WHAT IS CLOUD PROTECT SPAM FILTER?

An advanced custom program used to detect unsolicited, unwanted and virus-infected emails and prevent those messages from getting to a user's inbox.

How is this Cloud protect spam filter different from others?

The **Cloud Protect Spam Filter** is completely API driven. It does not require adjustments to mail flow and NO DNS entry, which means it can monitor your traffic without disruption or interference. **Cloud Protect** ensures all emails are scanned accurately; plus, if there are problems with SPF records set by companies in their environment, then this Cloud protect will learn about them over time thanks to its robust learning algorithm.

Don't most companies have a Spam filter already?

Most either do not have a spam filter already or they rely on the Office 365 filter.

Why should I use Cloud Protect if I have Microsoft 365 protection?

Microsoft provides a basic filter for identifying spam. It performs basic checks of the headers of an email to identify an incorrect sender, which does not work 100% of the time, but they make no spam identification. They only look for faulty, incorrectly verified email domains that can be spoofed and still reach your inbox. This method is not effective and can often miss spam messages. The Microsoft 365 filter is best suited for an individual user but does not provide adequate coverage for a company. That Cloud Protect does.

What if Cloud Protect blocks communications we need? How do I know that won't happen?

The Cloud Protect Spam Filter monitors your email for unsafe content so that you can get back to work. It runs in "observation mode" for 30 days before creating a baseline of a typical communication between a company or person on the list that are considered important mail - it will modify these scores based upon routine activity during this time period (spamming). When an email is marked as being declared unsafe by our algorithms, then they'll go into a folder called Junk; if not deemed to be correct there's no need to worry because those messages won't be accessible through any other means than getting rid of them manually! We recommend that IT admins access the spam portal. It will show top domains marked as Malicious, and they can either whitelist or blacklist emails.

If I have never had a problem, why change?

Just one issue could put you out of business. Clicking the wrong $350k invoice. This has happened to customers that previously didn't have a spam filter.

How much work will my team need to do to set this up?

With just one button, you can have peace of mind. The Zero Management Platform will take care of all mail flow traffic for your company while we monitor its performance during an observation period - 99% understood by our cloud protection system!

Is this a Microsoft-approved program?

It is a Microsoft preferred solution. It takes just 60 seconds to set up.

For more information, contact