# Top 5

## Ways to Protect Your Business Against Email-Borne Threats

Build a multi-layered security solution to safeguard your users, brand, and business from today's most advanced email threats.

Today's email threats are far more evasive and destructive than the simple, malware-bearing emails of the past. Gone are the days where traditional email security solutions were enough to detect or stop social-engineering attacks targeting individual high-risk users within your organization.

1

## Build a strong email security foundation

Make sure your email security covers the basics, such as having solid anti-spam and anti-malware protection. From there you need to ensure your solution has modern security features like Advanced Threat Protection, which helps block zero-day attacks. The final thing you need to consider for your strong email foundation is outbound protection to prevent malicious or accidental data leakage.

2

## Create an email defense that goes beyond the gateway

Email security gateway can only do so much when it comes to fully protecting your organization. Today's email security solution needs to include protection against spear phishing, account takeover, and business email compromise (BEC). From there, find a solution that can both identify attacks that bypass traditional security as well as identify attacks that don't carry malicious attachment and use 'zero-day' links. Finally, having visibility into internal email communication (i.e., attacks that originate and target internal users from compromised accounts) is important because you can quickly detect the insider risk and block the threat.

3

## Provide comprehensive security training to users

A lot of organizations tend to miss the most important defense layer—their end users. To do this, you first need to identify high-risk users, which are commonly C-level executives and folks that deal with your company's finances. However, even though these employees are often targeted, you still need to provide training to everyone in your organization to ensure full end user protection. To do this, train them using a solution that combines phishing simulations with security training.

4

## Ensure resiliency

Disasters and accidents happen, so ensuring email continuity and quickly restoring your data is critical to stay productive during system failures or downtime. The best way to guarantee continual uptime is to back up your data to make sure nothing is lost—whether it was lost by accident or as a result of an attack.

5

## Respond faster to email attacks

Some email-borne attacks can evade email security and land in your users' inboxes. When this happens, you need to act fast to identify and remediate these attacks immediately. Sure, your users can report these attacks, but you can also be proactive by analyzing patterns within delivered emails to identify threats that are already in their inboxes. Quickly prevent potential damage by easily identifying all affected uses within minutes using automated tools and incident response. You can also reduce the time it takes to respond to threats by automatically removing all instances of malicious email directly from users' inboxes.

Barracuda®
Your journey, secured.