/office-365-suffers-global-outage-due-to-high-resource-utilisation)

Complementing Office 365 with cloud security

As covered earlier the benefits of shifting to the cloud are numerous – no upgrades, no new servers, no maintenance and significant savings in management man hours. So it makes sense to look for a security solution that offers the same benefits. Here's a quick overview of the key features every cloud security solution complementing Office 365 needs:

1. Simple cloud-based management

Office 365 makes management easy – so should your security solution.

How many dashboards do you look at today? When choosing a security solution make sure that you can manage everything through a single pane of glass and save yourself significant amounts of time.

2. Integrated security for superior protection

Office 365 provides a full suite of interconnected functionality – so should your security solution.

Look for security solutions that share relevant information in order to make faster, more accurate decisions that provide better security. For example, are your files kept secure when moving from the cloud to your mobile and endpoint devices? Are compromised devices automatically isolated and their privileges revoked (e.g. removing encryption keys and network access)?

Additionally, there's a critical shortage of IT specialists in the security field. In fact, according to a recent Enterprise Strategy Group report, "...46% of organizations now claim they have a problematic shortage of cybersecurity skills... up significantly from last year 28%." Source: ESG Research Blog, High-Demand Cybersecurity Skill Sets, May, 2016

By choosing an integrated, easy-to-use system you're bypassing the issue.

3. Business email continuity

As covered earlier, the financial impact of email downtime is significant. You need a solution that will keep your email flowing if Office 365 goes down. Email spooling and an emergency inbox so employees can continue to access their email during an outage are critical features for every security solution. On-top of this look for powerful antivirus, anti-spam and anti-phishing protection.

Introducing Sophos Central

Sophos Central is a cloud-managed platform that brings all of your security needs together into one easy to use package. It delivers advanced protection right across your corporate network – for endpoints, mobile devices, web, email, WiFi, encryption, server and network. And best of all it's simple to use.

As a cloud-solution you don't need upgrades, new servers, or maintenance and you benefit from significant savings in management man hours. Plus it's delivered by a proven leader in IT security.

Get simple cloud-based management

Sophos Central uses a 'single pane of glass' for management, meaning you can access all of your security solutions in one place. For example, while managing your email gateway you'll get automatic alerts if a mobile device is compromised, there's no need to check each solution in turn.

Get better protection with synchronized security

Solutions in Sophos Central benefit from synchronized security, which shares contextual information to provide better security. For example a compromised endpoint device can be automatically isolated from the wider corporate network. The same device will have its encryption keys automatically revoked so that it can't access encrypted files.

Get critical email continuity and security

Sophos Email (in Sophos Central) complements Office 365 providing email spooling and an emergency inbox, so if Office 365 goes down, your email stays up. It also provides advanced antivirus, anti-spam, and anti-phishing defenses to secure against the latest malware attacks, phishing campaigns, and infected websites.

Summary

Office 365 is a fantastic tool for business productivity. While this is attractive, moving to Office 365 does not solve all your security or email availability challenges.

Supplementing your Microsoft infrastructure with technology from other suppliers made sense when you managed your own environment. The risks of security threats and email outages remain in your new cloud and Office 365 world. For many organizations, it still makes sense to bolster your Office 365 service with additional, cloud-delivered, threat protection and business continuity solutions.

Furthermore, as you've seen the benefit of moving your Microsoft business applications and communication and collaboration infrastructure to the cloud, it makes a lot of sense to consider delivering and managing all your security from the cloud. Choosing a solution that allows you to manage your email security alongside your endpoints, servers, web gateway and mobile security infrastructure saves you time and makes managing your security and budget easy.

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

2016-09-20 WP-NA (NP)

SOPHOS