Cyberinc Email Security

Attackers are opportunistic. During the pandemic, many hackers have taken advantage of victims' search for information. By luring online users into opening malicious emails, links, and attachments, these criminal groups have preyed on victims' insecurities during a precarious time. If traditional email security solutions were good enough, why do attackers still choose email to start ransomware and phishing attacks?

Organizations have reduced costs and improved service to remote users by moving to cloud email services. But the shift from native apps to web email clients on the endpoint isn't clear cut. Email like Office 365 may run from the browser, but that doesn't stop some users from opening the desktop app. Moving to the cloud email services hasn't reduced security requirements. It has added web email without removing the desktop client, increasing your attack surface.

Cyberinc Email Security

Isla has always been able to address the risk from the web as an attack surface, including webmail, documents, and email links. Now Isla is also able to protect against malicious attachments delivered to traditional email clients. By integrating email security, Cyberinc removes the administrative challenge of security vs. usability while simultaneously taking the burden of ensuring "click security" in email and web away from end users.

We want perfect security for our organizations, but our users aren't perfect. We can't stop users from clicking email links and attachments because users have to click to do their work. Fortunately, productivity must no longer be a cost of security. We can stop bad things from happening when users click links without compromising the user experience. With Cyberinc Email Security, organizations can close the email security gaps in Microsoft 365 by isolating links and scanning attachments to prevent email attacks via web and native Outlook clients.

Attachments

Malicious email attachments add a twist to protecting users. Viewing files in a remote disposable web browser is proven safe. But not all files open in a web browser, either because there is no browser-based tool or because the user prefers the desktop app. To prevent attacks through attachments, Cyberinc can quarantine the email, remove malicious attachments from the email base on filetype, size, etc. or render malicious attachments in a safe file format (PDF). Before the email reaches the mailbox, Cyberinc can scan the attachments for known and unknown threats using AV and network Sandbox like FireEye. With Cyberinc Email Security, email attachments cannot harm even the most gullible users.

Links

Browser isolation is proven to prevent attacks when users click on a link that opens in the web browser. No matter what your users click, ransomware and phishing attacks can't reach your endpoints or local network if you're using browser isolation. But what about links that may not open in the remote browser? Cyberinc protects users from email links by rewriting URLs to force them to open in an isolated web browser for additional security against phishing and credential theft attacks. No detection is required. Using a policy-based approach, administrators can control URL viewing in Isla or block URLs based on category. With Cyberinc Email Security, organizations protect their users whether they view email in the Outlook desktop app or a web browser.

User Experience

Cyberinc makes a simple, intuitive change to the user experience. If an email is quarantined, a warning is prepended to the subject line. If attachments are rendered or removed, they are replaced with notifications in the email body.

Architecture

Cyberinc Email Security is built as a standard Office 365 Connector to simplify deployment and complement existing email security. Using an API integration, O365 sends all email to the Cyberinc Connector before email reaches the Exchange mailbox. Cyberinc rewrites URLs, handles attachments, and applies policies. Then, the safe email continues to the user's mailbox. The solution is agentless. Web and desktop email clients work unchanged.

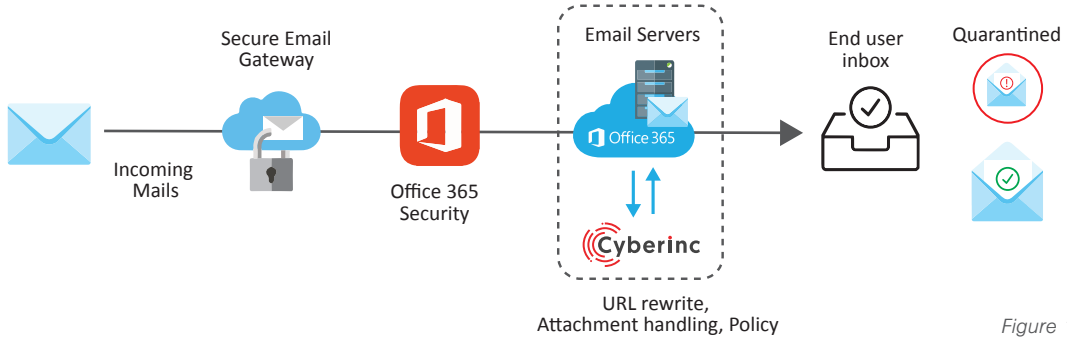
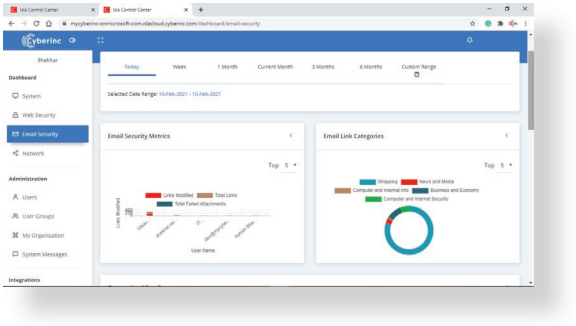


Figure 1: Cyberinc Email Security

Email Security Dashboard

Cyberinc provides central administration and reporting through a dashboard. Essential metrics for security administrators include high-risk users according to the number of attachments blocked and links rewritten, and the number of emails allowed, disallowed, quarantined, and released.



Benefits of Email Security

Simplified deployment	Agentless solution protects native desktop apps and web email clients
Simplified installation	Cyberinc Connector for O365 eliminates architecture requirement to alter Mail Exchanger (MX) records
Administrative controls	Adapt your security to suit your organizational needs with central policy management
Optimal end user experience	Maximize end user experience with in-message notifications - deliver safety without compromise or productivity loss.
Enhances existing email security	Complements Office 365 security and Secure Email Gateways (SEG)
Quick time to value	Optimize the time to security and maximize the ROI from your email security investment.

About Cyberinc

Cyberinc prevents web, email, and document-based threats before the breach. Cyberinc uses a Zero Trust model, powered by isolation-based security, to shrink the exposed threat surface and eliminate the risk of breach from an inadvertent click or document download. Cyberinc simplifies security by preventing threats before they become a breach. Cyberinc is trusted by business and government institutions around the world.

2021.02.11.1

Contact us

+1 925-242-0777
info@cyberinc.com