Symantec

TECHNICAL BRIEF

Prevent Ransomware When Using Microsoft Office 365

Symantec Email Security.cloud and CloudSOC give you the visibility and protection you need

Introduction

The world is moving to the cloud. Everyone knows the benefits—greater productivity, flexibility, scalability, cost savings, and more. As it happens, those benefits are nicely captured in Microsoft Office 365.

But as your organization moves quickly to capitalize on all Office 365 has to offer, despite all your organizational gains, you may be losing visibility into, and control over, what you send to, store in, and receive from the cloud.

Security that worked well in your on-premises environment just doesn't cut it in the cloud. Office 365 built-in security doesn't provide the same level of protection you would demand for your on-premises defense.

If you rely only on Office 365 built-in security, your organization may still be at risk for account takeover, ransomware attacks, and data loss.

Ransomware Attacks in Office 365

Bad actors attempt to exploit Office 365 in a number of ways (including email, cloud account access, cloud file sharing, and cloud-to-endpoint sync and share) to try to infect your environment with ransomware. A single mistake from a single user is all it takes for ransomware to get in and start encrypting hard drives and files, even those in cloud storage.

As your organization increasingly uses the cloud to operate applications, store and share data, and manage email, you need a cloud threat protection system that detects and analyzes malicious files and email, and prevents them from reaching your users.

To keep ransomware out of your organization, you need to prevent malicious files and email from reaching your users, and carefully control cloud-sharing permissions. If ransomware gets in your cloud environment, you need to minimize the damage by detecting, and interrupting, the start of a mass encryption event—this is especially important in Office 365 where you may be storing, sharing, and syncing a lot of your critical business data.

Compromised cloud login credentials, public links, and externally accessible file shares can also bring ransomware from other cloud apps into your Office 365 environment. Then ransomware can use the sync-and-share capabilities between your endpoints, Office 365, and other cloud repositories to quickly spread itself across your organization.

The Symantec Defense

Symantec helps stop ransomware in Office 365 (and other cloud services) by combining email security and cloud access security broker (CASB) technologies. Symantec Email Security.cloud helps detects ransomware (and other threats) in, or attached to, emails; it also blocks users from accessing links to malicious websites. CloudSOC, our CASB solution, extends security visibility and control deep into Office 365 and other cloud apps, helping to detect ransomware and preventing its spread.

Cyber criminals peddling ransomware may try to bypass security checks by sending clean emails with a link to a short-lived website. Symantec Email Threat Isolation allows users safely click on links and interact with these websites inside an isolated, secure, and disposable container: Downloads are prevented, and users cannot reveal their credentials (which could lead to further attacks). Symantec is the only vendor integrating this technology with its email security platform.

What about content hosted in Office 365 or originating from the cloud? Symantec employs several measures to identify and contain threats in content. Take advantage of both Symantec email security and CASB technologies for broader and deeper protection against threats contained in:

- Office 365 content including inbound and outbound email
- Files, email, and other content stored in Office 365
- Content in transactions between users and Office 365
- Content in cloud-to-cloud sharing

Both Email Security.cloud and CloudSOC make use of Symantec's highly effective antimalware engines, file and URL reputation insights, machine learning, and sandbox techniques to identify advanced threats. If Symantec Email Security.cloud finds an advanced threat, it automatically 'claws back' infected emails from a user's inbox before the threat gets activated.

Many attacks unfold in stages and it's always possible that a threat manages to sneak into your Office 365 environment. So CloudSOC uses a highly sophisticated, machine-learning-driven user behavior analytics engine that continuously monitors user behavior and account access to identify risky behavior patterns. These high-risk activities include:

- Encrypted file activity (a ransomware hallmark)
- Abnormal login and cloud access behavior Preventing data loss, whether it's accidental, negligent, or malicious, is essential to the success of any information security program
- Unsafe cloud access permissions
- Abnormal uploads, downloads, or data destruction

If it detects risky behavior, CloudSOC automatically protects your Office 365 environment with numerous policy-based enforcement actions such as removing access permissions, quarantining files, and blocking activities.

Finally, Symantec continuously updates our external threat detection capabilities with threat intelligence feeds from the Symantec Global Intelligence Network, the world's largest civilian threat database. Approximately 1000 cyber warriors monitor and analyze attack activity seen by millions of global endpoints to ensure new attacks are shut down as soon as they emerge.

Next Steps

To prevent ransomware, you need an integrated defense that protects against cloud and endpoint entry. Symantec Endpoint Protection (SEP) uses advanced machine learning to detect polymorphic malware, and intrusion protection that blocks ransomware attempts to download encryption keys. If SEP detects ransomware, it isolates the endpoint(s) to prevent lateral movement.

For More Information

Please visit the Symantec Securing Microsoft Office 365 page.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com