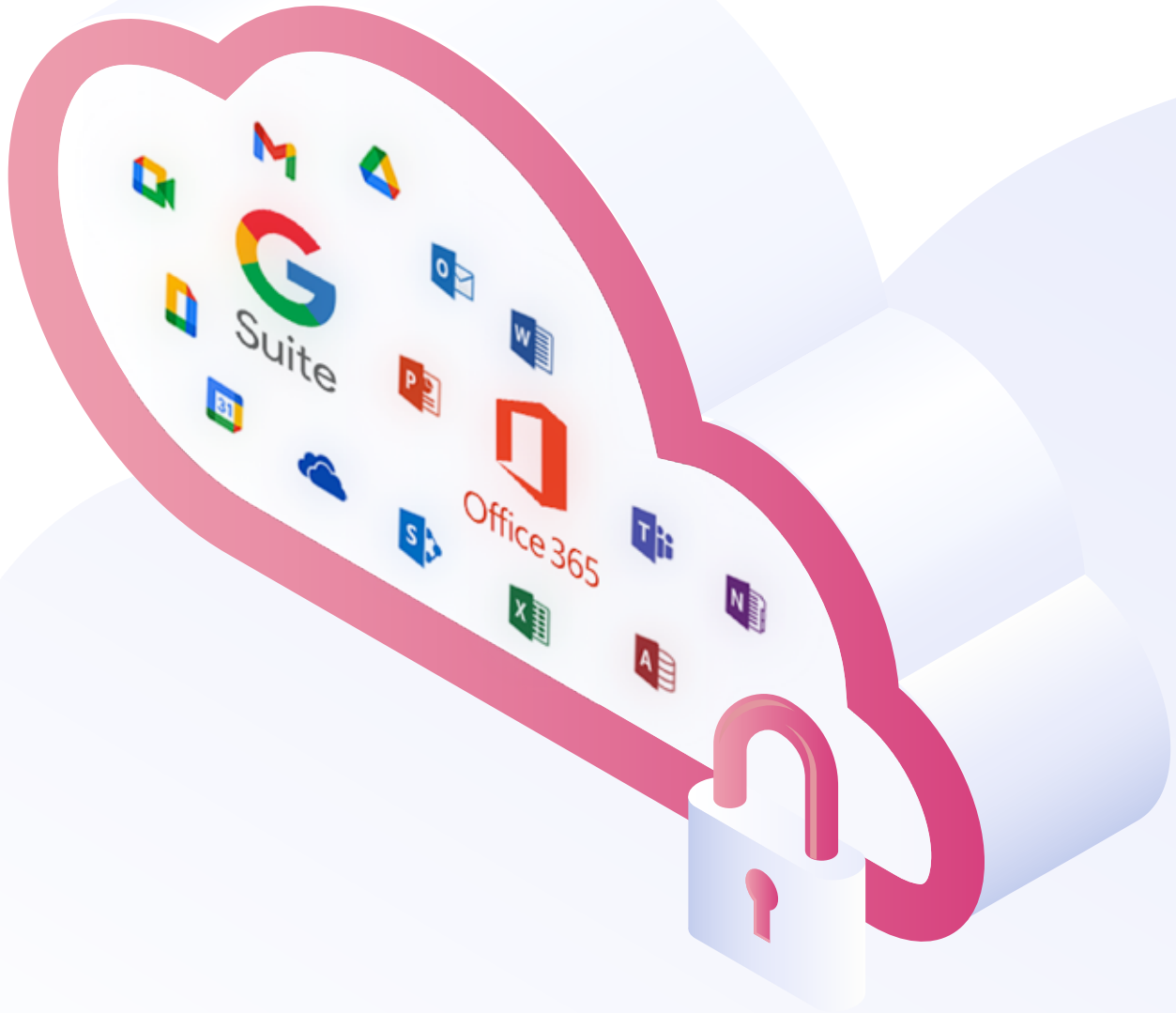
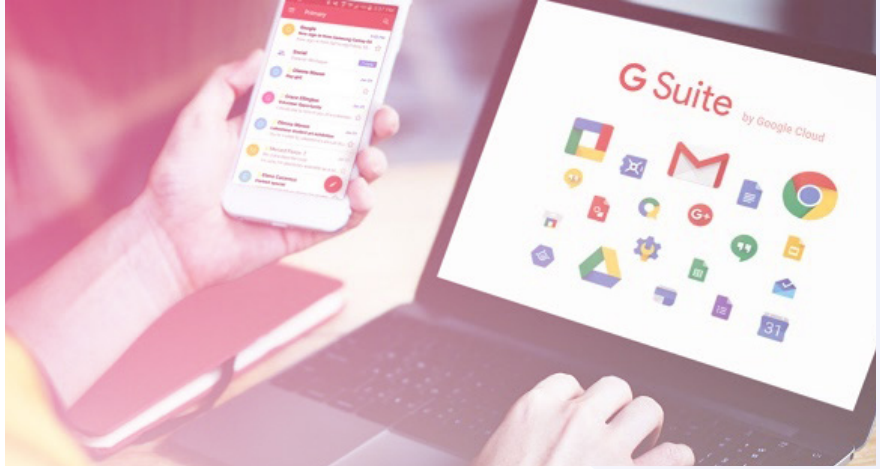
BUYER'S GUIDE TO

OFFICE 365 & G SUITE SECURITY

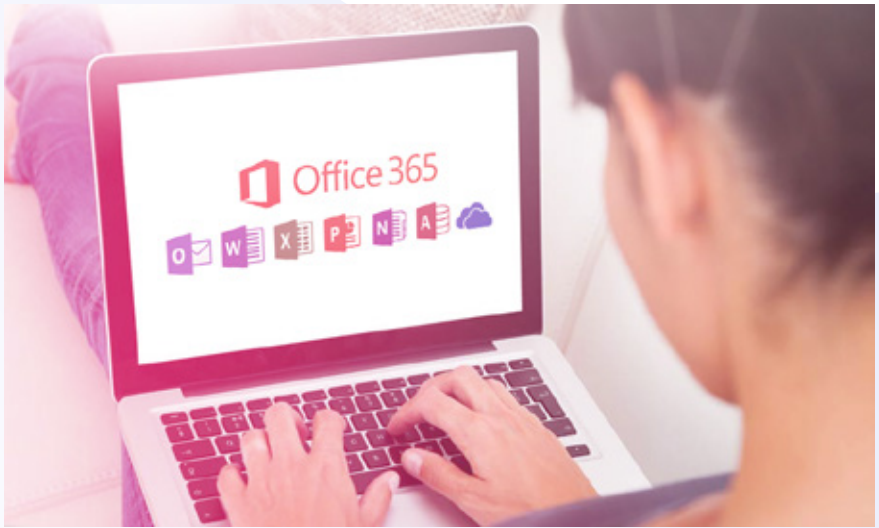
THE 5 MUST-HAVE CAPABILITIES OF THE OPTIMAL SECURITY SOLUTION FOR YOUR ORGANIZATION'S **CLOUD EMAIL AND PRODUCTIVITY APPLICATIONS**



Cyber Talk



CONTENTS



INTRODUCTION:

THE GROWING CHALLENGE OF OFFICE 365 & G SUITE PROTECTION

The COVID-19 pandemic brought on a huge shift in organizational structures.
A large portion of organizations' workforce moved to regularly working remotely, and relying heavily on their cloud mailboxes and productivity apps to complete important tasks, share sensitive information and send confidential files.

> *94% of malware, including Ransomware, infiltrate organizations through malicious emails – making email one the biggest attack vectors out there.* [1]

The many security gaps created by the sudden and massive shift to remote work, with the addition of employees naturally being less careful in the comfort of their home, created a sea of new opportunities for email and productivity applications attacks. Adding to that, the costs (and profits) of these attacks are enormous – Business Email Compromise (BEC) attacks averaged at $80,000 loss per attack in the second quarter of 2020 [3] while the average cost of ransom payment following a ransomware attack reached $84,000 in Q4 of 2019 [4] and is rising year-over-year.

The above, combined with the new remote work reality, make email attacks extremely lucrative for cybercriminals, which in turn constantly create increasingly sophisticated campaigns that are designed to bypass traditional security solutions, and exploit human nature. The latter is a crucial point that we would like to emphasize: **email attacks rely on the end-user to open the attachment, insert their account's credentials to a phishing site or pay a fake bank account, thinking it is a vendor's account.** The success of these attacks, and one of the main reasons they are so lucrative for cybercriminals, is that they rely on humans. That means that you need to deploy a security solution that is designed to block and prevent these malicious communications **before** they reach users.

> ***As cyber criminals always capitalize on crises, COVID-inspired attacks were the natural next step.** One of many recent examples includes a French pharmaceutical company which fell victim to a BEC scam and transferred nearly $7,000,000 to a Singapore bank account for protective masks and hand sanitizers. Needless to say, the company didn't receive the products, nor could they contact the fake supplier.* [2]

HOW TO DECIDE?

To help you choose the optimal cloud email & productivity suite security solution, we put together the following **5 must-have capabilities**, alongside the questions you should ask before making a decision.

CAPABILITY #1:

PHISHING PREVENTION

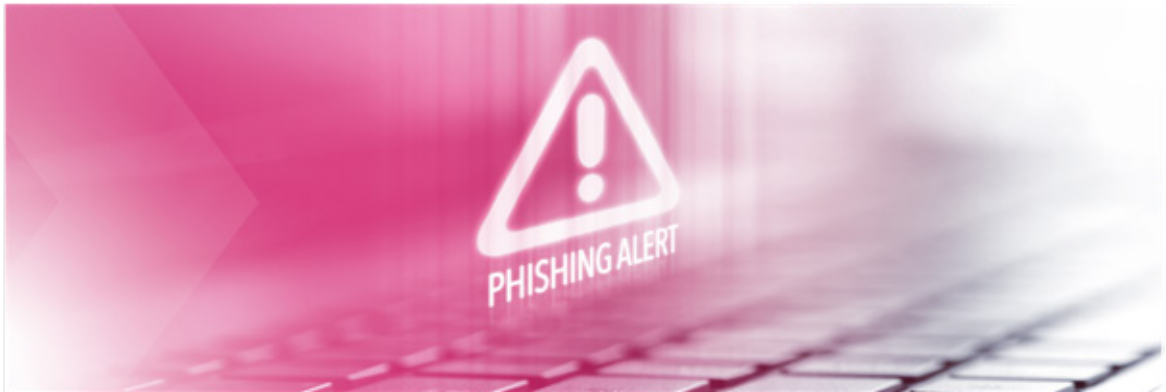
Phishing is one of the most common threats to organizations. It is also one of the most versatile and sophisticated forms of attacks.

For these reasons and many others, **real-time** phishing protection is crucial to ensuring that your organization is safe. Proper phishing protection should also cover your productivity suite, which includes cloud-based email and commonly used productivity applications such as SharePoint, OneDrive, Teams, Google Drive, and others. The protection for email only is limited and insufficient.

The phishing protection solution you select should be fully automated and AI-based to deal with the increasing sophistication of these attacks and prevent them BEFORE they reach the end-users.

The tool must also be able to examine the different aspects of advanced phishing emails, which include: inspecting metadata to validate the sender, inspecting email attachments to ensure that they are not malicious, validating links, checking the email against other domain intelligence, and applying click-time prevention so that links arealways validated as non-malicious, as they are clicked.

Lastly, the tool must also be able to check the language of the email. This is because phishing emails often include subtle indications of fraud, such as text signatures, credential harvesting patterns, and expressions of urgency or a call to action that is suspicious, such as 'change your password immediately' or 'pay this asap.'



QUESTIONS TO ASK:

- Does your email security solution provide REAL-TIME phishing protection?
- Does it cover productivity applications such as Microsoft OneDrive, Share Point, Teams, and the entire G suite?
- Does it inspect every aspect of the communications, including the language used in the body?

In Q3 2020, Microsoft was the most frequently targeted brand by cybercriminals. 19% of all brand phishing attempts were related to the technology giant, as threat actors sought to capitalize on large numbers of employees still working remotely during the Covid-19 pandemic. An email was the most popular platform for the delivery of phishing attacks. [5]

CAPABILITY #2:

MALWARE PROTECTION

Malware is another huge risk to organizations. A recent Check Point Research report states that 1 in 239 email attachments are malicious [6]. This may not sound like much, but if one stops to think about how many emails an organization handles every day, this number becomes extremely alarming.

When evaluating a malware protection tool, organizations must consider two key parameters: the impact on productivity and block rate.

To maintain productivity without compromising security, the solution you select must be able to clean any file of active content instantly so that it can deliver it within seconds to the end-user.

As for block rate, this is important because once malware reaches the end-user's machine, it's too late. The solution must examine every aspect of the file or attachment to ensure it is not a delivery vehicle for malware and use more than one means for detecting and preventing evasion techniques that may be employed by the attacker.

The final qualifier of the right malware protection solution is access to rich threat intelligence. The solution should be fed by a rich source of threat intelligence that is updated continuously.

1 IN 239 EMAIL ATTACHMENTS IS MALICIOUS

According to Check Point Research [6]

QUESTIONS TO ASK:

- Does it block the malware BEFORE it reaches users?
- Does the solution impact productivity (introduces latency)?

CAPABILITY #3:

ACCOUNT TAKEOVER PROTECTION

Hijacking users' accounts is a common practice among cybercriminals. This is typically achieved by gaining access to an account's credentials through a phishing attack, a breach to a third-party site, or even the dark web.

A hijacked account presents a huge risk to organizations as the hacker now has complete access to the organization's database, contacts, customer information, and other sensitive data. With account takeover, hackers also impersonate the account owner and send emails on their behalf, moving internally within your organization. Therefore, the solution you choose must protect against account takeover.

When evaluating an account takeover solution, it is important to consider that it should work in a layered approach. Most organizations use identity provider, which authenticates the user by verifying some basic credentials. However, when these credentials are stolen, an added security layer is necessary to augment the authentication process. The added layer should contribute extra information to the process, including MFA (multi-factor authentication), as well as anomaly detection that can be customized to the company's needs. This anomaly detection should block access based on parameters such as IP reputation, login location, approved devices, and others.

Organizations dealing with very sensitive data, such as banks, would need an agent to be installed on devices to grant access to accounts.

QUESTIONS TO ASK:

- Does it work in a layered approach to augment the existing authentication process?
- Does it enable both agent and agentless protection?
- Does it enable customizable anomaly detection?

In April this year, Check Point Research revealed the shocking story of the Florentine Banker Group. The hackers group used a phishing attack to hijack a financial firm's employee account and impersonate the victim, until finally achieving their goal of manipulating money transactions to their bank account, cashing in over £600,000. [7]

CAPABILITY #4:

DATA LEAK PREVENTION

Data leakage presents a huge risk to organizations. Employees can unintentionally or sometimes intentionally leak sensitive data to outside the organization. This can result in fines for non-compliance with regulations, losing a competitive advantage due to intellectual property being breached, and even damage to brand equity.

Employees who deal with sensitive data might not be aware of the risks that lie in sharing it through email and cloud-based applications. This is where automated data protection comes into play.

The solution you choose should enable you to set custom policies that work for your organization and automatically prevent employees from sending out sensitive information via email or any other productivity application they use.

For example, a medical facility would need to set DLP policies to block communications with patients' medical records from being sent outside the organization.

QUESTIONS TO ASK:

- Is it possible to set custom policies for the organization's needs?
- Does it prevent data leakage across productivity applications as well as email?

›››

CAPABILITY #5:

INTERNAL THREAT PREVENTION

This last capability may not be so obvious, but it is essential. As mentioned, some attacks are designed to enable the cybercriminal to move laterally inside the organization.

If your security solution examines only inbound communications, it will miss internal threats that might be infecting other devices within the organization. Similar to the Florentine Banker case mentioned earlier [7], a single compromised account can send a phishing email to the entire organization, which would seem credible as it has come from a colleague within the organization. If your security solution is not designed to identify malicious internal movement in real-time, your entire organization can be at risk from just one compromised account.

Real-time is the key here. These lateral movements have to be blocked BEFORE they reach any other user in the organization, because as noted earlier – once it has reached other users, it's too late.

QUESTION TO ASK:

is the solution capable of blocking internal threats in real-time?

IN SUMMARY

Most traditional email security solutions often provide insufficient protection, protecting only the email component, or scanning only inbound or outbound communications. To deal with the ever-growing sophistication and array of attacks, the solution you choose must provide complete, real-time protection against all threat vectors, and across your entire cloud email and productivity suite environment. The costs of these attacks are exponentially growing, and the danger they pose to organizations is too great to take lightly.

Consequently, the solution you choose must have the mentioned capabilities:

- Phishing prevention
- Data leak prevention
- Malware prevention
- Internal threats prevention
- Account takeover prevention