Microsoft

จัดการและรักษาความปลอดภัยการเข้าถึงแอปพลิเคชันของคุณด้วย Azure Active Directory



ส่วนที่ 1

ระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากรคืออะไร

ระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากรคืออะไร

การแปลงข้อมูลเป็นดิจิทัล

การประมวลผลแบบคลาวด์และอุปกรณ์เคลื่อนที่ได้แปลงโฉมสถานที่ทำงานยุคใหม่ บุคลากรทั่วโลกที่เพิ่มมากขึ้นมีความยืดหยุ่นในการทำงานจากทุกที่โดยใช้ซอฟต์แวร์ฟรีและมีต้นทุนต่ำเป็นแอปพลิเคชันการให้บริการซอฟต์แวร์ (SaaS) เพื่อแก้ไขปัญหาด้านประสิทธิภาพการทำงานและการทำงานร่วมกัน บริษัทขนาดใหญ่กำลังโยกย้ายแอปพลิเคชันและการประมวลผลไปยังระบบคลาวด์เพื่อทำให้สถาปัตยกรรมทันสมัย และสายงานธุรกิจกำลังใช้ประโยชน์จากบริการ Cloud ใหม่เพื่อสร้างแอปแบบกำหนดเองตามความต้องการเฉพาะของตน แม้ว่าบริษัทจะได้รับประโยชน์จากการมีเทคโนโลยีใหม่เพิ่มขึ้นอย่างรวดเร็วพร้อมประสิทธิภาพการทำงานที่มากยิ่งขึ้น แต่การแปลงข้อมูลเป็นดิจิทัลยังมีปัญหาใหม่สามอย่าง



ระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากรคืออะไร

ปัญหาใหม่

ความเสี่ยงด้านความปลอดภัย: ก่อนการปฏิวัติระบบคลาวด์ ฝ่าย IT ทำหน้าที่เป็นผู้ดูแลด้านเทคโนโลยี แอปและแพลตฟอร์มที่คุณจัดการและรักษาความปลอดภัยนั้นอยู่ภายในขอบเขตเครือข่าย และทุกคนที่ลงชื่อเข้าใช้ทรัพยากรขององค์กรจะได้รับการตรวจสอบโดยไฟร์วอลล์ก่อน วันเวลาเหล่านั้นจบลงแล้ว บุคลากรของคุณสามารถควบคุมเทคโนโลยีที่พวกเขาใช้ได้มากขึ้น ซึ่งส่วนใหญ่สามารถเข้าถึงได้ผ่านอินเทอร์เน็ต ผู้โจมตีทางไซเบอร์ได้เรียนรู้การใช้ประโยชน์จากช่องโหว่เหล่านี้ แม้ว่าผู้ใช้จะทราบรหัสผ่านที่ถูกต้องของบัญชี คุณก็ไม่สามารถมั่นใจได้ตลอดเวลาว่าพวกเขาเป็นบุคคลตามที่กล่าวอ้าง

ภาระในการจัดการดูแล: จำนวนปลายทางที่เพิ่มมากขึ้นทำให้ผู้ใช้มีวิธีเชื่อมต่อมากขึ้น แต่ก็ยังสร้างฝันร้ายในการจัดการดูแลอีกด้วย บริษัทจำนวนมากไม่ได้ทราบถึงเครื่องมือทั้งหมดที่พนักงานใช้งาน และแม้ว่าพวกเขาจะมีคลังเครื่องมือที่ดี แต่แอปในคลาวด์จำนวนมากหมายความว่าคุณต้องจัดการระบบข้อมูลประจำตัวหลายระบบ ซึ่งเพิ่มค่าใช้จ่ายและเพิ่มความเสี่ยงด้านความปลอดภัยที่มีอยู่

ประสบการณ์ใช้งานของผู้ใช้ที่ขาดประสิทธิภาพ: ผู้ใช้ยังได้รับผลกระทบด้วยเช่นกัน แม้พวกเขาจะชอบความยืดหยุ่น แต่ก็หงุดหงิดกับจำนวนข้อมูลประจำตัวที่พวกเขาต้องจำ

ปัญหาเนื่องจากการแปลงข้อมูลเป็นดิจิทัล



ความเสี่ยงด้านความปลอดภัย



ภาระในการจัดการดูแล



ประสบการณ์ใช้งานของผู้ใช้ที่ขาดประสิทธิภาพ

ระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากรคืออะไร

ระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากรคือพื้นที่ควบคุมส่วนกลาง

ลักษณะร่วมของปัญหาเหล่านี้คือระบบที่ไม่มีประสิทธิภาพในการตรวจสอบข้อมูลประจำตัว ข้อมูลประจำตัวได้แทนที่ขอบเขตเครือข่ายเป็นพื้นที่ควบคุมแบบใหม่ คุณต้องการโซลูชันที่เชื่อมต่อเครื่องมือ สถาปัตยกรรม อุปกรณ์ และบริการต่างๆ ทั่วทั้งองค์กรเพื่อป้องกันองค์กรได้ดียิ่งขึ้นและจัดการการเข้าถึงระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากร (IAM) สำหรับทั้งพนักงานและคู่ค้าภายนอกที่รวมการเข้าถึงภายใต้ระบบเดียว ซึ่งทำให้ควบคุมได้มากขึ้น และยังสามารถทำงานร่วมกันข้ามขอบเขตขององค์กรได้อย่างราบรื่น ขณะปรับปรุงการรักษาความปลอดภัยของทรัพยากรในองค์กรของคุณ โซลูชัน IAM ที่ดีจะช่วยให้คุณเชื่อมต่อผู้ใช้เข้ากับแอปพลิเคชันการทำงานทั้งหมดของพวกเขาผ่านข้อมูลประจำตัวชุดเดียว ไม่ว่าจะอยู่บนระบบคลาวด์หรือภายในองค์กร โซลูชัน IAM ได้รับการออกแบบมาเพื่อให้ผู้ใช้เข้าถึงทรัพยากรที่จำเป็นเท่านั้น และบล็อกไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลที่ไม่ควรเข้าถึง คุณสามารถจัดการสิทธิ์และการอนุญาตเข้าถึงของผู้ใช้จากพอร์ทัลส่วนกลาง ซึ่งช่วยลดขั้นตอนการดำเนินการด้วยตนเองจำนวนมากที่เกี่ยวข้องกับการเตรียมใช้งานและการยกเลิกการเตรียมใช้งานบัญชีผู้ใช้ โซลูชัน IAM ยังมีเครื่องมือในการจัดการนโยบายการรักษาความปลอดภัยในข้อมูลประจำตัวและแอปของคุณอีกด้วย โซลูชัน IAM ที่ดีที่สุดจะปกป้องข้อมูลประจำตัวได้ดียิ่งขึ้น ปรับปรุงประสบการณ์ใช้งานของผู้ใช้ และเพิ่มประสิทธิภาพในการจัดการดูแล

โซลูชัน IAM
แก้ไขปัญหาเหล่านี้



ปกป้องข้อมูลประจำตัวได้ดียิ่งขึ้น



ปรับปรุงประสบการณ์ใช้งานของผู้ใช้



เพิ่มประสิทธิภาพในการจัดการดูแล

ส่วนที่ 2

ภาพรวม Azure AD

ภาพรวม Azure AD

โซลูชันที่ครอบคลุม

Microsoft Azure Active Directory (Azure AD) คือโซลูชัน IAM ที่ครอบคลุมในระบบคลาวด์ และเป็นผู้นำในตลาดสำหรับการจัดการไดเรกทอรี การเข้าถึงแอปพลิเคชัน และการป้องกันข้อมูลประจำตัวขั้นสูง Azure AD ช่วยให้องค์กรสามารถจัดการและรักษาความปลอดภัยข้อมูลประจำตัวสำหรับพนักงาน คู่ค้า และลูกค้าในการเข้าถึงแอปและบริการที่พวกเขาต้องการ Azure AD ช่วยให้องค์กรนับล้านแห่งสามารถจัดการและรักษาความปลอดภัยข้อมูลประจำตัวมากกว่าหนึ่งพันล้านรายการ



ปรับปรุงการเข้าถึงให้ทันสมัย

จัดการและรักษาความปลอดภัยการเข้าถึงข้อมูลและทรัพยากรขององค์กรทั้งภายในองค์กรและบนระบบคลาวด์ เชื่อมต่อผู้ใช้แอปพลิเคชัน และอุปกรณ์ทั้งหมดเข้ากับระบบคลาวด์เพื่อการเข้าถึงที่ราบรื่นและปลอดภัย พร้อมการมองเห็นและการควบคุมที่ดียิ่งขึ้น การทำให้เป็นเวิร์กโฟลว์อัตโนมัติและการเปิดใช้งานตัวเลือกบริการตนเองจะช่วยลดค่าใช้จ่ายและปรับปรุงประสิทธิภาพการทำงานสำหรับผู้ใช้ของคุณ

รักษาความปลอดภัยและกำกับดูแล

เนื่องจากการโจมตีข้อมูลประจำตัวของผู้ใช้เพิ่มมากขึ้นทุกวัน วิธีการป้องกันการละเมิดจึงเป็นการติดตามพฤติกรรมปกติและผิดปกติอย่างต่อเนื่องในชุดสัญญาณที่กว้างที่สุดเท่าที่เป็นไปได้ และใช้ปัญญาประดิษฐ์และทำการตอบสนองอัตโนมัติ สร้างสมดุลระหว่างประสิทธิภาพการทำงานและการรักษาความปลอดภัยด้วยการเข้าถึงทรัพยากรที่ถูกต้องในเวลาที่เหมาะสม การยืนยันสิทธิ์เป็นประจำและการบังคับใช้นโยบาย

เชื่อมต่อและทำงานร่วมกัน

ขยายธุรกิจของคุณด้วยบริการ Cloud ที่เชื่อถือได้ ซึ่งสามารถปรับขนาดเข้ากับผู้ใช้หลายล้านคนด้วยการรักษาความปลอดภัยและความยืดหยุ่นชั้นนำในอุตสาหกรรม เชื่อมต่อกับผู้ใช้ภายนอกและส่งเสริมให้พวกเขามีประสิทธิภาพการทำงานมากขึ้นด้วยประสบการณ์บริการตนเองที่ใช้งานง่ายและตัวควบคุมการรักษาความปลอดภัยในตัว

พัฒนาและผสานรวม

สร้างแอปพลิเคชันที่ช่วยให้ผู้ใช้ลงชื่อเข้าใช้บัญชี Microsoft ส่วนบุคคล ของที่ทำงานหรือโรงเรียนหรือบัญชีเครือข่ายสังคมของตนได้อย่างง่ายดาย เริ่มต้นเชื่อมต่อกับ Microsoft Graph ซึ่งเป็นเกตเวย์ไปยังข้อมูลและข่าวกรองใน Microsoft 365 และสร้างแอปพลิเคชันที่สมบูรณ์แบบ เปิดใช้งานการลงชื่อเข้าระบบครั้งเดียว ทำให้การจัดเตรียมผู้ใช้เป็นระบบอัตโนมัติ และเข้าถึงองค์กรที่ใหญ่ที่สุดของโลก

ส่วนที่ 3

Azure AD
สำหรับแอปพลิเคชันของคุณ

Azure AD สำหรับแอปพลิเคชันของคุณ

แพลตฟอร์มสำหรับทุกอุปกรณ์

Azure AD ช่วยให้คุณสามารถจัดการข้อมูลประจำตัวทั่วไปสำหรับผู้ใช้แต่ละรายผ่านโครงสร้างพื้นฐานแบบไฮบริดของคุณเพื่อเข้าถึงแอปพลิเคชันทั้งหมดที่พวกเขาต้องการ รวมถึงแอปพลิเคชันสายงานธุรกิจในองค์กรและบนระบบคลาวด์ จัดการข้อมูลประจำตัวทั้งหมดของคุณจากแพลตฟอร์มสำหรับทุกอุปกรณ์ ซึ่งเพิ่มประสิทธิภาพในการจัดการดูแล และทำให้คุณควบคุมได้มากขึ้น ใช้นโยบายการรักษาความปลอดภัยในระดับแยกย่อยกับแต่ละแอปพลิเคชันที่ใช้ในองค์กรของคุณ



Azure AD สำหรับแอปพลิเคชันของคุณ

ประหยัดเวลาและค่าใช้จ่าย

Azure AD ผสานรวมกับแอปพลิเคชันจำนวนหลายพันไว้ล่วงหน้า รวมถึงตัวเลือกที่ได้รับความนิยม เช่น Workday, ServiceNow, SuccessFactors, Adobe และ Concur คุณจึงสามารถทำให้แอปดังกล่าวพร้อมใช้งานสำหรับผู้ใช้ได้สะดวกยิ่งขึ้น ปรับใช้นโยบายที่สอดคล้องกันและตรวจสอบสิทธิ์การเข้าถึงด้วยคอนโซลเดียว คุณสามารถทำให้เป็นเวิร์กโฟลว์อัตโนมัติสำหรับการจัดเตรียมผู้ใช้และการจัดการวงจรชีวิต พร้อมประหยัดเวลาและทรัพยากรด้วยการจัดการบัญชีแบบบริการตนเอง นอกจากนี้ คุณยังสามารถนำเข้าข้อมูลผู้ใช้จากเครื่องมือ HR เป็นแหล่งข้อมูลจริง ซึ่งกำจัดการใช้สคริปต์แบบกำหนดเองหรือขั้นตอนการดำเนินการด้วยตนเองเพื่อจัดการแอตทริบิวต์ผู้ใช้

แอปที่กำหนดค่าผ่าน Azure AD เปิดใช้งานการลงชื่อเข้าระบบครั้งเดียว (SSO) เพื่อการเข้าถึงที่ราบรื่นหมายความว่าผู้ใช้ไม่จำเป็นต้องจดจำข้อมูลประจำตัวสำหรับบัญชีแอปแต่ละบัญชี หรือใช้รหัสผ่านที่คาดเดาได้ง่ายอีกครั้งและเสี่ยงให้ข้อมูลรั่วไหล บัญชีที่กำหนดค่าสำหรับการเตรียมใช้งานอัตโนมัติจะช่วยให้ผู้ใช้สามารถเข้าถึงทรัพยากรใหม่ทันที สำหรับการเตรียมใช้งานขาเข้า Azure AD รับรองว่าพนักงานใหม่สามารถเข้าถึงทรัพยากรที่เกี่ยวข้องทั้งหมดได้ตั้งแต่วันแรก



ประหยัดเวลาและค่าใช้จ่าย



การผสานรวม SaaS ในตัว



การลงชื่อเข้าระบบครั้งเดียว



การเข้าถึงของผู้ใช้ในวันแรก

Azure AD สำหรับแอปพลิเคชันของคุณ

มอบการเข้าถึงแอปทั้งหมดของคุณที่ปลอดภัยยิ่งขึ้น

Azure AD มอบการป้องกันข้อมูลประจำตัวที่ครอบคลุมให้กับแอปทั้งหมดของคุณ ทั้งแอป SaaS และแอปสายงานธุรกิจภายในองค์กรของคุณ ไม่ว่าผู้ใช้จะร้องขอการเข้าถึง Microsoft Word หรือ Box Azure AD รับรองว่าข้อมูลประจำตัวของพวกเขาจะได้รับการยืนยันก่อนอนุญาตให้เข้าถึง คุณยังสามารถกำหนดนโยบายการกำกับดูแลการเข้าถึงเพื่อให้มั่นใจว่าผู้ใช้มีสิทธิ์เข้าถึงเฉพาะสิ่งที่พวกเขาต้องการเมื่อพวกเขาต้องการเท่านั้น คุณสามารถกำหนดให้ผู้ใช้ต้องขออนุญาตสำหรับการเข้าถึง และคุณสามารถกำหนดขีดจำกัดเวลาสำหรับระยะเวลาที่พวกเขาสามารถเข้าถึงแอปพลิเคชัน และดำเนินการตรวจสอบการปฏิบัติตามตามข้อบังคับของการเข้าถึงเป็นประจำ

Azure AD ยังใช้ประโยชน์จากพลังของ Microsoft Intelligent Security Graph และการเรียนรู้ของเครื่องมือเพื่อวิเคราะห์สัญญาณจำนวนหลายล้านล้านรายการจากผลิตภัณฑ์และบริการทั้งหมดของเราเพื่อเปิดเผยพฤติกรรมที่ผิดปกติและกำหนดความเสี่ยงให้แต่ละเซสชัน Azure AD จะดูที่อุปกรณ์ ตำแหน่งที่ตั้ง และข้อมูลบริบทอื่นๆ เพื่อประเมินความเสี่ยงของการลงชื่อเข้าใช้ คุณสามารถสร้างนโยบายการเข้าถึงแบบมีเงื่อนไขของ Azure AD ที่จะนำมาตรการรักษาความปลอดภัยไปใช้โดยอัตโนมัติ เช่น การบล็อกคำขอการเข้าถึงหรือการบังคับให้รีเซ็ตรหัสผ่าน เมื่อการลงชื่อเข้าใช้มีความเสี่ยงหรือตรงกับเงื่อนไขนโยบายเฉพาะ



มาตรการรักษาความปลอดภัยของแอปพลิเคชัน



การป้องกันข้อมูลประจำตัว



การกำกับดูแลการเข้าถึง



นโยบายการเข้าถึงแบบมีเงื่อนไข

ส่วนที่ 4

วิธีการจัดการและรักษาความปลอดภัยของแอปด้วย Azure AD

Azure AD ทำให้การควบคุมและลดค่าใช้จ่ายโดยใช้ระบบอัตโนมัติ บริการตนเอง และการบังคับใช้นโยบายกลายเป็นเรื่องง่าย

วิธีการจัดการและรักษาความปลอดภัยของแอปด้วย Azure AD



การผสานรวมแอป Azure AD

แกลเลอรีแอปพลิเคชัน Azure AD ทำให้ง่ายต่อการกำหนดค่าและเชื่อมต่อหนึ่งในแอปที่ผสานรวมไว้ล่วงหน้าจำนวนหลายพันแอปกับผู้เช่าของคุณ แอปเหล่านี้สนับสนุนประสบการณ์ SSO อย่างเต็มรูปแบบ และยังกำหนดค่าแอปสำหรับการเข้าถึงแบบมีเงื่อนไขของ Azure AD ของแต่ละแอปหรือนโยบายทั่วทั้งองค์กรได้อย่างง่ายดาย เมื่อคุณเพิ่มแอปและกำหนดค่าตามที่คุณต้องการแล้ว ผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงจะสามารถค้นหาได้อย่างง่ายดายในพอร์ทัลแอปของฉันของ Azure AD ซึ่งเป็นพอร์ทัลส่วนกลางสำหรับการค้นหาและเปิดใช้แอปสำหรับผู้ใช้

ถ้าคุณสร้างแอปเองหรือต้องการแอปที่ผสานรวมสำหรับองค์กรของคุณ คุณสามารถร้องขอให้แสดงรายการในแกลเลอรีแอปพลิเคชันของ Azure AD ได้

สำรวจแอปที่ผสานรวมไว้ล่วงหน้าหลายพันแอป >



รักษาความปลอดภัยการเข้าถึงแบบไฮบริด

ใช้พร็อกซีแอปพลิเคชัน Azure AD เพื่อมอบการเข้าถึงจากระยะไกลที่ปลอดภัยไปยังแอปพลิเคชันบนเว็บภายในองค์กรตามการร้องขอโดยไม่ต้องใช้ VPN พร็อกซีแอปต้องใช้การตั้งตัวเชื่อมต่อขนาดเล็ก และมอบประสบการณ์ใช้งานสำหรับฝ่าย IT และผู้ใช้เหมือนกับแอป SaaS ที่เชื่อมต่อผ่านแกลเลอรีแอปพลิเคชัน Azure AD

หรือถ้าคุณต้องการใช้ประโยชน์จากการลงทุนกับโครงสร้างพื้นฐานที่มีอยู่ เช่น กับคู่ค้าอย่าง F5 ZScaler, SAP, Oracle หรือ Ping Identity เพื่อเชื่อมต่อแอปชนิดอื่นๆ เช่น แอปที่ใช้โพรโทคอลการรับรองความถูกต้องแบบใช้ส่วนหัวหรือ Kerberos คุณสามารถทำเช่นนี้ได้และยังคงได้รับสิทธิประโยชน์จากการรวมศูนย์กลางและการรักษาความปลอดภัยของ Azure AD

อ่านวิธีการเพิ่มแอปพลิเคชันภายในองค์กรผ่านพร็อกซีแอป >

เชื่อมต่อเครือข่ายและระบบคลาวด์ของแอปคู่ค้าอื่นๆ >

วิธีการจัดการและรักษาความปลอดภัยของแอปด้วย Azure AD



การเตรียมใช้งานอัตโนมัติ

Azure AD ช่วยให้คุณทำให้การสร้าง การบำรุงรักษา และการลบข้อมูลประจำตัวผู้ใช้ในแอปพลิเคชัน SaaS ที่ได้รับความนิยมเป็นระบบอัตโนมัติ คุณสามารถสร้างบัญชีใหม่ในระบบที่เหมาะสมสำหรับผู้ใช้ใหม่โดยอัตโนมัติ เมื่อพวกเขาเข้าร่วมทีมหรือองค์กรของคุณ เมื่อมีคนออกจากทีมหรือองค์กร คุณสามารถกำหนดนโยบายที่จะปิดใช้งานบัญชีของพวกเขาจากระบบที่เหมาะสมโดยอัตโนมัติได้ เมื่อทำให้งานเหล่านี้เป็นระบบอัตโนมัติ คุณสามารถมั่นใจได้ว่าข้อมูลประจำตัวในแอปและระบบเป็นข้อมูลล่าสุดตามการเปลี่ยนแปลงในไดเรกทอรีหรือระบบทรัพยากรบุคคลของคุณ ซึ่งช่วยลดข้อผิดพลาดและประหยัดเวลา

เรียนรู้เพิ่มเติมเกี่ยวกับการตั้งค่าการเตรียมใช้งานและการยกเลิกการเตรียมใช้งานอัตโนมัติให้กับแอป SaaS >



การจัดการกลุ่ม

Azure AD ช่วยให้คุณอนุญาตการเข้าถึงทรัพยากรขององค์กรโดยการมอบสิทธิ์การเข้าถึงให้กับผู้ใช้หนึ่งรายหรือให้กลุ่ม Azure AD ทั้งกลุ่ม การใช้กลุ่มจะช่วยให้เจ้าของทรัพยากรสามารถตั้งค่าสิทธิ์การเข้าถึงสำหรับสมาชิกทุกคนในกลุ่มได้ แทนที่จะต้องมอบสิทธิ์ให้กับแต่ละคน วิธีนี้เป็นวิธีที่ปลอดภัยยิ่งขึ้น เนื่องจากคุณมีโอกาสน้อยที่จะให้สิทธิ์การเข้าถึงที่ไม่เหมาะสมกับบุคคลโดยไม่ตั้งใจและสามารถช่วยคุณประหยัดเวลาได้ คุณสามารถปรับขนาดการจัดการกลุ่มแบบไดนามิกได้โดยให้การลงทะเบียนเป็นไปโดยอัตโนมัติผ่านนโยบายตามแอตทริบิวต์ข้อมูลประจำตัว

เรียนรู้วิธีการสร้างกลุ่มในพอร์ทัล Azure >

วิธีการจัดการและรักษาความปลอดภัยของแอปด้วย Azure AD



บริการตนเองสำหรับผู้ใช้

งานบางอย่างไม่จำเป็นต้องให้มืออาชีพด้าน IT ดำเนินการ และ Azure AD ช่วยให้คุณสามารถมอบหมายงานเหล่านั้นให้กับผู้อื่นในองค์กรได้ คุณสามารถส่งเสริมให้ผู้ใช้สร้างและจัดการกลุ่มความปลอดภัยของตนใน Azure AD เจ้าของกลุ่มสามารถอนุมัติหรือปฏิเสธคำขอเป็นสมาชิก หรือพวกเขาสามารถมอบสิทธิ์การควบคุมการเป็นสมาชิกกลุ่ม

ตั้งค่ากลุ่มที่จัดการด้วยตนเอง >

บริการตนเองยังขยายไปยังผู้ใช้อีกด้วย ผู้ใช้สามารถลงทะเบียนบัญชีผ่านพอร์ทัลบริการตนเองได้หากพวกเขามีอีเมลที่ยืนยันแล้ว และพวกเขาใช้พอร์ทัลในการรีเซ็ตรหัสผ่าน วิธีนี้สามารถประหยัดเวลาและค่าใช้จ่ายให้เจ้าหน้าที่ให้ความช่วยเหลือได้เป็นอย่างมาก

กำหนดค่าการรีเซ็ตรหัสผ่านแบบบริการตนเอง >



ปรับปรุงการรับรองความถูกต้องให้ทันสมัย

ถ้าคุณกำลังใช้การรับรองความถูกต้องภายในองค์กร เช่น Active Directory Federation Services (AD FS) คุณควรพิจารณาโยกย้ายแอปของคุณไปยัง Azure AD คุณยังคงมีสิทธิประโยชน์เดิมของผู้ใช้ เช่น SSO แต่จะได้รับสิทธิประโยชน์ในการปรับขนาดและการรักษาความปลอดภัยที่พร้อมให้บริการจากระบบคลาวด์ เช่น การใช้ตัวควบคุมการเข้าถึงตามแอปพลิเคชันในระดับแยกย่อยโดยใช้การเข้าถึงแบบมีเงื่อนไขของ Azure AD หรืออนุญาตให้คู่ค้าเข้าถึงทรัพยากรด้วยการทำงานร่วมกันของ Azure AD B2B แอปที่ใช้มาตรฐาน SAML 2.0, WS-Federation, OAuth หรือ OpenID Connect สำหรับการลงชื่อเข้าระบบที่ติดต่อกับภายนอกสามารถโยกย้ายได้ทั้งหมด

สร้างนโยบายการเข้าถึงแบบมีเงื่อนไขของ Azure AD เพื่อรักษาความปลอดภัยการเข้าถึงแอปของคุณ >

ใช้ Azure AD B2B เพื่อทำงานร่วมกับคู่ค้าภายนอกของคุณอย่างราบรื่น >

เชื่อมต่อแอปทั้งบนระบบคลาวด์หรือเซิร์
ฟเวอร์กับ Azure AD อย่างปลอดภัย

เชื่อมต่อกับแอปที่มีผู้ใช้ง
านไม่ซ้ำกัน 1 ล้านแอป

เริ่มต้นใช้งานวันนี้

เริ่มต้น Azure AD รุ่นทดลองใช้ฟรีหนึ่งเดือนเพื่อดูว่าการจัดการการเข้าถึงแอปทั้งหมดของผู้ใช้และการรักษาความปลอดภัยบริษัทของคุณนั้นง่ายดายเพียงใด

