A Trend Micro White Paper | **Tháng 10/2020**

Đơn giản hóa Network Security trong hệ thống đám mây

>> Cách Trend Micro Cloud One™ giúp đưa bảo mật lớp hệ thống mạng vào môi trường đám mây của bạn một cách dễ dàng

Các doanh nghiệp đang chuyển sang hệ thống đám mây do độ đàn hồi, linh hoạt và khả năng mở rộng của nó. Tuy nhiên, cách để có được lợi ích đó đang trở thành thách thức khi bảo mật đám mây trở lên phức tạp, với vô số tường lửa khác nhau, bộ cân bằng tải và phải cài đặt cũng như quản lí các ứng dụng khác để kiểm tra lưu lượng. Tài liệu này sẽ khai phá cách Trend Micro Cloud One™ – Network Security giúp đơn giản hóa trong môi trường đa hoặc điện toán đám mây, bằng cách đem bảo mật lớp hệ thống mạng lên đám mây mà không gây gián đoạn nghiêm trọng cho ứng dụng của doanh nghiệp.

Phụ lục

BẢO VỆ CHO ĐÁM MÂY MÀ KHÔNG MẤT ĐI QUYỀN LỢI

Khi ngày càng nhiều tập đoàn chọn hệ thống đa hoặc điện toán đám mây, cấu trúc đám mây và đội ngũ bảo mật hệ thống mạng gặp khó khăn để bảo vệ tài sản quan trọng của doanh nghiệp trên khắp các môi trường đám mây khác nhau của họ. Họ cảm thấy những gì có thể hoạt động tại chỗ để đảm bảo an ninh thì không cần thiết phải đưa lên đám mây.

Việc triển khai là một thách thức

Nhiều giải pháp bảo mật hệ thống mạng hiện nay rất khó triển khai bởi vì chúng không được thiết kế cho đám mây. Một số yêu cầu thời gian ngừng hoạt động dài để được đưa vào nội tuyến, một số mô hình cấp phép dựa trên thông lượng đã lỗi thời, số khác không thể triển khai trong cơ sở hạ tầng đám mây sẵn có của doanh nghiệp. Ví dụ, giải pháp trên tác nhân/ máy chủ không phải lúc này cũng khả thi hoặc được như mong muốn với đám mây. Tập đoàn có thể không có quyền triển khai một tác nhân trên máy chủ ảo ở đám mây của nhà cung cấp của họ, hoặc có thể không muốn cung cấp phép tính cho tác nhân bằng chi phí của luồng việc khác.

Ngoài ra cũng có vấn đề về độ phức tạp. Một số lượng lớn thiết bị, bộ cân bằng tải và các "bộ phận luân chuyển" phải được cài đặt và quản lí để triển tra lưu lượng vào và ra. Nếu mỗi đám mây ảo công khai (VPC) cần tường lửa riêng; và nếu một tập đoàn có hàng trăm VPC, gánh nặng quản lí và chi phí sẽ nhanh chóng tăng lên.

Các thay đổi thường xảy ra với sơ sở hạ tầng của hệ thống mạng, để đáp ứng các thành phần được thêm vào như trên, với một vài giải pháp bảo mật yêu cầu địa chỉ IP để thay đổi hoặc xác định cấu trúc liên kết để triển khai. Thiết bị mới được cài vào hệ thống mạng cũng có thể trở nên "quan trọng" về sau, có nghĩa là chúng có thể dễ dàng (hoặc dễ được trả tiền) để bị xóa hoặc chỉnh sửa. Khi ngày càng nhiều thành phần được thêm vào, chúng sẽ bị kém hiệu quả và có thể làm gián đoạn hoặc chậm lưu lượng mạng, ảnh hưởng đến điều hành và hoạt động kinh doanh.

Tất nhiên, có những giải pháp bảo vệ đám mây gốc, nhưng thường chúng bị trói buộc vào nền tảng cụ thể, như là Amazon Web Services (AWS) hoặc Microsoft® Azure®. Có từng biện pháp bảo vệ khác nhàu dành cho mỗi hệ thống đám mây sẽ ngăn không cho tập đoàn có cái nhìn cụ thể về mối đe dọa họ gặp phải. Nó cũng tăng rủi ro quá tải việc quản lí bảng điều khiển/ kiểm soát, tăng khả năng bỏ lỡ thông báo bảo mật quan trọng. Các giải pháp đám mây một nền tảng cũng có xu hướng thiếu tính năng bảo mật chủ chốt, như là vá lỗi ảo ở lớp hệ thống mạng, lọc đầu ra và kiểm tra sâu.

Trên đám mây, việc bảo vệ là trách nhiệm chung

Giải pháp bảo vệ dễ triển khai là bắt buộc đối với doanh nghiệp bởi vì họ chịu trách nhiệm cuối cùng cho những gì họ đưa lên đám mây.

Trong khi nhà chung cấp đám mây đưa ra bộ biện pháp bảo mật toàn diện như một phần trong dịch vụ của họ, các kiểm soát đó thường chỉ bao quát cơ sở hạ tầng của đám mây: thuật toán, kho lưu trữa và v.v. Tập đoàn phải tự đảm bảo an toàn và bảo vệ dữ liệu, ứng dụng và hệ thống điều hành họ đặt hoặc tạo ra bên trong đám mây.

BẢO MẬT ĐƯỢC THIẾT KẾ DÀNH CHO HỆ THỐNG ĐÁM MÂY

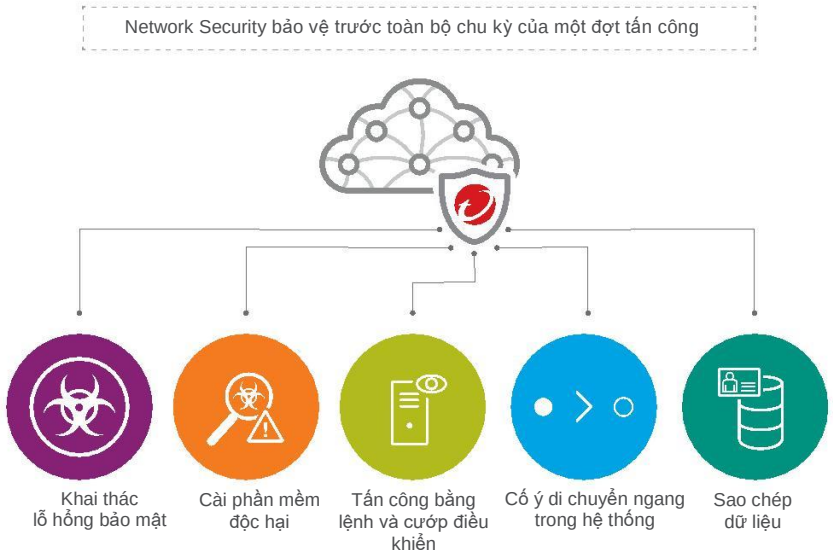
Dành cho tập đoàn tìm kiếm sự đàn hồi, linh hoạt và khả năng mở rộng, các thử thách trên có thể làm quên đi lí do tại sao ban đầu họ muốn chuyển sang hệ thống đám mây. Cái họ cần, chính là giải pháp được thiết kế dành cho đám mây. Nó cần có độ linh hoạt, cách triển khai minh bạch mà không gây gián đoạn cho doanh nghiệp, cùng với sự bảo vệ chủ động, toàn diện cho việc bảo vệ trong đám mây rộng lớn, nhiều lớp mạng, bao gồm toàn bộ khả năng của hệ thống ngăn chặn xâm nhập tại sơ sở (IPS).

Những tiêu chí đó là động lực thúc đẩy Trend Micro Cloud One™ – Network Security.

CẬN CẢNH NETWORK SECURITY TRONG HỆ THỐNG ĐÁM MÂY

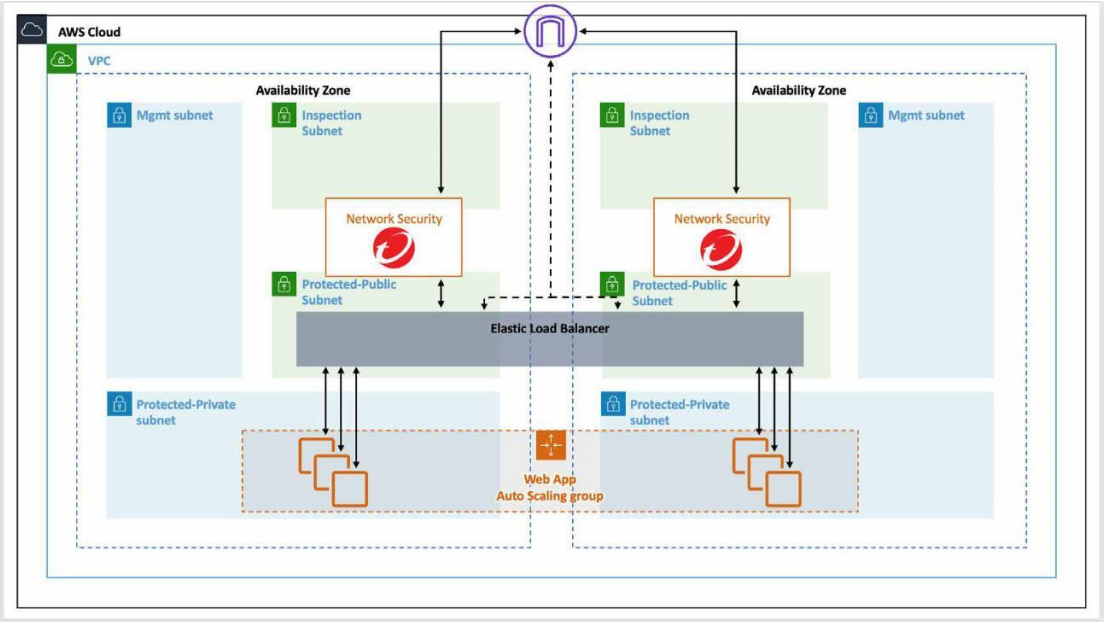
Trend Micro Cloud One™ là một nền tảng phần mềm dịch vụ cung cấp cách tiếp cận linh hoạt, tất cả trong một với bảo mật vật lý, ảo và đám mây. Dịch vụ Network Security của nó là giải pháp nội tuyến, được triển khai minh bạch, nhanh chóng phát hiện và ngăn chặn cuộc tấn công đã hoặc chưa được biết đến lên lớp hệ thống mạng, bảo vệ VPC trên quy mô lớn mà không gây gián đoạn ứng dụng hoặc lưu lượng mạng của doanh nghiệp.

Network Security có thể được triển khai với AWS hoặc Azure. Phương thức nhiều tùy chọn triển khai của nó giúp sản phẩm có thể chèn vào môi trường đám mây hiện có, bất cứ khi nào và tại bất cứ đâu khi cần đến. Nó cũng có thể được triển khai trong đa cấu hình, cho phép doanh nghiệp tự do chọn số lượng phiên bản cần thiết, kiểm tra lưu lượng, cách xử lí mối đe dọa đã bị phát hiện và hơn thế nữa.



Với Transit Gateway, tập đoàn có thể sử dụng một Network Security duy nhất để bảo vệ lưu lượng trên khắp VPC của họ. Thông qua cấu trúc hub-and-spoke tập trung vào việc kiểm tra, lưu lượng đến và đi từ mạng internet có thể được quan sát từ cùng một phiên bản. Cùng với việc mỗi VPC không còn cần bộ cân bằng tải riêng và tường lửa, tập đoàn có thể giảm đáng kể số thành phần trong cấu trúc hệ thống mạng của họ, tiết kiệm cả thời gian và chi phí. Chỉ có một phiên bản duy nhất quản lí tại một vị trí.

Do một số doanh nghiệp chưa áp dụng Transit Gateway, AWS đã ra mắt VPC Ingress Routing vào cuối năm 2019. Nó cho phép doanh nghiệp xác định quy tắc định tuyến để chuyển hướng lưu lượng truy cập sang thiết bị của bên thứ ba, như là Network Security, trước khi chúng đến đích cuối cùng. Từ khi VPC Ingress Routing ra mắt đến toàn thể khách hàng của AWS như một phần trong cơ sở hạ tầng của họ, đồng nghĩa với không yêu cầu thêm cài đặt hoặc cấu hình bổ sung, đây là cách triển khai Network Security nhanh và đơn giản vào môi trường của AWS.



Network Security được triển khai với AWS Transit Gateway

Ví dụ: Network Security sử dụng bộ cân bằng tải đàn hồi đã là một phần của môi trường AWS. Nếu phát hiện vấn đề, thay vì định tuyến lưu lượng truy cập lên kiểm tra mạng con để bảo vệ mạng con riêng, Network Security sử dụng cơ sở hạ tầng AWS để đi trực tiếp đến mạng con được bảo vệ của tập đoàn. Một hoặc nhiều phiên bản của Network Security có thể được triển khai trong một vùng khả dụng, với cả lưu lượng inbound và outbound đều được xử lí bởi cùng phiên bản, không cần bộ thiết bị inbound và outbound chuyên dụng.

Ngoài hai cấu hình này, doanh nghiệp cũng có thể linh hoạt chỉ thanh toán cho phần đã sử dụng (trong môi trường động) hoặc mua giấy phép thường niên (dành cho cấu trúc hệ thống mạng ít hoạt động hơn).

Một công cụ dựa trên dòng hoạt động để triển khai một cách minh bạch

Công cụ phát hiện dựa trên dòng hoạt động, dạng stateless không dữ liệu của Network Security cho phép nó được chèn dễ dàng và minh bạch vào cấu trúc đám mây sẵn có của công ty. Tường lửa tiêu chuẩn thường ở dạng “stateful”, đồng nghĩa chúng cần theo dõi từng kết nối và quy tắc bắt tay, cũng như nơi lưu lượng bắt đầu và dừng. Điều đó khiến chúng rất khó để thêm hoặc xóa khỏi hệ thống mạng. Network Security tập trung vào trạng thái mối đe dọa, hơn là kết nối hoặc chính sách của hệ thống mạng, sử dụng thông tin nó tích lũy được để xác định hoặc theo dõi thuộc tín của mối đe dọa thật sự và tiềm ẩn.

Với Network Security, doanh nghiệp có thể bắt đầu kiểm tra lưu lượng inbound và outbound khi đang hoạt động, nhận được bảo vệ ngay lập tức từ khi triển khai, mà không cần phải cấu trúc lại hoặc cài lại IP. Khách hàng và máy chủ trong hệ thống mạng sẽ không bao giờ biết Network Security đã được cài hay bị xóa, đồng nghĩa không có sự gián đoạn đến ứng dụng, kết nối mạng hoặc quy trình DevOp của doanh nghiệp. Kẻ tấn công cũng không biết có bảo vệ ở đó, đến khi chúng phát hiện thì lần tấn công thành công trước đã đột nhiên bị chặn.

Phương thức bảo vệ toàn diện, chủ động trước mối đe dọa

Network Security được xây dựng dựa trên chuyên môn và khả năng được lấy từ Trend Micro™ TippingPoint™ trong suốt 15 năm qua để mang lại hiệu quả bảo mật như bảo mật tại cơ sở lên đám mây. Thông qua vá lỗi ảo, bao bọc lỗ hổng, chặn khai thác, thông tin mối đe dọa tân tiến và phân tích giao thức, phát hiện điểm bất thường, trí tuệ nhân tạo và phân tích hành vi, phương thức phát hiện dựa trên chữ kí dạng cổ điển, và hơn thế nữa, Network Security cung cấp bảo vệ toàn diện chống lại các kỹ thuật và véc-tơ đe dọa ngày càng tiến hóa, toàn bộ cấp độ tấn công, cũng như mối đe dọa cụ thể đã có thông tin. Với cách chặn chủ động, nó thông báo cho đội bảo mật các phát hiện xâm phạm hoặc tấn công để họ có thể đưa ra bước tiếp theo phù hợp nhất.

Nhờ vào công cụ dựa trên dòng hoạt động, Network Security thậm chí có thể cung cấp mức bảo vệ sâu này trong môi trường bất đối xứng, nơi cả 2 bên của kết nối mạng (từ người bắt đầu kết nối - đến máy chủ - và quay lại) không được hiển thị. Điều này cho phép lưu lượng được kiểm tra trên nhiều tình huống mạng hơn mà không cần tái cấu trúc lại hệ thống mạng để khiến chúng đối xứng, khắc phục những hạn chế vốn có trong một số giải pháp bảo mật khác.

Do Network Security không cần theo dõi toàn bộ kết nối, đồng thời cung cấp giải pháp fail-open: nó sẽ được xóa khỏi quá trình kiểm tra mà không có rủi ro nào về việc mất mạng hoặc gián đoạn kết nối đã thiết lập. Các chế độ dự phòng failover linh hoạt cũng có thể thực hiện được. Ví dụ: Nếu chiến lược của công ty là đưa luồng việc sang một khu vực khác trong trường hợp - một vùng dịch vụ đám mây cụ thể bị ngoại tuyến, Network Security loại bỏ việc cần chia sẻ và duy trì trạng thái kết nối (điều khiển nguy cơ luồng việc không còn đồng bộ). Ngay cả khi chuyển đổi giữa các khu vực thì dữ liệu và luồng việc luôn trong trạng thái sẵn sàng.

Tập trung hiển thị dấu chân của đám mây

Network Security cung cấp cho đội ngũ bảo mật độ hiển thị mối đe dọa được tập trung, giúp họ tránh quá tải về quản lí bảng điều khiển kỹ thuật số/bộ điều khiển. Như một phần của nền tảng Trend Micro Cloud One, nó vượt xa IPS truyền thống khi không chỉ là một sản phẩm tại một điểm như sản phẩm khác. Nó hoạt động nhịp nhàng với dịch vụ khác của nền tảng để cung cấp quản lí bảo mật đồng nhất trên toàn bộ dấu chân của đám mây trong tập đoàn. Một bộ diều khiển quản lí duy nhất, được hợp nhất mang lại giải pháp tối ưu hóa quản lí trên toàn bộ phương thức bảo mật đám mây của tập đoàn, cải thiện trải nghiệm của người dùng và đạt được kết quả bảo mật tốt hơn.

Đơn giản hóa việc tuân thủ với các quy định bảo mật dữ liệu
Sự bảo vệ toàn diện trong Network Security giúp tổ chức hợp lý hóa việc tuân thủ với vô số dữ liệu cá nhân và quy định bảo mật.

Ví dụ: Tổ chức Chuẩn bảo mật an ninh dữ liệu thẻ thanh toán (PCI DSS) yêu cầu doanh nghiệp xử lí dữ liệu thẻ tín dụng đưa ra biện pháp *kiểm soát bồi thường* cho lỗ hổng bảo mật có thể tồn tại trong môi trường mạng của họ. Chỉ một lớp IPS hệ thống mạng đạt được chỉ tiêu của kiểm soát bồi thường, có nghĩa Network Security đưa cho tập đoàn cách đơn giản để đạt được yêu cầu và duy trì tuân thủ với chuẩn đó. Network Security cũng kết hợp hàng loạt phương pháp hay nhất trong ngành mà phù hợp với yêu cầu tuân thủ khác của PCI DSS, chẳng hạn như giảm tối đa truy cập vào lưu lượng outbound.

ĐƯỢC CÁC NGHIÊN CỨU HÀNG ĐẦU HỖ TRỢ

Network Security được xây dựng trên cùng công cụ và lịch sử phát triển với thế hệ Trend Micro™ TippingPoint™ IPS tiếp theo – hệ thống ngăn chặn xâm nhập đầu tiên trên thế giới. 15 năm trước sản phẩm này đã được công bố, lúc đó chỉ có hệ thống phát hiện xâm nhập, chúng tạo ra rất nhiều cảnh báo, nhưng không thật sự sự chặn được mối đe dọa tiếp cận.

Với bất kì IPS, dữ liệu và nghiên cứu là phần cần thiết để phát hiện cũng như đối phó với mối đe dọa hoặc đợt tấn công một cách nhanh chóng. Đồng thời giữ doanh nghiệp được bảo vệ trước các tác nhân độc hại mới và phức tạp nhất. Công nghệ đằng sau Network Security được Trend Micro Research cấp báo, với đội ngũ hơn 500 nhà nghiêm cứu toàn thế giới và chương trình hữu dụng, như là Trend Micro™ Zero Day Initiative™ (ZDI) và Trend Micro™ Smart Protection Network™.

Chương trình Zero Day Initative của Trend Micro

ZDI là chương trình ‘săn lùng lỗi của nhà cung cấp’ lớn nhất trên thế giới, trao thưởng cho các nhà nghiên cứu bảo mật độc lập vì đã tìm ra và báo cáo lỗ hổng bảo mật trong hệ thống điều hành cũng như phần mềm trước khi chúng có thể bị khai thác.

Giữa thời điểm tìm ra một lỗi nghiêm trọng và khi nhà cung cấp phát hành bản vá lỗi, các doanh nghiệp sẽ ở trong trạng thái nguy hiểm. Các nhà nghiên cứu của Trend Micro tiếp thu những gì đã được học từ chương trình ZDI để nhanh chóng phát triển và phân bổ bộ lọc bảo vệ để che chắn toàn bộ lỗ hổng, đảm bảo rằng khách hàng được bảo vệ đầy đủ trước khi nhà cung cấp có bản vá. Trong năm 2019, các bộ lọc ZDI được phân bổ trung bình 81 ngày trước bản vá của nhà cung cấp.

Chương trình ZDI dẫn đầu toàn cầu trong nghiên cứu và phát hiện lỗ hổng bảo mật, cũng là nhà cung cấp thông tin lỗ hổng bảo mật hàng đầu cho các tổ chức, như là Adobe®, Microsoft® và Nhóm ứng cứu khẩn cấp cho hệ thống kiểm soát ngành công nghiệp Hoa Kỳ.

Smart Protect Network của Trend Micro

Smart Protection Network thu thập, xác định và cung cấp thông tin tình báo bảo mật mới nhất để đảm bảo sản phẩm của Trend Micro có thể thích ứng và chống lại mối đe dọa có chiều hướng ngày càng tăng. Liên tục khai thác dữ liệu từ tập tin tốt hoặc xấu đã được xác nhận, các ứng dụng, cũng như URL trên khắp thế giới, Smart Protection Network có chức năng như là nguồn thông tin khổng lồ để thúc đẩy các công nghệ của Trend Micro.

Smart Protection Network bao gồm:

- Một mạng lưới toàn cầu với hơn 250 triệu bộ cảm biến thu thập thông tin mối đe dọa ở nhiều nơi, bao gồm dữ liệu trên tập tin, IP, URL, ứng dụng điện thoại, hệ thống điều hành và giao dịch điện tử (IoT).
- Thông tin tình báo mối đe dọa toàn cầu phân tích hàng nghìn dữ liệu hằng ngày, lấy từ cơ sở dữ liệu của gần 1 triệu tập tin tốt đã được xác minh để xác định hơn 5 triệu mối đe dọa mới mỗi năm.
- Bảo vệ chủ động, dựa theo hệ thống đám mây cho hơn 5 triệu doanh nghiệp trên khắp thế giới, ngăn chặn hơn 48 triệu mối đe dọa mỗi năm.

Công ty được công nhận dẫn đầu trong ngành an ninh mạng

Trend Micro hiện đang:

- Đứng thứ #1 trên Thị phần bảo mật luồng việc điện toán đám mây toàn thế giới của IDC, bài báo cáo vào năm 2019
- Dẫn đầu với điểm cao nhất ở hạng mục " sản phẩm hiện có" và "chiến lược" trong Forrester Wave™: Cloud Workload Security, vào Quý 4 năm 2019.

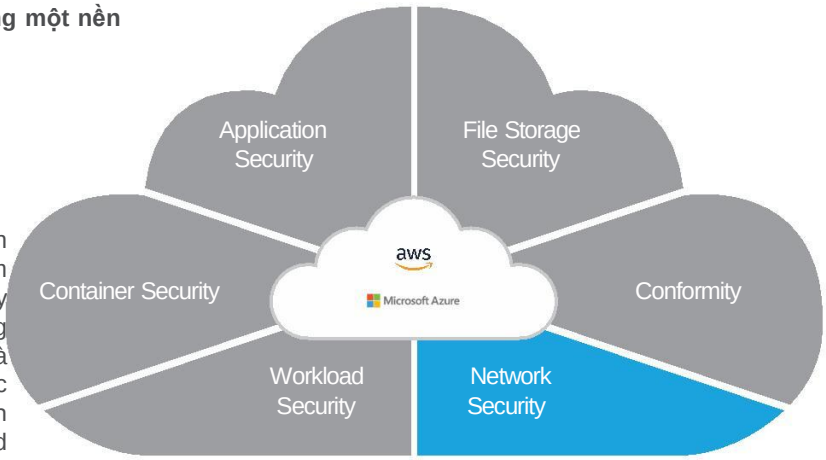
KẾT LUẬN

Khi bảo mật đám mây ngày càng trở nên phức tạp, Trend Micro Cloud One nhắm đến việc giữ mọi thứ đơn giản, có thể mở rộng và linh hoạt nhất cho doanh nghiệp. Thêm vào dịch vụ của Network Security, nền tảng này cũng cung cấp bảo vệ vùng chứa, luồng việc, dịch vụ lưu trữ tập tin đám mây, ứng dụng và chức năng không máy chủ cũng như các dịch vụ dành cho độ tuân thủ và quản lí cấu trúc bảo mật đám mây.

Trend Micro Cloud One là dịch vụ bảo mật tất cả trong một nền tảng duy nhất cho hệ thống xây dựng trên đám mây

Với phương thức tất cả trong một, Trend Micro Cloud One cung cấp cho doanh nghiệp chiều rộng, chiều sâu và bước đổi mới họ cần để đạt cũng như quản lí được việc bảo mật đám mây họ cần vào hiện tại và trong tương lai

Cho dù doanh nghiệp có tìm cách bao phủ bảo mật trên khắp các VPC khi chuyển sang đám mây hoặc muốn thêm một lớp bảo mật cho các ứng dụng đám mây được xây dựng bởi đội ngũ Devop của họ, Network Security cung cấp phòng thủ sâu một cách nhanh chóng và quy mô, mà không gây bất kì xung đột nào vào hệ thống mạng hoặc làm gián đoạn hoạt động doanh nghiệp. Bằng cách đơn giản hóa cách họ bảo vệ tài sản trong đám mây, Trend Micro đang giúp cho doanh nghiệp khai thác tối đa khoản đầu tư vào đám mây của họ.



[1] IDC, 06/2020. Worldwide Hybrid Cloud Workload Security Market Shares, 2019: Vendor Growth Comes in All Shapes and Sizes. Tài liệu #US46398420.

[2] Forrester, 12/2019. The Forrester Wave™: Cloud Workload Security, Qúy 4 2019.

TREND MICRO

Securing Your Connected World

Trend Micro Incorporated, một phần mềm bảo mật dẫn đầu toàn cầu, luôn nỗ lực giúp thế giới trao đổi thông tin kỹ thuật số an toàn hơn. Các sáng kiến của chúng tôi dành cho người dùng, doanh nghiệp và chính phủ cung cấp bảo mật nội dung nhiều lớp để bảo vệ thông tin trên thiết bị di động, điểm cuối, cổng kết nối, máy chỉ và đám mây. Tất cả giải pháp của chúng tôi được cung cấp dựa trên tin tình báo mối đe doạ dựa trên đám mây toàn cầu, Trend Micro™ Smart Protection Network™ và được hỗ trợ bởi hơn 1,200 chuyên gia mối đe dọa toàn cầu. Để biết thêm chi tiết, hãy truy cập www.trendmicro.com

TREND MICRO INC.

Tổng đài miễn phí tại Hoa kỳ: +1 800.228.5651

Điện thoại: +1 408.257.1500

Fax: +1 408.257.2003

Biên dịch bởi Thanh Hiền - Iworld.com.vn