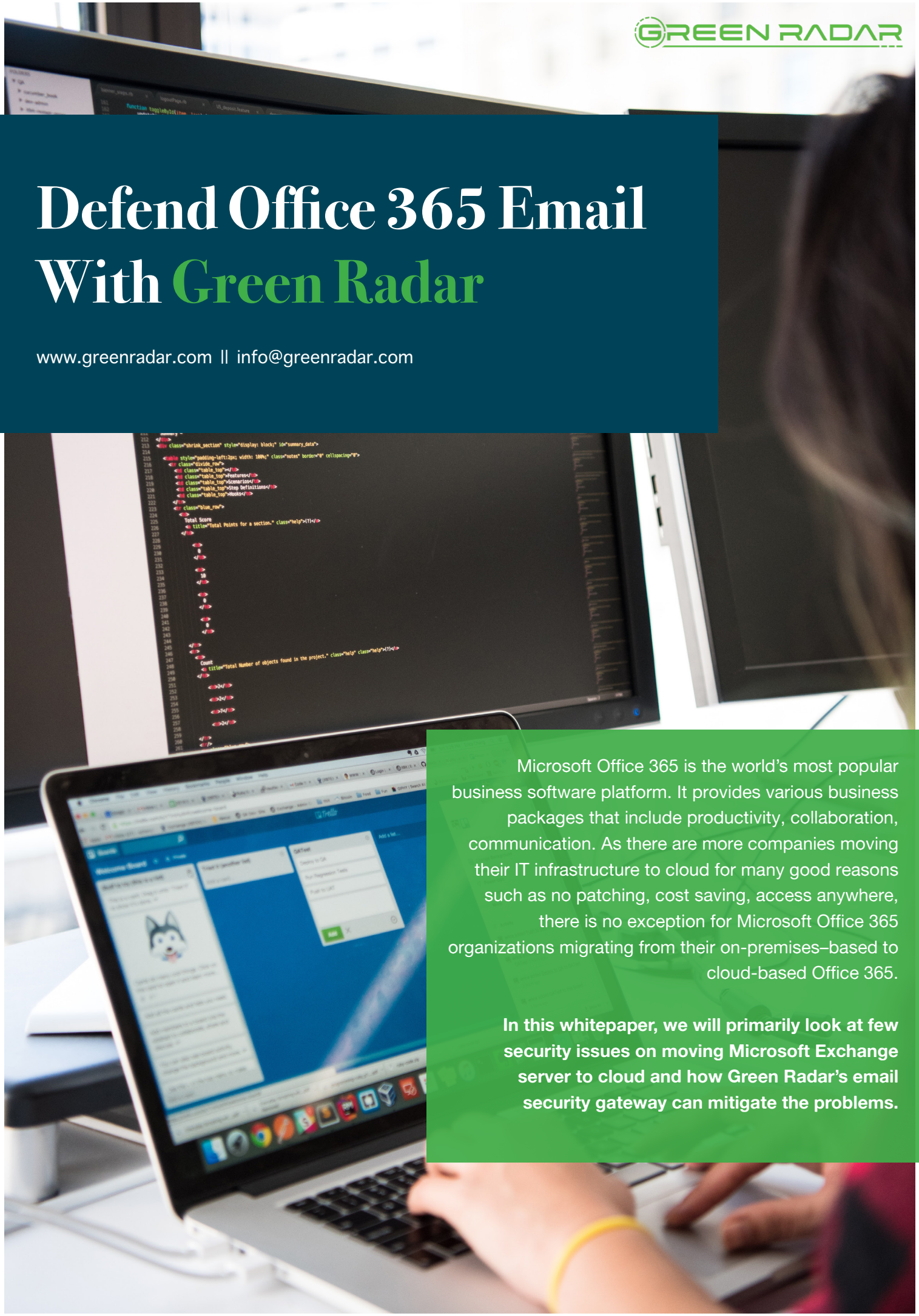


Defend Office 365 Email With Green Radar

www.greenradar.com || info@greenradar.com

Microsoft Office 365 is the world's most popular business software platform. It provides various business packages that include productivity, collaboration, communication. As there are more companies moving their IT infrastructure to cloud for many good reasons such as no patching, cost saving, access anywhere, there is no exception for Microsoft Office 365 organizations migrating from their on-premises–based to cloud-based Office 365.

In this whitepaper, we will primarily look at few security issues on moving Microsoft Exchange server to cloud and how Green Radar's email security gateway can mitigate the problems.

Office 365 and Email Security

More than 90% of cyberattacks starts from a simple email received in your mailbox. This is not a surprising phenomenon for anyone who have stayed in the IT industry long enough. Hackers like to start cyberattacks from email not only because email is still the most widely adopted communication tool in the business world but also because email spoofing is very easy to be done with tools available everywhere in the internet. For any company seriously consider moving their email system to cloud, we are very often to hear that they would have a concern on email storage security as well as the gateway filtering capabilities.

Firstly, on-premise email server implementation allows emails to store locally within the on-premise storage device versus emails was kept somewhere in the cloud that people outside your company may have a chance to read them.

Secondly, on-premise Microsoft exchange server allows users to buy additional email security gateway product in front of exchange server to filter out the virus, spam, ransomware etc. The additional security gateway provides extra protection to your exchange server which users are wondering if there is similar thing offering from cloud service providers.

"However, many independent security researchers have pointed out that the email security capabilities of Office 365 need some sort of 'improvement' from 3rd party security vendor."

To tackle the above two scenarios, the widely adopted solutions are:

Email storage - We generally agree keeping the email locally gives us a better privacy control. There is no doubt on it if the user has done enough protection keeping the email data away from the outsider. However, if we want to maintain similar email privacy in cloud, it will be implemented differently. There are many ways to do it like using encryption but the most widely adopted approach was either on hybrid or trusting the service provide. Hybrid approach is to keep the data locally within the company but is also using some email flow functions on the cloud. This gives users better privacy control on the email. Nevertheless, hybrid implementation is relatively harder to implement that sometimes stop users from migrating to cloud. By no means, when your email is reaching the internet, there is a chance of emails being seen by others unless it is encrypted. But encrypted email is not easy to manage which is not a popular implementation among all.

The relatively easier way to solve this issue is to find a reputable email services provider such as O365 and carefully work out the privacy agreement with them to ensure that no one will be able to read your email without your consensus.

3rd Party Security Gateway Solution - Microsoft provides many security features to patch their exchange server. Even Microsoft has mentioned that phishing email continues to be a top threat vector for users of Office 365. However, many independent security researchers have pointed out that the email security capabilities of Office 365 need some sort of "improvement" from 3rd party security vendor.

Those reports have indicated that many organizations adopting Office 365 are also adopting security products from other vendors. The difference is, company brought a physical security product in front of the exchange server in the old days versus buying a cloud service integrating with their cloud O365 email service now.

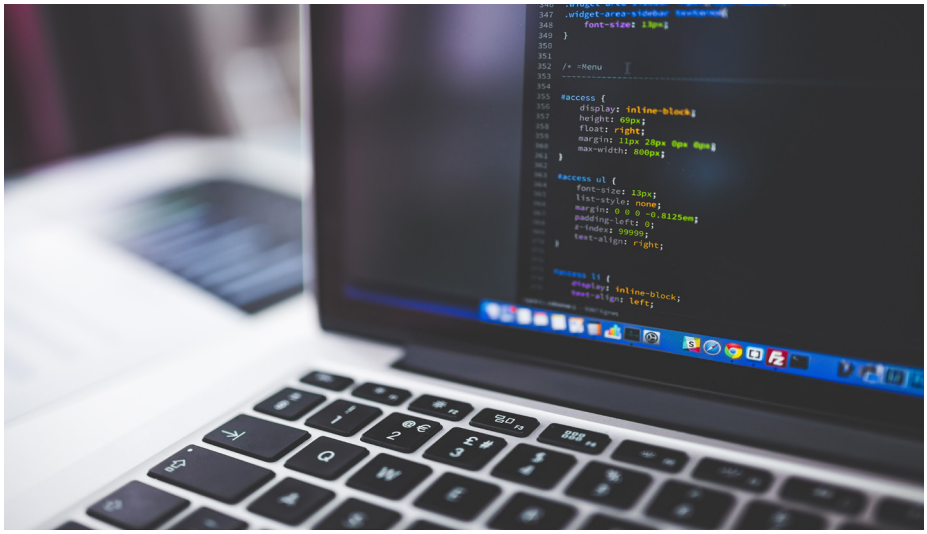
The Safe Links feature is based on policies set by an organization's administrators, such as links that are whitelisted (a custom "Do Not Rewrite URLs" list) or blacklisted (a custom blocked URLs list).

Microsoft Security Offering on Email Security

1 Exchange Online Protection

Microsoft has many security offerings to handle various types of situation related to their products. This section is focusing on handling email security in Office 365.

On email, Microsoft is mainly using detection-based technologies, offering as an add-on module attached to Office 365. There are two main offerings from their price book. One is an email filtering service that provides real-time antispam and signature-based, multi-engine antimalware protection—including antivirus and antispyware protection—as part of Microsoft's Exchange Online Protection (EOP). EOP is a messaging protection solution that parses received email through variety of filters. These filters will check the email sender's reputation, check if there is any known virus pattern and check if it looks like a spam.



Then based on all the things Microsoft's filters checked, a score is given to determine if the email should be put into a junk box or simply classified as a virus/malware. At the same time, a policy at MS Exchange can be set to tell the email server that how this email can be routed without breaking the rule set in the data loss prevention (DLP) engine.

2# Microsoft Advanced Threat Protection (ATP)

Microsoft also offers Advanced Threat Protection (ATP) as an add-on subscription service to its users who have EOP on Exchange Online, Office 365 Business, Office 365 Enterprise, or Office 365 Education. Microsoft ATP is also an email filtering service like Microsoft EOP with the major difference on adding a URL scanning service named Safe Links.

While email content is scanned, the URLs of any links within the email are rewritten to go through Office 365. The Safe Links feature is based on policies set by an organization's administrators, such as links that are whitelisted (a custom "Do Not Rewrite URLs" list) or blacklisted (a custom blocked URLs list). Depending on the user policies and administrative policies that have been put in place, once a user opens an email that they have received in their Office 365 email inbox and clicks on a link in that email, Safe Links will allow the

"Signature-based protections have proven to be ineffective against the more sophisticated email attacks that have evolved and been launched."

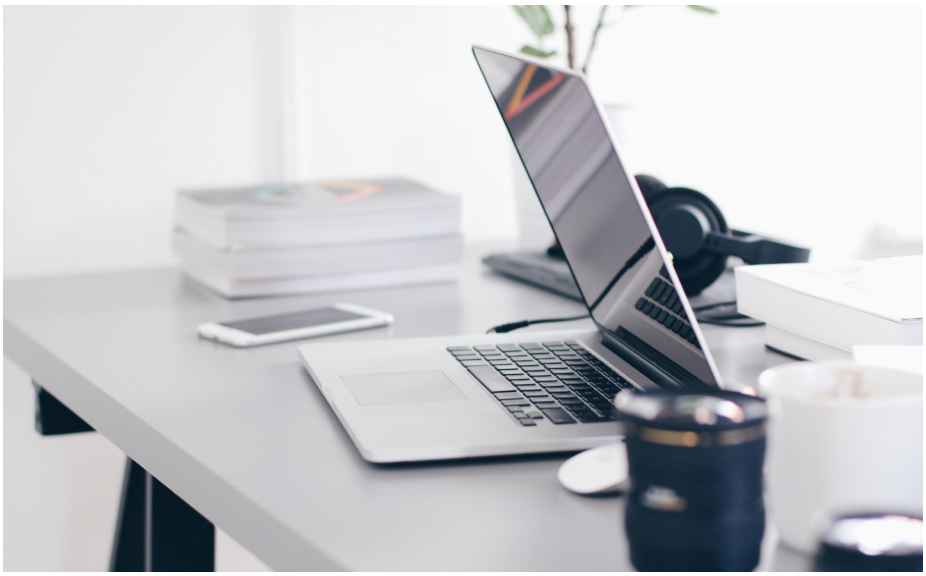
accessed website to open or will present the user with a warning page. Safe Links protects against users clicking on the links in email. Working hand in hand with the Safe Links feature is Microsoft ATP's Safe Attachment capabilities. Safe Attachment scans the attachments of incoming email for known virus and malware signatures. If the attachment has been cleared and declared safe, it is released for access by the user. Email attachments that have been declared unsafe are quarantined, with any embedded malware detonated before the document is released to the user. Microsoft ATP also allows an organization to review all senders who may be spoofing the organization's domain to determine if the sender should be allowed to continue sending the email, or should be blocked.

Office 365 Email Security Challenges

No doubt that Microsoft Exchange Online Protection (EOP) delivers email protections, which are enhanced with their Advanced Threat Protection (ATP) scheme, the reality is that there are many reasons to be concerned about Office 365 email security and still there are also many Office 365 users are exploring other options to supplement their O365 email security capabilities. Here are the few reasons why this is happening:

1 Microsoft EOP provides both antivirus and antispam engines, but it is only signature based. Signature-based protections have proven to be ineffective against the more sophisticated email attacks that have evolved and been launched. Key reason is for signature-based protections to work, the malware that they protect against must be known and must have had a signature created to uncover and stop the malware but attacks are obfuscated, easily circumventing signature-based malware protections.

Microsoft's ATP URL rewrite for Office 365 is only an "allow" or "block" decision, which is made at the time a user clicks on the link.



2 Microsoft's Advanced Threat Protection (ATP) fixes problems on their email vulnerability but doesn't fix all of them. For example, while Microsoft ATP includes the ability to detect malware embedded within attachments and can detonate the malware safely, Microsoft ATP allows the original attached document to be accessible to and downloaded by the user. However, most email-based attacks are moving toward fileless attacks. This means that there may be no executables or other signs that would indicate that the document is infected. If the document is released to user, and user open the document, the malware attack can be launched, even though the document had been determined to be safe before. Fileless attack doesn't include anything that may be detonated and there are no signatures to detect, effectively negating the ATP detection capabilities.

3 In addition, Microsoft's ATP URL rewrite for Office 365 is only an "allow" or "block" decision, which is made at the time a user clicks on the link. However, any click before the URL is "convicted" and user access is disallowed can lead to a risk of infection. So Microsoft's ATP does not provide a solution for web-based malware attacks. For example, when a user clicks on a link to allow the user to access the web page, Microsoft's ATP is no longer associated with the user's web session. So, if a web page included malware that was being delivered by malware, drive-by download attacks, etc, the user and their device would be infected, potentially creating a series of attacks for their organization. This is a reason why some Microsoft Office 365 users want to enhance their email security by moving to a 3rd party security vendor on it.

Green Radar's approach

Green Radar doesn't assume an email is good or bad. Some phishing emails appear to be very real and can't be filtered out by a signature-based engine either because no malicious links were found, or no virus signature was matched. Therefore, we can't just assume the email is good because we can't find malicious link or relevant signature.

Green Radar is using a hybrid detection approach which combines signature-based engine and email security expert's advice on threat hunting. Our threat intelligence comes from many sources including threats from the US, China and even locally from Hong Kong. For those threats which can't be discovered by signature, Green Radar uses the sandbox to examine any mischief behaviour behind the email and our security experts in our SOC will verify the sender's information.

Some phishing emails really carry no indication to be detected by any filtering engine. This is the reason why we always said we can't assume anything unless we find something bad on your email. Our ultimate solution to protect you from phishing emails is to adopt our isolated email platform. With Green Radar's isolated email platform, emails are being opened in our isolated cloud platform which gives you three extra protections.

Green Radar Three-Step Protection

Step 1 : - Traditional antispam/virus detection framework based on signature
Step 2: - Use Sandbox and human expert to monitor malicious email activities
Step 3 : - Isolation platform to protect users from phishing and malicious email

1 All input fields and URL link clicks are protected which means users can't input anything such as their ID/ account numbers etc or click on any URL links displayed in the email. In case users really want to click the link or input the information to the fields provided, they must implicitly tell the system that they need to do so.

2 Email Attachment is "washed out" and can only be read and displayed. All hidden coding behind the attachment is not allowed. When a user operates in our isolation platform, only safe, malware-free rendering information is delivered to a user's device. No web page component or active content, including any potential malware, leaves the platform to the user.

3 Green Radar Phishing Isolation solution is deployed within an existing Office 365 or Exchange Online email workflow - rewriting all web links a user receives in Office 365 email messages so that, if the user does click on a malicious web link in an email, their web browser is forced to open the questionable website within the cloud-based Isolation Platform. There is no judge whether the link is good or bad and no need for the organization to define whitelists or blacklists of URLs.

About Green Radar

Green Radar is a next generation IT security company which uses a combination of technology and skills to deliver:

- Email and Endpoint Threat Detection
- Deep Threat Analytics and Response

Our Security Operation Centre (SOC) is using a Managed Detection & Response (MDR) approach which helps our customer to manage threat detection & response on email and endpoint devices.

We are a wholly owned subsidiary of Edvance International (HKSE: 8410), with a long history of providing advanced IT security services and protecting many large enterprise's security.

info@greenradar.com

www.greenradar.com

Hong Kong: (852) 3184 9400

Singapore: (65) 6248 0601