Prevent Business Email Compromise
Detect, block and classify email designed to trick people into sending money or sensitive data. Our multi-layered approach includes authentication, robust email policies, dynamic classification and data loss prevention (DLP).

(FBI) "Business Email Compromise: The 5 Billion Dollar Scam" May, 2017

Visibility and Forensics
Cyber attacks target people. To respond effectively, you need a clear understanding of who is being targeted and what data is at risk. You need forensic detail about every attack. We help you respond faster and protect the people and data that matter most.

Stop Phishing and Account Compromise
We stop external phishing emails before they reach user inboxes. Plus, we help you identify and remediate compromised accounts that could be used for internal fraud or cyber attacks.


Accurate Bulk Mail Classification
The only thing worse than bulk email slipping through your inbox filters is legitimate email being blocked. We classify incoming email as spam, bulk or mission-critical with pinpoint accuracy.

Cloud App Protection
Controlling access to online data is critical. With our CASB solution, you can grant the right levels of access to users and third-party apps based on the risk factors that matter to you.

Threat Response
Auto-Pull
Reduce threat exposure and save hours of work per incident with our Auto-Pull feature. Auto-Pull automatically locates delivered emails with malicious URLs or attachments and pulls them into a quarantine so that your users can't click.

Easy Security Ecosystem Integration
Your security tools should work together for a far-reaching, cohesive defense. We integrate your security events with your existing infrastructure. This gives you better threat intelligence, faster threat containment and greater visibility. Integration Partners include Palo Alto Networks, Splunk, Okta, CyberArk and more.

Email Continuity
Modern business relies on email. In the event of an Office 365 outage, we keep your email flowing to keep your business humming. Avoid the security and compliance risks caused by frustrated employees turning to non-sanctioned communication channels.

Archiving, E-Discovery, and Supervision
Get comprehensive content capture for archiving, real-time e-discovery searches and streamlined supervision. This helps you stay compliant and avoid regulatory fines.

Want to learn more about how you can protect Office 365? www.proofpoint.com/office365

© Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.

Effective Protection with Great Customer Support
Of the global Fortune 100 with a 95% customers satisfaction rating. We protect 60% Top 10 Reasons For organizations migrating to the cloud, Microsoft Office 365 is a whole new way of working—one that requires a whole new approach to security and compliance. Today's cyber attacks target people, no matter where they're working or what device they're using. That's why Office 365 customers are turning to Proofpoint for a people-centered approach to security and compliance.

Customers Choose Proofpoint TO PROTECT Office 365