



Quản lý và bảo mật quyền truy nhập vào ứng dụng của bạn bằng **Azure Active Directory**



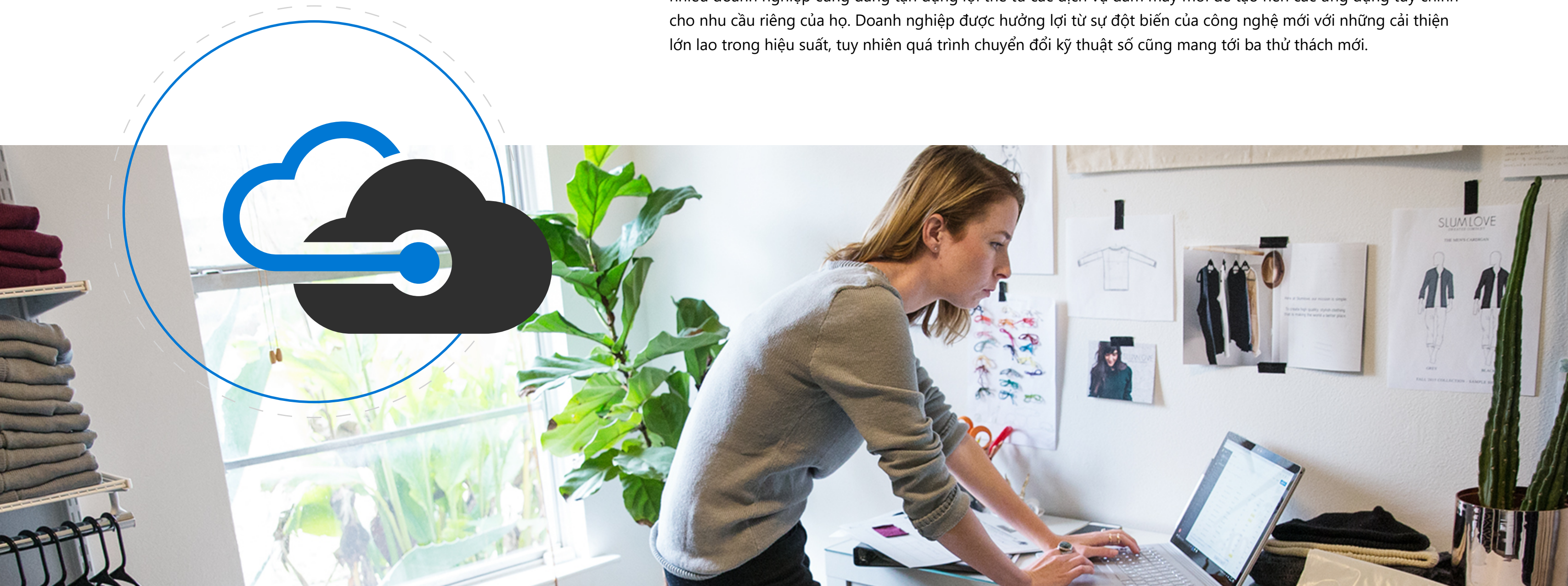
Mục 1

Quản lý danh tính và
quyền truy nhập là gì?

Quản lý danh tính và quyền truy nhập là gì?

Chuyển đổi kỹ thuật số

Điện toán đám mây và các thiết bị di động đã làm biến đổi nơi làm việc hiện đại. Một lượng lớn lực lượng lao động toàn cầu có thể linh hoạt làm việc từ mọi nơi bằng cách sử dụng các ứng dụng phần mềm dưới dạng dịch vụ (SaaS) miễn phí và chi phí thấp để giải quyết các thách thức về hiệu suất cũng như cộng tác. Các doanh nghiệp lớn đang di chuyển ứng dụng và hoạt động tính toán lên đám mây để hiện đại hóa kiến trúc của mình, đồng thời, nhiều doanh nghiệp cũng đang tận dụng lợi thế từ các dịch vụ đám mây mới để tạo nên các ứng dụng tùy chỉnh cho nhu cầu riêng của họ. Doanh nghiệp được hưởng lợi từ sự đột biến của công nghệ mới với những cải thiện lớn lao trong hiệu suất, tuy nhiên quá trình chuyển đổi kỹ thuật số cũng mang tới ba thử thách mới.



Quản lý danh tính và quyền truy nhập là gì?

Thử thách mới

Những thách thức
sinh ra từ quá trình
chuyển đổi kỹ thuật
số

Rủi ro về bảo mật: Trước thời kỳ cách mạng đám mây, bộ phận CNTT đóng vai trò là người canh gác về công nghệ. Các ứng dụng cùng với nền tảng bạn quản lý và bảo mật đều nằm trong vành đai mạng, tất cả những người đăng nhập vào tài nguyên công ty của bạn đều được xác thực trước bằng tường lửa. Những ngày đó đã qua rồi. Lực lượng lao động của bạn đã kiểm soát nhiều hơn những công nghệ họ sử dụng, đa phần trong số đó được truy nhập qua internet. Các kẻ tấn công qua mạng đã tìm hiểu cách để khai thác những lỗ hổng này. Ngay cả khi người dùng biết đúng mật khẩu để vào tài khoản thì không phải lúc nào bạn cũng có thể chắc rằng họ chính người mà họ tự xưng.

Gánh nặng quản trị: Sự bùng nổ của điểm cuối mang đến cho người dùng thêm nhiều cách để kết nối nhưng cũng đồng thời kéo theo cơn ác mộng về quản trị. Rất nhiều doanh nghiệp không nắm được toàn bộ những công cụ mà nhân viên sử dụng và kể cả khi họ kiểm kê đủ tốt thì số lượng ứng dụng đám mây khổng lồ cũng khiến họ phải quản lý nhiều hệ thống danh tính, tăng cao chi phí và làm trầm trọng hơn những rủi ro bảo mật hiện có.

Trải nghiệm người dùng kém: Người dùng cũng cảm thấy không hài lòng. Họ yêu thích sự linh hoạt nhưng cảm thấy chán nản vì lượng thông tin xác thực mình phải nhớ.



Rủi ro về
bảo mật



Gánh nặng
quản trị



Trải nghiệm
người dùng kém

Quản lý danh tính và quyền truy nhập là gì?

Quản lý danh tính và quyền truy nhập chính là nền tảng kiểm soát tập trung

Mẫu số chung của những vấn đề nhức nhối này là các hệ thống xác minh danh tính thiếu hiệu quả. Danh tính đã thay thế vành đai mạng để trở thành nền tảng kiểm soát mới. Bạn cần có giải pháp kết nối các công cụ, kiến trúc, thiết bị và dịch vụ riêng rẽ trong khắp doanh nghiệp để bảo vệ tổ chức và quản lý quyền truy nhập tốt hơn cho cả nhân viên lẫn đối tác bên ngoài, các hệ thống quản lý danh tính và quyền truy nhập (IAM) tập hợp quyền truy nhập trong một hệ thống sẽ giúp bạn kiểm soát dễ dàng hơn. Các hệ thống này mang tới khả năng cộng tác liền mạch giữa các ranh giới trong tổ chức bạn, đồng thời cải thiện khả năng bảo mật cho tài nguyên công ty bạn. Một giải pháp IAM đủ tốt sẽ cho phép bạn kết nối người dùng của mình với toàn bộ các ứng dụng làm việc của họ—bất kể là ứng dụng trong đám mây hay tại chỗ—qua một bộ thông tin xác thực. Các giải pháp IAM đều được thiết kế để mang tới cho người dùng quyền truy nhập vào đúng những tài nguyên họ cần, đồng thời ngăn chặn người dùng không có phân sự truy nhập những dữ liệu họ không được phép tiếp cận. Khả năng quản lý việc cấp phép và quyền truy nhập của người dùng từ cổng thông tin tập trung giúp giảm bớt đáng kể số quy trình thủ công liên quan tới việc cấp phép và hủy cấp phép tài khoản người dùng. Giải pháp IAM cũng cung cấp các công cụ giúp quản lý các chính sách bảo mật áp dụng với danh tính và ứng dụng của bạn. Những giải pháp IAM tốt nhất sẽ bảo vệ danh tính tốt hơn, cải thiện trải nghiệm người dùng và tăng cao sự hiệu quả trong quản trị.

Giải pháp IAM giải quyết các thách thức này



Bảo vệ danh tính tốt hơn



Cải thiện trải nghiệm người dùng



Tăng cao sự hiệu quả trong quản trị

Mục 2

Tổng quan về Azure AD

Tổng quan về Azure AD

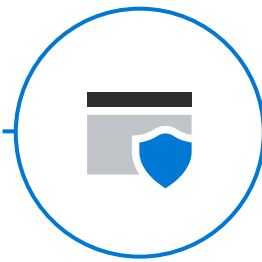
Một giải pháp toàn diện

Microsoft Azure Active Directory (Azure AD) là một giải pháp IAM toàn diện trong đám mây, đồng thời cũng là giải pháp hàng đầu thị trường về quản lý thư mục, quyền truy nhập ứng dụng và bảo vệ danh tính nâng cao. Azure AD hỗ trợ các tổ chức quản lý và bảo mật danh tính để giúp nhân viên, đối tác và khách hàng truy nhập vào các ứng dụng và dịch vụ họ cần. Azure AD giúp hàng triệu tổ chức quản lý và bảo mật hơn một tỉ danh tính.



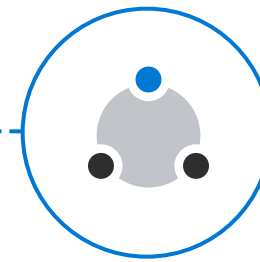
Hiện đại hóa quyền truy nhập

Quản lý và bảo mật quyền truy nhập vào dữ liệu cũng như tài nguyên của tổ chức ở tại chỗ và trong đám mây. Kết nối tất cả người dùng, ứng dụng và thiết bị với đám mây để mang tới khả năng truy nhập liền mạch và bảo mật, cùng khả năng quan sát và kiểm soát tốt hơn. Tự động hóa quy trình và hỗ trợ các tùy chọn tự phục vụ giúp duy trì chi phí thấp, cũng như cải thiện hiệu suất cho người dùng.



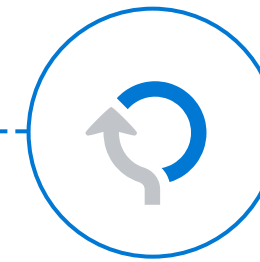
Bảo mật và quản trị

Với một lượng lớn các cuộc tấn công vào thông tin xác thực của người dùng mỗi ngày, cách thức để ngăn chặn xâm phạm chính là không ngừng theo dõi những hành vi thông thường và bất thường trong tập hợp tín hiệu rộng nhất có thể, áp dụng trí tuệ nhân tạo và tự động hóa các biện pháp ứng phó. Cân bằng hiệu suất và bảo mật nhờ cung cấp quyền truy nhập kịp thời vào tài nguyên phù hợp, cũng như định kỳ xem lại quyền truy nhập và thực thi chính sách.



Kết nối và cộng tác

Mở rộng doanh nghiệp bằng một dịch vụ đám mây đáng tin cậy có thể mở rộng quy mô ra hàng triệu người dùng, cùng khả năng bảo mật và tính linh hoạt đầu ngành. Kết nối với người dùng bên ngoài và hỗ trợ họ làm việc hiệu quả bằng trải nghiệm tự phục vụ thân thiện với người dùng cũng như các biện pháp kiểm soát bảo mật tích hợp sẵn.



Phát triển và tích hợp

Xây dựng những ứng dụng mang tới cho người dùng một cách thức đơn giản để đăng nhập bằng tài khoản Microsoft cá nhân, cơ quan hoặc trường học hay bằng tài khoản mạng xã hội của họ. Bắt đầu kết nối với Microsoft Graph, cổng thông tin về dữ liệu cũng như thông tin trong Microsoft 365, và xây dựng những ứng dụng phong phú. Kích hoạt đăng nhập một lần và tự động hóa việc cấp quyền cho người dùng, đồng thời tiếp cận các tổ chức lớn nhất thế giới.

Mục 3

Azure AD cho ứng
dụng của bạn

Azure AD cho ứng dụng của bạn

Một nền tảng chung

Azure AD cho phép bạn quản lý một danh tính chung cho từng người dùng trong hạ tầng kết hợp để truy nhập mọi ứng dụng họ cần, gồm cả những ứng dụng dòng kinh doanh trên đám mây và tại chỗ. Quản lý toàn bộ danh tính của bạn từ một nền tảng chung, tăng cao tính hiệu quả trong quản trị và mang tới thêm cho bạn khả năng kiểm soát. Áp dụng các chính sách bảo mật chi tiết cho từng ứng dụng được sử dụng trong tổ chức của bạn.



Azure AD cho ứng dụng của bạn

Tiết kiệm thời gian và tiền bạc

Azure AD được tích hợp sẵn với hàng nghìn ứng dụng, trong đó có cả những tùy chọn phổ biến như Workday, ServiceNow, SuccessFactors, Adobe và Concur, tạo điều kiện dễ dàng hơn để bạn cung cấp các ứng dụng đó cho người dùng của mình. Với một bảng điều khiển duy nhất, bạn có thể triển khai các chính sách nhất quán và giám sát quyền truy nhập. Bạn có thể tự động hóa quy trình cấp phép người dùng và quản lý vòng đời, đồng thời tiết kiệm thời gian và tài nguyên với khả năng tự quản lý tài khoản. Bạn còn có thể lấy thông tin người dùng từ các công cụ nhân sự để làm nguồn tin cậy, loại bỏ nhu cầu cần tới các tập lệnh tùy chỉnh hoặc quy trình thủ công để quản lý thuộc tính người dùng.

Những ứng dụng được đặt cấu hình thông qua Azure AD đều cho phép đăng nhập một lần (SSO) để mang tới khả năng truy nhập liền mạch, nghĩa là người dùng không cần phải nhớ thông tin xác thực của từng tài khoản ứng dụng hay tái sử dụng những mật khẩu yếu và gây ra rủi ro về vi phạm dữ liệu. Các tài khoản đã được đặt cấu hình để tự động cấp phép sẽ cung cấp cho người dùng quyền truy nhập vào các tài nguyên mới ngay khi có thể. Đối với việc cấp phép nội bộ, Azure AD đảm bảo nhân viên mới sẽ có quyền truy nhập vào mọi tài nguyên thích hợp ngay từ ngày làm việc đầu tiên.



Tiết kiệm thời gian và tiền bạc



Các tích hợp SaaS tích hợp sẵn



Đăng nhập một lần



Quyền truy nhập cho người dùng từ ngày đầu tiên

Azure AD cho ứng dụng của bạn

Cung cấp quyền truy nhập bảo mật hơn cho toàn bộ ứng dụng của bạn

Azure AD mang tới cho bạn khả năng bảo vệ danh tính toàn diện trong khắp các ứng dụng của mình – cả các ứng dụng SaaS lẫn các ứng dụng dòng kinh doanh tại chỗ. Bất kể là người dùng đang yêu cầu truy nhập vào Microsoft Word hay Box, Azure AD đều đảm bảo danh tính của họ được xác nhận trước khi cấp quyền truy nhập. Bạn cũng có thể tạo các chính sách quản trị quyền truy nhập để đảm bảo người dùng chỉ có quyền truy nhập vào đúng những nội dung họ cần, khi họ cần. Bạn có thể yêu cầu người dùng phải yêu cầu quyền truy nhập, đồng thời, có thể đặt giới hạn thời gian cho thời lượng họ có thể truy nhập vào ứng dụng, cũng như tiến hành đánh giá tuân thủ quyền truy nhập định kỳ.

Azure AD còn tận dụng sức mạnh của Microsoft Intelligent Security Graph và khả năng máy học để phân tích hàng nghìn tỉ tín hiệu trong khắp các sản phẩm và dịch vụ của chúng tôi nhằm phát hiện hành vi bất thường và gán rủi ro liên quan cho từng phiên. Azure AD quan sát thiết bị, vị trí và thông tin ngữ cảnh khác để đánh giá rủi ro của hoạt động đăng nhập. Bạn có thể thiết lập chính sách Truy nhập có điều kiện Azure AD để tự động áp dụng các biện pháp bảo mật, như chặn yêu cầu quyền truy nhập hoặc yêu cầu đặt lại mật khẩu khi đăng nhập có vẻ rủi ro hay khi khớp với các điều kiện chính sách cụ thể.



Các biện pháp bảo mật cho ứng dụng



Khả năng bảo vệ danh tính



Quản trị quyền truy nhập



Chính sách Truy nhập có điều kiện

Mục 4

Cách quản lý và bảo mật ứng dụng bằng Azure AD

Azure AD giúp bạn dễ dàng duy trì kiểm soát, đồng thời giảm bớt chi phí bằng cách sử dụng khả năng tự động hóa, tự phục vụ và thực thi chính sách.

Cách quản lý và bảo mật ứng dụng bằng Azure AD



Tích hợp ứng dụng Azure AD

Bộ sưu tập ứng dụng Azure AD giúp bạn dễ dàng đặt cấu hình và kết nối bất cứ ứng dụng nào trong số hàng nghìn ứng dụng được tích hợp sẵn với đối tượng thuê của bạn. Toàn bộ các ứng dụng này đều hỗ trợ trải nghiệm SSO, đồng thời, việc đặt cấu hình ứng dụng để sử dụng Truy nhập có điều kiện Azure AD trên cơ sở từng ứng dụng hoặc sử dụng các chính sách toàn doanh nghiệp cũng vô cùng đơn giản. Khi bạn đã thêm ứng dụng và đặt cấu hình theo nhu cầu của mình, những người dùng có quyền truy nhập được ủy quyền có thể dễ dàng tìm thấy ứng dụng trong cổng thông tin Ứng dụng của tôi Azure AD, một cổng thông tin tập trung để khám phá và cho chạy ứng dụng người dùng cuối.

Nếu bạn đã xây dựng một ứng dụng hoặc cần tích hợp ứng dụng cho tổ chức, bạn cũng có thể yêu cầu niêm yết ứng dụng trong bộ sưu tập ứng dụng Azure AD.

[Khám phá hàng nghìn ứng dụng được tích hợp sẵn >](#)



Bảo mật quyền truy nhập kết hợp

Sử dụng Proxy ứng dụng Azure AD để cung cấp quyền truy nhập từ xa bảo mật vào ứng dụng web tại chỗ dựa theo yêu cầu mà không cần phải sử dụng VPN. Proxy ứng dụng yêu cầu cài đặt một trình kết nối nhẹ và cung cấp trải nghiệm CNTT cũng như trải nghiệm người dùng cuối tương tự như các ứng dụng SaaS được kết nối thông qua bộ sưu tập ứng dụng Azure AD.

Hoặc nếu muốn, bạn cũng có thể tận dụng các khoản đầu tư hạ tầng hiện có, chẳng hạn với các đối tác như F5 ZScaler, SAP, Oracle hoặc Ping Identity, để kết nối với các loại ứng dụng khác, như những ứng dụng sử dụng các giao thức xác thực dựa trên tiêu đề hoặc Kerberos, mà vẫn có được những lợi ích về sự tập trung và bảo mật của Azure AD.

[Đọc cách thêm ứng dụng tại chỗ thông qua Proxy ứng dụng >](#)

[Kết nối các mạng ứng dụng đối tác và đám mây khác >](#)

Cách quản lý và bảo mật ứng dụng bằng Azure AD



Cấp phép tự động

Azure AD giúp bạn tự động hóa hoạt động tạo, bảo trì và loại bỏ danh tính người dùng trong các ứng dụng SaaS phổ biến. Bạn có thể tự động tạo tài khoản mới trong các hệ thống phù hợp cho người dùng mới khi họ tham gia nhóm hoặc tổ chức của bạn. Khi người dùng rời khỏi nhóm hoặc tổ chức, bạn có thể đặt chính sách để tự động hủy kích hoạt tài khoản của họ khỏi hệ thống phù hợp. Bằng cách tự động hóa những tác vụ này, bạn có thể đảm bảo rằng danh tính trong các ứng dụng và hệ thống của mình luôn được cập nhật dựa trên thay đổi trong thư mục hoặc hệ thống nhân sự, giảm bớt lỗi và thời gian.

[Tìm hiểu thêm về việc thiết lập cấp phép và hủy cấp phép tự động cho các ứng dụng SaaS >](#)



Quản lý nhóm

Azure AD giúp bạn cấp quyền truy nhập vào các tài nguyên trong tổ chức bằng cách cung cấp quyền truy nhập cho một người dùng hoặc toàn bộ nhóm Azure AD. Việc sử dụng nhóm cho phép chủ sở hữu tài nguyên đặt quyền truy nhập cho mọi thành viên trong nhóm, thay vì phải cấp quyền cho từng người một. Đây là phương pháp bảo mật hơn vì bạn ít có khả năng cấp nhầm quyền truy nhập không phù hợp cho một cá nhân nào đó, đồng thời lại tiết kiệm thời gian cho bạn. Bạn còn có thể mở rộng hoạt động quản lý nhóm một cách linh hoạt bằng cách tự động hóa quá trình đăng ký thông qua các chính sách dựa trên thuộc tính danh tính.

[Tìm hiểu cách tạo nhóm trong Cổng thông tin Azure >](#)

Cách quản lý và bảo mật ứng dụng bằng Azure AD



Người dùng tự phục vụ

Có những tác vụ không cần tới chuyên gia CNTT để hoàn thành và Azure AD giúp bạn giao những tác vụ đó cho người khác trong tổ chức. Bạn có thể hỗ trợ người dùng tạo và quản lý các nhóm bảo mật riêng của họ trong Azure AD. Chủ nhóm có thể chấp thuận hay từ chối các yêu cầu tư cách thành viên hoặc có thể ủy quyền kiểm soát tư cách thành viên nhóm.

[Thiết lập nhóm tự quản lý >](#)

Việc tự phục vụ cũng mở rộng đến người dùng. Người dùng có thể đăng ký tài khoản thông qua cổng thông tin tự phục vụ nếu họ có email được xác minh, đồng thời, có thể sử dụng cổng thông tin để đặt lại mật khẩu của mình. Việc này có thể giúp bộ phận hỗ trợ tiết kiệm vô số thời gian và tiền bạc.

[Đặt cấu hình cho chức năng tự đặt lại mật khẩu >](#)



Hiện đại hóa xác thực

Nếu đang sử dụng phương pháp xác thực tại chỗ như Active Directory Federation Services (AD FS) thì bạn có thể cân nhắc di chuyển ứng dụng của mình sang Azure AD. Bạn vẫn có được những lợi ích người dùng tương tự như ở SSO nhưng sẽ có thêm các lợi ích về khả năng mở rộng và bảo mật có sẵn từ đám mây, như áp dụng các biện pháp kiểm soát quyền truy nhập chi tiết theo từng ứng dụng bằng cách sử dụng Truy nhập có điều kiện Azure AD hoặc cấp quyền truy nhập đối tác vào các tài nguyên bằng khả năng cộng tác của Azure AD B2B. Những ứng dụng sử dụng các tiêu chuẩn SAML 2.0, WS-Federation, OAuth hoặc OpenID Connect cho khả năng đăng nhập liên kết đều có thể di chuyển được.

[Xây dựng các chính sách Truy nhập có điều kiện Azure AD để bảo mật quyền truy nhập vào ứng dụng của bạn >](#)

[Sử dụng Azure AD B2B để cộng tác liền mạch với các đối tác bên ngoài của bạn >](#)

Kết nối bảo mật mọi ứng dụng, trên mọi đám mây hoặc máy chủ với Azure AD.

1 triệu ứng dụng hiện hoạt, độc đáo đã kết nối.



Hãy bắt đầu ngay hôm nay.

Bắt đầu bản dùng thử một tháng miễn phí Azure AD để thấy được sự đơn giản trong việc quản lý quyền truy nhập người dùng cho mọi ứng dụng và bảo mật doanh nghiệp của bạn.

