MPS
WHITE PAPER

ADVANCED EMAIL SECURITY PROTECTION for OFFICE 365: WHAT YOUR COMPANY NEEDS TO KNOW

Many companies around the globe continue their rapid migration to the cloud. According to the Bitglass study in 2018, **global cloud adoption reached an all-time high of 81%**, as measured by enterprise use of major cloud productivity platforms, such as Microsoft Office 365 and G Suite. Using cloud Apps has become a common practice for many companies that wish to remain competitive and increase productivity.

However as long as many companies use this cloud APPS, with more and more users, it will draw more and more attackers, and for that reason more susceptible they are to be targeted has a flag of risk, because a user account might have been compromised. That's why it's important for companies to think about how to protect their email against today's advanced email threats.

Transitioning to the cloud, and particularly to a service that is constantly under threats due to its very large footprint, means involving a plan to upgrade your email security level. The last thing your company wants is to leave your account vulnerable and at risk of a data breach. According to the study of Ponemon Institute's, "2018 Cost of a Data Breach Study", **the average cost of a data breach globally is $3.86 million dollars**.

To minimize the potential of a compromised account, your company need to learn how to prioritize threats and strategize how to implement features and controls. While Office 365 comes with standard built-in data protection, you may find they're not enough to secure the platform from the most advanced threats, and you will need to find added layers of security that Microsoft is not able to offer with their standard product.

anubisnetworks™
a BITSIGHT company

1. Cybersecurity On The Rise

Fortunately, companies are becoming increasingly mature in terms of security knowledge - they are realizing that if they need to pay more to have the protection they need, they might as well use different, dedicated email security solutions instead of being limited to one vendor and one-dimensional approach for spam and virus filtering.

This will mean that the speed and breadth of the filters are complemented with another source to be sure that the latest threats are not missed.

The conclusions are simple: suspect the vendors with multiple products offering you different levels of protection, and if you need a dedicated Email Security Gateway on top of your standard filtering, pick one from a different vendor.

Companies must be aware that public clouds tend to be more secure, but Office 365 has become for hackers a major target for attacks, which means they need an advanced email security protection for Office 365.

2. Why Does Your Company Need an Advanced Email Security Protection for Office 365?

In a moment where cyber threats are reaching sophistication and spreading peaks, selling standard products that protect you “more or less” just will not protect your company against the most advanced threats. Often the more valuable protection is being sold on top of a product at a premium price, which is simply deceiving.

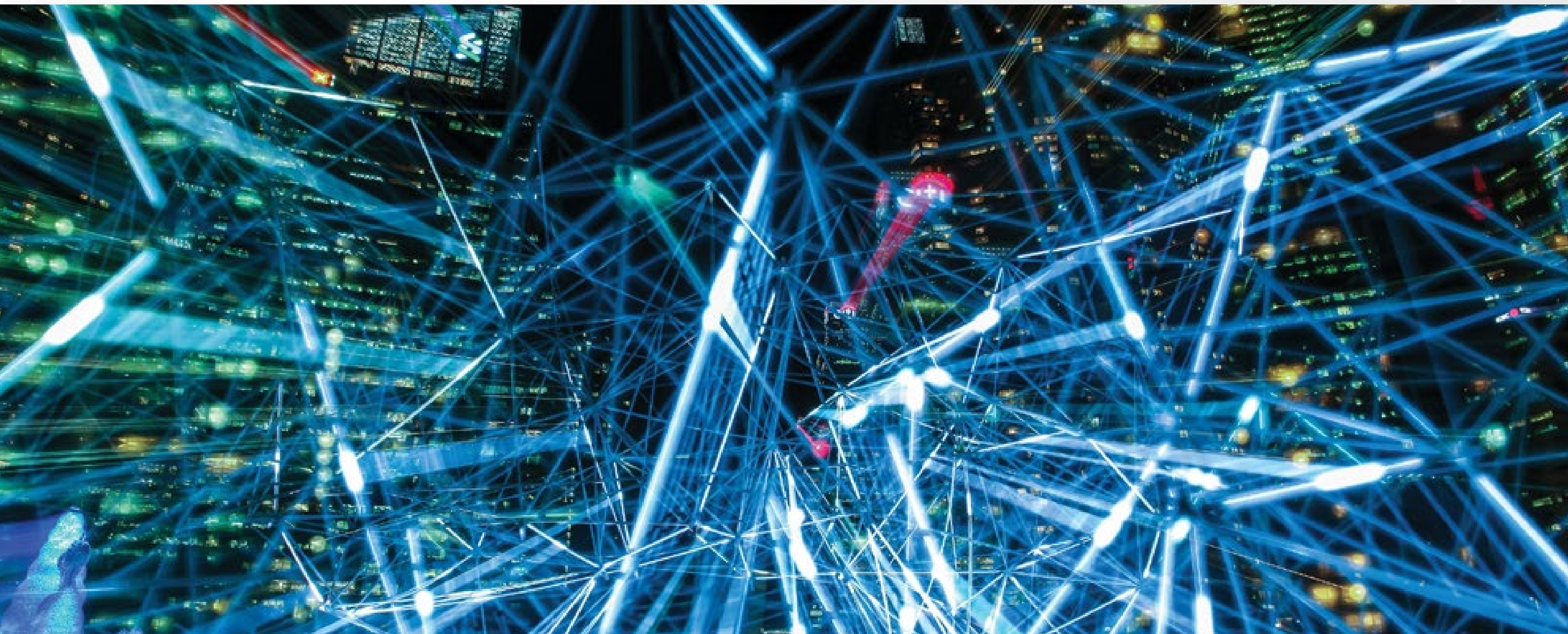
The cybersecurity market works basically like any other IT industry and segment: vendors have basic products or services to protect your company, but will then offer you their best products at a higher price. There is nothing wrong with this approach - especially if the vendor is targeting low budget customers. What needs to be clear, from the start, is **how basic the baseline offer may be for your company**, keeping in mind the sophisticated threats that your company will (surely) have to face.

Keep in mind that your company should stay away from simplified email security solutions because according to Verizon's 2018 Breach Investigations report: **92% of malware is still delivered by email and email continues to be the most common vector (96%)**. Also, **Phishing and pretexting represent 98% of social incidents and 93% of breaches.**

3. The Security and Control Layer on Top of MS Office 365

Most companies have transitioned some of their software tools and systems to the Cloud. In the past, this was valid for the server-like systems, such as storage or security, and some company-wide software suites such as Salesforce or Dynamics CRM.

What has been happening in the last few years is that companies have also transitioned the users' endpoint productivity tools, such as Microsoft Office, to the cloud. This has happened for several reasons: the load off the IT systems, the BYOD policies, and the higher internet.



4. Why Does Your Company Need a Multi-Layered Approach to Mitigate Office 365 attacks?

Platform-as-a-service solutions, especially Microsoft Office 365, are very successful because of the ability to aggregate a very large set of software products in the cloud. In the same “space”, users and organizations (especially SMBs) have the productivity suite, communication tools (emails, instant message), specialized software, and many other important functions such as synchronized calendars and contacts. All these being device agnostic without the need for local storage.

These tools serve a plethora of products to all kind of users and companies, providing a simple and clean experience in what is a very complex system. The issue is that its convergence means a lack of specialization. For this very reason, there is not a concern with very specific security features, much less with the customization of the case-by-case, business-to-business necessities of more advanced organizations.

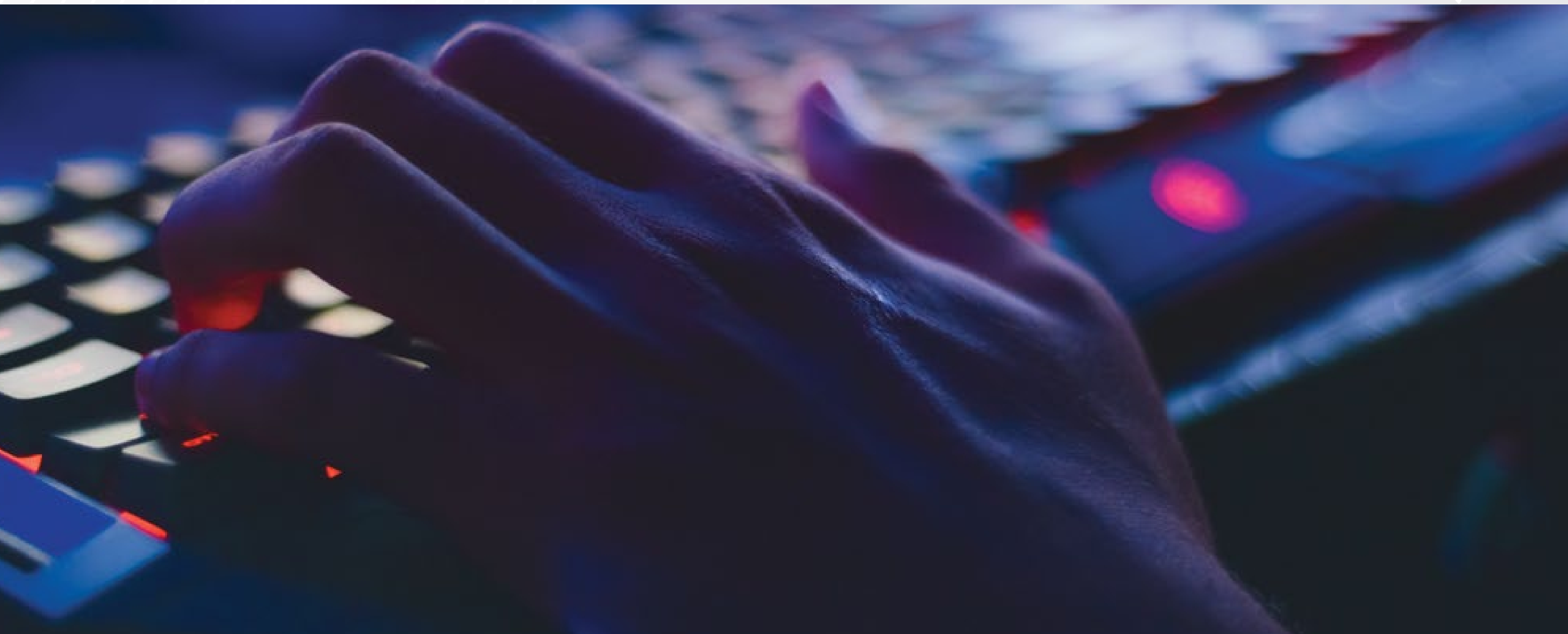
As long as more companies make more use of Office 365 in the cloud, the Microsoft platform is susceptible to see increasing attacks from hackers. Which means that companies really need a multi-layered approach to security.

Microsoft Office 365 does allow for some security management, but for adequate security, organizations need to upgrade their Office 365 with a dedicated Email Security system, ATP, previously EOP or Forefront, and even with this upgrade product, some modules still need to be obtained separately.

What we are seeing in the market is that the most concerned companies are looking for specific solutions from email cybersecurity companies that can integrate different email security with these solutions.

Overall, the advantages efficient and effective security as well as the ability to manage and customize their one system, have visibility over the email traffic, ensure the email deliverability is fail-safe, and keep filtering independent of storage (like in Microsoft Exchange).

While there are some great products on these platforms, it is best to avoid over-relying on systems where IT cannot have sufficient visibility and control. This capability will significantly improve protection and control against today’s advanced email threats.



5. Top Email Security Best Practices for Office 365

Transitioning to a service that is constantly under threat due to its very large footprint means involving a plan to upgrade your company email security level. The last thing you want is to leave your company account vulnerable and at risk of a data breach.

To minimize the potential of a compromised account, you need to learn how to prioritize threats and strategize how to implement features and controls. While Office 365 comes with standard built-in data protection, you may find they're not enough to secure the platform from current threats, and you will need to find added layers of security that Microsoft is not able to offer with their standard product.

From assessing the risk of implementing security and compliance controls for upgrading your email security level, here are the top email security best practices for Office 365:

Turn On Mailbox Auditing in Office 365
You need visibility into user activities to help you gain control over business-critical data: you can log mailbox access by mailbox owners, delegates, and administrators. You can now find out who logs into user mailboxes, sends messages, and other activities.

Enforce Strong Password Policies
Administrators should put strict password creation policies in place. Experts agree that a secure password should consist of no less than six characters and should be a combination of letters, numbers, and symbols. They should also be case-sensitive. Avoid any of the most-used or predictable passwords such as your birthday or pet's name.

Enable Multi-Factor Authentication
Multi-factor authentication (MFA) gives you an extra layer of defense by complementing a robust password strategy with additional acknowledgment via text message, phone call, or an app notification.

Secure Email Content with Multiple Antivirus Engines
To increase detection and prevent threats, use other products that ensure you multiple antivirus engines, for instance using endpoint systems or email gateways.

Enable Alerts Through Office 365 Cloud App Security
Enable alerts to monitor suspicious activity such as repeated failed sign-in attempts, unusually large data downloads, or sign-ins from unknown IP addresses. Because you're alerted of anomalous activity, you can quickly act on it before it's too late.

6. Complement Office 365 with Additional Dedicated, Email security

Office 365 does not offer advanced and targeted threat protection to protect your company against the latest advanced email security threats. Your company needs a better protection with an added layer of security, to tackle the risk against ransomware, spam, business email compromise (BEC), spoofing, and phishing.

An added layer of security, preferably using distinct technologies (AntiVirus, Sandbox, Reputation Blocklists) and with added visibility on all the filtering and managing aspects of such a critical infrastructure is a very common approach for businesses with some dimension, which need to guarantee all bad email (Phishing, Malware) is kept out of their employees mailboxes, as well as ensuring control protection for data leakage.

AnubisNetworks Mail Protection Service (MPS) integrates seamlessly with Office 365, delivering a security ecosystem that permanently monitors the world for botnets, IP reputation, email phishing, and malware campaigns. It allows you to set Anti-Botnet, Email Routing, and Control features and communicates with all MPS edge filters, delivering real-time proactive malware prevention. And to maintain your network reputation, it ensures the only legitimate email is received and provided.

To see exactly how to protect your Microsoft Office 365 users from sophisticated email attacks, get started right away with a free trial. The next step is yours!

References

https://pages.bitglass.com/FY18BR-CloudAdoption_LP.html
https://www.tripwire.com/state-of-security/featured/average-cost-data-breach-exceeds-3-8-million-claims-report/
https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
https://www.computerweekly.com/news/252445440/Ramp-up-security-to-mitigate-Office-365-attacks

FOLLOW US

- facebook.com/anubisnetworks
- twitter.com/anubisnetworks
- linkedin.com/company/anubisnetworks
- youtube.com/anubisnetworks

LISBON

Address
Centro Empresarial e Comercial Espaço 7 Rios
Escritório 50 (0.04), Piso -1
Rua de Campolide, Nº 351
1070-034 Lisbon, Portugal
Phone: +351 217 252 110

BOSTON

Address
111 Huntington Ave
Suite 2010
Boston, MA 02199
USA
Phone: +1 617 245 0469

www.anubisnetworks.com
info@anubisnetworks.com