zix®

Advanced Email
Threat Protection

From the #1 provider in email security

All-in-One Email Threat Protection | Email Continuity (Optional Add-On)

Benefits:

- Allows good email through, keeps bad email out
- Automatically guards against phishing, spam, threats, and email compromise
- Strong defense against emerging threats
- Keep employees efficient by reducing unwanted emails
- Save time with preset filters
- Increase adoption with an intuitive interface
- Easily customizable, straightforward integration
- Simple to manage and support from one Secure Cloud interface

Customer Ecosystem:

- 90,000+ customers from large enterprise to small business
- Companies with Microsoft 365, on-prem Exchange, and G-Suite
- 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+ Blue Cross Blue Shield (BCBS) plan

No organization today can afford to be without email threat protection

Like the Florida town that paid a $600,000 ransom, nobody sees it coming. That's why you protect.

Zix Email Threat Protection provides multi-layered filtering that permits legitimate email while blocking malicious threats such as phishing, impersonation, malware, ransomware, and spam-type messages—all automatically.

Features

Zix's Advanced Email Threat Protection is easy to use.

Automatic defense
The 99.9% catch rate and ultra low false-positive rate means there's less need to manage a quarantine

Easy to use portal
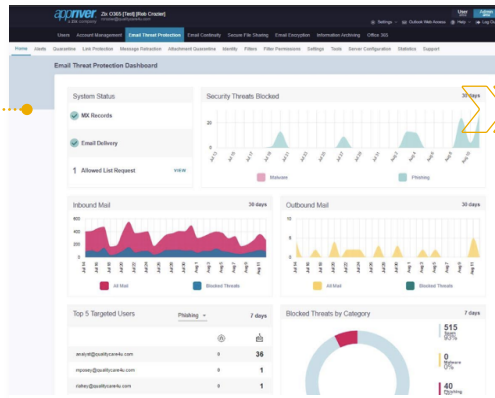Simple and intuitive when needed.

Mobile Access

Dashboards for intuitive management
At-a-glance updates on threats and highly-targeted users.

Message Retraction for Microsoft 365.

Optional add-ons
Email Continuity that spools incoming emails and provides a web portal with full functionality, IMAP/POP

- Impersonation and Domain Protection to prevent spoofing
- Multi-layer filtering
- 24/7/365 live threat analysts
- Daily threat reports and live dashboard
- Attachment scanning, disarming, sandboxing
- Link Protection with Time-of-Click Analysis
- Secure web interface

"A great tool to increase your email threat posture and helps ease your mind about clicky end users!"

- Dale Johnson, Horry Electric Cooperative, Inc.

How It Works

The multi-layer filtering engine delivers an extraordinary level of accuracy that reduces both false negatives (bad emails getting in) and false positives (good emails kept out). This reduces the time you spend managing the system and reduces friction for users.

With Advanced Zix Email Threat Protection You Get

Attachment Quarantine performs forensic analysis on attachments in Zix's secure, cloud-based sandbox environment. It can also deliver a disarmed version of files by removing macros or converting files to PDF.

Link Protection rewrites all links to safe versions and performs time-of-click analysis on the destination address. Based on testing, users are either automatically redirected to a safe site, provided a warning for suspicious sites, or blocked from potentially malicious sites.

Message Retraction (for Microsoft 365) enhances your incident response with the ability to retract malicious emails already delivered to users' inboxes. This minimizes risk by taking malicious email out of users' hands and quickens remediation. The system keeps a detailed audit trail.

24/7/365 Live Threat Analyst Team is constantly identifying new threats, updating the system, and providing warnings.
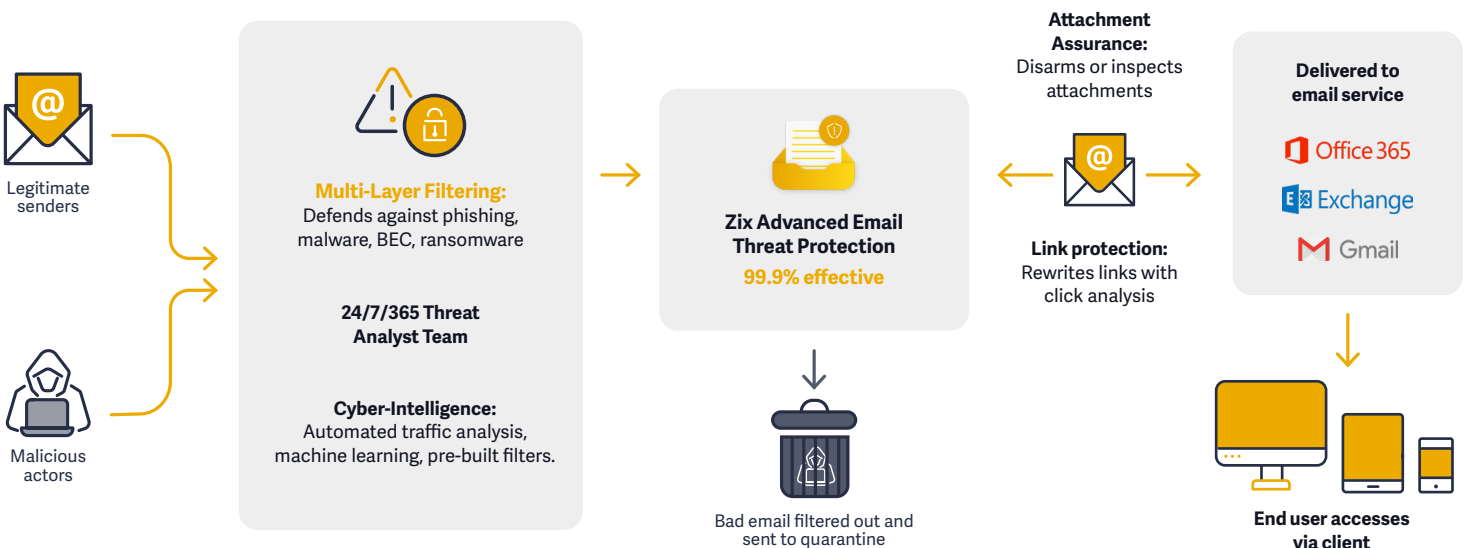
Complimentary
Office 365 Security Audit

Upon launch, Zix offers a complimentary Office 365 Security Audit that automatically checks for hidden vulnerabilities and malicious settings, and helps remediate them.

Office 365

Mailflow

Legitimate senders

Malicious actors

Multi-Layer Filtering:
Defends against phishing, malware, BEC, ransomware

24/7/365 Threat Analyst Team

Cyber-Intelligence:
Automated traffic analysis, machine learning, pre-built filters.

Zix Advanced Email Threat Protection
99.9% effective

Bad email filtered out and sent to quarantine

Attachment Assurance:
Disarms or inspects attachments

Link protection:
Rewrites links with click analysis

Delivered to email service

Office 365
Exchange
Gmail

End user accesses via client

Great for when:

- ◯ Users say legitimate emails aren't being delivered

- ◯ The current solution lets malicious emails or spam through

- ◯ There's concern about business email compromise (BEC)

- ◯ Your network is being targeted with phishing attempts

- ◯ You want to catch conversation hijacking attempts

- ◯ You need to achieve regulatory compliance

Why Now

With increases in social engineering, broad-based spam, and targeted attacks, cybercriminals are exploiting known vulnerabilities in the biggest email providers to steal privileged information. In many cases, businesses don't catch the breach, don't know how to assess the damage, or don't have tools for remediation.

- Attacks are growing more comprehensive and technically savvy
- The costs of a breach are rising
- Reputational risks are growing
- The best remediation is prevention

Why Zix Email Threat Protection?

Ninety-six percent of threats begin with email, reports Verizon. Email Threat Protection secures this major vulnerability in a way that's straightforward to implement and manage. Plus, as an integral part of Secure Cloud, Email Threat Protection works seamlessly with Zix's other Security, Compliance, and Productivity services. Together, they form a fully integrated platform that allows partners and customers to create a secure, modern workplace.

- Superior efficacy against email-borne threats
- Advanced protection against even zero-hour attacks
- Integrates seamlessly
- Intuitive and user-friendly

Learn more at Zix.com