ContentCatcher®
Email Security for Business

Solution Brief

ContentCatcher® for Office 365

Enable Advanced Security and Continuity for Small and Medium Enterprises

Office 365 represents Microsoft's cloud-based email and collaboration platform. Yet many—if not most—Office 365 customers have found themselves requiring more advanced security capabilities than are available.

The ContentCatcher® platform provides the additional layer of advanced threat protection functionality that enterprises running Office 365 need to stop phishing attacks. This enables organizations of all sizes to take full advantage of the benefits of Office 365 without sacrificing the key security requirements.

- **Advanced Threat Protection:** ContentCatcher®'s Targeted Attack Protection™ extends Microsoft® Office 365™ email security measures by protecting high value data from targeted spear-phishing attacks, imposter emails (including business email compromise), and zero-day malware.
- **Comprehensive Spam Detection:** ContentCatcher® MLX™ technology uses advanced machine learning techniques and analysis and works with the traditional spam engines of Microsoft® Office 365™ to protect users from the most cunning attacks.
- **Innovative Email Continuity:** The ContentCatcher® Emergency Inbox gives Microsoft® Office 365™ users automatic access to their email if unexpected Office 365 downtime hits, keeping business email fully operational at all times

Defending Against Targeted Attacks

Microsoft offers basic email security features with Microsoft Exchange Online Protection (EOP) to provide email hygiene services. It relies on traditional filtering techniques such as IP reputation, volume, and signature-based anti-virus scans. More is needed to protect against modern day attacks, particularly as email is the most reliable way for threats to reach your users. For example, at ContentCatcher®, we see 1 in 10 emails contain malicious attachments. More sobering, nearly 1 in 2 click on phishing links within the first hour of receipt[1].

ContentCatcher® for Office 365 takes a next generation approach to deliver industry-leading email security for SMEs to known and new attacks. These attacks may use non-malware based attacks using social engineering to target users with imposter emails, credential phish, or even use malicious attachments and URLs to compromise your business network. By taking advantage of our enterprise-class Targeted Attack Protection analysis techniques, you can protect your end users by adding security scrutiny that cannot be matched by traditional approaches.

Securing Email Communications

It's the data that makes a business attractive to an attacker, not the size of an organization. Corporate email typically contains up to 70% of an enterprise's sensitive data, making email one of the key exposure points for inadvertent data loss. Proper filtering of outbound email for sensitive content, and appropriate rejection or encryption of such messages is crucial, especially in light of increasingly stringent industry and government regulations with associated penalties.

How does ContentCatcher® work with Microsoft Office 365?

Getting set up on ContentCatcher® for Office 365 is a simple and intuitive process. ContentCatcher® is deployed between the Office 365 environment and the Internet. Inbound mail is routed to ContentCatcher® by changing your MX records. After email is processed by ContentCatcher® it is then routed to Office 365. Since ContentCatcher® sits in front of Office 365, the ContentCatcher® Emergency Inbox is activated instantly and automatically when it detects an Office 365 email service outage, enabling your users to access email (i.e. open, reply, compose, etc.) for business as usual. Outbound email is routed to ContentCatcher® before going to the internet. What's more, we have a dedicated support team to help you through the whole process of strengthening security for your Office 365 users easy and hassle-free, just as it should be.

ContentCatcher®
Email Security for Business

Office 365