Protecting Office 365 from Attack

Office 365 adoption is continuing at strong pace. With such a massive user base Office 365 is profitable prey for a persistent hacker familiar with how Office 365 works. As ransomware and phishing attacks increase, Office 365 has become a primary target, making it vital for IT professionals to take proactive steps and "hack-proof" their O365 environments. Microsoft has made great strides in cyber security, yet headlines continue to report countless exploits where hackers have undermined an O365 environment.

Targeted Attacks on Office 365

According to recent study by IBM Security, the number of emails containing ransomware has increased 6,000% between 2016 and 2017.

Today the risk is greater than ever. Without appropriate protection Cloud based email systems like Office 365 are vulnerable. Just last year the Office 365 environment was hit by waves of Jaff and Locky ransomware attacks.

At the start of 2018, specific threats targeting the Office 365 environment appeared, such as "**ShurL0ckr**", which goes undetected by Office 365.

6000% increase in emails containing ransomware between 2016 & 2017

What email protection Office 365 offers

If your company has moved to Office 365 as a hosted email solution, your email is being hosted in a Microsoft Data Centre and most likely being filtered using Microsofts Exchange Online Protection (EOP). Although the Office 365 spam filter offers a reasonable level of security, some businesses find it basic and lacking when it comes highly-sophisticated cyber threats especially advanced and persistent spear phishing attacks. Let's take a closer look at the strengths and weaknesses of Microsoft Office 365:

How to strengthen your Office 365 security against Spam and Malware through a defence in depth approach

With this approach security is not dependent on any single layer, especially in the event of an attack. Office 365 offers 2 levels of email security, "Exchange Online Protection" and "Advanced Threat Protection" for a protection level in the low-middle of the market, according to an SE Labs study, "Email-hosted protection" published in August 2017. As email security experts with over 20 years' experience we know new malware can penetrate the usual email filtering mechanisms. It has long been the case that older email protection technologies, like analysis reputation and fingerprinting, are no longer effective against the evolution of these threats.

Recent research by Osterman identifies that Microsoft's EOP can detect 100% of all known viruses with updates every 15 minutes. However, the research found it to be less effective against unknown or new malware delivered by email. System Administrators implementing Office 365 need to make sure it's secure by layering in a dedicated secure messaging and spam filtering solution like SpamTitan to protect against advanced persistent threats. To protect against advanced threats you need advanced protection.

Protecting Office 365 from Attack

Zero Day Attacks

A zero day attack can occur when you click on an email attachment infected with malware. Once you open the attachment, the malware can exploit any security holes that exist in your email client software or in your PC. The only secure solution for email uses the ability to anticipate new attacks is using prediction.

Unfortunately Office 365s email security features don't match the features of many dedicated on premises and cloud based email security gateways, which include pattern learning and intelligence. The only secure solution for email includes the ability to anticipate new attacks using predictive technology.

1. Predictive techniques including Bayesian analysis, heuristics and machine learning to block new varieties of spear phishing, whaling and zero day attacks before they reach your mailbox.
2. Default SpamTitan features which are optional with Exchange Online Protection such as advanced threat protection, anti-typosquatting protection, link protection and email encryption.
3. SpamTitan focuses on a defence in depth approach protecting against malware threats, spear phishing attempts and zero-day attacks.

Data Leak Prevention

While, SpamTitan includes enhanced spam blocking and protection from malware, viruses and phishing emails, the product adds an additional layer of protection from data loss while making your Office 365 implementation easier to manage. We also add powerful, data leak prevention rules to prevent internal data loss, as an example tagging key words, social security numbers, etc.

It takes powerful phishing protection solutions to defend your organization against ever-evolving email phishing scams as well as protecting your organizations mission critical data.

Advanced Phishing Protection

SpamTitan provides phishing protection to prevent whaling and spear phishing by scanning all inbound email in real-time. SpamTitan searches for key indicators in the email (header, domain information and content) which suggest an email might be a phishing attempt. SpamTitan will also perform reputation analysis on all links (including shortened URLs) contained in emails and block malicious mails before being delivered to the end user.

1. URL reputation analysis during scanning against multiple reputation
2. Detect and block malicious spear-phishing emails with either existing or new malware.
3. Heuristic rules to detect phishing based on message headers et al. These are updated frequently to address new threats.
4. Easy synchronization with Active Directory and LDAP.
5. Spam Confidence Levels can be applied by user, user-group and domain.
6. Whitelisting or blacklisting senders/IP addresses.
7. Infinitely scalable and universally compatible.

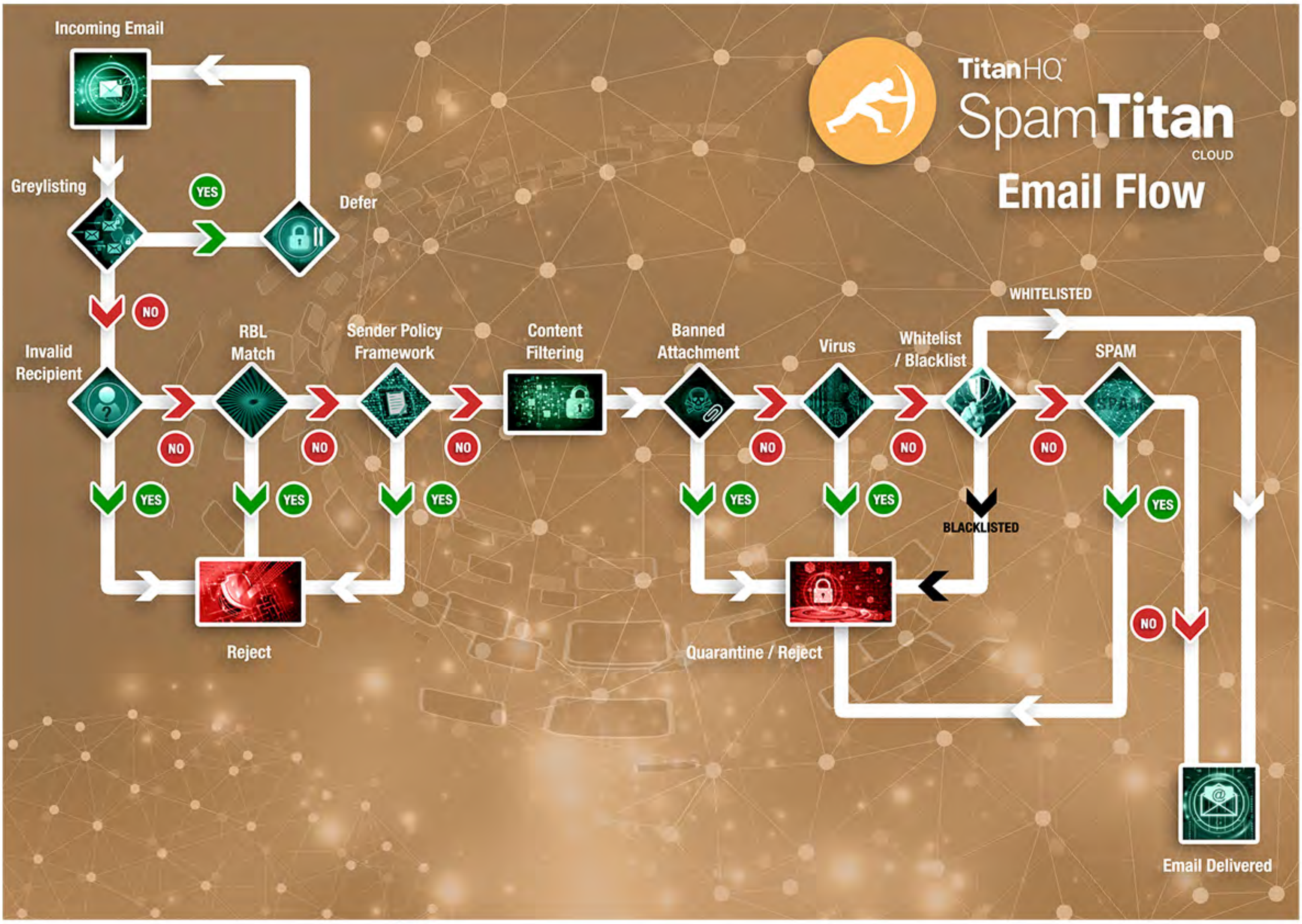
The combination of these features ensures SpamTitan protects users, businesses, and brands from whaling, spear phishing, impersonation attempts, and business email compromise (BEC), and cyber fraud.

Protecting Office 365 from Attack

TitanHQ SpamTitan CLOUD

How SpamTitan works:

You can strengthen your Office 365 security against malware and phishing with a defense in depth approach. Superior email filtering like SpamTitan uses predictive techniques to block new varieties of malware, spear phishing and zero-day attacks before they reach the user's mailbox.



Although most email services provide some level of proprietary spam detection, third-party spam filters for incoming mail increase the level of spam email detection considerably. Organizations that fail to implement a third party mail spam filter like SpamTitan continue to have spam delivered to their employees´ inboxes.

TitanHQ SpamTitan CLOUD

Protecting Office 365 from Attack

Feature Comparison – O365 v SpamTitan

Office 365 has many built-in security features however for organizations accustomed to dedicated security solutions with advanced filtering and advanced reporting, Microsoft's default security offering is likely to fall short.

	Office 365 - Exchange Online Protection (EOP)	SpamTitan	Feature Description
Email Protection against malware and zero day attacks	✗	✓	SpamTitan uses predictive techniques including Bayesian analysis, heuristics and machine learning to block new varieties of phishing, and zero day attacks before they reach your mailbox. Not available in Office365.
Protection from email links to malicious sites	✗	✓	SpamTitan checks every URL in every email against known blacklists with 100% active web coverage. Not available in O365.
Multiple Antivirus Scanning Engines	✗	✓	SpamTitan includes Double Anti-Virus scanners and partners with Bitdefender and ClamAV along with TitanHQ threat intelligence. With O365 you get basic AV.
Dedicated RBLs	✗	✓	SpamTitan includes 6 specialist Real Time Blacklists (RBLs). 80% of all problem emails are auto detected by these RBLs with zero false positives. No RBLs with O365.
DLP	✗	✓	SpamTitan includes comprehensive content filtering rules – allows you to delete, redirect, whitelist, quarantine or bounce mail that matches the rule. Not available with O365
Greylisting	✗	✓	Available by default with SpamTitan. Solutions with a Greylisting feature are more effective at preventing spam from evading detection and reduce the risk of a business falling victim to a phishing attack, malware or ransomware. Not an option on O365.
Security against infected attachments	✗	✓	SpamTitan allows the blocking of specified attachments by type (per domain). e.g. zip files (previously used in several Locky attacks). Not available with O365
Threat Intelligence	✗	✓	SpamTitan has inbuilt Bayesian auto learning & Heuristics – continually learning from email patterns and content. Adjusts spam scoring intelligently. Not available on O365.
Customizable Policies	✗	✓	With SpamTitan each user, domain, domain group and overall system level has its own white/block list. Each of these can have their own settings for notification reports. Also custom spam thresholds can be set per mailbox and domain. Not available on O365.
Spam Blocking	✗	✓	SpamTitan blocks 99.9% of spam. Real time blocking. Microsoft spam filters work retrospectively. Only after a customer has reported a spam email will Microsoft add the IP address to its "real-time block

SpamTitans email filter have SURBL filtering and malicious URL detection mechanisms to minimize the likelihood a phishing email avoids detection, and dual anti-virus software to inspect the content of inbound emails and their attachments for malware and ransomware.

Protecting Office 365 from Attack

TitanHQ SpamTitan CLOUD

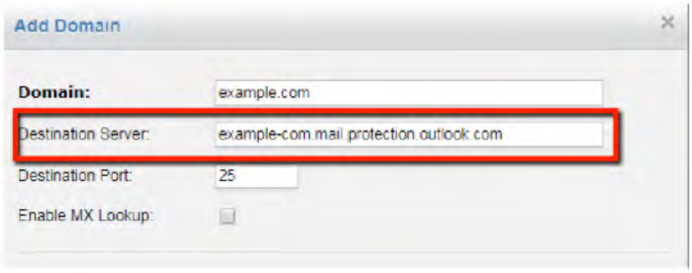
Simple Implementation

It’s easy to combine SpamTitan Cloud or our premise email security gateways with Office 365. It couldn't be simpler to implement this crucial layer of added protection to bulletproof your O365 environment from attack. You can specify the SpamTitan Email Filter as an inbound mail gateway through which all incoming mail for your domain passes before reaching your Office 365 account.

Step 1: Follow this guide

https://helpdesk.spamtitan.com/support/solutions/articles/4000094185-office-365-ip-throttling-rate-limit-using-spamtitan

Step 2: Add your domain and destination server to SpamTitan

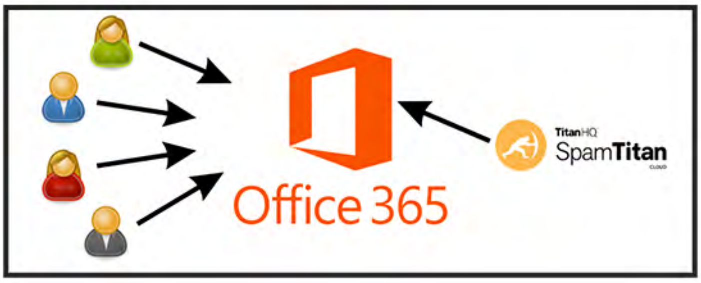


Add Domain

Domain:	example.com
Destination Server:	example-com.mail.protection.outlook.com
Destination Port:	25
Enable MX Lookup:	□

Step 3: Direct MX Records to SpamTitan

How your final set-up will look:



Advanced Threat Protection SHOULD NOT mean advanced spending.

Office365 continues to be the leader in the productivity and collaboration space for companies large and small. Because email is mission critical to organizations it’s vital to use a reliable third party vendor specializing in email and web security. With the onslaught of phishing attacks and ransomware entering through networks, and email systems, IT budgets are being built with security in mind.

Email Security and Web Security and Compliance do not need to cost an arm and a leg for those looking to save costs in their IT security spend and productivity. Security is a feature that Microsoft has added to 0365 and for most organizations this does not meet their security benchmarks. Since 1999 SpamTitan has been building up threat intelligence that will dramatically reduce the risk of a successful attack on your organization. Unlike Microsoft, security is all we do!

Are you concerned with Phishing and Malware in Office 365? Get a free personalized demo and see how SpamTitan can help secure your Office 365 environment today.