Symantec

TECHNICAL BRIEF

Prevent Account Takeovers 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.

Account Takeovers in Office 365

In the cloud, your credentials are the keys to the kingdom. When bad actors own your username and password, they in effect become you. This fact can make Office 365 a tantalizing, extremely popular one-stop-shop opportunity for attackers: With your credentials, they can log in as you across all Office 365 functions. Unfortunately, Office 365 native security may not provide the visibility you need to tell whether a cloud-based account is being used by an authorized user or being exploited by cyber criminals.

Most successful account takeovers start as phishing attacks (which mimic legitimate requests to reset usernames and passwords), brute force attacks (in which bad actors try repeatedly to get your credentials), and malware (which enters from compromised endpoints or as shared content from other cloud accounts). You need to protect your Office 365 accounts against all of these.

The Symantec Defense

Help protect your Office 365 environments from account takeover with Symantec Email Security.cloud and CloudSOC, our cloud access security broker (CASB).

Most attacks target email. Symantec Email Security.cloud scans external email—contents, attachments, and links—at the cloud perimeter, helping to snuff out malware, block user access to suspicious websites, and identify attempts to impersonate legitimate users. Symantec CloudSOC scans internal email, both at rest in the Office 365 cloud and as it travels within the organization.

Symantec Email Security includes Email Threat Isolation, which renders suspicious websites (accessed via email) in read-only mode, thus helping to prevent infection and stop users from entering their credentials. Symantec is the only email security vendor that integrates this technology with its email security platform.

Working alongside Email Security, CloudSOC helps you see into all Office 365 application activity and monitors transactions between your users and Office 365 apps. In this way, it identifies malicious behavior even when users are remote or using personal, unmanaged endpoints. CloudSOC also helps detect the use of unsanctioned cloud apps and email and applies appropriate protection.

CloudSOC applies data science-driven user behavior analytics to identify strange and malicious activity in Office 365 apps (such as email, OneDrive, SharePoint, Teams, and Yammer)—it then assigns each user a ThreatScore, which adjusts whenever individual behaviors exhibit less or more riskiness. You can enforce policies via alerts, enhanced user authentication requirements, or even by quarantining or blocking users, or blocking their access to data.

With this capability, CloudSOC helps protect against brute force login attacks, excessive uploads or downloads, data destruction, the sending or sharing of sensitive data to external entities—all behaviors that indicate an account has been taken over. It's critical that you implement strong antimalware, reputation, sandboxing, and other capabilities to combat advanced persistent threats in the cloud and on the endpoint. Malware drives account takeovers by hijacking active user sessions, and compromised accounts use cloud accounts to spread malware organization wide.

Next Steps

You can further defend against account takeover by adding strong multifactor authentication at login. Symantec Validation and ID Protection helps ensure that, even if a user's credentials have been compromised, attackers are frozen out unless they provide additional authentication (such as a token code, fingerprint scan, push notification, or one-time passcode). Symantec Validation and ID Protection also determines whether the device or web browser is healthy, and accommodates different levels of access risk by stepping up authentication.

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