**HỌC VIỆN KỸ THUẬT MẬT MÃ**

KHOA AN TOÀN THÔNG TIN

-----🙞🙜🕮🙞🙜-----

**BÀI TẬP LỚN MÔN:**

**An Toàn Điện Toán Đám Mây**

**Đề Tài:**

**Tìm hiểu về giải pháp Office 365 Security của Symantec**

Giảng viên hướng dẫn : Bùi Việt Thắng

Sinh viên thực hiện : Phạm Thừa Quảng

Nguyễn Thành Nam

**Hà Nội, tháng 10 năm 2020**

**MỤC LỤC**

[**MỤC LỤC i**](#_Toc26453305)

[**DANH MỤC HÌNH ẢNH ii**](#_Toc26453306)

[**MỞ ĐẦU iii**](#_Toc26453307)

[**CHƯƠNG I: Tổng quan về mô hình điện toán đám mây office 365 1**](#_Toc26453308)

[1.1. TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY 1](#_Toc26453309)

[1.1.1. Giới thiệu về điện toán đám mây 1](#_Toc26453310)

[1.1.2 Mô hình điện toán đám mây office 365 2](#_Toc26453311)

[1.1.3. Tiện ích trong Office 365 3](#_Toc26453312)

[1.1.4. Chế độ an toàn và bảo mật thông tin trên Office 365 6](#_Toc26453313)

[**Chương II: Tìm hiểu về giải pháp Office 365 Security của Symantec 8**](#_Toc26453314)

[2.1 Giới thiệu về Symantec 8](#_Toc26453315)

[2.2 Phân tích các nguy cơ mất an toàn trong office 365 9](#_Toc26453316)

[2.3 Giải pháp Office 365 Security của Symantec 9](#_Toc26453317)

[2.3.1 Ngăn chặn chiếm đoạt tài khoản. 9](#_Toc26453318)

[2.3.2 Ngăn chặn tấn công Ransomware (Mã độc). 10](#_Toc26453319)

[2.3.3 Ngăn ngừa mất dữ liệu. 10](#_Toc26453321)

[2.4 Symantec CloudSOC CASB and Email Security.cloud. 11](#_Toc26453326)

[2.4.1 Chức năng của giải pháp. 12](#_Toc26453328)

[2.4.1.1 Bảo vệ thiết bị đầu cuối. 12](#_Toc26453329)

[2.4.1.2 Bảo vệ dữ liệu bí mật của bạn. 13](#_Toc26453334)

[2.4.1.3 Bảo vệ doanh nghiệp với các người dùng có nguy cơ tấn công cao. 14](#_Toc26453339)

[2.4.1.4 Bảo vệ khỏi các cuộc tấn công nâng cao 15](#_Toc26453342)

[2.4.1.5 Ngăn chặn các cuộc tấn công email 16](#_Toc26453346)

[2.4.1.6 Bảo vệ các dữ liệu nhạy cảm. 17](#_Toc26453351)

[2.4.1.7 Nhanh chóng điều tra và ứng phó sự cố an ninh 18](#_Toc26453356)

[2.4.2 Cách thức triển khai trong hệ thống mạng. 18](#_Toc26453360)

[2.4.3 Lợi ích của giải pháp. 21](#_Toc26453380)

[2.4.4 Ưu điểm và Nhược điểm. 24](#_Toc26453385)

[**Tài Liệu Tham Khảo 25**](#_Toc26453386)

# DANH MỤC HÌNH ẢNH

[Hình 1: công cụ điện toán đám mây office 365 2](#_Toc26453486)

[Hình 2: Các ứng dụng trong Office 365 3](#_Toc26453487)

[Hình 3: danh mục sẳn phẩm của Symantec 8](#_Toc26453489)

[Hình 4: Ngăn chặn các tấn công tới các thiết bị đầu cuối. 12](#_Toc26453504)

[Hình 5: kiểm soát dữ liệu khỏi các đe dọa 13](#_Toc26453509)

[Hình 6: bảo vệ doanh nghiệp với người dùng 14](#_Toc26453513)

[Hình 7:Bảo vệ khỏi các cuộc tấn công nâng cao 15](#_Toc26453517)

[Hình 8: Ngăn chặn các cuộc tấn công email 16](#_Toc26453522)

[Hình 9: mã hóa các dữ liệu nhạy cảm 17](#_Toc26453527)

[Hình 10: điều tra ứng phó với các sự cố an ninh 18](#_Toc26453531)

[Hình 11: Mô hình triển khai giải pháp trên hệ thống mạng. 19](#_Toc26453535)

# MỞ ĐẦU

Cho đến nay, hầu hết tất cả các ngành, lĩnh vực trong cuộc sống đều áp dụng công nghệ thông tin vào công việc xử lý thông tin vì vậy khối lượng dữ liệu mà nó tạo ra vô cùng lớn. Nhiều doanh nghiệp coi dữ liệu là một vấn đề nhạy cảm, vì nó ảnh hưởng đến sự sống còn cũng như sự phát triển của doanh nghiệp đó. Chính vì vậy, vấn đề bảo mật và lưu trữ dữ liệu rất được quan tâm, nhiều doanh đã phải bỏ rất nhiều tiền của cũng như công sức để có được nhưng giải pháp cho bài toán lưu trữ dữ liệu của riêng mình Với sự phát triển của công nghệ thông tin như hiện nay vấn đề lưu trữ và bảo mật thông tin đã có hướng giải quyết đó là Office 365. Symantec là một công ty hàng đầu về bảo mật đã đưa ra các giải pháp công nghệ mới khá mềm dẻo, mang đến cho các doanh nghiệp nhiều sự lựa chọn khác nhau, tùy thuộc vào tình hình tài chính của mình. Nếu doanh nghiệp có đủ kinh phí thì có thể tự xây dựng cho riêng mình một giải pháp, trái lại doanh nghiệp có thể đi thuê dịch này của một nhà cung cấp dịch vụ và phải trả một khoảng kinh phí nhất định tùy thuộc vào nhu cầu và mức độ sử dụng. Symantec cũng đã đưa ra nhưng gải pháp để giúp các doanh nghiệp sử dụng công cụ office 365 làm nền tảng dữ liệu cho doanh nghiệp mình.

**Chương I: Tổng quan về mô hình điện toán đám mây office 365**

**Chương II: Tìm hiểu về giải pháp Office 365 Security của Symantec**

**CHƯƠNG I:** **Tổng quan về mô hình điện toán đám mây office 365**

## **1.1. TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY**

* + 1. **Giới thiệu về điện toán đám mây**

Điện toán đám mây đang nhanh chóng nổi lên như một xu hướng công nghệ, hầu hết các nhà cung cấp công nghệ hoặc sử dụng phần mềm, phần cứng và cơ sở hạ tầng đều có thể tận dụng. Công nghệ và kiến trúc dịch vụ điện toán đám mây cho phép khách hàng của các dịch vụ này không sở hữu tài sản trong các đám mây điện tử nhưng trả tiền trên cơ sở mỗi lần sử dụng. Về bản chất, họ đang thuê cơ sở hạ tầng vật lý và các ứng dụng trong kiến trúc dùng chung. Dịch vụ điện toán đám mây có thể từ lưu trữ dữ liệu cho đến các ứng dụng Web của người dùng cuối, cùng với các dịch vụ điện toán tập trung khác.

Một sự khác biệt quan trọng giữa mô hình tính toán truyền thống và điện toán đám mây là khả năng mở rộng và tính chất co giãn mà điện toán đám mây cung cấp. Thay vì một kiến trúc hệ thống tĩnh, điện toán đám mây hỗ trợ khả năng tự động mở rộng quy mô và nhanh chóng thu hẹp quy mô, cung cấp cho khách hàng các dịch vụ có độ tin cậy cao, thời gian đáp ứng nhanh chóng và sự linh hoạt để xử lý các biến động thông lượng và nhu cầu. Điện toán đám mây cũng hỗ trợ nhiều người dùng, cung cấp các hệ thống cấu hình trong suốt một cách thống nhất mang tính chia sẻ được. Công nghệ ảo hóa cho phép các nhà cung cấp điện toán đám mây có thể chuyển đổi một máy chủ thành nhiều máy ảo, do đó loại bỏ máy tính client-server với các hệ thống một mục đích. Điều này tối đa hóa khả năng phần cứng và cho phép khách hàng tận dụng triệt để và việc đầu tư sẽ theo quy mô sử dụng.

Theo nghiên cứu của Gartner đưa ra doanh thu trên toàn thế giới từ điện toán đám mây năm 2009 là 58.6 tỷ USD, dự báo đạt 148 tỷ USD vào 2015. Nghiên cứu gần đây của IDC 4 chỉ rõ doanh thu trên toàn thế giới từ điện toán đám mây công cộng (public cloud) năm 2010 là hơn 21,5 tỷ USD và đạt 72,9 tỷ USD vào năm 2015, tốc độ tăng trưởng hàng năm là 27,6%. Tốc độ tăng trưởng này gấp hơn bốn lần so với tốc độ tăng trưởng dự báo cho toàn thị trường CNTT trên thế giới nói chung (6,7%). Cũng theo IDC, điện toán đám mây luôn nằm trong tốp 10 các công nghệ đình đám nhất trong các năm từ 2009 đến nay trong lĩnh vực công nghệ thông tin.

Mặc dù có những lợi ích và tiềm năng phát triển như vậy nhưng điện toán đám mây vẫn còn gặp nhiều khó khăn trong việc chấp nhận và nhân rộng, chủ yếu là vấn đề an toàn. Tạm gác qua vấn đề kỹ thuật, từ quan điểm của người dùng thì các vấn đề chủ yếu cản trở việc chấp nhận điện toán đám mây là :

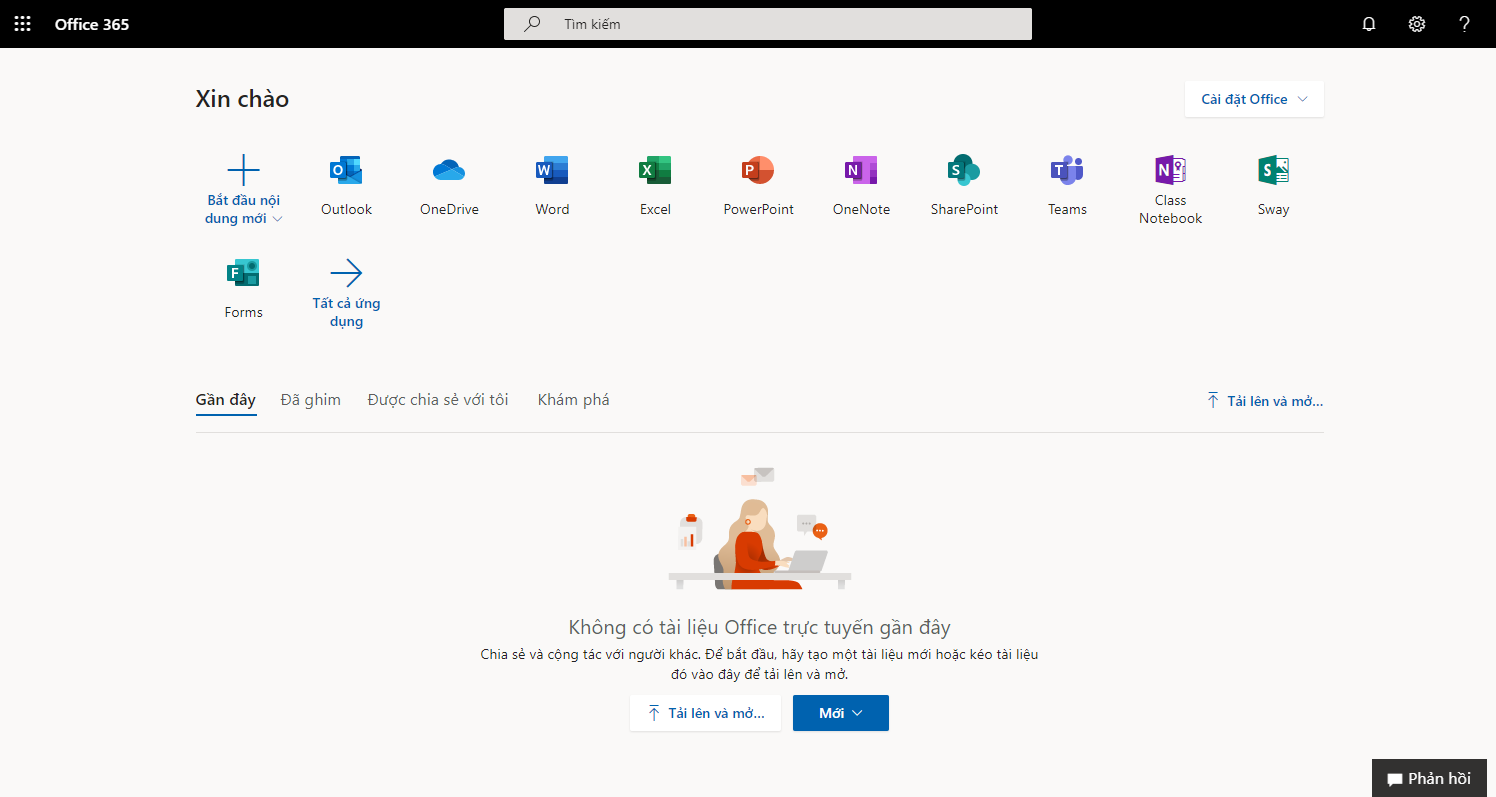
- Các doanh nghiệp giao việc quản lý an ninh cho một bên thứ ba nên có thể không kiểm soát được vấn đề an ninh.

- Tài sản của nhiều người khác nhau nằm trong cùng một vị trí (server) và sử dụng cùng một dịch vụ mà không biết rõ cách thức kiểm soát an ninh, bảo mật của nhà cung cấp.

- Thiếu sự đảm bảo an toàn, an ninh trong các hợp đồng giữa người dùng (người thuê bao) điện toán đám mây và các nhà cung cấp điện toán đám mây.

- Các máy chủ tập trung các tài sản có giá trị và công khai cơ sở hạ tầng làm tăng xác suất các cuộc tấn công nguy hiểm.

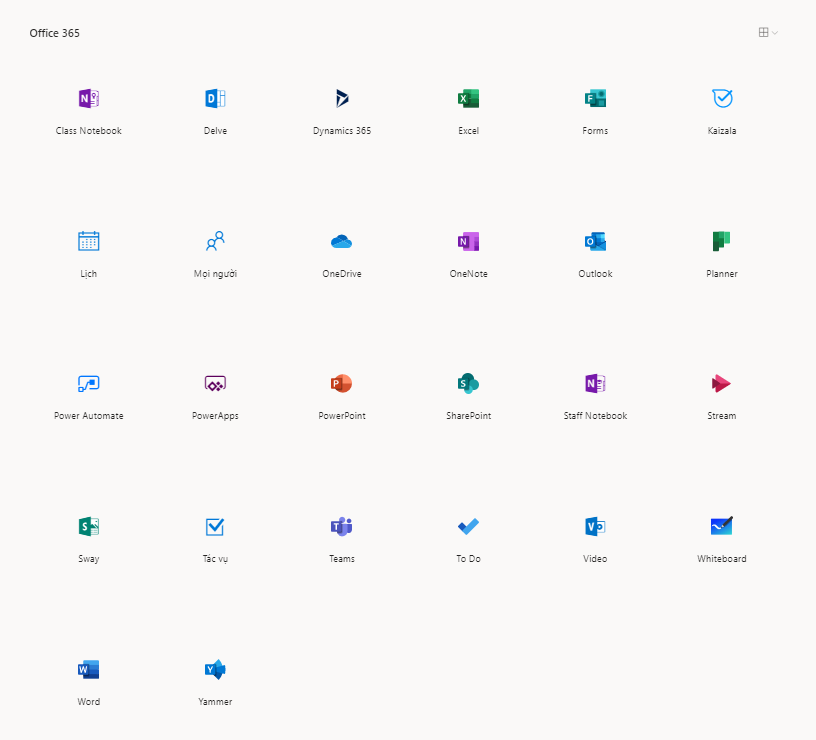
### 1.1.2 Mô hình điện toán đám mây office 365



# *Hình 1: công cụ điện toán đám mây office 365*

**Office 365**: là gói phần mềm dịch vụ thương mại cung cấp các phiên bản đám mây của các phần mềm thông dụng của Microsoft trong đó bao gồm: gói ứng dụng văn phòng [Microsoft Office](https://vi.wikipedia.org/wiki/Microsoft_Office) và các phần mềm máy chủ như [Exchange Server](https://vi.wikipedia.org/wiki/Exchange_Server), [SharePoint Server](https://vi.wikipedia.org/w/index.php?title=SharePoint_Server&action=edit&redlink=1), và [Lync Server](https://vi.wikipedia.org/w/index.php?title=Lync_Server&action=edit&redlink=1).

**1.1.3. Tiện ích trong Office 365**



# *Hình 2: Các ứng dụng trong Office 365*

* + - 1. **Office 365 – OneDrive**

OneDrive là dịch vụ lưu trữ đám mây có thể hoạt động trên nhiều hệ điều hành.

OneDrive for Business cung cấp cho người dùng 1 TB lưu trữ dữ liệu, hỗ trợ lưu toan bộ hình ảnh, video và các tài liệu quan trọng tại một không gian, đồng thời có thể truy cập dữ liệu từ nhiều thiết bị như máy tính, tablet, điện thoại chạy trên các hệ điều hanh như Windows, Mac, Windows Phone, iOS, Android và Xbox.

Người sử dụng OneDrive có thể cộng tác trực tuyến với 5 người cùng lúc thông qua tính năng Office Online để dễ dàng chia sẻ và làm việc cùng nhau trên Word, Excel,

PowerPoint và thậm chí là OneNote Online.

Dễ dàng lưu trữ, truy nhập và khám phá các tệp công việc cá nhân và dùng chung của bạn trong Office 365, bao gồm Microsoft Teams, từ tất cả các thiết bị của bạn. Các chỉnh sửa bạn thực hiện ngoại tuyến sẽ được tải lên tự động trong lần kết nối tiếp theo.

Làm việc nhanh hơn và thông minh hơn với bất cứ ai trong hoặc ngoài tổ chức của bạn. Chia sẻ tệp bảo mật và làm việc cùng nhau trong thời gian thực bằng Word, Excel và PowerPoint trên web, thiết bị di động và máy tính.

Tạo, xem, chỉnh sửa và chia sẻ tệp mọi lúc mọi nơi với ứng dụng OneDrive dành cho thiết bị di động. Dễ dàng chụp bảng trắng và quét thư báo công việc, danh thiếp và các tài liệu bằng giấy khác để giữ an toàn.

OneDrive giúp bảo vệ tệp của bạn. Bạn có thể dễ dàng khôi phục tệp do vô tình xóa hoặc các cuộc tấn công độc hại và người quản trị có thể quản lý chính sách bảo mật để giúp giữ thông tin của bạn an toàn.

* + - 1. **Office 365 - OutLook**

Là bộ công cụ Email trên office 365 giúp chia sẻ lưu trữ dữ liệu 1 cách dễ dàng, là một kênh giao tiếp.

**1.1.2.3 Office 365 – Công cụ soạn thảo**

Trình soạn thảo cung cấp các công cụ kiểm lỗi nâng cao cho người đăng ký Office 365. Phía sau các cảnh, Dịch vụ thông minh xác định chính tả, ngữ pháp và các vấn đề về cơ bản và ngăn trình soạn thảo sẽ giúp bạn hiểu được các gợi ý để bạn có thể thực hiện các lựa chọn cải thiện văn bản của mình.

* **Ưu và nhược điểm của Office 365**

**Ưu điểm**

* Luôn giữ gìn thông tin bí mật của doanh nghiệp:
* Bảo mật dữ liệu cấp độ doanh nghiệp.
* Truy cập dữ liệu đã mã hóa ở bất kỳ đâu, bất cứ khi nào.
* Không khai thác dữ liệu của doanh nghiệp với mục đích quảng cáo
* Truy cập dữ liệu bất kỳ lúc thiết bị nào và thời gian nào
* Toàn vẹn dữ liệu trên tất cả thiết bị
* Dễ dàng chỉnh sữa và chia sẽ dữ liệu
* Làm việc trực tuyến hay ngoại tuyến
* Gia tăng năng suất: Kết hợp cùng nhau để tạo ra, cộng tác và giao tiếp với nhau
* Độ chính xác: Tạo tài liệu theo khuôn mẫu từ người này sang người khác, toàn vẹn tài liệu trên mọi nền tảng, giữ nguyên định dạng tài liệu, tính tương thích cao, giảm độ phức tạp
* Dể dàng thực hiện.
* Dể dàng quản lý.
* Phát triển doanh nghiệp một các linh hoạt.

**Nhược điểm:**

Mặc dù có rất nhiều ưu điểm quan trọng, tuy nhiên vẫn còn mắc phải một số nhược điểm sau:

* *Tính riêng tư*

Các thông tin người dùng và dữ liệu được chứa trên điện toán đám mây bảo được riêng tư, và liệu các thông tin đó có bị sử dụng vì một mục đích nào khác?

* *Tính săn dùng*

Liệu các dịch vụ đám mây có bị “treo” bất ngờ, khiến cho người dùng không thể truy cập các dịch vụ và dữ liệu của mình trong những khoảng thời gian nào đó khiến ảnh hưởng đến công việc.

* *An toàn dữ liệu*

Một vài dịch vụ lưu trữ dữ liệu trực tuyến trên đám mây bất ngờ ngừng hoạt động hoặc không tiếp tục cung cấp dịch vụ, khiến cho người dùng phải sao lưu dữ liệu của họ từ “đám mây” về máy tính cá nhân. Điều này sẽ mất nhiều thời gian. Thậm chí một vài trường hợp, vì một lý do nào đó, dữ liệu người dùng bị mất và không thể phục hồi được.

* *Tinh di động của dữ liệu và quyền sở hữu*

Một câu hỏi đặt ra, liệu người dùng có thể chia sẻ dữ liệu từ dịch vụ đám mây này sang dịch vụ của đám mây khác? Hoặc trong trường hợp không muốn tiếp tục sử dụng dịch vụ cung cấp từ đám mây, liệu người dùng có thể sao lưu toàn bộ dữ liệu của họ từ đám mây? Và làm cách nào để người dùng có thể chắc chắn rằng các dịch vụ đám mây sẽ không hủy toàn bộ dữ liệu của họ trong trường hợp dịch vụ ngừng hoạt động.

* *Khả năng bảo mật*

Vấn đề tập trung dữ liệu trên các “đám mây” là cách thức hiệu quả để tăng cường bảo mật, nhưng mặt khác cũng lại chính là mối lo của người sử dụng dịch vụ của điện toán đám mây. Bởi lẽ một khi các đám mây bị tấn công hoặc đột nhập, toàn bộ dữ liệu sẽ bị chiếm dụng.

Tuy nhiên, đây không thực sự là vấn đề của riêng “điện toán đám mây”, bởi lẽ tấn công đánh cắp dữ liệu là vấn đề gặp phải trên bất kỳ môi trường nào, ngay cả trên các máy tính cá nhân.

**1.1.4. Chế độ an toàn và bảo mật thông tin trên Office 365**

Những vấn đề về an ninh trên Cloud

Trong những năm gần đây, dịch vụ trực tuyến đang dần trở thành một xu hướng phát triển công nghệ điện toán đám mây. Tình hình an ninh mạng có diễn biến rất phức tạp. Các cuộc tấn công ngày càng trở nên tinh vi hơn. Điểm yếu dễ bị tấn tông công đó là nằm ở chính những lỗ hổng bảo mật của các tổ chức do không kịp update bản vá. Trong khi đó dấu vết các cuộc tấn công ngày càng ít, khiến việc truy lùng và tìm kiếm thủ phạm ngày càng phức tạp.

Có ba nguy cơ về an ninh bảo mật đặc thù của điện toán đám mây: Nguy cơ khi chia sẻ tài nguyên, công nghệ; Mất thông tin, lộ thông tin bí mật.Theo đánh giá của các chuyên gia thì lộ thông tin truy nhập dịch vụ là một nguy cơ khá phổ biến trong môi trường điện toán đám mây

Theo các chuyên gia bảo mật CNTT hàng đầu trong lĩnh vực điện toán đám mây quan tâm đến 5 xu hướng bảo mật lớn như:

- Kết nối dữ liệu trên thiết bị điện thoại Smart

- Kiểm soát các truy cập và quản lý danh tính

- Tuân thủ các tiêu chuẩn

- Rủi ro của việc cho thuê điện toán đám mây.

- Sự xuất hiện của các tiêu chuẩn và chứng chỉ liên quan đến điện toán đám mây.

**Chương II: Tìm hiểu về giải pháp Office 365 Security của Symantec**

**2.1 Giới thiệu về Symantec**

**Symantec** (**Symantec Corporation**, thường gọi là **Symantec**) là một [công ty phần mềm](https://vi.wikipedia.org/wiki/C%C3%B4ng_ty_ph%E1%BA%A7n_m%E1%BB%81m) Hoa Kỳ có trụ sở tại [Mountain View, California](https://vi.wikipedia.org/wiki/Mountain_View,_California" \o "Mountain View, California), [Hoa Kỳ](https://vi.wikipedia.org/wiki/Hoa_K%E1%BB%B3). Công ty sản xuất [phần mềm](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m" \o "Phần mềm) [bảo mật](https://vi.wikipedia.org/w/index.php?title=Ph%E1%BA%A7n_m%E1%BB%81m_b%E1%BA%A3o_m%E1%BA%ADt&action=edit&redlink=1" \o "Phần mềm bảo mật (trang chưa được viết)), lưu trữ, sao lưu và sẵn sàng - và cung cấp [dịch vụ chuyên nghiệp](https://vi.wikipedia.org/w/index.php?title=D%E1%BB%8Bch_v%E1%BB%A5_chuy%C3%AAn_nghi%E1%BB%87p&action=edit&redlink=1" \o "Dịch vụ chuyên nghiệp (trang chưa được viết)) để hỗ trợ cho phần mềm của họ. [Netcraft](http://news.netcraft.com/archives/2015/05/13/counting-ssl-certificates.html) đánh giá Symantec (bao gồm cả các công ty con) là [nhà cung cấp chứng thực số](https://vi.wikipedia.org/wiki/Nh%C3%A0_cung_c%E1%BA%A5p_ch%E1%BB%A9ng_th%E1%BB%B1c_s%E1%BB%91" \o "Nhà cung cấp chứng thực số) được sử dụng nhiều nhất. Symantec là một công ty [Fortune 500](https://vi.wikipedia.org/wiki/Fortune_500" \o "Fortune 500) và là thành viên của chỉ số thị trường chứng khoán [S&P 500](https://vi.wikipedia.org/wiki/S%26P_500). Công ty cũng có trung tâm phát triển ở Pune, Chennai và Bengaluru (Ấn Độ).

Vào ngày 9 tháng 10 năm 2014, Symantec tuyên bố nó sẽ tách thành hai công ty kinh doanh độc lập vào cuối năm 2015. Một công ty sẽ tập trung vào bảo mật, công ty còn lại về [quản lý thông tin](https://vi.wikipedia.org/w/index.php?title=Qu%E1%BA%A3n_l%C3%BD_th%C3%B4ng_tin&action=edit&redlink=1" \o "Quản lý thông tin (trang chưa được viết)). Vào ngày 29 tháng 1 năm 2016, doanh nghiệp quản lý thông tin đã được tách ra với tên gọi [Veritas Technologies](https://vi.wikipedia.org/w/index.php?title=Veritas_Technologies&action=edit&redlink=1" \o "Veritas Technologies (trang chưa được viết)) và được bán cho công ty đầu tư [The Carlyle Group](https://vi.wikipedia.org/w/index.php?title=The_Carlyle_Group&action=edit&redlink=1).

Tên gọi Symantec được ghép lại từ các từ **syntax** (cấu trúc), **semantics** (ngữ nghĩa), và **technology** (công nghệ).

Một thương hiệu phần mềm bảo mật doanh nghiệp được [Broadcom Inc.](https://en.wikipedia.org/wiki/Broadcom_Inc." \l "Symantec_Enterprise_Security" \o "Broadcom Inc.) mua vào tháng 8 năm 2019



# *Hình 3: danh mục sẳn phẩm của Symantec*

## **2.2 Phân tích các nguy cơ mất an toàn trong office 365**

Rất tốt cho việc chia sẻ dữ liệu nhưng kh ngăn chặn được việc phơi bày dữ liệu

Việc xóa dự liệu chỉ là xóa dữ liệu cá nhân tại bản thân và những ai chưa nhìn thấy nó. Và điều này giúp office 365 dễ dàng khôi phục lại dữ liệu.

## **2.3 Giải pháp Office 365 Security của Symantec**

Mọi người đều biết những lợi ích của năng suất cao hơn, tính linh hoạt, khả năng mở rộng, tiết kiệm chi phí và hơn thế nữa. Khi điều đó xảy ra, những lợi ích đó được nắm bắt một cách độc đáo trong Microsoft Office 365. Nhưng khi tổ chức của bạn nhanh chóng tận dụng tất cả Office 365, bất chấp tất cả lợi ích tổ chức của bạn, bạn có thể mất khả năng hiển thị và kiểm soát những gì bạn gửi đến, lưu trữ và nhận từ đám mây. Bảo mật hoạt động tốt trong môi trường tại chỗ của bạn chỉ không cắt nó trên đám mây. Bảo mật tích hợp trong Office 365 không có cung cấp mức độ bảo vệ tương tự mà bạn sẽ yêu cầu đối với hệ thống phòng thủ tại chỗ của mình. Nếu bạn chỉ dựa vào bảo mật tích hợp trong Office 365, tổ chức của bạn vẫn có thể gặp rủi ro khi tiếp quản tài khoản, tấn công ransomware và mất dữ liệu.

**Giải pháp giải quyết các vấn đề gì?**

# Ngăn chặn chiếm đoạt tài khoản.

Trong đám mây, thông tin đăng nhập của bạn là chìa khóa của vương quốc. Khi đối tượng xấu sở hữu tên người dùng và mật khẩu của bạn, họ vào hiệu ứng trở thành bạn. Thực tế này có thể làm cho Office 365 trở nên hấp dẫn, cơ hội một cửa cực kỳ phổ biến cho những kẻ tấn công: Với thông tin đăng nhập của bạn, họ có thể đăng nhập như bạn trên tất cả Office 365 chức năng. Thật không may, bảo mật gốc Office 365 có thể không cung cấp khả năng hiển thị mà bạn cần để biết liệu dựa trên đám mây tài khoản đang được sử dụng bởi người dùng được ủy quyền hoặc đang bị khai thác bởi tội phạm mạng. Hầu hết các vụ chiếm đoạt tài khoản bắt đầu như các cuộc tấn công lừa đảo (bắt chước các yêu cầu hợp pháp để đặt lại tên người dùng và mật khẩu), các cuộc tấn công vũ phu (trong đó các diễn viên xấu cố gắng liên tục để có được thông tin đăng nhập của bạn) và phần mềm độc hại (nhập vào từ các điểm cuối bị xâm phạm hoặc như nội dung được chia sẻ từ khác tài khoản đám mây). Bạn cần bảo vệ tài khoản Office 365 của mình chống lại tất cả những điều này.

# Ngăn chặn tấn công Ransomware (Mã độc).

# Các đối tượng xấu cố gắng khai thác Office 365 theo một số cách (bao gồm email, truy cập tài khoản đám mây, chia sẻ tệp trên đám mây, và đồng bộ hóa và chia sẻ từ đám mây đến điểm cuối) để cố gắng lây nhiễm môi trường với ransomware. Một lỗi từ một người dùng là tất cả những gì cần thiết để ransomware xâm nhập và bắt đầu mã hóa ổ đĩa cứng và tập tin, ngay cả những người trong lưu trữ đám mây. Khi tổ chức của bạn ngày càng sử dụng đám mây để hoạt động ứng dụng, lưu trữ và chia sẻ dữ liệu và quản lý email cần một hệ thống bảo vệ mối đe dọa đám mây phát hiện và phân tích các tệp và email độc hại và ngăn chặn chúng khỏi tiếp cận người dùng của bạn. Để tránh ransomware ra khỏi tổ chức của bạn, bạn cần phải ngăn chặn các tệp độc hại và email tiếp cận người dùng của bạn, và kiểm soát cẩn thận quyền chia sẻ đám mây. Nếu ransomware vào môi trường đám mây của bạn, bạn cần giảm thiểu thiệt hại bằng cách phát hiện và làm gián đoạn sự khởi đầu của một khối sự kiện mã hóa, điều này đặc biệt quan trọng trong Office 365 nơi bạn có thể lưu trữ, chia sẻ và đồng bộ hóa rất nhiều dữ liệu kinh doanh quan trọng. Thông tin đăng nhập đám mây thỏa hiệp, liên kết công khai và chia sẻ tập tin có thể truy cập bên ngoài cũng có thể mang lại ransomware từ các ứng dụng đám mây khác vào môi trường Office 365 của bạn. Sau đó ransomware có thể sử dụng các khả năng đồng bộ hóa và chia sẻ giữa điểm cuối của bạn, Office 365 và các kho lưu trữ đám mây khác để nhanh chóng lan rộng khắp tổ chức của bạn

# Ngăn ngừa mất dữ liệu.

# Các ứng dụng đám mây, chẳng hạn như những ứng dụng trong Office 365, di chuyển thông tin chính ngoài chu vi công ty truyền thống, vô tình vạch trần tổ chức của bạn Sở hữu trí tuệ và tuân thủ - thông tin nhạy cảm với rủi ro lớn hơn. Mất dữ liệu bí mật có thể là vô tình / không mong muốn. Nó cần chỉ một lúc để tải tệp lên thư mục OneDrive được chia sẻ, thêm nội dung vào tài liệu trong Nhóm hoặc gửi email chứa dữ liệu bí mật. Mất dữ liệu cũng có thể độc hại và cố tình Tin tặc và phần mềm độc hại đang tìm kiếm trên đám mây cho dữ liệu bí mật để đánh cắp. Ngăn chặn mất dữ liệu là rất quan trọng hơn bao giờ hết tổ chức cố gắng tuân thủ mở rộng và phát triển quy định (HIPAA, GDPR) và tránh sự tàn phá hậu quả của việc vi phạm dữ liệu.

# Dữ liệu bí mật là gì?

# Dữ liệu bí mật bao gồm thông tin kinh doanh quan trọng cũng như dữ liệu được quy định như nhận dạng cá nhân thông tin (PII), thông tin chăm sóc sức khỏe được bảo vệ (PHI), và thông tin thẻ thanh toán (PCI).

# => Giúp bảo vệ môi trường Office 365 của bạn khỏi việc tiếp quản tài khoản với Symantec Email Security.cloud and CloudSOC, our cloud access security broker (CASB).

# 2.4 Symantec CloudSOC CASB and Email Security cloud.

# Giữ các ứng dụng, email và nội dung Office 365 của bạn an toàn với bảo mật hàng đầu trong ngành bảo mật. Với Symantec CloudSOC CASB và Email Security.cloud cho Office 365, bạn có thể bảo vệ email và ứng dụng của mình trước các mối đe dọa, bảo vệ dữ liệu bí mật của bạn và giành quyền kiểm soát cách các tài khoản và nội dung trong chúng được truy cập, sử dụng, gửi email và chia sẻ bởi bạn, nhân viên, nhà thầu, nhà cung cấp và khách hàng.

# 2.4.1 Chức năng của giải pháp.

# 2.4.1.1 Bảo vệ thiết bị đầu cuối.

# Bảo vệ email và dịch vụ ứng dụng Office 365 của bạn từ đầu đến cuối trước các mối đe dọa.

# 

# *Hình 4: Ngăn chặn các tấn công tới các thiết bị đầu cuối.*

# Liên tục phân tích các giao dịch email bên ngoài và bên trong, hoạt động trong ứng dụng, giao dịch với ứng dụng, chuyển động nội dung và nghỉ ngơi nội dung trong Office 365 để phát hiện, chặn hoặc cách ly các mối đe dọa với Symantec Cloud Email Security và CloudSOC CASB. Bảo vệ chống lại các cuộc tấn công mới và mới nổi với bảo vệ nhiều lớp bao gồm học máy, cách ly mối đe dọa email, kiểm soát mạo danh, bảo vệ liên kết, hộp cát trên đám mây, phân tích hành vi và thông tin danh tiếng trên các tệp, URL và nguồn. Có được tầm nhìn sâu nhất vào các cuộc tấn công tinh vi và ưu tiên các sự cố bảo mật với các phân tích bảo mật nâng cao.

# 2.4.1.2 Bảo vệ dữ liệu bí mật của bạn.

# Bảo vệ dữ liệu bí mật của bạn khỏi các mối đe dạo hoặc tiếp xúc.

# 

# *Hình 5: kiểm soát dữ liệu khỏi các đe dọa*

# Nhanh chóng xác định và giảm thiểu mất dữ liệu từ Office 365 bằng DLP có độ chính xác cao trong đám mây quét và tự động phân loại nội dung có cấu trúc, không cấu trúc và tương tác trong OneDrive, Email, Trang web SharePoint, Nhóm và Nhóm và Yammer. Thực thi các điều khiển DLP trên dữ liệu chuyển động và dữ liệu tại phần còn lại từ người dùng cuối đến tài khoản đám mây của bạn đến quản lý email Office 365 của bạn.

# 2.4.1.3 Bảo vệ doanh nghiệp với các người dùng có nguy cơ tấn công cao.

# 

# *Hình 6: bảo vệ doanh nghiệp với người dùng*

# Tự động xác định tài khoản người dùng có rủi ro cao, tài khoản bị xâm nhập và các mối đe dọa trong nội bộ với phân tích hành vi người dùng theo định hướng khoa học dữ liệu. Thông báo, cách ly hoặc chặn người dùng truy cập nội dung và tài khoản nhạy cảm dựa trên người dùng động ThreatScore. Phát hiện các chuỗi lọc dữ liệu phức tạp, chẳng hạn như mẫu tải xuống nội dung từ ứng dụng Office 365 của công ty và sau đó tải nội dung đó lên ứng dụng chia sẻ tệp cá nhân hoặc chụp màn hình bất thường và lặp đi lặp lại, xóa email và xóa tệp.

# 2.4.1.4 Bảo vệ khỏi các cuộc tấn công nâng cao

# 

# *Hình 7:Bảo vệ khỏi các cuộc tấn công nâng cao*

# Liên tục quét nội dung, email và giao dịch Office 365 để khắc phục và ngăn chặn sự phát triển của ransomware, APT và các mối đe dọa phần mềm độc hại mới nổi khác. Cloud Email Security và CloudSOC CASB sử dụng học máy, UBA và Symantec bảo vệ mối đe dọa nâng cao với hộp cát trên đám mây để bảo vệ hiệu quả tổ chức của bạn khỏi các mối đe dọa mới xuất hiện thông qua email hoặc lây nhiễm tài khoản trên đám mây. Phát hiện các cuộc tấn công email tinh vi bằng các đánh giá URL thời gian thực và kiểm soát mạo danh.

# 2.4.1.5 Ngăn chặn các cuộc tấn công email

# Liên kết email vô hại để đánh bại các cuộc tấn công lừa đảo, ngăn chặn hành vi trộm cắp thông tin và nhiễm phần mềm độc hại.

# 

# *Hình 8: Ngăn chặn các cuộc tấn công email*

# Liên kết các Email an toàn, bảo vệ chống lại các email có liên kết đến các trang web độc hại, vì vậy chúng không thể cung cấp phần mềm độc hại, ransomware hoặc các cuộc tấn công nâng cao khác. Bảo vệ này tận dụng Symantec Web Isolation để thực hiện các phiên web cách xa các điểm cuối, chỉ gửi thông tin kết xuất an toàn tới người dùng các trình duyệt. Nó cũng ngăn người dùng gửi thông tin đăng nhập của công ty và thông tin nhạy cảm khác đến các trang web không xác định và độc hại bằng cách hiển thị các trang ở chế độ chỉ đọc.

# 2.4.1.6 Bảo vệ các dữ liệu nhạy cảm.

# Bảo vệ dữ liệu nhạy cảm với mã hóa tự động và quản lý quyền.

# 

# *Hình 9: mã hóa các dữ liệu nhạy cảm*

# Đáng tin cậy, bảo mật dữ liệu nhạy cảm cho dù đó là Lướt trên đám mây (ví dụ: Office 365), trên thiết bị USB, email hoặc tại chỗ. Xác định dữ liệu bằng cách sử dụng phát hiện tự động hoặc phân loại người dùng, trước khi kích hoạt mã hóa liên tục và quản lý quyền kỹ thuật số. Dữ liệu có thể được chia sẻ với bất kỳ người đáng tin cậy nào, chỉ cần sử dụng danh tính để giải mã dữ liệu. Quản trị viên có thể nhanh chóng hình dung ai đang truy cập dữ liệu nhạy cảm, xác định hành vi rủi ro hoặc bất thường và nếu cần, truy cập từ xa. Bảo vệ đầu cuối với Mã hóa trung tâm thông tin Symantec.

# 2.4.1.7 Nhanh chóng điều tra và ứng phó sự cố an ninh

# 

# *Hình 10: điều tra ứng phó với các sự cố an ninh*

# Theo dõi hoạt động trong các ứng dụng Office 365 và cung cấp những hiểu biết quan trọng về tuân thủ, kiểm toán và các bên liên quan khác khi xảy ra sự cố bảo mật. Sử dụng CloudSOC để nhanh chóng điều tra người dùng hoặc hoạt động, tương quan các sự kiện và khám phá những gì thực sự xảy ra với tìm kiếm dữ liệu và trực quan hóa mạnh mẽ hoặc xuất nhật ký sự cố chi tiết sang SIEM của bạn để phân tích. Phản ứng nhanh với các cuộc tấn công bằng các phân tích bảo mật email nâng cao cung cấp khả năng hiển thị sâu nhất vào các chiến dịch tấn công được nhắm mục tiêu và nâng cao bao gồm Các chỉ số thỏa hiệp (IOC) như URL, băm tập tin và thông tin tấn công được nhắm mục tiêu. Truyền dữ liệu đến Trung tâm điều hành bảo mật (SOC) của bạn để nhanh chóng xác định mức độ nghiêm trọng và phạm vi của một cuộc tấn công.

# 2.4.2 Cách thức triển khai trong hệ thống mạng.

# 

# *Hình 11: Mô hình triển khai giải pháp trên hệ thống mạng.*

# Triển khai giải pháp Email Security.cloud ở cửa ngõ dữ liệu an toàn và phần mạng chung không an toàn.

# Bảo vệ email doanh nghiệp khỏi các mối đe dọa nâng cao trong nước như thỏa hiệp email doanh nghiệp, ransomware và lừa đảo.

# Chặn mất dữ liệu nhạy cảm ra bên ngoài thông qua nội dung email và các tệp đính kèm.

# Triền khai giải phải CloudSOC tại cửa ngõ giữa các thiết bị cá nhân và phần mạng được chia sẻ nội bộ chung.

# Bảo vệ các ứng dụng Office 365 như OneDrive, Email, Sharepoint, Yammer và Nhóm khỏi các mối đe dọa và phơi nhiễm dữ liệu nhạy cảm.

# Chặn các mối đe dọa và phơi nhiễm dữ liệu nhạy cảm thông qua các giao dịch người dùng bên trong hoặc bên ngoài với các ứng dụng Office 365 và bảo vệ dữ liệu.

# Đồng thời tích hợp các công cụ bảo vệ không gian mạng:

# Data Loss Prevention (DLP): giúp bảo vệ dữ liệu nhạy cảm khỏi mất mát với các chính sách thống nhất và phát hiện toàn diện.

# Malware Protection: Bảo vệ phần mềm độc hại nâng cao bằng cách sử dụng danh tiếng, phân tích hành vi và công cụ nhận biết máy ảo.

# Web Isolation: liên kết các email tin cậy bảo vệ chống lại các email có liên kết đến các trang web độc hại.

# Encryption: Mã hóa trung tâm thông tin (ICE) cho phép quản lý quyền kỹ thuật số đầu cuối.

# CloudSOC và Email Security.Cloud là những phần không thể thiếu của Nền tảng bảo vệ mạng tích hợp Symantec, cung cấp mối đe dọa đa kênh và bảo vệ dữ liệu hoàn chỉnh trên web, thiết bị đầu cuối, email và ứng dụng đám mây được hỗ trợ bởi các nguồn cấp dữ liệu từ xa Symantec GIN, được tổng hợp và chưng cất từ ​​các sản phẩm Symantec.

# Tích hợp thêm các giải pháp bảo vệ:

# Bảo vệ chống lại các mối đe dọa bên ngoài: Phân tích email đến, phần còn lại nội dung và giao dịch người dùng nội bộ với email trên đám mây, chia sẻ tệp, nhắn tin, v.v., để ngăn chặn các mối đe dọa tinh vi như ransomware, APT, lừa đảo và tấn công spam.

# Protect against internal threats: Quét email nội bộ, giao dịch đám mây và nội dung đám mây để tìm phần mềm độc hại, ransomware và APT. Tự động xác định hành vi đáng ngờ của người dùng để cảnh báo, cách ly hoặc chặn các hành động và tài khoản có rủi ro cao.

# Quản trị dữ liệu nhạy cảm ở mọi nơi: Thực thi DLP khi nghỉ ngơi dữ liệu trong Office 365, chuyển động dữ liệu giữa các nhân viên, chia sẻ tệp bên ngoài và email gửi đi để bảo vệ dữ liệu bí mật khỏi bị lộ, mất và vi phạm.

# Mã hóa dữ liệu bí mật: Tự động mã hóa các tệp chứa nội dung bí mật và kiểm soát quyền truy cập kỹ thuật số trong vòng đời của tệp được mã hóa.

# 2.4.3 Lợi ích của giải pháp.

## Bảo vệ dữ liệu nhạy cảm nhất của bạn với bảo vệ cho Office 365 và tất cả các dịch vụ đám mây:

* Tự động phát hiện tài sản trí tuệ chính và thông tin nhạy cảm tuân thủ trên Office 365, OneDrive, Email, SharePoint, Yammer, Azure, cũng như hơn 100 ứng dụng đám mây.
* Thực hiện bảo mật dữ liệu đơn giản nhưng không thỏa hiệp để kiểm soát quyền truy cập vào văn phòng đám mây của bạn; đẩy mạnh xác thực đa yếu tố (MFA) để đảm bảo quyền truy cập được ủy quyền; và thêm một lớp mã hóa tin nhắn và tập tin để bảo vệ chống lại các vi phạm và đáp ứng các yêu cầu GDPR.
* Thống nhất chính sách bảo vệ dữ liệu, sự cố và báo cáo cho Microsoft Office 365 và Azure, Dịch vụ web của Amazon và hơn 100 ứng dụng SaaS. Áp dụng cùng một chính sách phối hợp cho dữ liệu tại chỗ của bạn, bảo vệ điểm cuối và ngăn ngừa mất dữ liệu mạng.

Chuyển đổi an toàn sang email Office 365:

Email rất nguy hiểm: đó là con đường trực tiếp từ tội phạm mạng đến nhân viên của bạn. Đóng cổng với Symantec Email Security.cloud, mang lại hiệu quả chống thư rác và chống phần mềm độc hại cao nhất hiện có.

* Cô lập các liên kết có khả năng độc hại được sử dụng trong các cuộc tấn công lừa đảo và thông tin xác thực, củng cố bảo mật email Office 365 của bạn.
* Chặn các cuộc tấn công thỏa hiệp email (BEC) tinh vi bằng các phương thức tiên tiến vượt xa các giao thức xác thực người gửi.
* Quét và xóa các tệp phần mềm độc hại với công cụ học máy, hộp cát và phân tích hành vi nâng cao.
* Nhận phân tích tấn công được nhắm mục tiêu với trí thông minh để xác định và khắc phục các cuộc tấn công bảo mật email rất tiên tiến.

## **Bảo mật Office 365 từ nhà môi giới bảo mật truy cập đám mây hàng đầu**

Symantec CloudSOC bảo vệ email và ứng dụng của bạn trước các mối đe dọa, bảo vệ dữ liệu bí mật của bạn và cho phép bạn kiểm soát cách tài khoản và nội dung bên trong được truy cập, sử dụng và chia sẻ.

* Bảo vệ quá trình chuyển đổi của bạn sang email và ứng dụng Office 365 và đến thế giới rộng lớn hơn của các ứng dụng cơ sở dữ liệu và ứng dụng đám mây SaaS.
* Có được khả năng hiển thị, kiểm soát, quản trị truy cập, bảo mật dữ liệu và bảo vệ mối đe dọa cho Office 365 và hơn thế nữa.

## Dữ liệu và ứng dụng của bạn được chuyển lên đám mây - Bảo mật của bạn cũng vậy

Di chuyển lên đám mây giới thiệu các rủi ro bảo mật và tuân thủ mới, nhưng nó cũng cho phép các chiến lược phòng thủ mới cực lớn. Bảo mật mạng được phân phối trên đám mây giúp tăng tính linh hoạt và tăng hiệu suất của Office 365, đồng thời bảo vệ người dùng bằng các chính sách phòng ngừa mối đe dọa và tuân thủ dữ liệu nhất quán ở bất cứ nơi nào họ đi.

Symantec Web Security Service cung cấp một loạt các khả năng tiên tiến, bao gồm cổng web bảo mật (SWG), quét chống vi-rút, hộp cát, cách ly web, ngăn ngừa mất dữ liệu (DLP) và bảo mật email. Khi người dùng của bạn truy cập trực tiếp vào web, bạn có thể mở rộng các chính sách nhất quán theo dữ liệu nhạy cảm của mình mọi lúc mọi nơi. Dịch vụ bảo mật web Symantec cung cấp:

* [Symantec Web Isolation Các](https://www.symantec.com/content/symantec/english/en/products/web-isolation) trang web củaPPPventvent cung cấp phần mềm độc hại 0 ngày cho nhân viên.
* Cơ sở hạ tầng đám mây hiệu suất cao với nội dung tiên phong cho Microsoft và các nhà cung cấp Cloud SaaS khác
* Chính sách bảo mật tự động thích ứng với các thay đổi trong Microsoft Office 365.

Bảo mật dữ liệu và email trong Office 365

Tham gia với nhà phân tích công nghiệp ESG Mark Bowker, Kiến trúc sư bảo mật đám mây của Insight, Richard Diver và Giám đốc kỹ thuật hệ thống của Symantec, Jereme Lee, để tìm hiểu cách:

* Tận dụng tối đa phiên bản Office 365 của bạn bằng cách tăng cường bảo mật đám mây
* Hiểu những gì bảo mật Microsoft cung cấp và cách Symantec bổ sung cho ưu đãi của họ
* Nâng cao bảo mật email, ứng dụng và bảo mật dữ liệu Office 365 của bạn, có thể được sử dụng trên tất cả các ứng dụng đám mây của bạn

# Symantec giới thiệu CloudSOC Mirror Gateway để bảo mật truy cập đám mây doanh nghiệp

  Symantec vào thứ ba đã công bố các bản cập nhật cho danh mục bảo mật đám mây của mình, bao gồm tích hợp Luminate được mua gần đây cũng như một số tính năng mới được thiết kế để bảo vệ khối lượng công việc và ứng dụng đám mây trên toàn doanh nghiệp.

Điểm mấu chốt trong các bản cập nhật là CloudSOC Mirror Gateway mới, nhằm bảo vệ các ứng dụng SaaS mà không can thiệp vào năng suất của người dùng cuối. Nó sử dụng công nghệ Symantec Web Isolation để cung cấp các điều khiển Nhà môi giới bảo mật truy cập đám mây (CASB) cho các thiết bị không được quản lý, cho phép nhân viên truy cập các ứng dụng từ bất kỳ thiết bị nào trong khi vẫn tuân thủ các chính sách bảo mật của quản trị viên.

Ngoài ra, tích hợp mới trong CloudSOC CASB Gateway cho phép kiểm soát chính sách chi tiết trong suốt phiên đám mây bằng cách sử dụng xác thực đa yếu tố thích ứng thông qua Symantec VIP hoặc các giải pháp từ đối tác Symantec TIPP Okta.

"Symantec hiểu sự cần thiết của cách tiếp cận Zero Trust, giúp giảm sự nhấn mạnh vào bảo mật dựa trên vành đai và tập trung vào việc cung cấp quyền truy cập an toàn cho nhân viên bất kể vị trí hoặc thiết bị", Art Gilliland, EVP và GM của các sản phẩm doanh nghiệp cho Symantec nói. "Symantec có một danh mục bảo mật internet và đám mây mạnh mẽ. Chúng tôi tiếp tục đổi mới và tích hợp để giúp khách hàng cải thiện an ninh trong bối cảnh phát triển, đồng thời giảm chi phí và sự phức tạp."

Ngoài ra, Symantec cho biết công nghệ chu vi được xác định bằng phần mềm từ nó [mua lại Luminate gần đây](https://www.zdnet.com/article/symantec-acquires-luminate-security-makers-of-software-defined-perimeter-technology/) hiện được kết hợp trong danh mục đầu tư của mình để cung cấp thêm một lớp bảo vệ cho các ứng dụng doanh nghiệp được triển khai trong môi trường IaaS. Symantec đã mua lại công ty khởi nghiệp Palo Alto vào tháng Hai với kế hoạch gấp hệ thống đám mây truy cập an toàn của Luminate vào Nền tảng phòng thủ mạng tích hợp của nó.

**2.4.4 Ưu điểm và Nhược điểm.**

**Ưu điểm:**

* Ngăn ngừa mất dữ liệu.
* Bảo vệ tài khoản cá nhân và tổ chức.
* Tự đông phát hiện nội dung bí mật để bảo vệ.
* Ngăn chặn các email độc hại.
* Tự động mã hóa các nội dung quan trong cần bảo vệ.
* Khôi phục lại dữ liệu đã xóa do vô tình hoặc bị tấn công.
* Chặn tải lên hoặc tải xuống các dữ liệu không an toàn.

**Nhược điểm:**

* Chi phí duy trì và sử dụng cao.
* Hàng rào bảo mật cao nên hạn chế việc chia sẻ dữ liệu.
* Yêu cầu người dung phải thật sự hiểu và mức độ nguy hiểm để lựa chọn phương pháp bảo vệ phù hợp nhất.

# Tài Liệu Tham Khảo

# Bộ công cụ Office 365 : <https://www.office.com/apps?auth=2&home=1>

# Giới thiệu về office 365 của Microsoft: <https://products.office.com/vi-vn/business/security-and-compliance>

# Giải pháp Office 365 Security của Symamtec : <https://www.symantec.com/solutions/office365>