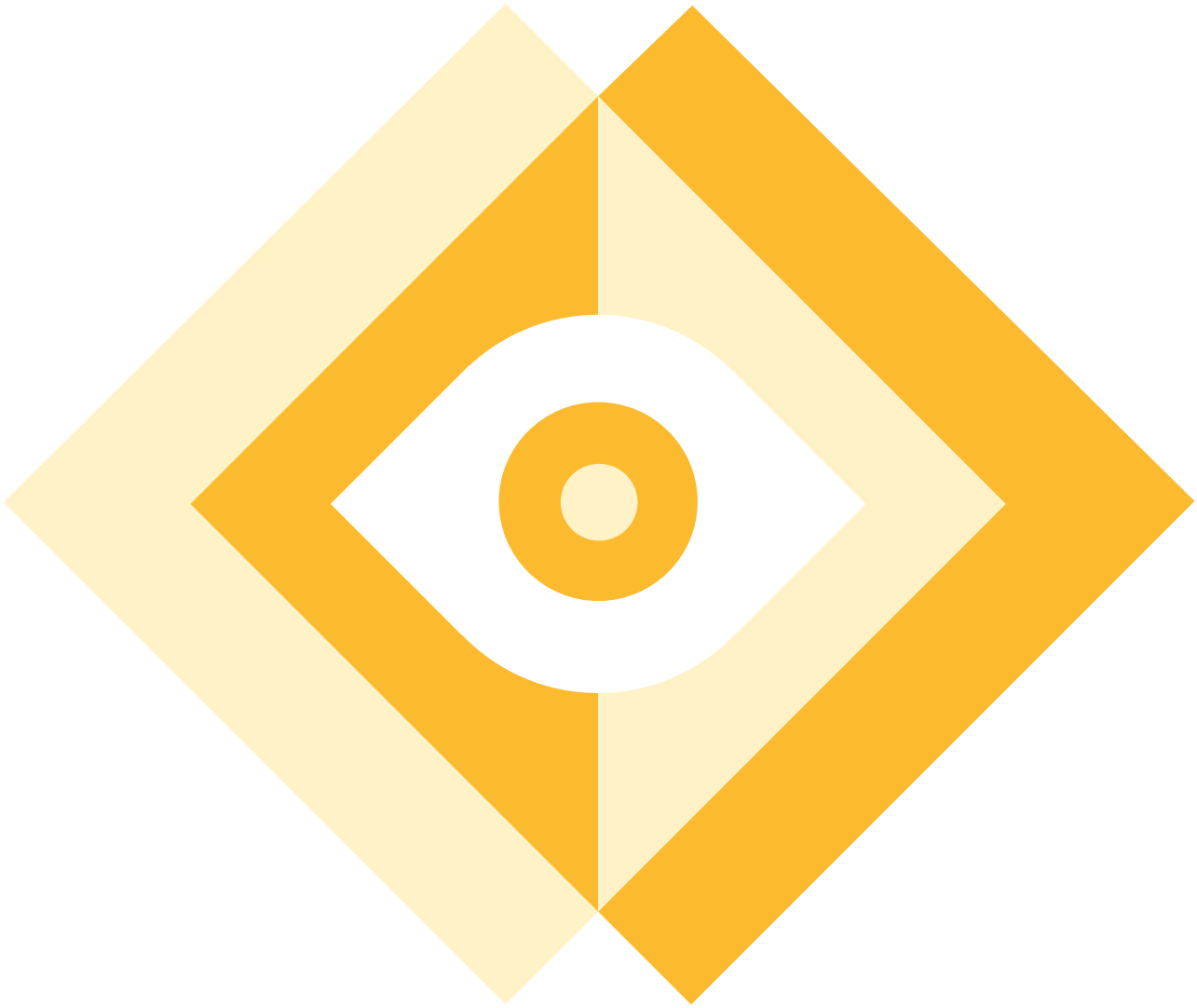

Prevent Account Takeovers, Ransomware Attacks, and Data Loss When Using Microsoft Office 365

WHITE PAPER

Symantec™

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's built-in security, your organization may still be at risk for account takeovers, 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), or 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

Better 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—content, 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 lets 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.

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. You also need the ability to 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 prevent 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 to 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 help 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 help 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
- 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 1,000 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 stop ransomware, you need an integrated defense that protects across the cloud and endpoints. Symantec Endpoint Protection (SEP) has advanced machine learning to detect polymorphic malware, and intrusion protection that blocks ransomware's attempt to download encryption keys. If SEP detects ransomware, it isolates the endpoint(s) to prevent lateral movement.

Data Loss in Office 365

Cloud apps, such as those in Office 365, move key information outside the traditional corporate perimeter, inadvertently exposing your organization's intellectual property and compliance-sensitive information to greater risk.

Confidential data loss can be accidental/unwitting. It takes only a moment to upload a file to a shared OneDrive folder, add content to a document in Teams, or send an email that contains confidential data. Data loss can also be malicious and deliberate. Hackers and malware are looking to the cloud for confidential data to steal.

What Is Confidential Data?

Confidential data includes critical business intelligence as well as regulated data such as personally identifiable information (PII), protected healthcare information (PHI), and payment card information (PCI).

Preventing data loss is more critical than ever as your organization strives to comply with expansive and evolving regulations (HIPAA, GDPR) and avoid the devastating consequences of a data breach.

The Symantec Defense

Symantec CloudSOC, our cloud access security broker (CASB), and Email Security.cloud combine to further your organization's ability to identify, protect, and control access to sensitive data.

Symantec CloudSOC automates data security, data loss prevention, and access control to limit data loss and exposure in Office 365. It automatically detects confidential content exposed in apps such as email, OneDrive, SharePoint, and Teams. It also provides visibility into all your confidential data in Office 365: Where it is, who is responsible for it, what type of confidential data it is, and who has access to it.

CloudSOC also monitors user activity within Office 365 and in transactions with Office 365 in real time, detecting unsafe data practices and enforcing policies to:

- Undo unsafe sharing actions
- Delete highly sensitive content that doesn't belong in Office 365
- Block unsafe uploads or downloads
- Quarantine sensitive content

CloudSOC ContentIQ uses a highly accurate data classification engine that automatically and accurately helps detect and classify your company's sensitive data—providing some much needed visibility into what's in your Office 365 apps, and into what sensitive content is at risk of exposure.

ContentIQ examines a broad range of file and field types (including documents, databases, sound and video, graphics, executables, custom forms, and more). It can examine structured, unstructured, and interactive content in emails,

messages, notes, storage, and more in the cloud. It inspects virtually any file type and detects forms specific to your organization that contain sensitive data, even in handwritten content. Unlike other CASB tools, CloudSOC doesn't need time-consuming custom tuning because of its sophisticated machine learning engine.

With CloudSOC ContentIQ, you control exactly how Office 365 accounts and content are accessed, used, emailed, and shared by employees, contractors, vendors, and clients. And you enforce policies based on location, device type, user role or group, user behavioral risk level, and more across email, file sharing, collaboration, and other Office 365 apps.

Symantec Email Security.cloud offers tools to discover and protect sensitive data in outbound email. These include using policy configuration, compliance and regulatory templates, email encryption, and more. Email Security.cloud analyzes multiple email components (including the email body, subject, headers, and attachments) and takes a range of actions when content matches administrator-created rules; meanwhile, approved messages pass through to their intended recipients. Emails with sensitive content are automatically protected with policy-based encryption so they can be safely exchanged with external recipients.

Next Steps

Your organization can go a step further to enforce data protection, using one centrally managed Symantec solution for all cloud apps, email, endpoints, data centers, and network. Both CloudSOC and Email Security.cloud seamlessly integrate with Symantec Data Loss Prevention to enforce the same data protection policies across your organization.

Conclusion

Office 365 has provided many organizations a great first brush with the cloud, enhancing employee productivity and streamlining IT. However, to keep your organization and data safe, Office 365 should be shored up with Symantec security. Symantec Email Security.cloud and CloudSOC minimize the risk of account takeover—verifying sender identity and helping protect user accounts from phishing attempts, malware, and more. Together, Symantec CloudSOC and Email Security.cloud help detect, contain, and block ransomware, whether it originates from cloud email, compromised files, or targeted attacks against your users. And they help give you visibility into, and control over, cloud apps and data so you can prevent data loss, whether accidental, negligent, or malicious. It's what you need to take full advantage of all Office 365 benefits.

Try a Free Risk Assessment

Discover your exposure with a **Free Office 365 Data Risk Assessment**.

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

19B186343_WP_O365-use-cases_EN