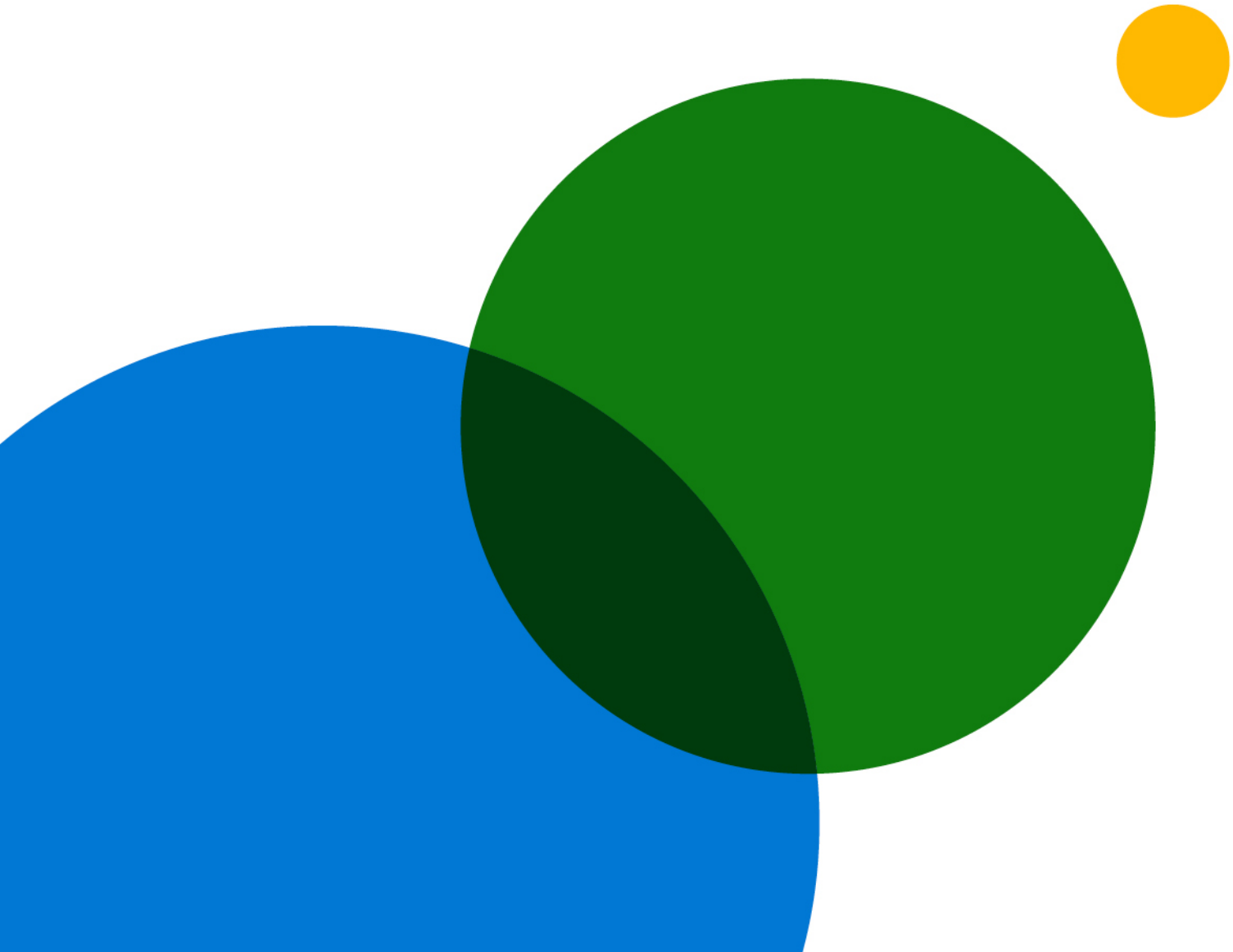
Microsoft Security

hypothesis

Laporan Penerapan Zero Trust



Daftar Isi

Pengantar

Vasu Jakkal / Wakil Presiden Korporat, Keamanan, Kepatuhan, dan Identitas

Dalam tahun terakhir ini telah menjadi luar biasa dalam evolusi keamanan siber dan meningkatnya Zero Trust sebagai strategi panduan untuk industri dan organisasi kami di seluruh dunia.

Pada awal pandemi, tempat kerja menjadi hampir sepenuhnya dilakukan dari jarak jauh dalam semalam. Pergeseran ini memaksa banyak organisasi untuk dengan cepat beradaptasi guna mendukung karyawan untuk menyelesaikan pekerjaan mereka dengan cara apa pun yang mereka bisa — menggunakan perangkat pribadi, berkolaborasi melalui layanan cloud, dan berbagi data di luar perimeter jaringan perusahaan. Saat organisasi beradaptasi dengan transformasi ini, mereka juga menghadapi penjahat siber yang semakin canggih yang terus-menerus mengembangkan penargetan, taktik, dan sumber daya mereka.

Saat ini, pekerjaan hibrid adalah realitas baru. Dengan latar belakang ini, dan dalam menghadapi perubahan yang cepat, organisasi yang kami survei memberi tahu kami bahwa mereka mengandalkan Zero Trust untuk meningkatkan ketangkasan keamanan dan kepatuhan, meningkatkan kecepatan deteksi ancaman dan remediasi, serta meningkatkan kesederhanaan dan ketersediaan analitik keamanan.

Berdasarkan prinsip-prinsip verifikasi secara eksplisit, menggunakan akses minimal dengan hak istimewa, dan mengasumsikan pelanggaran, arsitektur Zero Trust yang komprehensif menciptakan perlindungan di dalam dan di seluruh identitas, titik akhir, aplikasi, infrastruktur, jaringan, dan data, yang bermitra dengan peningkatan visibilitas, otomatisasi, dan orkestrasi. Kami tidak hanya merekomendasikan pendekatan ini kepada pelanggan dan mitra, kami menerimanya dalam pendekatan untuk keamanan global dan pengembangan perangkat lunak di sini di Microsoft.

Laporan ini menerangi jalur Zero Trust yang diadopsi di berbagai pasar dan industri. Kami berharap bahwa pembelajaran yang diperoleh dari penelitian ini dapat membantu mempercepat penerapan strategi Zero Trust Anda sendiri, menjelaskan kemajuan kolektif rekan-rekan Anda, dan memberikan wawasan tentang keadaan masa depan dari ruang yang berkembang pesat ini.

Metodologi

Microsoft menugaskan Hypothesis Group, sebuah lembaga wawasan, desain, dan strategi, untuk menjalankan laporan dan penelitian Penerapan Zero Trust. Penelitian ini mencakup dua tahap di AS untuk menyoroti tren dan momentum dalam penerapan Zero Trust, dengan tambahan pasar yang ditambahkan dalam fase kedua untuk mengungkap tren global.

Penelitian awal dilakukan pada bulan Agustus 2020, ketika survei online 15 menit dilakukan di AS dengan 300 orang SDM (Security Decision Maker) yang terlibat dalam keputusan strategi Zero Trust di perusahaan enterprise dari berbagai industri. Selain survei online, lima wawancara mendalam dilakukan secara online pada bulan September 2020 di kalangan SDM dari berbagai industri di AS.

Pada bulan April 2021, penelitian global dilakukan di AS, Jerman, Jepang, dan Australia/Selandia Baru di seluruh grup yang serupa dengan pengambil keputusan keamanan. Lebih dari 900 peserta mengikuti survei online 15 menit dengan pertanyaan seputar adopsi strategi Zero Trust mereka, praktik terbaik, manfaat, tantangan, dan bagaimana mereka berniat untuk berinvestasi di masa depan.

Beberapa hal yang perlu diketahui tentang penerapan Zero Trust

01 / Banyak organisasi yang siap untuk memanfaatkan strategi Zero Trust, yang dipercepat dengan beralih ke tempat kerja hibrid dan Covid-19

Para pengambil keputusan keamanan (SDM) ini mengatakan bahwa mengembangkan strategi Zero Trust adalah prioritas keamanan nomor 1 mereka, dengan 96% menyatakan bahwa hal itu penting bagi keberhasilan organisasi mereka. Motivator utama untuk mengadopsi strategi Zero Trust adalah untuk meningkatkan postur keamanan mereka secara keseluruhan dan pengalaman pengguna akhir. Peralihan ke tempat kerja hibrid, yang dipercepat oleh COVID-19, juga mendorong adopsi yang lebih luas dari strategi Zero Trust: 81% organisasi perusahaan telah mulai bergerak menuju tempat kerja hibrid, dengan 31% sepenuhnya sudah di sana. Namun, 94% memiliki kekhawatiran tentang transisi, terutama, penyalahgunaan oleh karyawan, peningkatan beban kerja TI, dan serangan siber. Mengingat hal ini, pertimbangan utama untuk strategi termasuk peningkatan pelatihan bagi karyawan dan autentikasi multifaktor (MFA) untuk memastikan transisi dan pengalaman pengguna yang lancar.

02 / Strategi Zero Trust memungkinkan fleksibilitas di mana organisasi dapat mulai menerapkannya sehingga pendekatan tersebut dapat disesuaikan dengan kebutuhan mereka

Kurang dari 15% organisasi mulai menerapkan strategi Zero Trust di area risiko keamanan yang sama. Ini sebagian besar karena implementasi dilakukan sebagai proses ujung-ke-ujung di seluruh pilar dan kemampuan arsitektur keamanan daripada sebagai serangkaian teknologi yang berbeda dan terpisah. Demikian pula, urutan di mana komponen individu Zero Trust dalam bidang risiko keamanan yang diimplementasikan sangat bervariasi, dengan profesional keamanan yang secara substansial berbeda dalam komponen yang pertama kali mulai mereka terapkan.

03 / Meskipun strategi Zero Trust secara luas diadopsi dan meningkatkan kemampuan organisasi untuk mengelola ancaman, masih ada pekerjaan yang harus dilakukan

76% organisasi setidaknya mulai menerapkan strategi Zero Trust, dengan 35% mengklaim sepenuhnya telah menerapkannya. Namun, mereka yang mengklaim sepenuhnya telah mengimplementasikan mengakui mereka belum selesai menerapkan strategi Zero Trust di semua area dan komponen risiko keamanan. Strategi Zero Trust sangat menarik karena memberikan peningkatan kelincahan, kecepatan mendeteksi ancaman, dan peningkatan kemampuan untuk mengelola keamanan IoT (Internet of Things) dan OT (Operational Technology). Adopsi meningkat di AS (70% pada Agustus 2020 hingga 79% pada April 2021); AS juga lebih jauh di depan dalam penerapan Zero Trust relatif dibandingkan dengan negara lain yang mulai mengadopsinya kemudian, dan organisasi di AS mengklaim tidak terlalu dibatasi oleh anggaran. Namun, meskipun 57% organisasi mengklaim berada di depan dari yang lainnya dalam hal penerapan, sekitar setengahnya masih memiliki lebih banyak pekerjaan yang harus dilakukan karena mereka belum sepenuhnya menerapkan Zero Trust di semua area dan komponen risiko keamanan.

04 / Dengan memandang ke depan, strategi Zero Trust akan tetap menjadi prioritas utama dan memerlukan pengambilan keputusan yang cermat ketika menyangkut karyawan dan vendor

Strategi Zero Trust diharapkan untuk tetap menjadi prioritas keamanan nomor 1 dalam dua tahun dari sekarang dan organisasi mengantisipasi peningkatan investasinya. Mengatasi tantangan dengan karyawan mereka (termasuk penempatan staf dalam tim keamanan dan dukungan dari kepemimpinan) akan menjadi kunci untuk menggandakan investasi Zero Trust. Dalam hal strategi vendor, para pembuat keputusan keamanan memiliki sedikit preferensi untuk bekerja dengan penyedia holistik atau terkonsolidasi mengingat bahwa pemilihan vendor sering kali bergantung pada ketersediaan keahlian internal. Manfaat dari pendekatan best-in-suite mencakup peningkatan keahlian, sumber daya, dan kesederhanaan, meskipun dapat memerlukan waktu yang lebih lama untuk diterapkan, lebih sulit untuk diintegrasikan ke dalam arsitektur keamanan yang ada, dan meningkatkan potensi kerentanan.

Sasaran kami

Global

Pengambil Keputusan Keamanan

mereka yang bekerja di perusahaan berskala enterprise*

90%

Familiar dengan Zero Trust

Menyatakan diri, lulus uji pengetahuan

76%

dalam Implementasi Zero Trust

24%

Merencanakan/Mempertimbangkan Zero Trust

*1.000 lebih karyawan di AS; 500 lebih karyawan di Jerman, Jepang, Australia/Selandia Baru

Pembelajaran keseluruhan penelitian

Banyak organisasi yang siap untuk memanfaatkan strategi Zero Trust

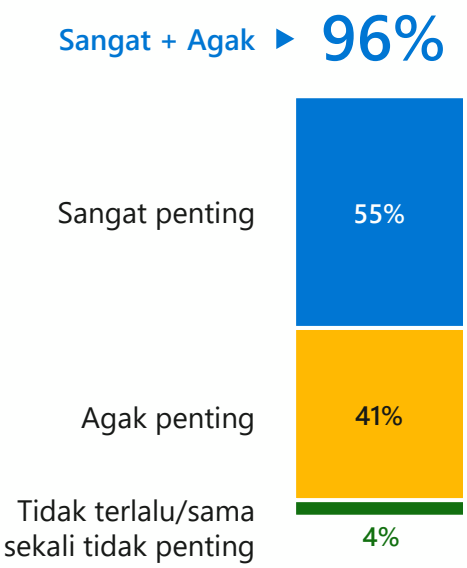
Strategi Zero Trust saat ini menjadi prioritas keamanan nomor 1 di seluruh pasar dan industri, dengan sejumlah organisasi mengadopsi strategi Zero Trust dalam beberapa tahun terakhir. Meskipun Zero Trust merupakan yang terbaik untuk semua (53%), ini adalah prioritas utama bagi organisasi di Amerika Serikat (56%) dan Jerman (53%).

Hampir semua profesional keamanan (96%) percaya bahwa strategi Zero Trust sangat penting untuk keberhasilan organisasi mereka. (Lihat Paparan 1) Selain untuk memperkuat postur keamanan mereka secara keseluruhan dan meningkatkan pengalaman pengguna akhir, profesional keamanan mencari strategi Zero Trust untuk menyederhanakan prosedur keamanan bagi karyawan. (Lihat Paparan 2)

Sebagai salah satu pembuat keputusan keamanan AS di Hospitality menjelaskan, "*Tujuannya adalah untuk meningkatkan postur keamanan kami secara keseluruhan, tetapi ini semua tentang mengurangi gesekan pada pengalaman pengguna akhir dan membuat hidup lebih mudah bagi mereka.*"

Selain itu, 31% dari profesional keamanan melihat strategi Zero Trust sebagai alat penting dalam pergeseran terdekat menuju tempat kerja hibrid pasca-pandemi; pendorong ini terutama menonjol di Australia/Selandia Baru (44%).

Paparan 1. Zero Trust sangat penting



Paparan 2. Motivator Zero Trust

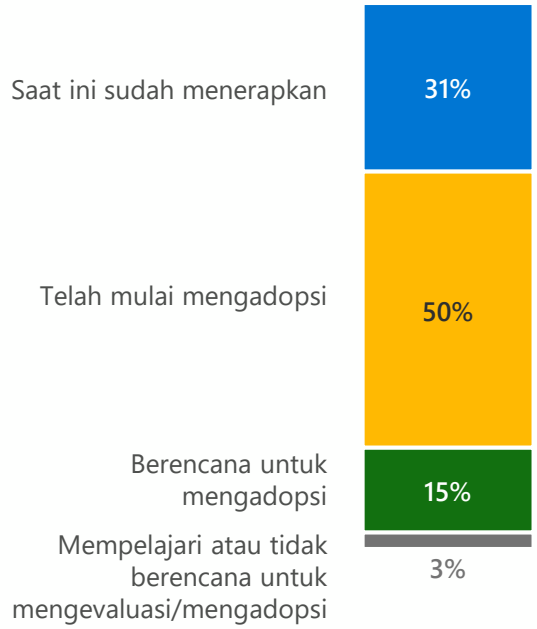
Motivator Teratas	
Menyempurnakan keseluruhan postur keamanan	47%
Meningkatkan pengalaman dan produktivitas pengguna akhir	44%
Mengubah cara tim keamanan bekerja bersama	38%
Merampingkan tumpukan keamanan	35%
Mengurangi biaya keamanan	35%

Pergeseran ke tempat kerja hibrid mendorong penerapan strategi Zero Trust yang lebih luas

81% organisasi perusahaan telah mulai bergerak menuju tempat kerja hibrid, dengan 31% sudah sepenuhnya mengadopsi. Meskipun demikian, tingkat adopsi penuh tidak konsisten di seluruh pasar: sementara Australia dan Selandia Baru memimpin di 37%, Jerman jauh di belakang, dengan hanya 20% organisasi yang telah pindah ke model hibrid. (Lihat Paparan 3)

Bahkan ketika pasar global bergerak menuju tempat kerja hibrid pada tingkat yang berbeda, sebagian besar (91%) organisasi yang belum menyelesaikan transisi mengantisipasi hal tersebut dalam lima tahun ke depan. Yang terpenting, 94% mengkhawatirkan transisi, dengan penyalahgunaan karyawan, peningkatan beban kerja TI, dan peningkatan risiko serangan siber sebagai daftar masalah teratas. (Lihat Paparan 4)

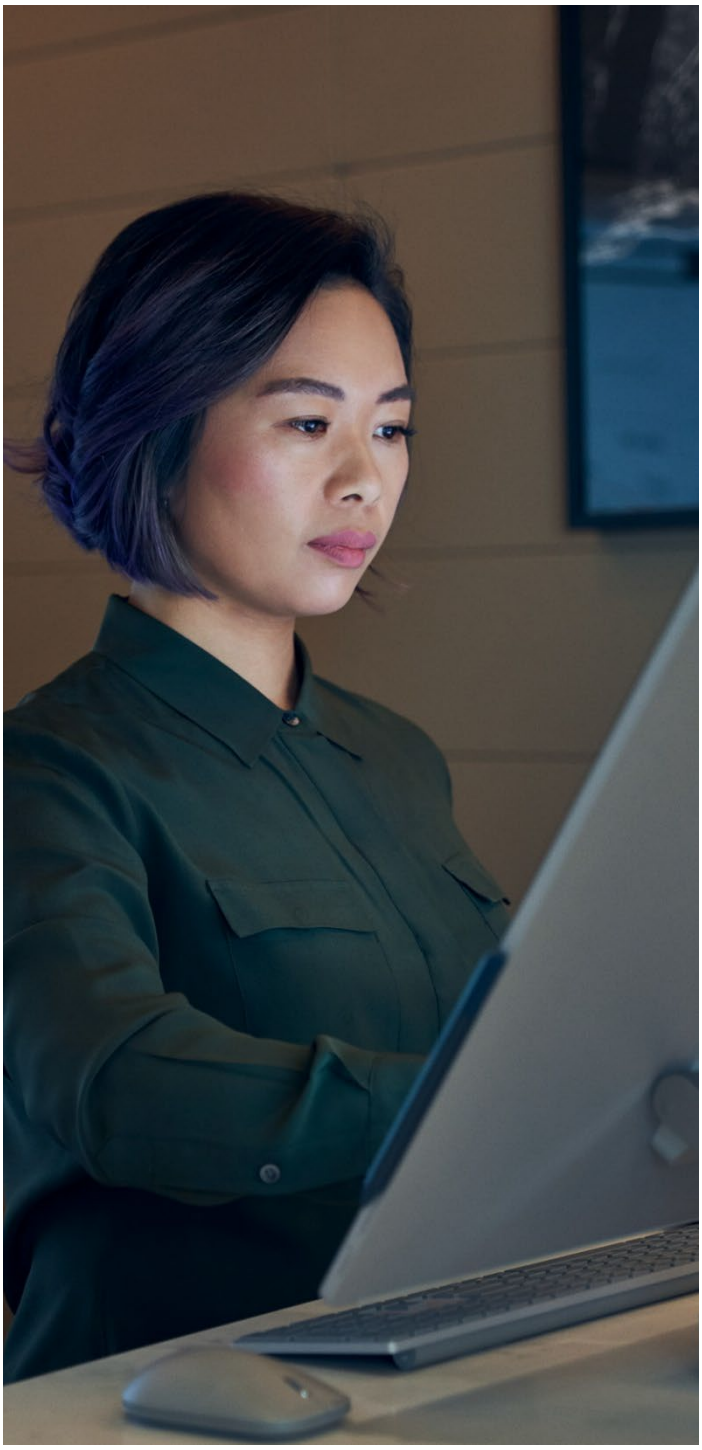
Paparan 3. Tujuan tempat kerja hibrid



Paparan 4. Kekhawatiran mengenai tempat kerja hibrid

Karyawan mengunduh aplikasi yang tidak aman	37%
Peningkatan beban kerja TI	37%
Serangan Ransomware	36%
Serangan phishing	35%
Penggunaan perangkat pribadi yang tidak semestinya	34%
Akses ke data yang tidak sah	31%
Ketidakmampuan untuk mengelola semua perangkat	30%
Penggunaan akun email pribadi	30%
Ketidakpatuhan terhadap peraturan data	24%

Covid-19 telah membawa pertimbangan baru yang mempercepat perpindahan ke strategi Zero Trust



Dalam upaya untuk meminimalkan potensi masalah, pemangku kepentingan menekankan pentingnya peningkatan pelatihan bagi karyawan (54%) (terutama di Jepang (61%) dan Jerman (58%)) dan autentikasi multi-faktor (MFA) (50%) (terutama di Amerika Serikat (52%) dan Jerman (56%)) untuk memastikan pengalaman pengguna dan transisi yang lancar.

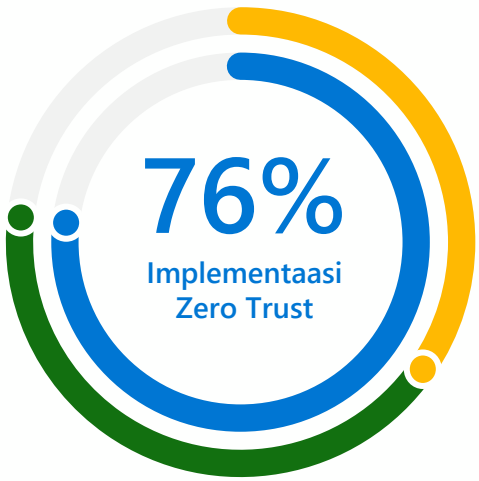
Karena pekerjaan jarak jauh dan hibrid yang aman dapat dibantu dengan strategi Zero Trust, COVID-19 telah mempercepat adopsi strategi Zero Trust untuk 72% organisasi, meskipun asimetri muncul di antara pasar. Sementara pandemi mengkatalisis adopsi untuk sekitar tujuh dalam sepuluh organisasi di AS (76%), Jepang (71%), dan Australia/ Selandia Baru (69%), tingkat implementasi telah lebih rendah di Jerman (62%), mungkin karena transisi yang lebih lambat ke tempat kerja hibrid.

Zero Trust diterapkan secara luas di seluruh dunia dan berkembang di AS

Zero Trust bukan sekadar kata kunci; ini adalah kenyataan. 76% organisasi setidaknya mulai menerapkan strategi ini dan 35% percaya bahwa mereka sepenuhnya telah mengimplementasikan. Namun, data ini melukiskan gambaran yang terlalu optimis karena banyak organisasi yang menganggap dirinya sepenuhnya telah mengimplementasikan, dengan pengakuan mereka sendiri, tidak selesai mengeksekusi di semua area risiko keamanan. Hari ini, AS berada di posisi terdepan dalam penerapan strategi Zero Trust yang relatif terhadap pasar lain dan terus tumbuh pesat: dibandingkan dengan Agustus 2020, penerapan strategi Zero Trust di AS meningkat dari 70% menjadi 79%, lompatan yang cukup besar hanya dalam waktu delapan bulan. (Lihat Paparan 5)

Meskipun strategi Zero Trust saat ini mendominasi ruang keamanan, keberadaannya relatif baru. 82% perusahaan menerapkan strategi Zero Trust dalam tiga tahun terakhir, dengan 21% melakukannya dalam 12 bulan terakhir. Dikatakan bahwa, 26% organisasi di AS memulai implementasi 3+ tahun yang lalu, dibandingkan 19% organisasi di Jepang, 6% organisasi di Australia/Selandia Baru, dan 3% organisasi di Jerman. Implementasi lebih awal di AS ini, — bersamaan dengan kendala anggaran yang lebih sedikit — mungkin membantu menjelaskan mengapa organisasi di AS menjadi yang terdepan dalam penerapan Zero Trust dibandingkan dengan organisasi di pasar lain. Dalam nada yang serupa, kelahiran relatif Zero Trust di Jerman membantu untuk menentukan tingkat adopsinya yang lebih rendah: 97% organisasi di Jerman baru memulai implementasi dalam tiga tahun terakhir.

Paparan 5. Penerapan Zero Trust



	AS (2020)	AS	DE	JP	AUS/NZ
Implementasi Zero Trust	70%	79%	75%	76%	71%
• Sepenuhnya mengimplementasikan	27%	44%	19%	32%	28%
• Dalam proses	43%	35%	56%	44%	43%

35% Sepenuhnya mengimplementasikan

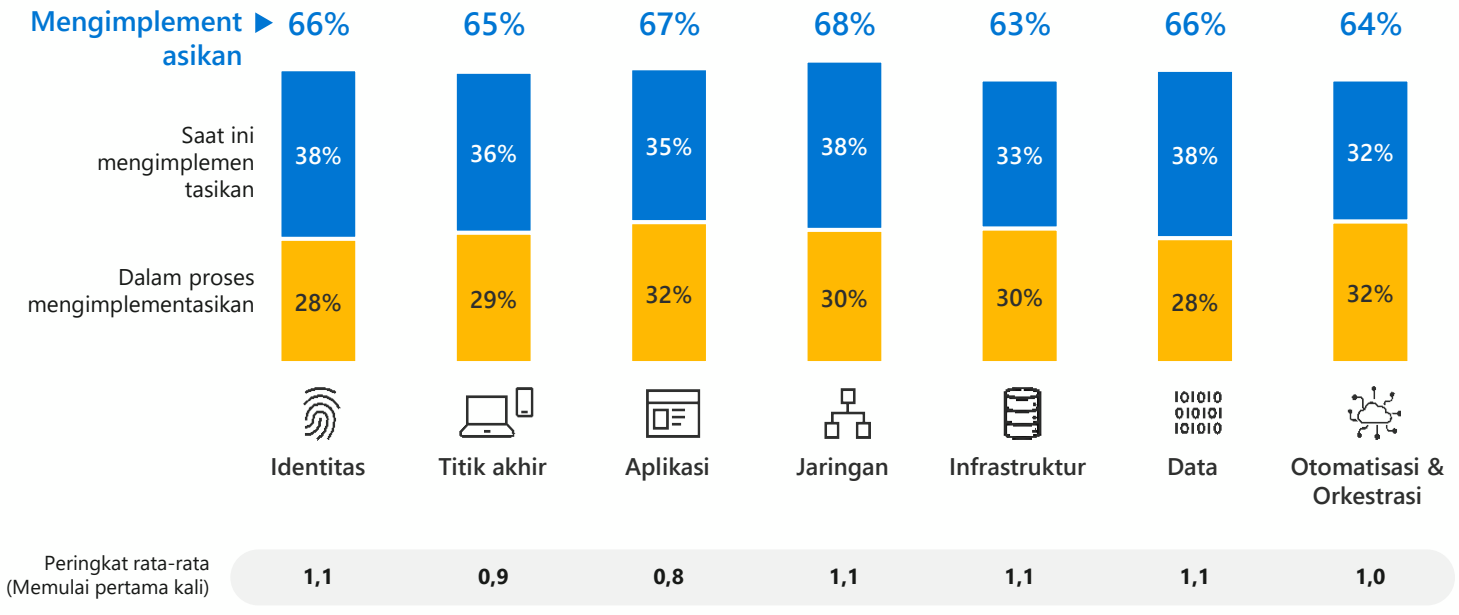
42% Implementasi dalam proses

Tidak ada pendekatan yang satu ukuran cocok untuk semua untuk implementasi Zero Trust, memberikan izin untuk memulai di mana saja

Tidak ada satu pun area risiko keamanan (Identitas, Titik Akhir, Aplikasi, Jaringan, Infrastruktur, Data, Otomatisasi & Orkestrasi) yang menonjol sebagai titik awal utama untuk strategi Zero Trust, kurang dari 15% memulainya dengan area risiko keamanan yang sama. Beberapa organisasi memulai di tempat yang berbeda kemungkinan didasarkan pada kebutuhan dan sumber daya internal yang tersedia. Akhirnya, mereka berusaha untuk mengadopsi strategi Zero Trust di semua area risiko keamanan untuk memastikan lebih banyak perlindungan terhadap ancaman, sehingga Zero Trust dianggap sebagai strategi end-to-end yang akan diselesaikan dari waktu ke waktu. (Lihat Paparan 6)

Di luar area risiko keamanan strategi Zero Trust, organisasi harus mengidentifikasi komponen individu dari setiap area risiko keamanan untuk diprioritaskan. Untuk Titik akhir, Aplikasi, Jaringan, Data, dan Otomatisasi/Orkestrasi, tidak ada titik awal yang jelas; profesional keamanan sangat bervariasi dalam komponen yang mereka nilai sebagai prioritas utama mereka. Namun, autentikasi yang kuat biasanya diimplementasikan terlebih dahulu untuk identitas, dan alat deteksi ancaman adalah prioritas yang jelas dalam infrastruktur. (Lihat Paparan 7)

Paparan 6. Implementasi Zero Trust saat ini – Area risiko keamanan



Paparan 7. Implementasi komponen Zero Trust (3 Teratas) – Peringkat No. 1 (mengimplementasikan pertama kali)

Identitas	
Autentikasi kuat (misalnya, autentikasi multifaktor, autentikasi tanpa kata sandi)	32%
Deteksi dan remediasi risiko otomatis	27%
Kebijakan akses adaptif untuk gerbang akses ke sumber daya	22%

Titik akhir	
Kebijakan/kontrol Pencegahan Kehilangan Data untuk semua perangkat yang tidak terkelola dan terkelola	27%
Evaluasi risiko perangkat real-time/ deteksi ancaman titik akhir	26%
Perangkat terdaftar dengan penyedia identitas	24%

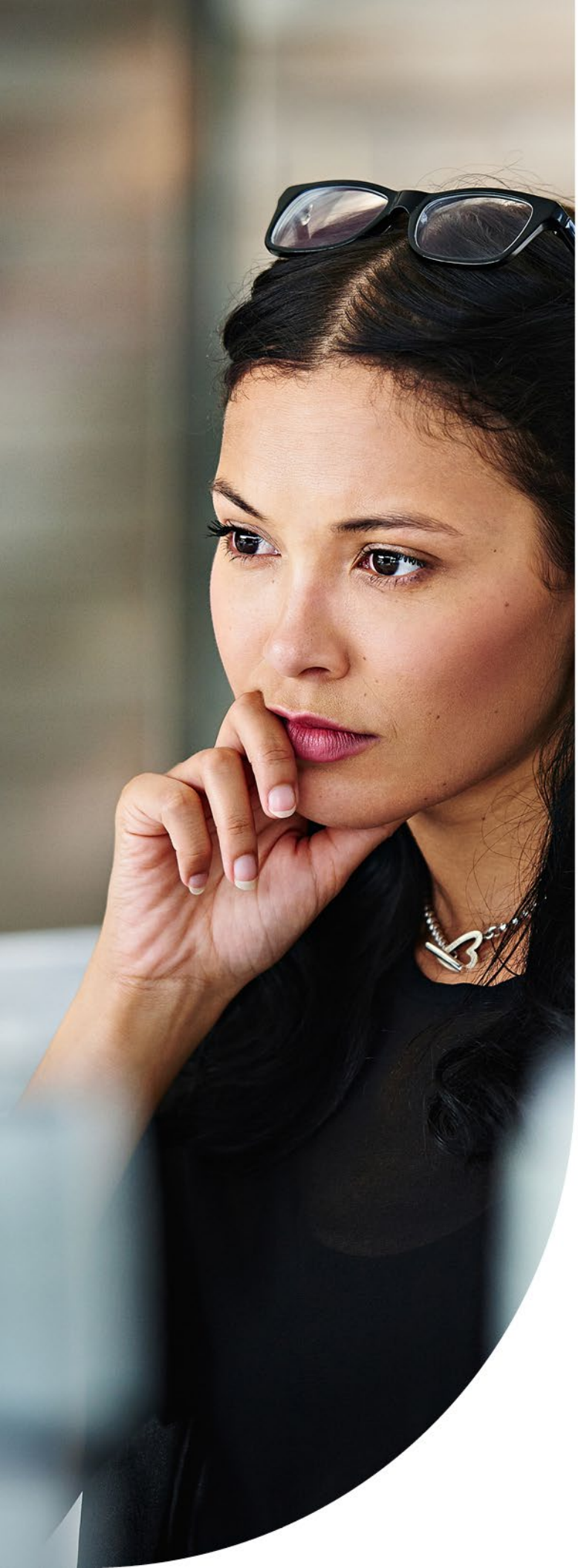
Aplikasi	
Penemuan dan penilaian risiko TI Bayangan (Shadow IT) yang berkelanjutan	23%
Kontrol akses granular ke aplikasi Anda (seperti visibilitas terbatas atau hanya baca)	22%
Kontrol akses berbasis kebijakan untuk aplikasi	20%

Jaringan	
Kontrol akses yang aman untuk melindungi jaringan	25%
Perlindungan terhadap ancaman dan pemfilteran dengan sinyal berbasis konteks	24%
Semua lalu lintas dienkripsi	20%

Infrastruktur	
Akses tim operasi keamanan ke alat deteksi ancaman	25%
Perlindungan beban kerja cloud di seluruh hibrid dan multi-cloud	19%
Kontrol akses dan visibilitas granular di semua beban kerja (mesin virtual, server, dll.)	17%

Data	
Keputusan akses diatur oleh mesin kebijakan keamanan	21%
Data diklasifikasikan dan diberi label	21%
File yang paling sensitif secara persisten dilindungi dengan enkripsi	20%

Otomatisasi & Orkestrasi	
Visibilitas ujung ke ujung ditetapkan dengan platform terpusat untuk penyelidikan dan respons	29%
Data ancaman dikumpulkan dan dianalisis di seluruh domain (identitas, titik akhir, aplikasi, jaringan, infrastruktur)	28%
Penyelidikan dan respons otomatis diaktifkan	22%



Kami tidak melihatnya hanya sebagai serangkaian teknologi, tetapi sebagai strategi dan pendekatan untuk memperlakukan setiap sumber daya pengguna, baik di dalam jaringan atau di luar jaringan kami, sebagai tidak tepercaya hingga dapat diverifikasi."

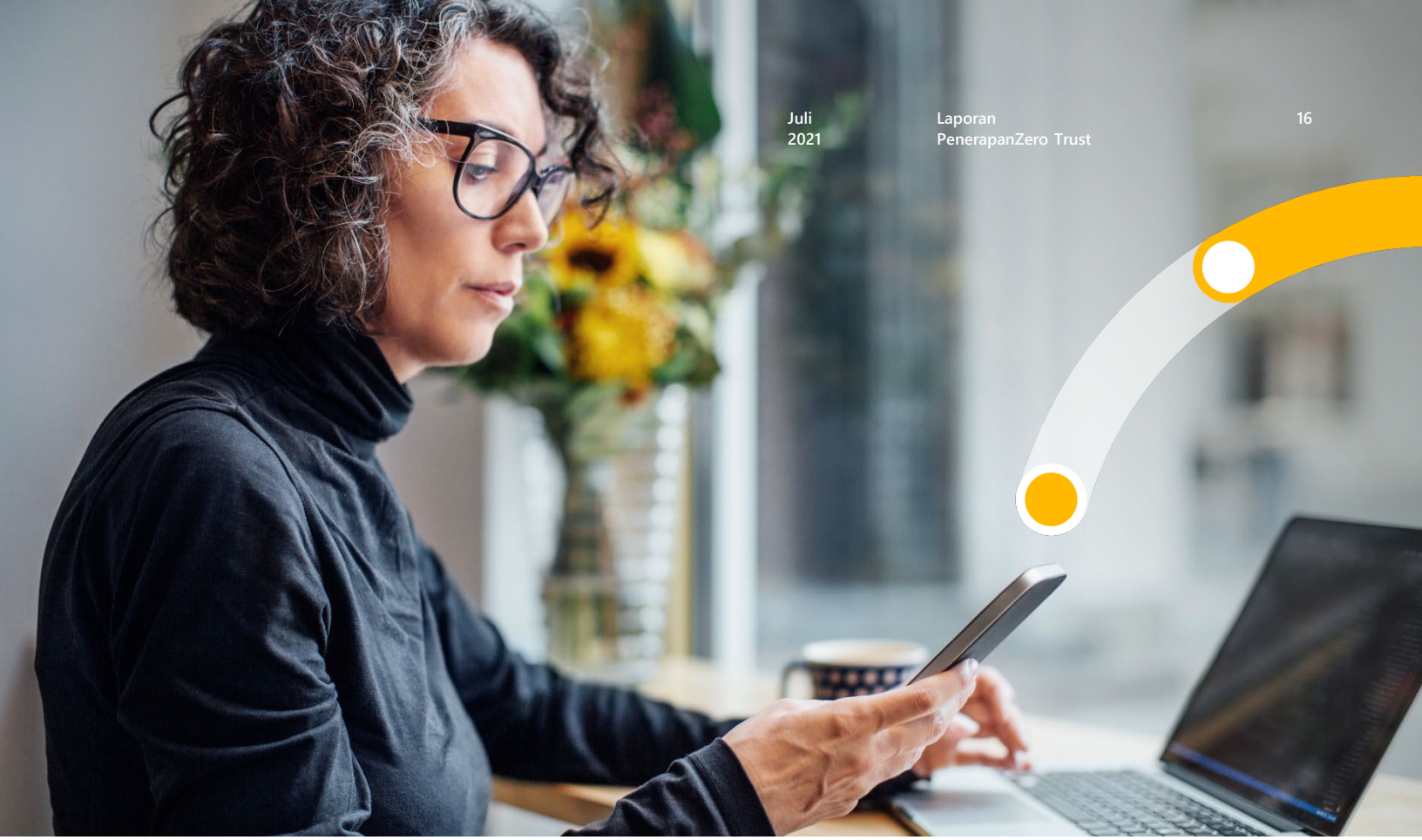
Pengambil Keputusan Keamanan di AS Keramahan

Setelah organisasi mulai menerapkan strategi Zero Trust, manfaat utama mencakup peningkatan ketangkasan, kecepatan, dan perlindungan; keuntungan sumber daya kurang umum

Setelah Strategi Zero Trust diimplementasikan, organisasi mendapatkan manfaat dari peningkatan ketangkasan (37%), kecepatan (35%), dan perlindungan data pelanggan (35%). (Lihat Paparan 8) Namun, manfaat langsung bagi karyawan termasuk tim keamanan yang dibebaskan (27%) dan kebutuhan untuk lebih sedikit sumber daya untuk mengelola infrastruktur (22%), kurang sering terwujud.

Yang terpenting, organisasi percaya bahwa strategi Zero Trust akan membantu mereka mengelola sebagian besar ancaman dan perubahan pada lingkungan, terutama sehubungan dengan keamanan IoT dan OT (47%).

Paparan 8. Keunggulan Zero Trust



Organisasi merasa yakin dalam mendapatkan manfaat maksimal dari strategi Zero Trust mereka

79% merasa yakin tentang kemampuan mereka untuk menangani ancaman keamanan secara menyeluruh, meskipun kepercayaan diri ini berkurang ketika ancaman melibatkan fabrikasi kebenaran: SDM merasa tidak yakin dalam berurusan dengan ancaman yang melibatkan identitas sintetis (20%) dan deepfake (10%).

Mengingat manfaat yang diperoleh, Zero Trust umumnya mengumpulkan asosiasi positif. Di empat pasar, SDM melihat pendekatan organisasi mereka sebagai praktis dan aspirasional secara bersamaan, menggambarkannya sebagai percaya diri (37%) dan efisien (31%) serta memotivasi (25%), menginspirasi (25%), dan menarik (25%). Di Jepang secara khusus, profesional keamanan menjelaskan Zero Trust karena menuntut (27%) dan transformasional (25%), menunjukkan bahwa — meskipun tidak mudah untuk diterapkan, jangkauan manfaatnya jauh sekali bila diterapkan.

Banyak yang percaya bahwa mereka berada di depan dengan implementasi Zero Trust, tetapi mereka masih memiliki banyak hal untuk dilakukan

Meskipun hanya 35% organisasi yang sepenuhnya menerapkan strategi Zero Trust, 52% mengatakan bahwa mereka berada di depan dengan berencana untuk melakukannya dan 57% percaya bahwa mereka berada di depan organisasi lain. Organisasi menganggap diri mereka terutama lebih unggul dari yang lainnya di Jepang (66%) dan Australia/Selandia Baru (63%). Meskipun kepercayaan diri berlimpah di seluruh pasar, tampaknya ada jurang antara persepsi dan realitas: di antara mereka ada yang merasa lebih maju dari organisasi lain, hanya 42% mengklaim telah sepenuhnya menerapkan strategi Zero Trust. (Lihat Paparan 9)

Meskipun banyak organisasi yakin dalam strategi Zero Trust dan merasa siap untuk menangani ancaman keamanan di masa mendatang, masih ada banyak pekerjaan yang harus dilakukan untuk sepenuhnya diterapkan di seluruh area risiko. Di antara organisasi yang mempertimbangkan strategi Zero Trust mereka untuk sepenuhnya diimplementasikan, misalnya, hampir setengahnya saat ini belum menerapkan di seluruh area risiko keamanan, dengan Infrastruktur dan Identitas yang paling kecil kemungkinannya untuk diterapkan.

Paparan 9. Perbandingan penerapan Zero Trust

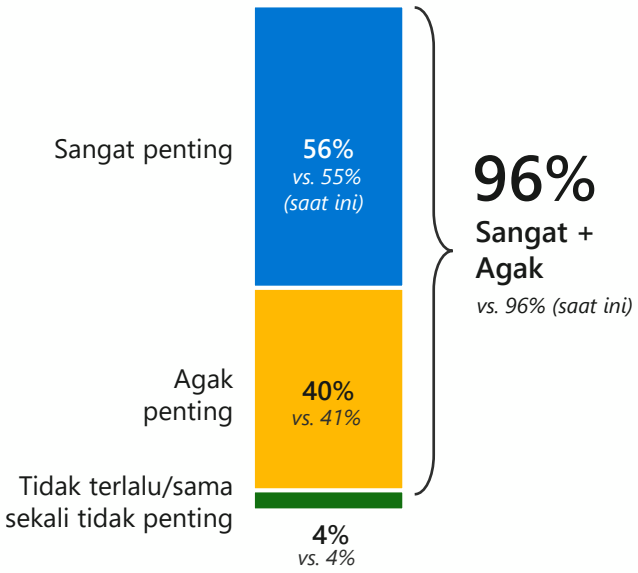
	AS	DE	JP	AUS/NZ
Terdepan	59%	46%	66%	63%
Setara	40%	52%	34%	32%
Tertinggal	2%	2%	0%	6%

Dengan melihat ke depan dalam dua tahun berikutnya, strategi Zero Trust akan tetap menjadi prioritas keamanan yang utama

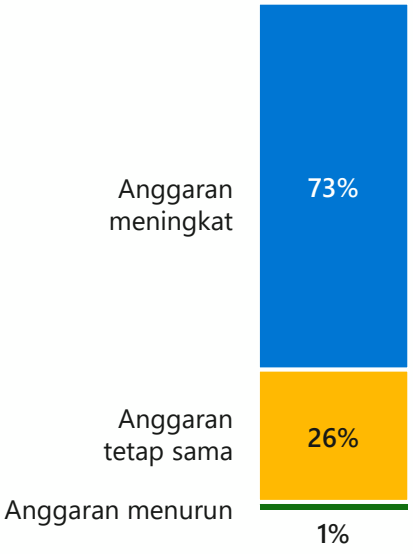
Organisasi mendukung strategi Zero Trust, dan pembuat keputusan mengatakan, ini akan terus menjadi prioritas keamanan utama selama dua tahun ke depan. Pentingnya strategi Zero Trust sebagai inisiatif keamanan diproyeksikan meningkat (53% menjadi 58%) pada 2023, karena SDM mengantisipasi bahwa strategi ini akan tetap penting untuk keberhasilan secara menyeluruh (96%). (Lihat Paparan 10)

Antisipasi pentingnya terutama tinggi di kalangan organisasi di Jepang, dengan 70% mengatakan strategi Zero Trust akan menjadi sangat penting dalam dua tahun ke depan dibandingkan dengan rata-rata keseluruhan 56%. Anggaran strategi Zero Trust juga diharapkan tumbuh dengan 73% organisasi berharap untuk meningkatkan anggaran mereka. Meskipun, jumlah ini sedikit lebih rendah di Jerman (67%), di mana 31% mengantisipasi bahwa anggaran mereka akan tetap sama. (Lihat Paparan 11)

Paparan 10. Antisipasi pentingnya Zero Trust dalam dua tahun ke depan

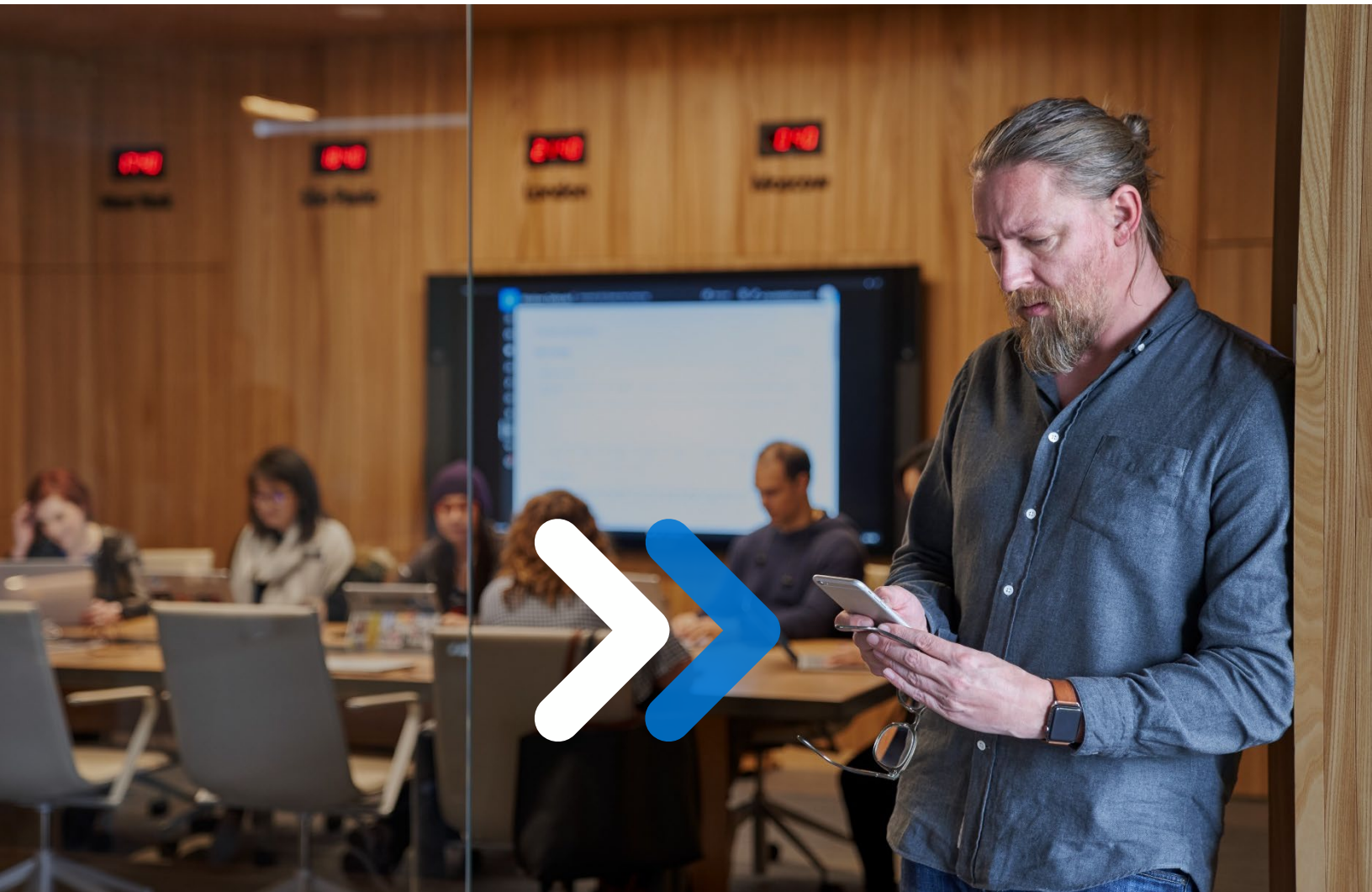


Paparan 11. Antisipasi anggaran Zero Trust dalam dua tahun ke depan



Bukti keberhasilan strategi Zero Trust dapat menjadi penggerak investasi lebih lanjut

Organisasi yang sepenuh hati merangkul Zero Trust berharap dapat menggandakan investasi mereka dalam dua tahun ke depan, dan mereka yang belum mulai mengadopsi risiko tertinggal lebih jauh di belakang. Organisasi ini tidak hanya mengikuti rekan-rekan mereka yang sepenuhnya telah menerapkan dalam hal memprioritaskan Zero Trust dalam rencana keamanan mereka (42% vs. 66%) dan mengantisipasi kenaikan anggaran (66% vs. 72%), tetapi juga merasa kurang percaya diri secara signifikan dalam mengelola keamanan IoT dan OT di masa depan (40% vs. 53%).



Mengatasi tantangan dengan karyawan akan menjadi kunci untuk menggandakan investasi Zero Trust

Meskipun terdapat kemajuan pesat dalam penerapan strategi Zero Trust, organisasi harus mengatasi berbagai tantangan jika mereka ingin maju lebih jauh dengan implementasinya. (Lihat Paparan 12) Tantangan sumber daya dan kepemimpinan paling lazim dalam kategori ini. Waktu yang dibutuhkan untuk menerapkan strategi Zero Trust dan kurangnya dukungan dari kepemimpinan level eksekutif menjadi hambatan utama, di mana yang terakhir sangat menonjol di Australia/Selandia Baru (65%).

Selain itu, kendala anggaran — yang oleh 45% organisasi diidentifikasi sebagai penghalang — kemungkinan juga berperan dalam tantangan sumber daya dan kepemimpinan.

Misalnya, 21% dari SDM mengutip kesulitan dalam membuktikan ROI investasi dalam Zero Trust sebagai penghalang untuk implementasi, tantangan yang dapat mengakibatkan kurangnya dukungan dari pimpinan level eksekutif. Oleh karena pasar non-AS cenderung memiliki kendala anggaran (60% organisasi di jepang; 57% organisasi di Jerman; 57% dari organisasi di Australia/Selandia Baru), ada kemungkinan bahwa ini memiliki efek riak, yang mengarah pada implementasi strategi Zero Trust yang lebih rendah dan lebih lambat di Jepang, Jerman, dan Australia/Selandia Baru dibandingkan dengan AS.

Paparan 12. Hambatan Zero Trust

Tantangan Sumber Daya 60%	Kepemimpinan 53%	Teknologi 46%	Vendor 46%	Kendala Anggaran 45%
20% Perlu waktu terlalu lama untuk menerapkannya	**20%** Kurangnya dukungan dari kepemimpinan level eksekutif	**21%** Kesulitan dalam mengintegrasikan solusi keamanan	**21%** Memerlukan dukungan implementasi dari vendor	**21%** Biaya penerapan strategi Zero Trust
19% Kurangnya manajemen perubahan internal	**19%** Kurangnya dukungan dari pemangku kepentingan	**19%** Ketidakcocokan dengan sistem legasi	**21%** Kesulitan dalam mengidentifikasi vendor yang tepat	**21%** Kesulitan dalam membuktikan ROI
18% Membutuhkan materi edukasi lebih banyak	**19%** Memerlukan bantuan untuk membuat kasus bisnis yang menarik	**19%** Kesulitan menyesuaikan skala di seluruh organisasi	**17%** Ketidakmampuan untuk menemukan mitra yang inovatif	**14%** Tidak memiliki anggaran yang cukup besar
17% Tidak diperlukan bagi organisasi ukuran kami	**18%** Kurangnya dukungan organisasi			
16% Tidak memiliki talenta yang tepat untuk menerapkannya dengan benar				

“ Dukungan awal menantang tetapi setelah kami sepakat sebagai pemangku kepentingan bahwa kami akan berinvestasi dalam proyek ini, semua orang akan ikut serta.”

Pengambil Keputusan Keamanan di AS FinTech

Pengambil keputusan keamanan memiliki sedikit kecenderungan untuk penyedia holistik atau terkonsolidasi

Dalam hal strategi vendor Zero Trust, organisasi dihadapkan untuk mengambil pendekatan best-in-suite atau best-in-breed. Strategi sebelumnya melibatkan pembelian rangkaian produk untuk seluruh arsitektur Zero Trust dari penyedia holistik atau terkonsolidasi, solusi yang diyakini oleh SDM menawarkan lebih banyak keahlian, sumber daya, dan kesederhanaan bagi mereka yang memiliki kekurangan sumber daya secara internal. Namun, masalah dengan pendekatan ini mencakup peningkatan kerentanan dan kurangnya fleksibilitas. (Lihat Paparan 13)

Strategi yang terakhir, best-in-breed, melibatkan mendapatkan komponen teknologi Zero Trust individu dari vendor khusus. Tidak seperti best-in-suite, strategi ini bergantung pada penyedia yang mengkhususkan diri dalam area yang berbeda dan dengan demikian menawarkan fleksibilitas yang lebih besar dan dapat lebih erat selaras dengan strategi organisasi. Meskipun demikian, para profesional keamanan melihat best-in-breed ini lebih mahal, membutuhkan lebih banyak sumber daya, dan menghambat visibilitas, kelemahan yang pada akhirnya mengarah pada tantangan vendor dan anggaran. (Lihat Paparan 14)

Meskipun sebagian besar organisasi terbagi, mayoritas kecil dari SDM (55%) lebih suka bekerja dengan penyedia holistik (best-in-suite). (Organisasi di Australia/Selandia Baru, bagaimanapun, condong ke arah yang berlawanan, dengan 52% lebih memilih best-in-breed.)

Paparan 13. Keunggulan & hambatan Best-in-Suite – Peringkat 2 Teratas

⊕ Keunggulan Best-in-Suite	
Vendor memiliki keahlian khusus industri di seluruh solusi	24%
Lebih banyak sumber daya yang tersedia untuk membantu merencanakan strategi Zero Trust	23%
Penyederhanaan tumpukan keamanan	22%

⊖ Kekurangan Best-in-Suite	
Ketergantungan pada vendor tunggal meningkatkan kerentanan	34%
Memerlukan integrasi yang lebih kompleks dengan arsitektur legasi	33%
Fleksibilitas kurang untuk fungsi khusus	29%

Paparan 14. Keunggulan & hambatan Best-in-Breed – Peringkat 2 Teratas

⊕ Keunggulan Best-in-Breed	
Fleksibilitas untuk mengejar solusi terbaik untuk setiap komponen strategi Zero Trust	33%
Dapat menyelaraskan solusi secara lebih erat dengan arsitektur atau strategi organisasi saya	30%
Peningkatan peluang untuk inovasi dengan berbagai vendor	26%

⊖ Kekurangan Best-in-Breed	
Peningkatan biaya	29%
Ketidakmampuan untuk berbagi data di berbagai solusi	26%
Volume tinggi solusi bagi tim internal untuk mengadopsi dan mengelola	26%

Pemikiran terakhir

Oleh karena risiko keamanan menjadi tidak hanya lebih sering tetapi juga lebih jahat, organisasi di seluruh pasar dan industri memilih strategi Zero Trust yang memandu kita untuk "jangan percaya, selalu lakukan verifikasi." Strategi Zero Trust adalah prioritas keamanan teratas bagi organisasi yang ingin meningkatkan postur keamanan mereka secara menyeluruh, pengalaman pengguna akhir, dan produktivitas, menyederhanakan prosedur keamanan bagi karyawan, dan mengurangi biaya. Namun, meskipun manfaat dari strategi Zero Trust ini sudah mapan, sumber daya terbatas dan skeptisisme di antara kepemimpinan menghalangi penerapan secara universal.

Adopsi strategi Zero Trust telah dipercepat dalam tiga tahun terakhir, sebagian karena pandemi COVID-19. Secara krusial, pergeseran ke tempat kerja jarak jauh dan hibrid mendorong penerapan pendekatan Zero Trust yang lebih luas, yang menjanjikan untuk melindungi sistem dan data bahkan saat karyawan mengaksesnya di luar lokasi, terkadang di perangkat pribadi. Percepatan adopsi karena COVID adalah prediktor yang baik dari kesiapan Zero Trust secara keseluruhan, dengan organisasi yang merangkul strategi ini selama pandemi yang telah menerapkannya di lebih banyak area risiko keamanan daripada rekan-rekan mereka.

Meskipun demikian, bahkan pengadopsi strategi Zero Trust yang paling canggih pun memiliki pekerjaan yang harus dilakukan, dan kesalahan persepsi organisasi tentang kedewasaan Zero Trust mereka sendiri dapat memberikan beberapa kerentanan yang bahkan tidak mereka ketahui.

Mayoritas organisasi di seluruh pasar percaya bahwa kritik terhadap strategi Zero Trust hanya akan tumbuh seiring waktu dan pada gilirannya berharap anggaran mereka akan meningkat. Pergeseran yang diantisipasi dalam prioritas ini sangat penting untuk pasar selain AS, di mana masalah anggaran adalah hambatan yang menonjol untuk adopsi. Berjuang untuk implementasi penuh mungkin secara finansial dan logistik berlebihan; namun, manfaat dari pendekatan Zero Trust ini tidak dapat disangkal, dan Microsoft akan siap untuk memandu dan mendukung organisasi saat mereka memulai bidang yang semakin berkembang ini.

Untuk mempelajari lebih lanjut tentang Zero Trust dan melakukan penilaian terhadap kematangan Zero Trust organisasi Anda, kunjungi

aka.ms/zerotrust

Tujuan penelitian terperinci & rekrut pemirsa

Tujuan dari penelitian ini mencakup:

Memahami kondisi terkini dari pendekatan Zero Trust

Mengungkap pola pikir, praktik terbaik, keunggulan, dan tantangan dalam mengadopsi pendekatan Zero Trust

Menjelajahi pendekatan Zero Trust di masa depan

Mengontekstualisasikan inovasi dan tren dalam pendekatan Zero Trust

Untuk memenuhi kriteria penyaringan, para pengambil keputusan keamanan perlu untuk:

Bertanggung jawab atas keamanan dalam organisasi mereka, termasuk Keamanan Siber, Operasi Keamanan, Perlindungan terhadap Ancaman, Manajemen Identitas, Manajemen Risiko, Keamanan Aplikasi, Forensik Digital, dan Respons Insiden

Mempekerjakan secara purna-waktu di perusahaan setingkat enterprise (1000 lebih karyawan di AS; 500 lebih karyawan di Jerman/Jepang/Australia/ Selandia Baru)

Usia 25-75 tahun

Familiar dengan Zero Trust

Terlibat dalam pengambilan keputusan untuk pengembangan/implementasi Strategi Zero Trust

Dari 911 Pengambil Keputusan Keamanan yang diwawancarai untuk gelombang penelitian pada bulan April 2021:

Di AS, 477 SDM diwawancarai

Di Jerman, 201 SDM diwawancarai

Di Australia/Selandia Baru, 126 SDM diwawancarai

Di Jepang, 107 SDM diwawancarai

Catatan: Penelitian dilakukan selama pandemi global COVID-19, yang berada di berbagai tahap eskalasi/ penahanan

Microsoft Security hypothesis