Three keys to securing Microsoft 365

Barracuda

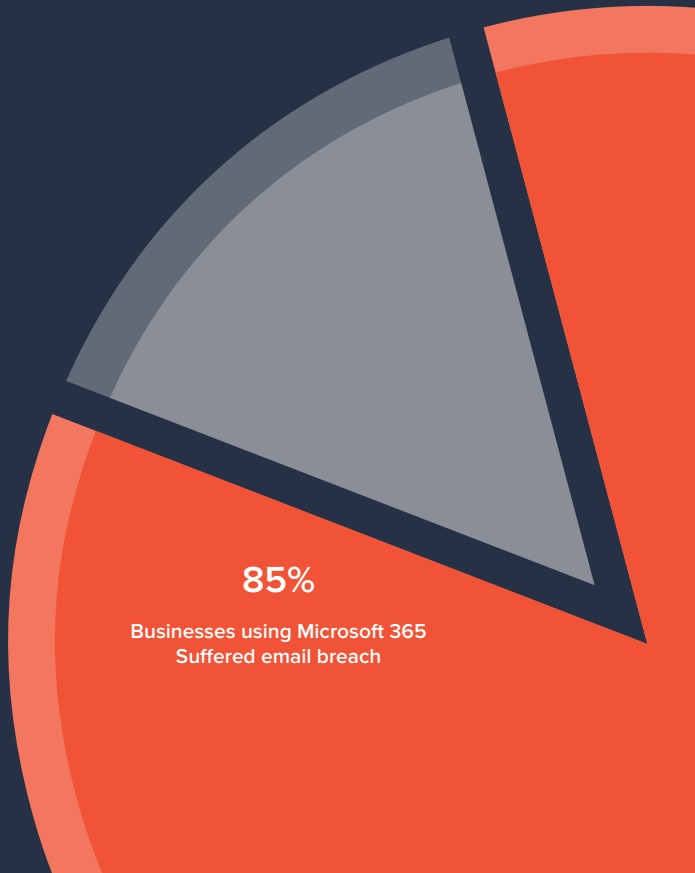
Popularity brings exploitation

Over 1 million organizations today rely on Microsoft 365, a suite of tools that support productivity and communications, including email, cloud storage, document sharing, and messaging. Microsoft Outlook and Teams became an even more integral part of business communications in response to the COVID-19 pandemic and the broader adoption of remote working.

However, Microsoft 365 has its weaknesses. Research by Egress found that 85% of businesses using Microsoft 365 suffered an email breach and reported a 67% increase in data leaks via email since March 2020. With IBM reporting the average cost of a business email compromise (BEC) attack at a massive $4.89 million, one thing is clear: email attacks remain a favorite and lucrative vector for cybercriminals to exploit.

$4.89M

average cost of a BEC attack at **IBM**



Microsoft 365 suffers gaps in security

While Microsoft 365 does include its own security infrastructure — Microsoft Defender for Office 365 (MDO) — it has its gaps.

First, Microsoft's native capabilities are simply not enough to protect against targeted and personalized threats. To protect against these threats, Gartner supports the recommendation of using third-party solutions, highlighting that it's important to:

"Supplement the native capabilities of your existing cloud email solutions with third-party security solutions, to provide phishing protection for collaboration tools and to address both mobile- and BEC-type phishing scenarios."

Second, your Microsoft 365 data is not secured from accidental or malicious deletion. In fact, in its service agreement, Microsoft recommends that you "regularly backup content and data that you store using third-party apps and services," acknowledging that without a third-party solution for backing up data, businesses risk losing important information.

To patch the gaps left open by the insufficient security capabilities of MDO, we at Barracuda recommend a 3-pillared approach to secure Microsoft 365 — **threat prevention, detection and response**, **and data protection and compliance**. This ebook will walk you through how to approach each of these pillars to ensure that your Microsoft 365 applications are secure, implementing a line of defence against costly email threats.

Barracuda

Threat prevention

Prevention is always better than cure. But how do you approach prevention in the face of high-volume email attacks, which are growing in sophistication daily? True prevention happens before emails reach business email inboxes. Anything after that is remediation and puts your systems at risk.

Successful email attacks put both your data and your business continuity at risk, so it's vital that you put systems in place to prevent these disruptions. AI-powered email protection tools can target phishing attacks, and Zero Trust Network Access (ZTNA) — the approach to securing users' access to business critical applications — should be your first step. ZTNA ensures that you are protecting your access by being specific about which users can access different parts of the network, and not granting unnecessary access to users who don't require it — which could lead to issues with confidential data being accessed or shared.

Traditional email gateways are designed to prevent attacks and act as a first line of defence to prevent spam, malware, and other email messages with malicious payloads from landing in users' inboxes. However, hackers deploy social engineering tactics to circumvent this protection. Taking a step beyond traditional email gateway defense, third-party solutions leverage API-based inbox defense layers, which identify threats that bypass the gateway to successfully reach users' email inboxes. API-based defenses integrate with employee mailboxes to access historical external and internal mail flow. They learn the behavioral patterns of each user to spot anomalies and block attacks, including those originating from internal accounts — critical for detecting account takeover.

At the heart of this kind of solution is an AI engine that detects and blocks socially engineered attacks in real time and identifies the employees at the highest risk. The engine leverages multiple classifiers to map the social networks of every individual inside the company and detects anomalous signals in message metadata and content, offering real-time protection against targeted attacks. Traditional, secure email gateways have no visibility into internal communications, so they can't intercept attacks coming from internal users. In addition, their over-reliance on pre-determined policies means they miss those targeted attacks. API-based defences are a step beyond these traditional solutions, identifying risks in internal and external communications to protect organisations from anomalies or attacks in both cases. As mentioned previously, solutions such as these are the extra layer of defence that Gartner recommends.

Absolutely vital to successful email threat prevention is implementing solutions that can block malicious emails from getting through the gateway to business email accounts in the first place.

While MDO includes capabilities for antispam, antimalware, and data exfiltration prevention, more sophisticated attacks such as lateral phishing and impersonation can still make their way into inboxes. These attacks are designed to bypass traditional email gateway solutions, making it crucial to employ third-party solutions to protect your business email accounts.

Detection and response

As good as any prevention method is, there will always be the potential that some sophisticated, malicious emails will reach users' inboxes. Your staff can play a vital role in keeping the business safe. Educating your staff on the risks of email threats and what to do when they arise is vital, no matter how strong the solutions you have in place are.

Using an API-based defense layer removes a large part of the risk associated with BEC, but training on how to respond to a threat that reaches a user's inbox should remain an integral part of your strategy for securing Microsoft 365. Using a Security Awareness Training (SAT) tool to help educate users on the risks and identification of phishing and social engineering attacks is vital to ensure that your staff are best placed to detect and respond to potential threats in their inboxes. On top of being able to detect potential threats, it's important that staff understand who they should report them to. This should be part of your phishing training, supplemented by additional SAT tools or exercises.

Once you've implemented identification tools and educated your staff, the next step is risk remediation — what happens next when you've identified an attempted or successful email attack? You need tools to research, identify, scope, and remediate post-delivery threats. Many of these tools leverage AI and automation to automatically remove all instances of a threat-containing email from inboxes within your organization. Automated incident response ensures the rapid and comprehensive removal of all threats within staff inboxes, which is much more difficult and time-consuming to tackle manually.

Data protection and compliance

The final pillar of your strategy to secure your Microsoft 365 applications is data protection and compliance. Barracuda's research found that 67% of organizations using Microsoft 365 rely solely on capabilities built into the software to back up and recover Microsoft 365 data. As Microsoft acknowledges, relying on Microsoft 365's cloud-based data storage does not guarantee that your data is safe. Ransomware can still seize this data and take it offline, and human error — the number one cause of data loss — can still result in lost data and potential disruption of operations when critical data can no longer be accessed.

To this end, it's vital that you regularly back up your Microsoft 365 data using a third-party cloud backup solution.

Many organizations face regulatory requirements to retain and securely archive their email communications. A good email archiving solution will ensure that you can retain an immutable, tamper-proof copy of every email sent and received by your business. Microsoft 365 has its own archiving solution, but implementing a third-party cloud archiving solution ensures that no matter what happens within Microsoft 365, you will still have access to your email archive to enable you to meet compliance requirements with tamper-proof archiving and granular retention policies.

There are other methods available to bolster your compliance efforts, too. One such method is using a Data Classification and Discovery tool, which secures your environment against improperly stored sensitive data and latent malware. These tools give you insights into existing and new instances of sensitive data to ensure the highest levels of compliance, helping you avoid the risks of reputational damage and hefty fines.

How Barracuda can help

Your approach to enhancing the security posture of Microsoft 365 requires a solid understanding of the threats lurking within your email inboxes. This is where Barracuda can help.

For organizations that want to protect their businesses, brands, and people against the most advanced email-based threats, Barracuda Email Protection is a comprehensive, easy-to-use solution that delivers gateway defense, API-based impersonation and phishing protection, incident response, data protection, and compliance capabilities.

Get started today with our Email Threat Scanner. Its's a free, non-intrusive service that looks at the past 12 months of data within your Microsoft 365 email inboxes. It then provides a detailed report and breakdown of every threat found, with individual analysis.

You can get access to our free email threat scanner to find out what threats are hiding in your inbox today.

Barracuda

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.