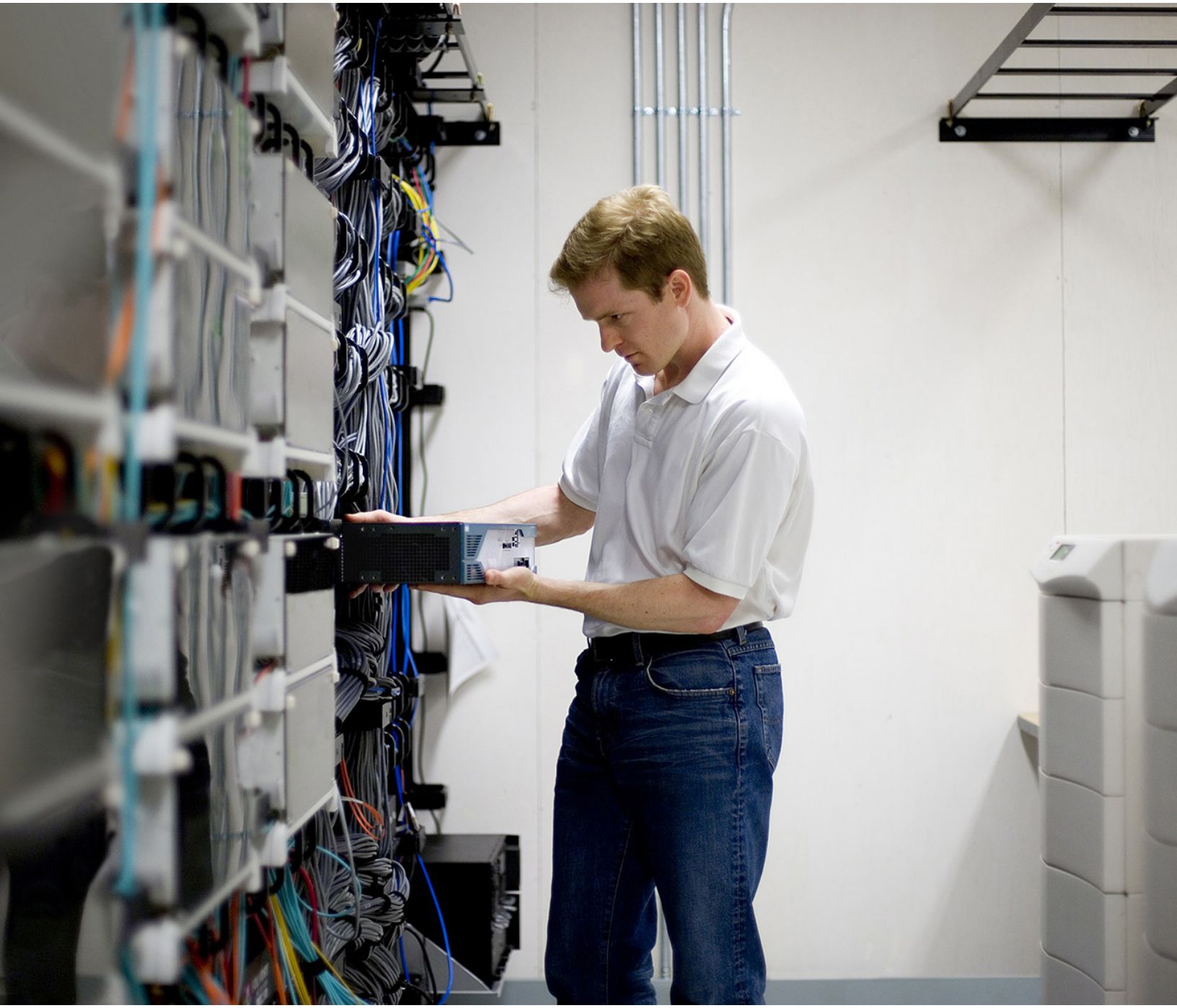
Làm cho Biên Mạng của bạn Trở nên Thông minh và Đáp ứng Nhu cầu trong Tương lai ngay Hôm nay



Tóm tắt Chung

Trong thực tế về doanh nghiệp kỹ thuật số mới, biên mạng chưa bao giờ quan trọng hơn thế. Thường bị xem nhẹ nhưng biên mạng chính là nền tảng quyết định có đạt được thành công trong thời đại kỹ thuật số hay không. Xem xét mọi thứ xảy ra ở biên mạng.

- Đây là phòng tuyến đầu tiên chống lại sự xâm nhập của các thiết bị không tin cậy hoặc độc hại.
- Đó là kênh mang lại các dịch vụ và ứng dụng thường đầu tư nhiều tiền bạc cho đối tượng mục tiêu.
- Đó là cổng chiến lược để kết nối các tổ chức phân bố rộng rãi.
- Đó là cầu nối giữa tổ chức và khách hàng của bạn.
- Đó là nơi mà các thiết bị thuộc Mạng lưới Thiết bị Kết nối Internet (IoT) được kết nối và quản lý.
- Đó là nơi tối ưu để thực sự hiểu những gì đang xảy ra với doanh nghiệp của bạn.

Biên mạng đôi khi được triển khai với niềm tin rằng tất cả các giải pháp mạng cơ bản đều giống nhau. Điều này không đúng, bởi vì doanh nghiệp kỹ thuật số mới đòi hỏi mức độ thông tin cao hơn ở biên mạng. Cisco cung cấp các giải pháp và chức năng chiến lược để đạt được thành công trong kinh doanh. Chúng tôi cung cấp một kiến trúc mạng mới bắt đầu với người dùng cuối và tiếp tục mở rộng ra nơi lưu trữ các ứng dụng, với trọng tâm là:

- **Cho phép đổi mới nhanh hơn** thông qua trải nghiệm tốt hơn và thông tin chuyên sâu cực kỳ chi tiết về người dùng, thiết bị, ứng dụng và các mối đe doạ.
- **Giảm chi phí và độ phức tạp** để dễ dàng thiết lập chính sách và quản lý thay đổi trên quy mô lớn trong khi vẫn giảm số lượng phần cứng và phần mềm trên mạng có dây, không dây và WAN.
- **Giảm rủi ro** nhờ khả năng hiển thị mối đe doạ và bảo vệ đầy đủ trước những rủi ro nội bộ và bên ngoài trên mạng có dây, không dây và WAN.

Ngày nay, mạng rất quan trọng trong việc hỗ trợ sự thay đổi ở hầu như mọi tổ chức khi họ thực hiện quá trình chuyển đổi kỹ thuật số. Quá trình này sẽ giúp các tổ chức đổi mới nhanh hơn, giảm chi phí, độ phức tạp và rủi ro. Quá trình này cũng giúp tăng tính nhanh nhạy, nâng cao năng suất của nhân viên, tương tác tốt hơn với khách hàng, cũng như bảo vệ quyền sở hữu trí tuệ và tài sản quan trọng.

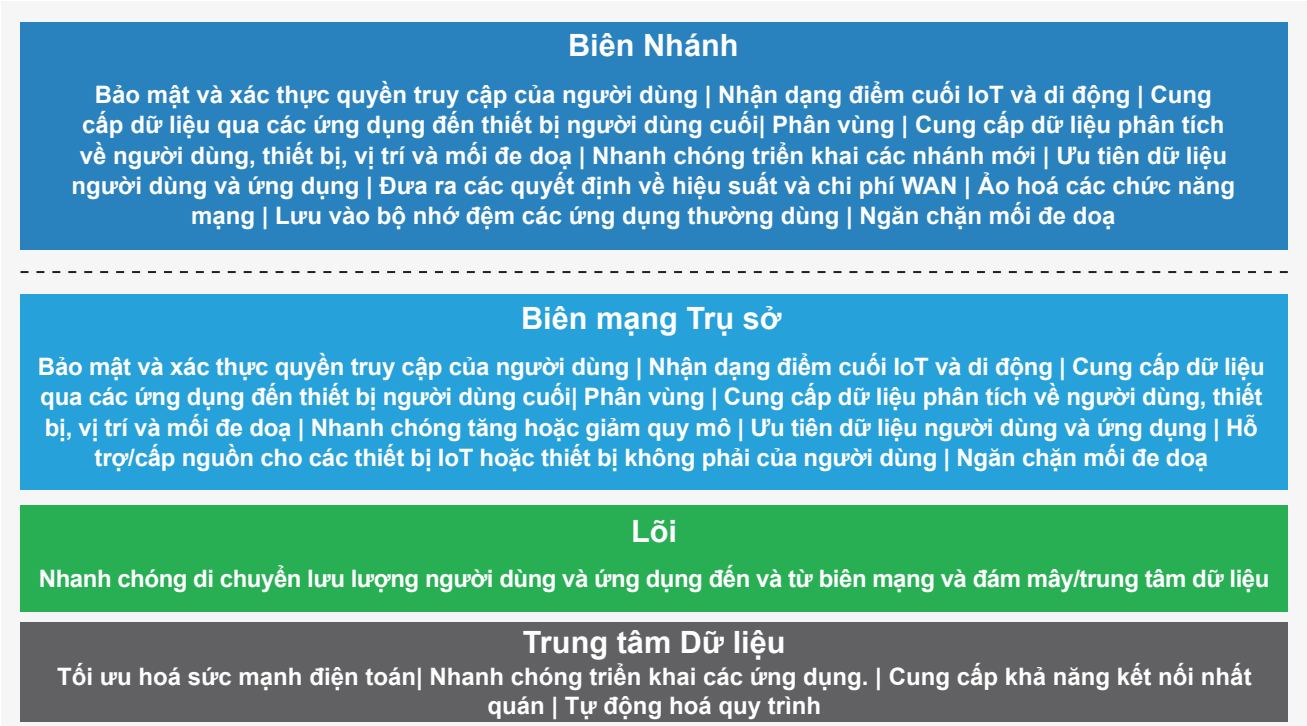
Biên mạng đóng vai trò quan trọng trong quá trình chuyển đổi này và có lẽ đảm nhận nhiều trách nhiệm nhất so với mạng lõi và mạng trung tâm dữ liệu. Như minh hoạ ở Hình 1, khi so sánh các lớp khác nhau của mạng, biên mạng chịu trách nhiệm lớn tại trụ sở. Điều này cũng đúng đối với nhánh.

Vai trò của Biên Mạng

Chuyển đổi kỹ thuật số khiến biên mạng trở nên quan trọng hơn bao giờ hết. Xem xét mọi thứ xảy ra ở biên mạng:

- **Đây là phòng tuyến đầu tiên.** Biên mạng là nơi chính sách được áp dụng và xác thực, mà không giới hạn khả năng truy cập vào những thứ bạn cần. Nếu quyền truy cập không được quản lý đúng cách thì doanh nghiệp rất dễ bị xâm nhập hoặc phát tán mối đe doạ, và mức độ nghiêm trọng tăng lên khi phạm vi mối đe doạ tăng. Thiết bị, chương trình cơ sở và thậm chí cả hệ điều hành đều là điểm bị xâm phạm.

Hình 1. Lớp Mạng và Chức năng của chúng



- **Đó là kênh mang lại các ứng dụng thường đầu tư nhiều tiền bạc.** Biên mạng là nơi diễn ra ưu tiên. Một trải nghiệm kém tại biên mạng sẽ làm chậm quá trình áp dụng ứng dụng, dẫn tới giảm lợi tức đầu tư.
- **Đó là cổng chiến lược để kết nối các tổ chức phân bố rộng rãi.** Mang lại một trải nghiệm liền mạch cho nhân viên, đối tác và khách hàng dù họ ở đâu là điều quan trọng nhất. Một mạng loại hai sẽ cung cấp mức độ dịch vụ sai lệch cho đối tượng chính.
- **Đó là cầu nối giữa tổ chức và khách hàng.** Nếu bạn thuộc một doanh nghiệp bán lẻ hoặc khách sạn thì khả năng truy cập dưới mức trung bình sẽ làm giảm khả năng kết nối với khách hàng của bạn trên một mức độ cá nhân và ảnh hưởng tiêu cực đến thương hiệu của bạn.
- **Nó được xây dựng để cấp nguồn và hỗ trợ cho các nhu cầu thiết bị IoT ngày càng tăng.** Biên mạng thích ứng với môi trường thực tế bằng cách chuyển hầu như mọi ngành sang thời đại kỹ thuật số thông qua việc cải thiện hoạt động và giảm chi phí. Nếu không có chức năng phù hợp tại biên mạng, các tổ chức có thể tụt hậu về mặt giảm chi phí và hiệu quả hoạt động.
- **Đó là nơi tối ưu để hiểu những gì đang xảy ra với doanh nghiệp.** Trong một mạng phân tán, chỉ biên mạng mới nhìn thấy tất cả lưu lượng dữ liệu, bằng cách thu thập dữ liệu và phân tích từ biên.

Dữ liệu về người dùng, ứng dụng, thiết bị và mối đe doạ mà các doanh nghiệp có thể truy xuất thông tin chi tiết thực sự hữu ích trong việc đưa ra quyết định đúng đắn hơn nhằm hỗ trợ nhân viên, giảm rủi ro và chi phí, đồng thời cung cấp thông tin các đối tượng mục tiêu. Nếu không có mức độ chi tiết nhất quán phù hợp, dữ liệu này sẽ trở nên sai lệch và không tin cậy.

Sử dụng Đại trà Biên mạng có phải là Điều Tốt không?

Nhiều tổ chức đang nỗ lực trở thành tổ chức ưu tiên kỹ thuật số nhằm mang đến đổi mới nhanh hơn, trải nghiệm tốt hơn và mức độ bảo mật cao hơn. Tuy nhiên, làm mới mạng để đáp ứng các yêu cầu này là một công việc khó khăn vì nền tảng mạng được thiết lập hiện tại sẽ cần phải hỗ trợ doanh nghiệp trong những năm tới. Việc lựa chọn nhà cung cấp mạng là một quyết định quan trọng. Quyết định này sẽ giúp bạn liên tục đổi mới và đồng hành cùng doanh nghiệp hay sẽ làm chậm tốc độ trong khi phải vật lộn với khả năng kém.

Với chuyển đổi kỹ thuật số, không ai thực sự biết tương lai phía trước sẽ như thế nào, nhưng có một điều rõ ràng là: nhu cầu về mạng của bạn sẽ gia tăng theo cấp số nhân. Cho dù đó là IoT, đám mây, các mối đe doạ bảo mật phức tạp hay thậm chí là thực tế gia tăng khác, chuyển đổi kỹ thuật số sẽ vẫn thay đổi cách bạn hoạt động và phục vụ doanh nghiệp.

Điều gì đủ tốt ngày hôm nay, sẽ không được chấp nhận trong tương lai gần và tất cả đều bắt đầu với mạng. Bạn phải đổi mới nhanh hơn, giảm chi phí, độ phức tạp và kiểm soát rủi ro. Các tổ chức thực sự sẵn sàng chuyển đổi kỹ thuật số biết rằng khi họ hướng tới những thay đổi này, họ không được phép làm ảnh hưởng đến những gì quan trọng.

Rủi ro là gì?

Việc sẵn sàng cho thế giới ưu tiên kỹ thuật số không phải là nhắm tới một nơi duy nhất trong mạng. Việc này bắt đầu tại biên truy cập mạng và sử dụng chức năng phổ biến trong mạng lõi và WAN với phương pháp tiếp cận kiến trúc sẵn sàng cho kỹ thuật số. Tại sao phương pháp tiếp cận rộng này lại cực kỳ quan trọng? Đó là do thế giới ưu tiên kỹ thuật số ngày nay chuyển động và thay đổi nhanh hơn, có nghĩa là bạn và mạng của bạn cần phải sẵn sàng. Các tổ chức sẵn sàng cho thế giới kỹ thuật số không mạo hiểm thực hiện những việc không cần thiết làm ảnh hưởng đến những gì quan trọng. Họ biết rằng:

1. **Chỉ một trải nghiệm kém cũng có thể làm cho cải tiến mới nhất của bạn trở nên vô dụng.**

   Bên trong doanh nghiệp của bạn, đổi mới là điều quan trọng. Nhưng tại biên mạng, nơi các ứng dụng của bạn tiếp xúc với thế giới thực và nơi các thiết bị IoT mới sẽ thúc đẩy sự thay đổi cơ bản của doanh nghiệp, thì kết nối không phù hợp và hiệu suất chậm có thể khiến người dùng gặp khó khăn. Điều này ảnh hưởng đến hiệu suất thiết bị và loại bỏ thông tin chi tiết mà bạn cần để duy trì lợi thế cạnh tranh. Với Cisco, thông tin chi tiết nằm trong DNA của bạn: không chỉ thông tin chi tiết về mạng giúp cải thiện hiệu suất, mà còn là thông tin chi tiết theo thời gian thực về người dùng giúp mang lại những trải nghiệm cá nhân hơn.

2. **Chỉ một câu trả lời "không" cũng có thể hủy hoại danh tiếng của bạn.**

   Thế giới của bạn đang thay đổi nhanh chóng và nếu không thể bắt kịp, bạn sẽ bị đào thải, về cơ bản là khiến cho bạn trở nên tụt hậu. Ngoài sự phức tạp này, nguồn lực và ngân sách cũng rất hạn chế. Định cấu hình và định cấu hình lại lần lượt từng nhánh mạng và từng thiết bị có thể biến một cập nhật "đơn giản" thành phễu hút TCO. Với Cisco, tự động hoá nằm trong DNA của bạn. Điều này cho phép bạn tự động hoá và quản lý toàn bộ mạng của mình—có dây, không dây tại trụ sở, thông qua WAN và trong các nhánh—như một thực thể duy nhất từ một nơi duy nhất.

3. **Chỉ một sự cố cũng có thể trở thành vấn đề của mọi người.**

   Chắc bạn cũng hiểu rõ thời gian mạng ngừng hoạt động tiêu tốn bao nhiêu tiền. Bạn cũng hiểu rõ mức độ quan trọng của an ninh mạng trong việc đảm bảo thời gian hoạt động bằng cách ngăn chặn phần mềm độc hại đe doạ các dịch vụ mạng của bạn.

   Vậy tại sao bạn lại mua cơ sở hạ tầng mạng mà không kiểm soát quyền truy cập, ngăn chặn các cuộc tấn công, phát hiện và ngăn chặn xâm phạm? Làm thế nào bạn có thể uỷ thác cho một công ty xây dựng mạng cơ sở khi công ty đó không thể giữ an toàn cho mạng? Với Cisco, bạn có thể biến mạng thành một cảm biến giúp phát hiện mối đe doạ và một công cụ thực thi chính sách bảo mật, tại chi nhánh và trụ sở, mạng có dây và không dây. Đừng giao phó vấn đề bảo mật cho các tổ chức khác.

Cisco Cung cấp Thông tin tại Biên Mạng

Các tổ chức sẵn sàng chuyển đổi kỹ thuật số xây dựng trên Kiến trúc Mạng Kỹ thuật số (DNA) của Cisco®. Kiến trúc Mạng này mang lại đổi mới và thông tin ở khắp mọi nơi trên mạng. Tại sao? Nguyên nhân rất đơn giản. DNA của Cisco tập trung vào việc bảo vệ, đơn giản hoá và hỗ trợ doanh nghiệp từ đầu đến cuối. Chỉ Cisco mới có thể mang lại điều này vì DNA của Cisco là giải pháp duy nhất cho phép bạn:

1. **Cung cấp trải nghiệm tốt hơn và có được thông tin chuyên sâu cực kỳ chi tiết** về người dùng, thiết bị, ứng dụng và các mối đe doạ. Sẵn sàng chuyển đổi kỹ thuật số đồng nghĩa với việc mang lại trải nghiệm phù hợp để trao quyền cho nhân viên, thu hút khách hàng và cung cấp thông tin chi tiết có giá trị để tối ưu hoá trải nghiệm người dùng, phát triển các nguồn doanh thu mới và kiểm soát chi phí. Cơ sở hạ tầng có tính khả dụng cao xác định các thay đổi và tự động thích ứng để hỗ trợ khả năng bổ sung. Là đối tác mạng chiến lược duy nhất với Apple, Cisco cho phép các tổ chức mang lại chất lượng âm thanh cao hơn tới 20%, giảm tới 90% lỗi trình duyệt web và 86% mức tải tin nhắn qua mạng từ các thiết bị iOS trong khi chuyển vùng. Độ chính xác vị trí lên đến 1 mét, đứng đầu ngành và khả năng sử dụng dữ liệu NetFlow trong thời gian thực mang lại thông tin chính xác về tương tác người dùng và ảnh hưởng của mối đe doạ. Điều này giúp mô tả thực tế những gì đang thực sự xảy ra trong môi trường của bạn.

2. **Dễ dàng thiết lập chính sách và quản lý thay đổi trên quy mô lớn** trong khi vẫn giảm số lượng phần cứng và phần mềm trên mạng có dây, không dây và WAN. Khả năng quản lý tất cả các miền mạng như một kết cấu mạng duy nhất từ một vị trí tập trung giúp đẩy nhanh thời gian thích ứng với mạng và tối ưu hoá trải nghiệm người dùng, nhờ đó các tổ chức giảm được 79% chi phí triển khai. Một cơ sở hạ tầng mở và có thể lập trình cung cấp các API trên mạng LAN, WLAN và WAN cũng như trong các kho dữ liệu chiến lược khác cho phép bạn thu thập, phát triển và triển khai ứng dụng mới cùng các cơ chế kiểm soát trên những ứng dụng đó.

Có một cộng đồng nhà phát triển rộng lớn để học hỏi và cùng xây dựng nhằm hưởng lợi từ các phương pháp hiệu quả nhất và hướng dẫn của Cisco để đáp ứng bất kỳ trường hợp sử dụng nào.

Các giải pháp bổ sung có thể quản lý một hoặc hai miền mạng, chẳng hạn như có dây và không dây, nhưng không cung cấp khả năng quản lý tập trung đầu cuối. Các giải pháp cạnh tranh chỉ sử dụng API không có tính cộng đồng chặt chẽ và chuyên môn như Cisco cung cấp.

3. **Khả năng hiển thị mối đe doạ và bảo vệ đầy đủ trước những rủi ro nội bộ và bên ngoài** trên mạng có dây, không dây và WAN. Mạng hoạt động như một cảm biến và công cụ thực thi bằng cách xác thực lưu lượng dựa trên chính sách ở mọi phần đường dẫn (hop) của mạng. Khả năng này cho phép mạng xác định và khắc phục các mối đe doạ tiềm ẩn một cách nhanh chóng, giảm thiểu rủi ro và duy trì sự tuân thủ. Đổi lại, các tổ chức tránh được 99,2% mối đe doạ và điều chỉnh mạng để thích ứng với các mối đe doạ mới nhanh hơn 98% so với các phương pháp truyền thống. Họ cũng đạt được lợi tức đầu tư 140%.

   Các giải pháp khác chỉ tìm kiếm mối đe doạ ở lớp truy cập và sử dụng thông tin từ phần mềm độc hại đã xác định. Điều này có nghĩa là phần mềm độc hại hiện nay có thể xâm nhập vào mạng bằng cách ngụy trang như một lưu lượng thông thường, sau đó tiến hành các hoạt động gây hại từ bên trong mạng. Tổ chức có nhiệm vụ phải giải được thông tin từ dữ liệu khác nhau được lấy mẫu nhằm xác định nơi xảy ra tác động để họ có thể khắc phục.

Các tổ chức kỹ thuật số cũng đang phá bỏ những cản trở tiêu cực, hiểu rằng mạng sản xuất và trung tâm dữ liệu cần phải hoạt động một cách hài hoà để mang lại trải nghiệm người dùng, thiết bị và ứng dụng tốt hơn. DNA của Cisco tập trung vào phân tích, đơn giản hoá, tự động hoá và bảo vệ doanh nghiệp bằng cách mang lại đổi mới và thông tin từ nơi người dùng bắt đầu cho tới nơi ứng dụng kết thúc.

Mang đến Trải nghiệm Tốt hơn và Có được Thông tin Chuyên sâu Cực kỳ Chi tiết

Biên mạng là điểm mà tại đó nhân viên được trao quyền, khách hàng được tương tác và các thiết bị IoT được kích hoạt. Đó là một nguồn thông tin chi tiết có giá trị.

- **Mang đến trải nghiệm người dùng tuyệt vời nhất cho iPhone và iPad trên mạng công ty.** Với những tính năng mới trong iOS 10 kết hợp với phần mềm và phần cứng mạng mới nhất của Cisco, các doanh nghiệp ở khắp mọi nơi có thể tận dụng cơ sở hạ tầng của họ để mang đến trải nghiệm người dùng tuyệt vời cho các ứng dụng, gọi điện và cộng tác. Cisco và Apple đã cùng nỗ lực phát triển để cung cấp kết nối không dây tốt nhất cho nhân viên di động của bạn và mang đến cho bộ phận CNTT một cách dễ dàng để ưu tiên các ứng dụng quan trọng nhất với doanh nghiệp khi sử dụng các thiết bị iOS trên mạng Cisco. Hiện không có nhà cung cấp nào khác trong ngành cung cấp mức độ tương kết này.
- **Có được độ tin cậy mọi lúc, mọi nơi ở cấp mạng, truy cập và thiết bị cuối để không ảnh hưởng đến người dùng.** Giải pháp của Cisco mang đến cho mạng khả năng phục hồi nhiều lớp để đảm bảo rằng mạng luôn sẵn sàng khi cần, đồng thời đảm bảo bạn và các thiết bị IoT được hỗ trợ và phục vụ cho doanh nghiệp bạn.
- **Tự động điều chỉnh mạng Wi-Fi khi cần thiết.** Mang đến một trải nghiệm chất lượng cao liên tục nhờ sự đổi mới mạng không dây vượt xa tiêu chuẩn mạng không dây. Mạng Cisco cải thiện khả năng của các thiết bị di động cũ và mới nhất, loại bỏ nhiễu và điều chỉnh khả năng để đáp ứng các nhu cầu khác nhau.
- **Hỗ trợ tốt hơn cho các thiết bị IoT với nguồn không bao giờ bị lỗi để đảm bảo tính khả dụng và nâng cao hiệu suất.** Mạng Cisco tích hợp nguồn không bao giờ bị lỗi vào thiết bị chuyển mạch nơi kết nối các thiết bị IoT, cùng với điện toán đám mây mang đến khả năng tự động quyết định nơi tối ưu để xử lý dữ liệu từ các thiết bị IoT. Mạng Cisco được chuẩn bị cho thế giới kết nối mới.

Sự khác biệt giữa phù hợp với doanh nghiệp và chỉ đơn thuần là một tiện ích khác phụ thuộc vào mức độ trải nghiệm người dùng được cung cấp và độ chính xác của dữ liệu.

Các doanh nghiệp có thể kỳ vọng độ tin cậy cao hơn cho các ứng dụng trong thời gian thực, với chất lượng âm thanh cho cuộc gọi qua Wi-Fi tăng tới 20%, chi phí quản lý mạng giảm 50% do ít mã nhận dạng nhóm dịch vụ (SSID) hơn và hiệu suất tăng lên với mức tải tin nhắn qua mạng từ các thiết bị iOS giảm tới 86%, trong khi người dùng cuối chuyển vùng có thể được hưởng lợi nhờ tuổi thọ pin lâu hơn khi sử dụng các thiết bị iOS trên mạng Cisco.

- **Có được góc nhìn thực tế về người dùng, thiết bị, ứng dụng và mối đe doạ với độ chính xác lên đến 1 mét.** Cisco cung cấp mức độ chi tiết đầu ngành cho dữ liệu dựa trên vị trí để hiểu rõ hơn về cách người dùng tương tác với môi trường nhằm đưa ra các quyết định kinh doanh tốt hơn.

Các tổ chức doanh nghiệp với khách hàng (B2C) như nhà bán lẻ, khách sạn và tổ chức giáo dục đã có thể đạt được độ chính xác về vị trí dưới 1 mét nhờ sự kết hợp giữa Wi-Fi và Bluetooth Năng lượng Thấp (BLE) và tạo ra các khoản tăng doanh thu trực tiếp. Một số ví dụ bao gồm doanh thu không phải từ phòng của Hyatt Regency tăng 20%, thời gian lưu trú của khách hàng tăng gấp 3 lần và trải nghiệm người dùng cải thiện 80% tại trung tâm mua sắm Starry Bowar - đồng thời vẫn mang lại trải nghiệm di động được cá nhân hoá.

Dễ dàng Thiết lập Chính sách và Quản lý Thay đổi trên Quy mô lớn

Các tổ chức nỗ lực loại bỏ những hoạt động tốn kém và mất nhiều thời gian do việc liên tục định cấu hình lại và điều chỉnh lần lượt từng thiết bị mạng để đáp ứng nhu cầu ngày càng tăng của doanh nghiệp. Cisco cung cấp một cách để dễ dàng quản lý mạng, cho dù đó là một hay nhiều cơ sở. Doanh nghiệp kỹ thuật số đòi hỏi mạng phải nhanh nhạy hơn, có nghĩa là mạng cần phải tự động hoá các quy trình và dịch vụ mới với khả năng thực hiện tức thời và trong một ngày, đồng thời loại bỏ nhu cầu phải can thiệp thủ công. Khả năng này cho phép doanh nghiệp kỹ thuật số triển khai và duy trì một mạng phù hợp với bối cảnh phát triển nhanh chóng hiện nay.

- Quản lý một chính sách chất lượng dịch vụ (QoS) duy nhất và điều chỉnh theo hiệu suất trên mạng. Các giải pháp của Cisco sử dụng cùng một chính sách QoS trên mạng LAN, WLAN và WAN để cung cấp khả năng xử lý ứng dụng tốt hơn từ đầu đến cuối. Các giải pháp này có thể tự động ưu tiên các ứng dụng quan trọng, chẳng hạn như thoại nhạy cảm với độ trễ và cộng tác, dựa trên mức sử dụng và xếp hạng dịch vụ, với khả năng hiển thị ứng dụng và kiểm soát có tính đến những thay đổi trong môi trường cùng với các định nghĩa QoS để đảm bảo các ứng dụng quan trọng đối với doanh nghiệp có được mức độ ưu tiên cao.
- Tìm ra các phân vùng và nhánh mạng mới nhanh hơn với chi phí triển khai không chạm thấp hơn. Ứng dụng cắm là chạy của Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) giúp giảm mức độ tiêu thụ tài nguyên và thời gian cần thiết để định cấu hình, triển khai và tăng tốc các phân vùng và nhánh mạng mới nhờ khả năng triển khai không chạm cho các bộ định tuyến, thiết bị chuyển mạch và bộ điều khiển không dây Mạng Doanh nghiệp của Cisco.
- Thêm chức năng phần mềm và phần cứng mới mà không cần thay thế thiết bị. Mạng Cisco cho phép tổ chức sử dụng các điểm truy cập, bộ điều khiển và thiết bị chuyển mạch hiện có để bổ sung chức năng mới khi chức năng này khả dụng mà không ảnh hưởng đến hiệu suất.
- Có khả năng quản lý và chuyển đổi giấy phép đơn giản cho các nâng cấp cơ sở hạ tầng. Tận dụng các khả năng mới quan trọng với doanh nghiệp mà không cần trải qua quá trình quản lý giấy phép mất nhiều thời gian. Chuyển giấy phép phần mềm hiện có sang phần cứng mới khi nâng cấp cơ sở hạ tầng.
- Mở rộng chức năng bằng cách sử dụng quy mô và sức mạnh của điểm truy cập không dây hiện có để đáp ứng các trường hợp sử dụng mới. Thêm chức năng mới qua mô-đun cho các điểm truy cập hiện có để bổ sung chức năng mới theo tiêu chuẩn ngành hoặc chức năng từ các đối tác hệ sinh thái của bên thứ ba.

Cisco có thể đẩy nhanh tốc độ triển khai và giảm chi phí triển khai 79% bằng cách tách phần mềm khỏi phần cứng và ảo hoá biên WAN.

Khả năng Hiển thị Mối đe doạ và Bảo vệ Đầy đủ trước Rủi ro Nội bộ và Bên ngoài

Biên mạng là điểm hàng đầu của hoạt động truy cập trái phép hoặc thù địch, bởi vì đó là nơi người dùng và thiết bị truy cập vào cả trụ sở và nhánh. Biên mạng phải đáng tin cậy để xác định và kiểm soát những gì đang kết nối với mạng. Nó cũng cần phải hoạt động hài hoà với các giải pháp bảo mật trong mạng lõi và nhánh để chống lại các cuộc tấn công bằng phần mềm độc hại mới nhất.

Với Công cụ Dịch vụ Nhận dạng Cisco, Cisco TrustSec® và Cisco StealthWatch, bạn có thể biến mạng thành một cảm biến và công cụ thực thi để cải thiện khả năng bảo vệ và thời gian ứng phó. Có nghĩa là bạn có thể tránh, xác định và xử lý các mối đe doạ khi chúng xâm nhập vào mạng hoặc khi chúng phát tán qua mạng, nếu đã vượt qua điểm truy cập ban đầu. DNA của Cisco cho phép bạn:

- **Quản lý quyền truy cập của người dùng và thiết bị bằng cách phân vùng phần mềm,** không cần nhiều VPN và SSID tĩnh. Đảm bảo rằng các nhân viên, khách, nhà thầu, công nhân tạm thời và khách hàng có thể truy cập vào những thứ họ cần chứ không phải thông tin họ không cần. Phương pháp tiếp cận nhóm thiết bị và người dùng dựa trên phần mềm này cung cấp quy mô lớn hơn, đồng thời cho phép bạn giảm lỗi cấu hình, thêm thiết bị khác nhanh hơn, phân loại đúng cách người dùng và thiết bị tốt hơn so với các phương pháp thủ công truyền thống, dẫn tới khả năng thay đổi nhanh hơn 98%.
- **Tích hợp bảo mật ở khắp mọi nơi để phát hiện và ngăn chặn mối đe doạ tại điểm truy cập và trong mạng.** Xác thực lưu lượng tại mỗi điểm giao nhau của mạng trong mạng truy cập, mạng lõi và mạng nhánh. Ngay cả khi phần mềm độc hại xâm nhập qua một thiết bị người dùng hoặc thiết bị IoT, hoặc ai đó đang cố ý đánh cắp dữ liệu, thì cơ sở hạ tầng mạng của Cisco có thể nhận biết nơi mối đe doạ hiện hữu và hành động để ngăn chặn hoặc hạn chế tác động.
- **Nhanh chóng phân tích và khắc phục ảnh hưởng của mối đe doạ bằng dữ liệu NetFlow trong thời gian thực.** Vượt xa khả năng phát hiện mối đe doạ thông thường và khai thác sức mạnh của NetFlow. Nhờ đó, bạn có được khả năng hiển thị mạng, phân tích và bảo vệ nâng cao. Bạn sẽ nhìn thấy mọi thứ đang diễn ra trên mạng của mình. Bạn có thể phát hiện các cuộc tấn công vượt qua vành đai và xâm nhập vào môi trường nội bộ của mình.
- **Sử dụng một hệ sinh thái toàn cầu để chặn đứng các mối đe doạ mới nhất trên toàn bộ mạng.** Luôn cập nhật về các mối đe doạ mới nhất để tránh hoặc nhanh chóng loại bỏ các mối đe doạ trên toàn bộ mạng từ một nơi duy nhất, sử dụng dữ liệu về mối đe doạ được chia sẻ từ khắp thế giới để ngăn chặn các cuộc tấn công ngay cả khi bạn không thể nhìn thấy chúng, kịp thời thông báo cho bạn về sự tồn tại của chúng và đóng cửa để ngăn chặn truy cập vào các kho dữ liệu hoặc thiết bị khác trên mạng.

Bảo vệ các tài sản quan trọng tại biên mạng. Các tổ chức có thể ngăn chặn gần như 100% số vụ xâm nhập mạng bằng cách dùng mạng làm cảm biến và công cụ thực thi. Điều này có thể thực hiện được trong khi vẫn cung cấp thông tin chuyên sâu hơn để tăng cường bảo vệ và có khả năng ứng phó nhanh hơn.

Báo cáo nghiên cứu gần đây của Forrester cho thấy rằng Cisco TrustSec cho phép bộ phận CNTT thực hiện những thay đổi nhanh hơn 98%, giảm chi phí lên đến 80% và mang lại lợi tức đầu tư 140%.

Đổi mới Liên tục tại Biên Mạng

Với sự bùng nổ kết nối dự kiến mang lại cơ hội lớn, các công ty đang bắt đầu nhận ra rằng sự chuyển đổi này sẽ đòi hỏi các thay đổi cơ bản cho cơ sở hạ tầng mạng của họ và khả năng quản lý cũng như phân tích dữ liệu. Chúng tôi đang dẫn đầu quá trình chuyển đổi này bằng cách thúc đẩy đổi mới trong cơ sở hạ tầng mạng, quản lý cơ sở hạ tầng và phân tích để trích xuất thông tin chi tiết hữu ích từ dữ liệu.

Mục đích của Cisco là chuyển đổi quá trình khắc phục sự cố từ ứng phó thành chủ động, và giảm thời gian giải quyết từ nhiều ngày xuống còn vài phút. Chúng tôi sẽ làm như vậy bằng cách coi mọi thiết bị trong mạng là một cảm biến và một thành phần xử lý dữ liệu phân tán. Bằng cách nhận dữ liệu từ các thiết bị ở biên mạng, phân phối xử lý ở gần với nguồn dữ liệu hơn, chúng tôi có thể thực hiện phân tích ở tốc độ tối đa để tạo ra những thông tin chi tiết hữu dụng thông qua học máy.

Với nền tảng được cài đặt lớn nhất và các giải pháp ASIC tùy chỉnh, Cisco là doanh nghiệp duy nhất có thể thiết kế phần cứng và phần mềm được tối ưu hoá cho phân tích. Khai thác sức mạnh của nền tảng được cài đặt. Một mạng có dây và không dây kết hợp sẽ đồng nghĩa với việc thông tin trên biên mạng có thể giúp bạn khắc phục sự cố, cho dù chúng xảy ra ở biên mạng hay không, chỉ trong vài giây. Và theo thời gian, khắc phục các sự cố tiềm ẩn ngay cả trước khi chúng xảy ra. Điều này sẽ giúp bộ phận CNTT cung cấp thoả thuận mức độ dịch vụ (SLA) để đạt được hiệu suất mạng và ứng dụng cần thiết cho tương lai.

Kết luận

Với sự phụ thuộc rất nhiều vào biên mạng, việc sử dụng đại trà mạng LAN và WAN có dây và không dây cho thấy nguy cơ có thể dẫn đến xâm phạm bảo mật, mất năng suất và doanh thu, mất cơ hội và thiếu khả năng hiển thị. Biên mạng Cisco cho phép các tổ chức vượt xa phương pháp tiếp cận bị ràng buộc theo tiêu chuẩn, sẵn có, mang lại thông tin có giá trị cao ở biên mạng để đổi mới nhanh hơn, giảm chi phí và độ phức tạp cũng như giảm rủi ro. Phương pháp này cho phép tổ chức:

- Bảo vệ doanh nghiệp bằng phòng tuyến vững chắc đầu tiên
- Tự tin cung cấp các ứng dụng cho đối tượng mục tiêu
- Mang lại một trải nghiệm liền mạch cho nhân viên ở mọi nơi
- Tương tác với khách hàng để tăng dòng doanh thu mới
- Quản lý tốt hơn các thiết bị IoT và tối ưu hoá môi trường thực tế
- Mang đến cái nhìn tối ưu về những gì đang thực sự xảy ra trong doanh nghiệp

Để biết Thêm Thông tin

Để tìm hiểu thêm, hãy truy cập trang Công nghệ Cisco Unified Access™ tại http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

C11-737691-01 11/16