



ZixProtect for Office 365

Enhance Office 365 with Added Email Threat Protection, Encryption and Data Loss Prevention



Who uses Zix?

- 19,000+ customers including:
- All Federal Financial Institutions Examination Council (FFIEC) regulators
 - The U.S. Securities and Exchange Commission (SEC)
 - 30% of U.S. banks
 - 1,200+ U.S. hospitals
 - 30% of Blue Cross Blue Shield (BCBS) plans

Benefits:

- Seamless integration with Office 365
- Protection from malware, phishing, ransomware, business email compromise, spam and more
- Automatic encryption of sensitive information in email communication
- Convenient user experience for increased adoption of email security
- Improved compliance with regulations and corporate policies
- 24/7/365 phone support with a threat specialist to address any question or need

Features:

- Multi-layer threat filtering combined with machine learning and live threat protection
- Attachment quarantine and sandbox analysis
- URL re-write with time-of-click analysis
- Policy-based email encryption and data loss prevention with pre-built filters for regulatory compliance
- Transparent, bi-directional encryption between Zix customers
- Mobile-friendly secure portal for delivering encrypted emails to anyone, anywhere

ZixProtect for Office 365 is a cloud-based security solution that protects email by combining advanced threat protection, encryption and data loss prevention to deliver increased security with an easy to use experience.

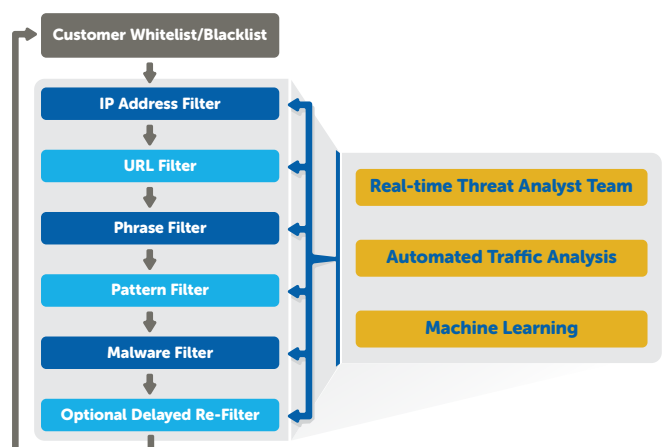
Email Threat Protection

ZixProtect for Office 365 provides 99.5% accuracy in detecting spam, viruses, phishing, zero-day malware, and ransomware. ZixProtect's multi-layer filtering engine provides the highest level of accuracy that reduces both false negatives (bad emails getting in) and false positives (good emails kept out). This reduces the time your IT team has to spend managing the system and improves business communication flow.

Multi-layer filtering

ZixProtect's multi-layer filtering engine provides accurate threat protection by analyzing email content and the source of the email. ZixProtect for Office 365 combines standard IP address and URL filters with targeted phrase, pattern and malware filters. Phrase filters look for complete phrases to precisely identify unwanted solicitation or phishing emails. Customized pattern filters allow specific attack campaigns to be identified and blocked. Finally malware filters identify both known and zero-day malware attacks, and the re-filtering technology allows additional analysis of questionable emails.

These robust filters are combined with automated traffic analysis, sophisticated machine learning, and live threat analysts to create a system that is able to accurately identify even zero-hour attacks.



About Zix

To better meet your company's data protection and compliance needs, Zix can enhance your Office 365 environment with advanced threat protection, email encryption, data loss prevention, archiving and bring your own device (BYOD) mobile security. Zix delivers a superior experience and easy-to-use solutions that have earned the trust of more than 19,000 organizations including the nation's most influential institutions in healthcare, finance and government.

Leveraging our more than 15 years of hosted experience, you can have confidence that Zix email security integrates seamlessly with Office 365. You also benefit from the support of the ZixData Center, a state-of-the-art facility with PCI DSS 3.2 certification, SOC2 accreditation and SOC3 certification. Staffed 24/7/365, ZixData Center has a track record of consistent 99.999% availability. In addition, Zix delivers exceptional customer support - available by phone 24/7/365 to address any question or need.

With reliability, experience and superior support, Zix enhances the security and compliance of your Office 365 environment. To learn more, visit www.zixcorp.com/office365.

Business Email Continuity

Additionally, ZixProtect for Office 365 includes email continuity to ensure access to business emails during an Office 365 service disruption. ZixProtect for Office 365 spools incoming emails for up to 5 days and automatically delivers them when Office 365 comes back up. Users can also access 30-days' worth of emails through a web-based interface where they can compose new messages and read, reply, and forward existing messages.

Email Encryption

ZixProtect Premium for Office 365 provides email encryption that automatically determine the most efficient way to securely deliver sensitive emails using our patented Best Method of Delivery®. Through the Best Method of Delivery, encrypted emails are delivered to anyone, anywhere and often transparently.

As part of the Best Method of Delivery, Zix offers the industry's only bi-directional transparent email encryption, enabling senders and recipients to exchange encrypted email without any extra steps. When you send an encrypted email to another Zix customer, the message and replies are encrypted transparently, so that not even a password is needed. ZixProtect Premium for Office 365 also offers a secure way to try sending using Transport Layer Security (TLS) without being susceptible to a man-in-the-middle attack.

When sending to recipients who do not have email encryption capabilities, Zix offers a secure web portal that makes receiving an encrypted email easy, even on a mobile device. The secure web portal can be branded and configured to meet your business needs and can be integrated into your corporate website.

Email Data Loss Prevention

ZixProtect Premium for Office 365 provides robust filtering technology that enables you to define and manage policy rules for protecting sensitive email content and ensuring compliance. Pre-defined filters are available for healthcare, financial services, state privacy, education and more. Based on the email content, policies can be defined to determine if the email should be blocked, routed, quarantined or encrypted.

ZixProtect Bundles

ZixProtect for Office 365 is available in three different bundles:

	Protect Essentials	Protect Plus	Protect Premium
<i>Email Threat Protection</i>	✓	✓	✓
<i>Targeted Threat Protection</i> <ul style="list-style-type: none"> • Attachment Sandboxing • URL Re-Write/Analysis 		✓	✓
<i>Email Encryption</i>			✓
<i>Data Loss Prevention</i>			✓