



Kelola dan lindungi akses ke aplikasi Anda dengan **Azure Active Directory**



Bagian 1

Apa yang dimaksud dengan manajemen identitas dan akses?

Apa yang dimaksud dengan manajemen identitas dan akses?

Transformasi digital

Komputasi cloud dan perangkat seluler telah mengubah tempat kerja masa kini. Banyak tenaga kerja global mulai bekerja secara fleksibel dari mana saja menggunakan aplikasi perangkat lunak sebagai layanan (SaaS) yang tersedia gratis dan dengan harga terjangkau untuk mengatasi tantangan produktivitas dan kolaborasi. Perusahaan besar mulai memigrasikan aplikasi dan komputasi ke cloud untuk memodernkan arsitektur mereka, sementara lini bisnis mulai memanfaatkan layanan cloud baru untuk merancang aplikasi kustom sesuai kebutuhan. Perusahaan ini telah membuktikan manfaat dari berbagai teknologi baru yang lebih produktif. Sayangnya, transformasi digital juga menyebabkan munculnya tiga tantangan baru.



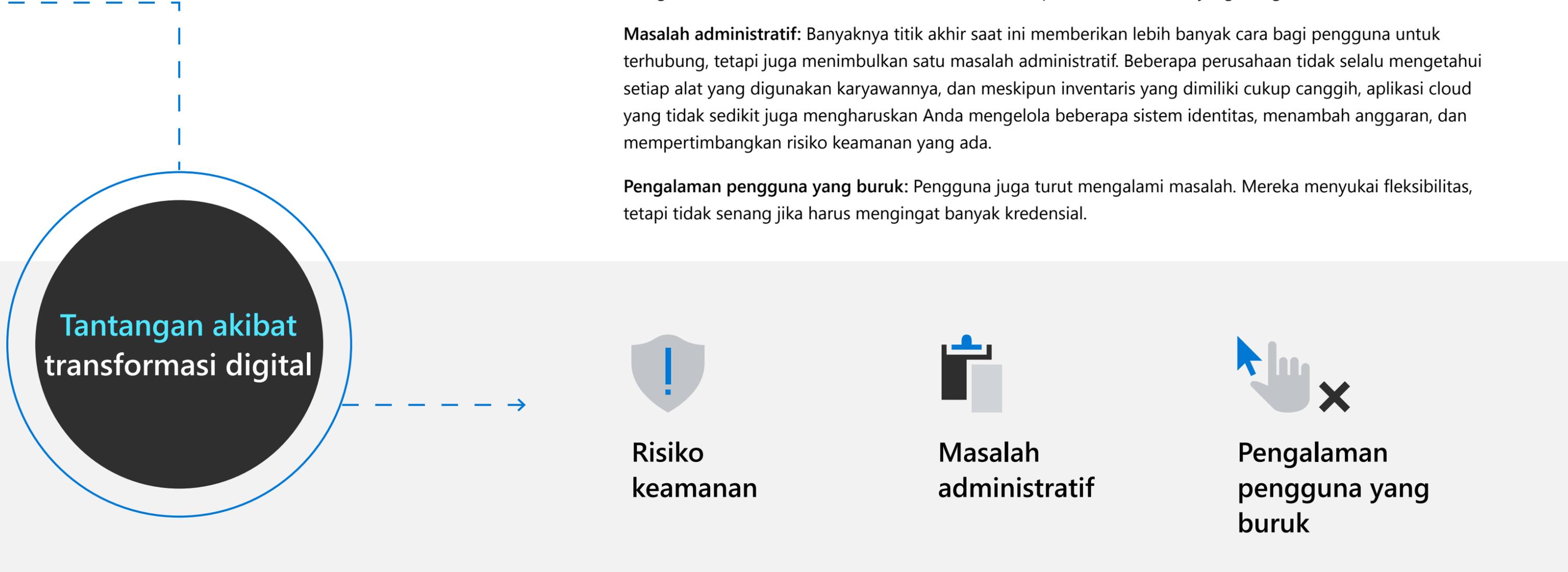
Apa yang dimaksud dengan manajemen identitas dan akses?

Tantangan baru

Risiko keamanan: Sebelum revolusi cloud, TI bertindak sebagai penyeleksi teknologi. Aplikasi dan platform yang Anda kelola dan lindungi dimasukkan ke dalam perimeter jaringan, dan semua orang yang mengakses sumber daya perusahaan akan divalidasi terlebih dahulu oleh firewall. Masa-masa tersebut sudah berakhir. Tenaga kerja Anda kini memiliki kontrol yang lebih menyeluruh atas teknologi yang mereka gunakan, yang sebagian besarnya diakses melalui internet. Penyerang cyber berhasil menemukan celah untuk mengeksploitasi kerentanan ini. Meskipun pengguna mengetahui kata sandi suatu akun, Anda tak akan tahu apakah benar mereka yang mengakses akun tersebut.

Masalah administratif: Banyaknya titik akhir saat ini memberikan lebih banyak cara bagi pengguna untuk terhubung, tetapi juga menimbulkan satu masalah administratif. Beberapa perusahaan tidak selalu mengetahui setiap alat yang digunakan karyawannya, dan meskipun inventaris yang dimiliki cukup canggih, aplikasi cloud yang tidak sedikit juga mengharuskan Anda mengelola beberapa sistem identitas, menambah anggaran, dan mempertimbangkan risiko keamanan yang ada.

Pengalaman pengguna yang buruk: Pengguna juga turut mengalami masalah. Mereka menyukai fleksibilitas, tetapi tidak senang jika harus mengingat banyak kredensial.



Tantangan akibat transformasi digital



Risiko keamanan



Masalah administratif



Pengalaman pengguna yang buruk

Apa yang dimaksud dengan manajemen identitas dan akses?

Manajemen identitas dan akses sebagai sarana kontrol terpusat

Penyebab umum masalah ini adalah sistem verifikasi identitas yang tidak efisien. Identitas telah menggantikan perimeter jaringan sebagai sarana kontrol yang baru. Anda memerlukan solusi yang menghubungkan berbagai alat, arsitektur, perangkat, dan layanan di seluruh perusahaan untuk meningkatkan perlindungan bagi organisasi serta mengelola akses untuk karyawan dan mitra eksternal. Sistem manajemen identitas dan akses (IAM) memadukan akses dalam satu sistem sehingga Anda dapat mengontrol semuanya secara lebih menyeluruh. Solusi ini memungkinkan kolaborasi tanpa masalah di seluruh organisasi sekaligus meningkatkan keamanan sumber daya perusahaan Anda. Solusi IAM yang tepat memungkinkan Anda menghubungkan pengguna ke semua aplikasi kerjanya, baik ketika bekerja di cloud maupun secara lokal, melalui serangkaian kredensial. Solusi IAM dirancang untuk memungkinkan pengguna mengakses sumber daya yang diperlukan saja, dan memblokir pengguna yang tidak berwenang agar tidak mengakses data secara tidak sah. Hak dan izin akses pengguna dikelola dari portal yang terpusat, meminimalkan proses manual yang harus dilakukan untuk menyediakan dan menonaktifkan akun pengguna. Solusi IAM juga menyediakan alat untuk mengelola kebijakan keamanan bagi identitas dan aplikasi. Solusi IAM terbaik dapat melindungi identitas secara lebih baik, meningkatkan pengalaman pengguna, dan meningkatkan efisiensi administratif.

Solusi IAM mengatasi tantangan ini



Melindungi identitas secara lebih baik



Meningkatkan pengalaman pengguna



Meningkatkan efisiensi administratif

Bagian 2

Gambaran Umum
Azure AD

Gambaran Umum Azure AD

Solusi yang komprehensif

Microsoft Azure Active Directory (Azure AD) adalah solusi IAM komprehensif berbasis cloud, dan merupakan solusi terbaik untuk mengelola direktori, akses aplikasi, dan perlindungan identitas tingkat lanjut. Azure AD memungkinkan organisasi untuk mengelola dan melindungi identitas karyawan, mitra, dan pelanggan untuk mengakses aplikasi dan layanan yang diperlukan. Azure AD membantu jutaan organisasi mengelola dan melindungi lebih dari satu miliar identitas.



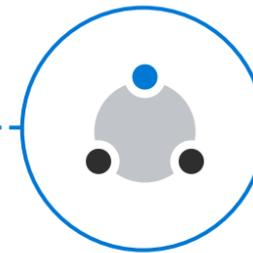
Mutakhirkan akses

Kelola dan lindungi akses ke data dan sumber daya organisasi Anda di cloud dan lokal. Hubungkan semua pengguna, aplikasi, dan perangkat ke cloud untuk mendapatkan akses yang aman dan tanpa masalah, serta visibilitas dan kontrol yang lebih menyeluruh. Otomatiskan alur kerja dan sediakan opsi layanan mandiri untuk menghemat biaya dan meningkatkan produktivitas pengguna Anda.



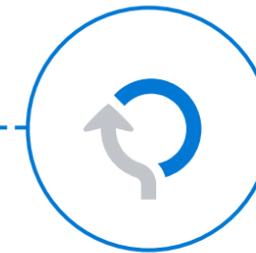
Lindungi dan kontrol

Dengan banyaknya serangan terhadap kredensial pengguna setiap harinya, salah satu cara untuk mencegahnya adalah dengan terus memantau perilaku normal dan abnormal pada rangkaian sinyal terluas, menerapkan kecerdasan buatan, dan mengotomatiskan respons. Selaraskan produktivitas dan keamanan dengan akses tepat waktu ke sumber daya yang tepat serta peninjauan akses berkala dan penerapan kebijakan.



Terhubung dan berkolaborasi

Perluas bisnis Anda dengan layanan cloud andal yang dapat disesuaikan untuk jutaan pengguna dengan keamanan dan fleksibilitas terbaik di industri. Jangkau pengguna eksternal dan dorong mereka agar selalu produktif dengan pengalaman mandiri yang ramah pengguna dan kontrol keamanan bawaan.



Kembangkan dan integrasikan

Rancang aplikasi yang memudahkan pengguna untuk masuk dengan akun Microsoft pribadi, kerja, atau sekolah mereka, atau dengan akun sosial. Mulai gunakan Microsoft Graph, yang merupakan portal untuk mengakses data dan kecerdasan di Microsoft 365, lalu rancang aplikasi yang kaya. Sediakan akses menyeluruh serta otomatiskan penyediaan pengguna, dan jangkau berbagai organisasi terbesar di dunia.

Bagian 3

Azure AD untuk
aplikasi Anda

Azure AD untuk aplikasi Anda

Platform universal

Azure AD memungkinkan Anda mengelola identitas umum bagi setiap pengguna pada infrastruktur hibrid untuk mengakses semua aplikasi yang diperlukan, termasuk aplikasi lini bisnis lokal dan cloud. Kelola semua identitas Anda dari platform universal untuk meningkatkan efisiensi administratif dan mendapatkan kontrol yang lebih luas. Terapkan kebijakan keamanan yang menyeluruh ke setiap aplikasi yang digunakan di organisasi Anda.



Azure AD untuk aplikasi Anda

Hemat waktu dan anggaran

Azure AD telah terintegrasi dengan ribuan aplikasi, termasuk yang cukup populer seperti Workday, ServiceNow, SuccessFactors, Adobe, dan Concur sehingga Anda dapat menyediakannya dengan lebih mudah kepada pengguna. Terapkan kebijakan yang konsisten dan pantau hak akses dengan satu konsol. Anda dapat mengotomatiskan alur kerja untuk penyediaan pengguna dan manajemen siklus hidup, serta menghemat waktu dan sumber daya dengan manajemen akun layanan mandiri. Anda juga dapat mengumpulkan informasi pengguna dari alat HR sebagai sumber yang valid sehingga skrip kustom atau proses manual untuk mengelola atribut pengguna tidak lagi diperlukan.

Aplikasi yang dikonfigurasi melalui Azure AD mendukung akses menyeluruh (SSO) untuk akses yang tanpa masalah; pengguna tidak perlu mengingat kredensial untuk setiap akun aplikasi atau menggunakan lagi kata sandi yang tidak aman dan berisiko mengakibatkan pelanggaran data. Akun yang telah dikonfigurasi untuk penyediaan otomatis memberi pengguna akses ke sumber daya baru dengan cepat. Untuk penyediaan baru, Azure AD memastikan karyawan baru dapat mengakses semua sumber daya yang relevan sejak hari pertama bekerja.



Hemat waktu dan anggaran



Integrasi SaaS bawaan



Akses menyeluruh



Akses pengguna sejak awal

Azure AD untuk aplikasi Anda

Berikan akses yang lebih aman ke semua aplikasi Anda

Azure AD memberikan perlindungan identitas yang komprehensif untuk semua aplikasi, baik aplikasi SaaS maupun aplikasi lini bisnis lokal. Azure AD memastikan bahwa identitas pengguna yang meminta akses ke Microsoft Word maupun Box akan dikonfirmasi sebelum diizinkan. Anda juga dapat menerapkan kebijakan tata kelola akses agar pengguna hanya mengakses informasi yang diperlukan ketika mereka memerlukannya. Anda dapat mewajibkan pengguna untuk meminta izin akses, serta mengatur batas waktu untuk akses aplikasi mereka dan melakukan peninjauan kepatuhan rutin terhadap akses tersebut.

Azure AD juga memanfaatkan kecanggihan Microsoft Intelligent Security Graph dan pembelajaran mesin untuk menganalisis triliunan sinyal di seluruh produk dan layanan kami untuk menemukan perilaku tidak normal dan menetapkan risiko relatif pada setiap sesi. Azure AD memantau perangkat, lokasi, dan informasi kontekstual lainnya untuk mengevaluasi risiko akses masuk. Anda dapat menerapkan kebijakan Akses Bersyarat Azure AD yang menerapkan tindakan keamanan secara otomatis, seperti memblokir permintaan akses atau mengharuskan pengaturan ulang kata sandi apabila akses masuk dianggap berisiko atau memenuhi ketentuan kebijakan tertentu.



**Tindakan
keamanan aplikasi**



**Perlindungan
identitas**



**Tata kelola
akses**



**Kebijakan
Akses Bersyarat**

Bagian 4

Cara mengelola dan melindungi aplikasi dengan Azure AD

Azure AD membantu Anda mengontrol semuanya dan menghemat biaya dengan automasi, layanan mandiri, dan pemberlakuan kebijakan.

Cara mengelola dan melindungi aplikasi dengan Azure AD



Integrasi aplikasi Azure AD

Galeri aplikasi Azure AD memudahkan Anda mengonfigurasi dan menghubungkan aplikasi ke penyewa dari ribuan opsi yang telah terintegrasi. Semua aplikasi ini mendukung pengalaman SSO, dan Anda dapat mengonfigurasinya dengan mudah untuk Akses Bersyarat Azure AD pada skala kebijakan tingkat perusahaan maupun per aplikasi. Setelah aplikasi ditambahkan dan dikonfigurasi sesuai kebutuhan, pengguna dengan akses yang sah dapat menemukannya di portal Aplikasi Saya di Azure AD, portal terpusat untuk menemukan dan meluncurkan aplikasi pengguna akhir.

Jika sudah membuat aplikasi atau perlu mengintegrasikannya untuk organisasi, Anda juga dapat memintanya disertakan dalam galeri aplikasi Azure AD.

[Jelajahi ribuan aplikasi yang telah terintegrasi >](#)



Akses hibrid aman

Gunakan Proksi Aplikasi Azure AD untuk menyediakan akses jarak jauh yang aman ke aplikasi web lokal berdasarkan klaim tanpa harus menggunakan VPN. Proksi Aplikasi memerlukan penginstalan konektor ringan, serta memberikan pengalaman TI dan pengguna akhir yang sama seperti aplikasi SaaS yang terhubung melalui galeri aplikasi Azure AD.

Selain itu, jika ingin memanfaatkan investasi infrastruktur yang sudah ada, misalnya dengan mitra seperti F5 ZScaler, SAP, Oracle, atau Ping Identity untuk menghubungkan tipe aplikasi lain seperti yang menggunakan protokol autentikasi berbasis header atau Kerberos, Anda juga dapat melakukannya dan tetap mendapatkan manfaat keamanan yang terpusat dari Azure AD.

[Baca cara menambahkan aplikasi lokal melalui Proksi Aplikasi >](#)

[Sambungkan jaringan dan cloud aplikasi mitra lainnya >](#)

Cara mengelola dan melindungi aplikasi dengan Azure AD



Penyediaan otomatis

Azure AD memungkinkan Anda mengotomatiskan pembuatan, pemeliharaan, dan penghapusan identitas pengguna di beberapa aplikasi SaaS populer. Anda dapat membuat akun baru secara otomatis dalam sistem yang tepat bagi anggota baru dalam tim atau organisasi Anda. Ketika ada yang meninggalkan tim atau organisasi, Anda dapat menetapkan kebijakan yang menonaktifkan akun mereka secara otomatis dari sistem yang sesuai. Dengan mengotomatiskan tugas ini, Anda dapat memastikan bahwa identitas dalam aplikasi dan sistem akan selalu diperbarui sesuai perubahan dalam direktori atau sistem SDM Anda, yang akan meminimalkan kesalahan dan menghemat waktu.

[Pelajari selengkapnya tentang menyiapkan penyediaan dan pembatalan otomatis untuk aplikasi SaaS >](#)



Manajemen grup

Azure AD membantu Anda memberikan akses ke sumber daya organisasi dengan menyediakan hak akses ke satu pengguna atau ke seluruh grup Azure AD. Dengan grup, pemilik sumber daya dapat mengatur izin akses bagi semua anggota grup tanpa harus menyediakan hak secara satu per satu. Metode ini lebih aman karena meminimalkan kemungkinan pemberian akses tidak sah secara tidak sengaja kepada seseorang sehingga Anda dapat menghemat waktu. Anda juga dapat menyesuaikan manajemen grup secara dinamis dengan mengotomatiskan pendaftaran melalui kebijakan berbasis atribut identitas.

[Pelajari cara membuat grup di portal Azure >](#)

Cara mengelola dan melindungi aplikasi dengan Azure AD



Layanan mandiri untuk pengguna

Beberapa tugas tidak perlu dilakukan oleh profesional TI, dan Azure AD memungkinkan Anda mendelegasikannya kepada orang lain di organisasi. Anda dapat mendukung pengguna untuk membuat dan mengelola grup keamanannya sendiri di Azure AD. Pemilik grup dapat menyetujui atau menolak permintaan keanggotaan, atau mendelegasikan kontrol atas keanggotaan grup.

[Menyiapkan grup yang dikelola secara mandiri >](#)

Layanan mandiri juga mencakup pengguna. Pengguna dapat mendaftar untuk mendapatkan akun melalui portal layanan mandiri jika memiliki email yang terverifikasi, serta mengatur ulang kata sandi melalui portal tersebut. Cara ini dapat membantu staf dukungan Anda menghemat waktu dan anggaran.

[Mengonfigurasi pengaturan ulang kata sandi mandiri >](#)



Mutakhirkan autentikasi

Jika saat ini Anda menggunakan autentikasi lokal seperti Layanan Federasi Direktori Aktif (AD FS), pertimbangkan untuk memindahkan aplikasi ke Azure AD. Anda akan mendapatkan manfaat pengguna yang sama, seperti SSO, serta manfaat skalabilitas dan keamanan yang tersedia dari cloud seperti menerapkan kontrol akses per aplikasi yang menyeluruh menggunakan Akses Bersyarat Azure AD atau mengizinkan mitra mengakses sumber daya dengan kolaborasi B2B Azure AD. Aplikasi yang menggunakan standar SAML 2.0, WS-Federation, OAuth, atau OpenID Connect untuk akses gabungan juga dapat dimigrasikan.

[Membuat kebijakan Akses Bersyarat Azure AD untuk melindungi akses ke aplikasi Anda >](#)

[Menggunakan B2B Azure AD untuk berkolaborasi dengan mudah bersama mitra eksternal >](#)

Hubungkan aplikasi apa pun dengan aman,
di cloud maupun server, ke Azure AD.

1 juta aplikasi aktif
khusus telah terhubung.



Mulai sekarang juga.

[Mulai uji coba gratis Azure AD selama satu bulan](#) dan buktikan betapa mudahnya mengelola akses pengguna ke semua aplikasi dan melindungi perusahaan Anda.

