GEBYAR

AUTO-ID

BULETIN EDISI 68
SEPTEMBER 2024

[-] E-Buletin

PERKUAT KEAMANAN SIBER DI PERUSAHAAN ANDA DENGAN ZERO TRUST NETWORK ACCESS

- **MENGENAL UEM: SOLUSI TERPADU UNTUK PENGELOLAAN PERANGKAT DI ERA KERJA HIBRID**
- **Mespro:** Membantu Anda Menuju Kesiapan Industri 4.0
- **TIPS & TRIK:** Jangan Biarkan Baterai Unit Anda Sampai Habis!

MEDIA KOMUNIKASI PELANGGAN
ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

EDITORIAL

Para pembaca yang terhormat,

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga kita semua dalam keadaan sehat dan dapat terus berkarya.

Di era digital saat ini, data menjadi aset yang sangat berharga, baik bagi individu maupun organisasi. Perlindungan dan mitigasi untuk mengamankan data merupakan tantangan yang perlu dipikirkan dan diimplementasikan dalam jaringan infrastruktur organisasi. Terlebih lagi, kemudahan transaksi data yang kini menjadi tren dalam teknologi informasi membuka celah keamanan jika tidak diimbangi dengan sistem perlindungan yang kuat.

Zero Trust Network Access (ZTNA) akan menjadi fokus utama buletin edisi kali ini, yang bisa menjadi solusi atas tantangan perlindungan data. Prinsip kerjanya adalah "selalu melakukan verifikasi" dan tidak mempercayai apapun, sehingga identifikasi terhadap akses dari internal maupun eksternal selalu dilakukan.

Selain pembahasan utama, buletin ini juga menyajikan berbagai rubrik menarik seperti produk unggulan (Zebra Technologies, ZKTeco, HPE Instant On, dan Ivanti), tips, serta informasi korporat dan prinsip yang bermanfaat bagi rekan bisnis.

Semoga buletin ini dapat memberikan informasi berharga dan bermanfaat bagi rekan-rekan bisnis, serta dapat menciptakan kolaborasi bisnis yang baik di masa depan.

Salam Hangat

Maulana Ibrahim

Professional Services Supervisor

PT. Autojaya Idetech

PT. Solusi Periferal

PEMIMPIN REDAKSI
Andre S.Kouanak

SEKRETARIS REDAKSI
Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
A.A. Ayu Isna Surya Dewi (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Nuning Kustiawita
Chandra Sari

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Maulana Ibrahim
Nopah Hermanto
Richard Andrian
Arijanto Hartanto
Taufiq Rahman
Jemis Pangaribuan
Liana Andari
Angelina Rasta Perbina Ginting
Agung Atmoko

ALAMAT REDAKSI
Jakarta (HO)
Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
T : +6221-4208221, 4205187
E : acs.marcom@acsgroup.co.id

CONTENT

PERKUAT KEAMANAN SIBER DI PERUSAHAAN ANDA DENGAN ZERO TRUST NETWORK ACCESS (ZTNA)

by **Maulana Ibrahim**, Professional Services Supervisor | ACS Group

Ancaman siber yang semakin canggih telah membuat model keamanan tradisional "percaya dulu, baru verifikasi" ("*trust but verify*") tidak lagi relevan. Untuk menghadapi tantangan ini, kita perlu mengadopsi pendekatan yang lebih kuat dan handal.

Dalam dunia keamanan siber yang semakin kompleks, *Zero Trust Network Access* (ZTNA) semakin populer. Teknologi ini menawarkan pendekatan yang lebih aman untuk mengelola akses ke jaringan dan aplikasi, dengan menghilangkan asumsi bahwa semua yang berada di dalam jaringan dapat dipercaya. Mari kita simak lebih dalam tentang ZTNA dan manfaatnya bagi organisasi atau perusahaan.

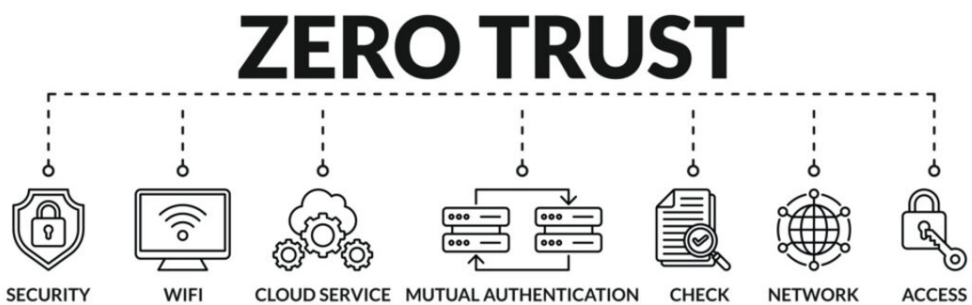
Apa Itu Zero Trust Network Access (ZTNA)?

ZTNA adalah model keamanan jaringan yang tidak memberikan kepercayaan secara otomatis kepada siapa pun atau apa pun, baik itu pengguna di dalam maupun di luar jaringan. **ZTNA mengharuskan setiap pengguna** dan perangkat untuk diverifikasi secara berulang dan konsisten sebelum diberikan akses ke dalam jaringan.

Pada prinsipnya ZTNA tidak memberikan kepercayaan implisit. Ini berarti setiap permintaan akses harus diverifikasi, meskipun permintaan tersebut berasal dari dalam jaringan yang sudah dinyatakan bersih. Verifikasi berulang memastikan bahwa hanya pengguna dan perangkat yang sudah di verifikasi yang dapat mengakses sumber daya tertentu.

Perbedaan ZTNA dengan Sistem Keamanan Tradisional

Sistem keamanan tradisional seringkali mengandalkan *firewall* untuk melindungi perimeter jaringan. Model tradisional sering kali gagal mendeteksi ancaman dari dalam jaringan. Oleh karena itu, ZTNA mengadopsi pendekatan "tidak percaya siapa pun) sampai mereka berhasil dive-



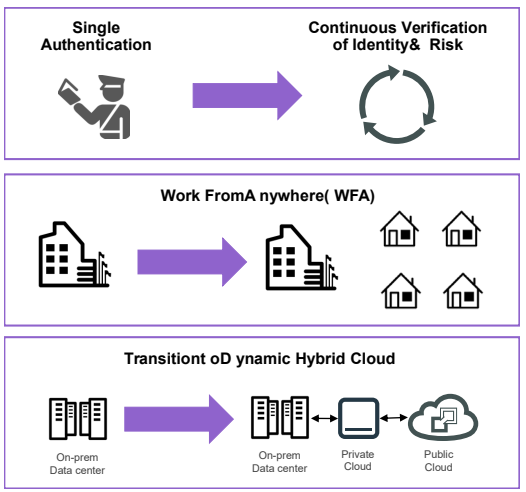
rifikasi. Hal ini membuat ZTNA jauh lebih efektif dalam menangkal ancaman dari dalam jaringan.

ZTNA meningkatkan keamanan dengan membatasi akses dan segmentasi jaringan secara cermat. Pengguna hanya diberikan ijin untuk mengakses aplikasi dan data yang mereka butuhkan. Dengan begitu, risiko penyalahgunaan akses dan serangan siber dapat diminimalisir.

ZTNA dirancang berdasarkan asumsi bahwa ancaman bisa datang dari mana saja. Oleh karena itu, setiap permintaan akses harus melalui proses dan otorisasi yang ketat, terlepas dari lokasi pengguna atau lingkungan jaringan.

Keunggulan ZTNA untuk Organisasi Modern

Dalam era di mana lingkungan jaringan semakin dinamis, organisasi membutuhkan solusi keamanan yang fleksibel dan skalabel. ZTNA menawarkan fleksibilitas yang memungkinkan organisasi untuk mengadaptasi perubahaan dan memperluas jaringan tanpa mengorbankan keamaman.



Dengan semakin populernya gaya kerja dari mana saja (WFH dan WFA), kebutuhan akan solusi keamanan yang dapat diandalkan di mana saja pun semakin mendesak. ZTNA menawarkan pendekatan yang komprehensif untuk mengamankan akses jaringan, baik bagi karyawan yang bekerja dari kantor, maupun mereka yang bekerja dari jarak jauh.

Seiring dengan semakin dinamisnya cara kita mengakses jaringan, ZTNA hadir sebagai solusi yang lebih aman dan efisien. ZTNA merupakan generasi terbaru dari teknologi akses jaringan yang menawarkan peningkatan signifikan dibandingkan VPN (*Virtual Private Network*) tradisional.

Manfaat dari penerapan ZTNA

ZTNA tidak hanya sekadar lapisan keamanan tambahan, tetapi juga merupakan kunci untuk meningkatkan efisiensi operasional. Berikut adalah beberapa manfaat utama:

1. **Meningkatkan Level Keamanan**

   ZTNA meningkatkan keamanan dengan mengurangi risiko akses ilegal. Setiap akses didasarkan pada otentikasi ketat, sehingga meminimalisir ancaman atau adanya anomali di dalam jaringan. Model keamanan yang adaptif dan tidak memberikan kepercayaan secara otomatis membuat jaringan Anda jauh lebih aman dari ancaman.

2. **Menambah Keamanan Akses Jarak Jauh**

   ZTNA juga memastikan akses yang aman bagi pengguna jarak jauh. Berbeda dengan VPN tradisional, ZTNA hanya memberikan akses ke aplikasi yang dibutuhkan, sehingga risiko kebocoran data dapat diminimalkan.

3. **Pengelolaan Akses yang Lebih Baik**

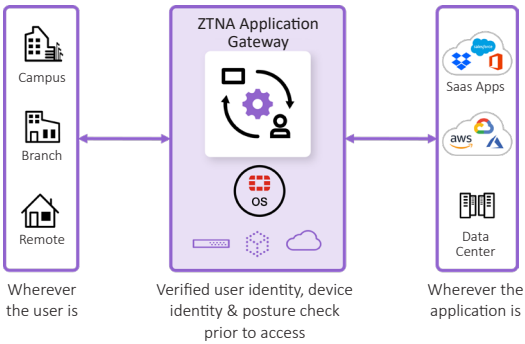
   Dengan ZTNA, pengelolaan akses menjadi lebih baik dan cepat. Setiap permintaan akses akan dievaluasi berdasarkan identitas dan konteksnya, sehingga Anda memiliki kontrol penuh atas siapa yang bisa mengakses apa dan kapan. Ini membantu dalam mengurangi risiko dan meningkatkan standar keamanan keseluruhan.

Bagaimana Cara Kerja ZTNA ?

Konsep ZTNA berangkat dari asumsi dasar bahwa ancaman keamanan bisa datang dari mana saja, baik dari luar maupun dari dalam jaringan itu sendiri. Setiap upaya akses, tanpa terkecuali, dianggap sebagai potensi ancaman. Oleh karena itu, ZTNA tidak mempercayai siapa pun, baik pengguna internal maupun eksternal sebelum identitas mereka terverifikasi secara menyeluruh.

Perangkat lunak yang berfungsi sebagai penghubung ini terintegrasi langsung ke jaringan perusahaan. Dengan teknologi enkripsi yang canggih, setiap koneksi yang melaluinya akan diperiksa secara ketat. Baik itu akses dari dalam atau luar jaringan, semua lalu lintas data harus mengikuti kebijakan keamanan yang telah ditetapkan.

Saat Anda mencoba mengakses aplikasi perusahaan menggunakan perangkat pribadi, ZTNA akan terlebih dahulu memeriksa perangkat Anda secara menyeluruh. Proses ini disebut *rule tagging*. ZTNA akan memastikan bahwa perangkat Anda telah memenuhi semua persyaratan keamanan yang telah ditetapkan. Jika lolos, Anda baru akan diizinkan masuk. Namun, jika perangkat Anda belum memenuhi standar keamanan, akses Anda akan langsung ditolak.



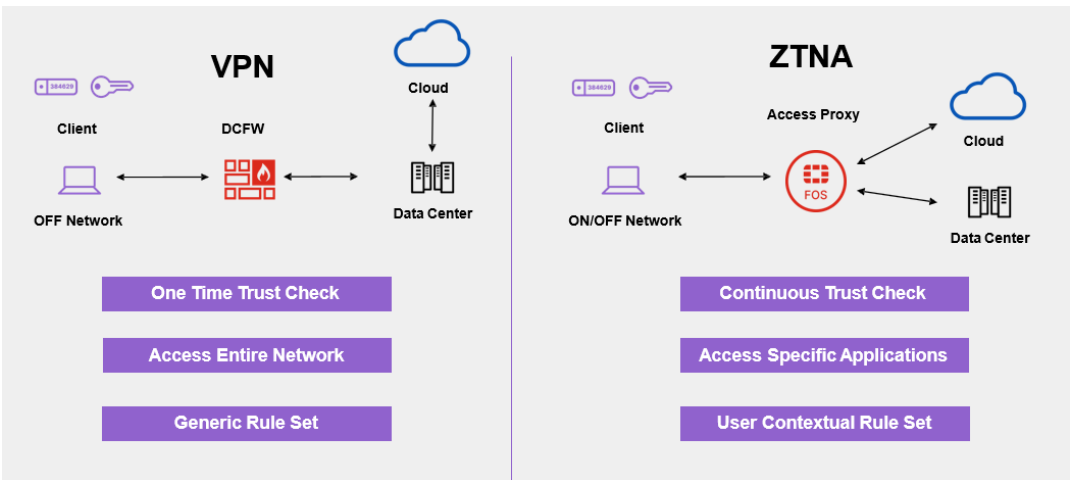
ZTNA bekerja dengan cara memverifikasi setiap akses, baik itu dari pengguna, aplikasi, maupun perangkat.

- **Pengguna**

  ZTNA memastikan identitas setiap orang yang mengakses sistem benar-benar valid melalui autentikasi yang kuat. Selain itu, kondisi perangkat yang digunakan juga diperiksa untuk mencegah akses dari perangkat yang tidak aman.

- **Aplikasi**

  ZTNA tidak langsung mempercayai aplikasi. Setiap perilaku aplikasi akan dipantau secara terus-menerus selama proses berja-



Evolusi dari tradisional VPN menjadi ZTNA

lan (*runtime*) untuk memastikan aplikasi tersebut tidak melakukan aktivitas yang mencurigakan atau membahayakan.

- ***Infrastruktur***

  ZTNA mencakup semua komponen, mulai dari router, switch, hingga perangkat IoT. Pendekatan ini memastikan bahwa setiap bagian dari infrastruktur terlindungi dengan baik.

Keunggulan utama ZTNA adalah kemampuannya membatasi akses dari luar jaringan. Karena ZTNA hanya mengizinkan koneksi keluar (*outbound*), maka tidak perlu lagi membuka port pada *firewall* untuk akses masuk (*inbound*). Hal ini sangat efektif dalam mencegah serangan seperti virus, malware, DDoS, dan lainnya.

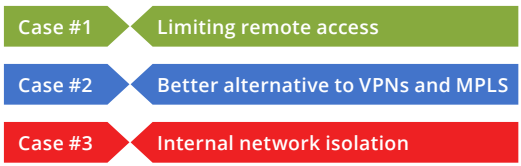
ZTNA juga sangat fleksibel dalam menangani berbagai jenis perangkat, baik yang dikelola maupun yang tidak dikelola. Untuk perangkat yang dikelola, ZTNA menggunakan agen khusus yang terpasang pada perangkat. Klien bertanggungjawab untuk mengumpulkan informasi mengenai perangkat tersebut dan mengirimkannya ke layanan ZTNA. Dengan begitu, ZTNA dapat memastikan bahwa hanya perangkat yang aman dan terpercaya dapat mengakses sistem.

Mengimplementasikan prinsip *Zero Trust* tidak berarti harus membangun ulang seluruh jaringan dari nol. Inti dari implementasi *Zero Trust* adalah merancang strategi yang tepat dan memilih alat yang sesuai untuk menciptakan lapisan keamanan ekstra. Ini berarti mengubah cara kita mengelola akses dan menjaga keamanan di seluruh lingkungan perusahaan.

Sistem keamanan ini akan bekerja dengan cara mengidentifikasi data, aset, aplikasi, dan layanan jaringan secara menyeluruh. Dengan mengidentifikasi aset yang paling penting, perusahaan dapat memfokuskan upaya untuk memprioritaskan dan melindungi aset tersebut.

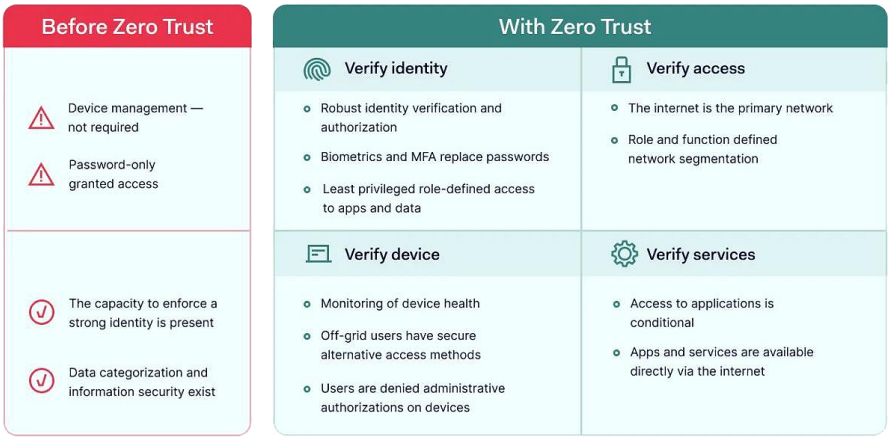
Zero Trust bekerja dengan cara memetakan seluruh aset digital perusahaan, mulai dari data, aplikasi, hingga layanan jaringan. Dengan memahami aset-aset penting ini, perusahaan dapat memprioritaskan perlindungan. Selanjutnya, sistem akan melacak setiap pengguna dan perangkat yang mencoba mengakses jaringan. Setiap akses akan melalui proses verifikasi yang ketat untuk memastikan keamanan.

Beberapa Kasus Penggunaan ZTNA



ZTNA adalah solusi keamanan siber yang sangat berguna untuk melindungi aset digital perusahaan. Berikut adalah beberapa contoh bagaimana ZTNA dapat diterapkan:

1. Gaya kerja dari mana saja (WFH/WFA) semakin meningkat. Akibatnya risiko keamanan juga meningkat. ZTNA memberikan akses yang sangat terkontrol ke aplikasi-aplikasi tertentu, sehingga karyawan dapat bekerja dengan aman tanpa harus membuka seluruh jaringan internal perusahaan. Hal ini meminimalisir risiko kebocoran data yang mungkin terjadi akibat akses jarak jauh yang tidak terkendali.
2. ZTNA merupakan alternatif yang lebih aman dari VPN dan MPLS. ZTNA memiliki kemiripan teknologi VPN. Meskipun begitu, "*Zero Trust*" yang dianutnya membuat ZTNA jauh lebih aman. Setiap akses yang dilakukan akan selalu diverifikasi ulang, sehingga risiko intrusi dari pihak luar dapat diminimalisir.
3. ZTNA menciptakan batas-batas akses yang sangat ketat. Dengan kata lain, pengguna hanya akan diberikan akses yang benar-benar dibutuhkan untuk menjalankan tugas mereka. Hal ini membuat jaringan internal perusahaan terisolasi dengan baik dan terlindungi dari ancaman seperti peretas.



Manfaat *Zero Trust* Terhadap Pelaku Bisnis atau Perusahaan

1. Akses ke jaringan secara otomatis diblokir sebelum identitas pengguna terverifikasi. Akses dianggap sebagai privilege yang terus-menerus dipantau. Jika ada aktivitas mencurigakan, akses dapat langsung dicabut. Hal ini menciptakan pertahanan yang jauh lebih kuat terhadap ancaman siber.
2. *Zero Trust* meminimalkan dampak dari pelanggaran data. Setiap permintaan akses, baik dari dalam maupun luar jaringan, akan melalui pemeriksaan ketat. Dengan asumsi setiap koneksi adalah potensi ancaman, sistem akan memastikan bahwa hanya permintaan yang aman yang diizinkan. Ini membatasi ruang gerak bagi hacker untuk melakukan aksi jahat.

Zero Trust adalah solusi ideal untuk lingkungan kerja modern yang dinamis. Ketika lalu lintas jaringan semakin kompleks, terutama dengan meningkatnya jumlah akses jarak jauh, *Zero Trust* memastikan bahwa semua aktivitas jaringan, baik internal maupun eksternal, selalu terjaga keamanannya.

Bagaimana Cara mengimplementasikan ZTNA?

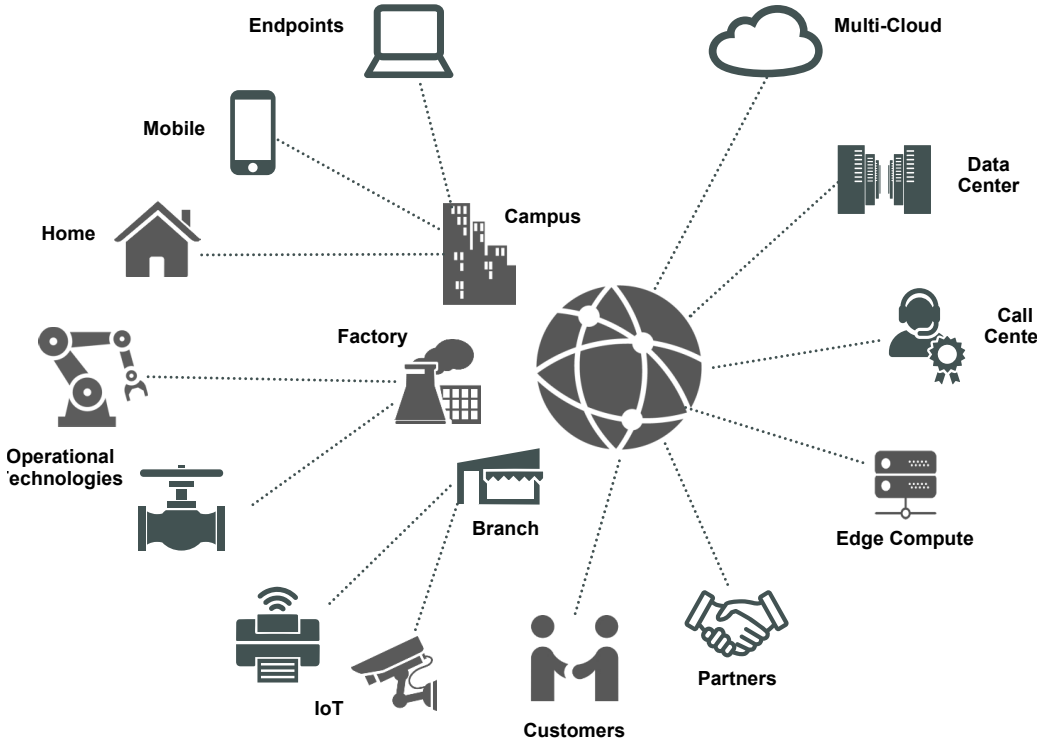
Implementasi ZTNA dapat dilakukan melalui dua metode utama:

- *Agent-Based (end-point initiated):* Pada metode ini, perangkat lunak ZTNA perlu diinstal pada setiap perangkat (seperti komputer, smartphone) yang ingin mengakses aplikasi.
- *Service-based (Service initiated):* Metode ini tidak memerlukan instalasi perangkat lunak pada setiap perangkat. Sebaliknya, layanan ZTNA ditempatkan di antara perangkat pengguna dan aplikasi yang ingin diakses. Layanan ini akan secara proaktif memverifikasi identitas pengguna dan koneksi sebelum memberikan akses.

Model Pengiriman ZTNA

ZTNA dapat diterapkan dalam dua model utama:

- ***Standalone***: Organisasi memiliki kendali penuh atas seluruh komponen ZTNA. Model ini memberikan fleksibilitas tinggi namun memerlukan pengelolaan yang lebih kompleks.
- ***As-a-Service***: Organisasi "menyewa" layanan ZTNA dari penyedia pihak ketiga. Model ini cocok bagi organisasi yang ingin mengadopsi ZTNA tanpa perlu membangun infrastruktur dari awal.

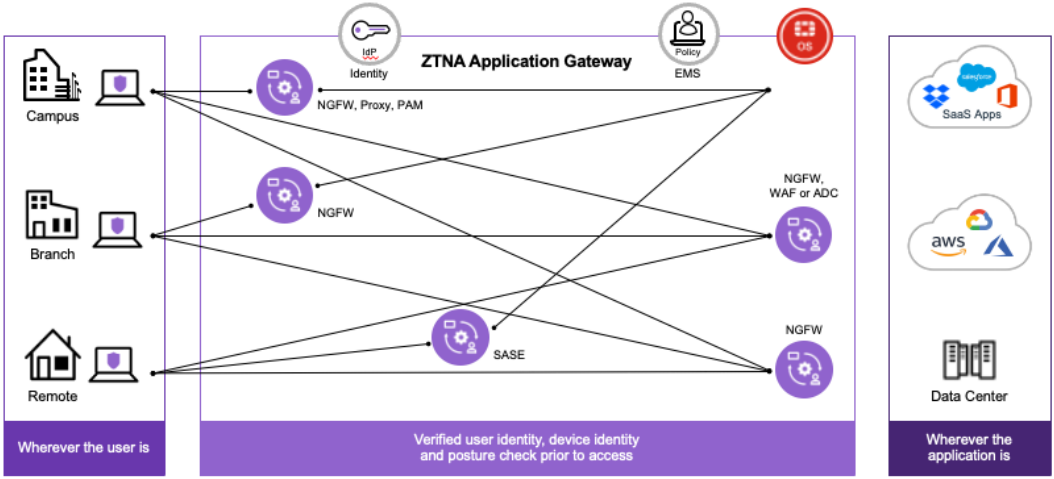


Kontrol Akses dan visibilitas jaringan ZTNA

Langkah-langkah Implementasi *Zero Trust*

Untuk memulai implementasi *Zero Trust*, pertimbangkan langkah-langkah berikut:

1. **Identifikasi Aset Kritis:** Tentukan dengan jelas data, aplikasi, dan sistem mana yang paling berharga dan perlu dilindungi. Ini adalah langkah awal yang krusial dalam membangun strategi keamanan yang efektif.
2. **Petakan Interaksi Aplikasi:** Memahami bagaimana aplikasi berkomunikasi satu sama lain akan membantu Anda mengidentifikasi titik-titik yang rentan terhadap serangan dan menentukan kontrol akses yang tepat
3. **Sesuaikan Arsitektur:** *Zero Trust* dapat diimplementasikan dengan berbagai arsitektur, termasuk yang sudah ada. Pilih arsitektur yang paling sesuai dengan lingkungan Anda. Langkah-langkah selanjutnya adalah membatasi akses ke area jaringan yang sifatnya kritikal atau penting untuk dilindungi
4. **Definisikan Kebijakan:** Buat kebijakan yang jelas dan rinci tentang siapa yang boleh mengakses apa, kapan, dan bagaimana. Model "Six Ws" (Who, What, When, Where, Why, How) dapat membantu Anda merumuskan kebijakan yang komprehensif. Metode yang juga dikenal dengan metode "kipling" ini adalah cara efektif untuk menentukan verifikasi akses jaringan. Tidak boleh ada komunikasi antara pengguna dan aplikasi yang tidak diketahui oleh administrator jaringan.
5. **Implementasi dan Monitoring:** Terapkan kebijakan ZTNA dan pantau secara berkala untuk memastikan efektifitasnya. Dokumentasikan semua perubahan dan aktivitas untuk memudahkan troubleshooting dan audit.



Apa yang Perlu Diperhatikan Saat Menerapkan ZTNA?

Ketika memutuskan untuk menerapkan *ZTNA*, ada beberapa hal krusial yang harus diingat oleh organisasi. Pertama, **autentikasi multi-faktor** adalah kunci untuk memvalidasi identitas setiap pengguna. Kedua, **pemeliharaan perangkat** yang baik, termasuk pembaruan perangkat lunak secara berkala, sangat penting untuk menjaga keamanan jaringan. Ketiga, **pemantauan yang komprehensif** memungkinkan administrator untuk mengidentifikasi potensi ancaman dan menyesuaikan kebijakan keamanan secara proaktif. Terakhir, **pengendalian akses yang ketat** terhadap aplikasi, data, dan aset sangat penting untuk membatasi potensi kerusakan akibat pelanggaran keamanan.

Tantangan dalam Menerapkan ZTNA

Meskipun ZTNA menawarkan perlindungan yang kuat, implementasinya tidak tanpa tantangan. Pemantauan yang konsisten diperlukan untuk memastikan keamanan jaringan terus terjaga. Selain itu, sosialisasi yang efektif kepada pengguna sangat penting agar mereka memahami pentingnya prosedur keamanan baru. Awalnya, proses autentikasi yang lebih ketat mungkin terasa merepotkan, namun manfaatnya jauh lebih besar dalam jangka panjang. ZTNA dapat membantu organisasi melindungi diri dari berbagai ancaman siber yang semakin canggih.

Konsep dan Proses ZTNA

Bagaimana *Best Practice Zero Trust?*

Berikut adalah beberapa praktik terbaik (*best Practice*) penerapan *Zero Trust*:

1. **Mulai dengan Tujuan yang Jelas:** Sebelum menerapkan *Zero Trust*, tentukan terlebih dahulu tujuan bisnis yang ingin dicapai. Pertimbangkan aspek mana saja yang dapat ditingkatkan dengan keamanan siber yang lebih modern. *Zero Trust* bisa menjadi solusi jika perusahaan pernah mengalami serangan siber. Dengan begitu, kita bisa fokus melindungi aset-aset kritis.

Zero Trust Best Practices

1	Start with clear business objectives
2	Understand the protection surface
3	Map out your network assets
4	Create a strong device identity
5	Introduce centralized monitoring
6	Don't trust your local network
7	Segment your network
8	Combine multiple verificaition methods
9	Implement Zero Trust policies

2. **Petakan Aset yang Kritis:** Identifikasi semua aset jaringan yang perlu dilindungi, mulai dari perangkat, pengguna, hingga layanan. Pemetaan aset dapat memberikan visibilitas data yang perlu diamankan. Aset yang paling beresiko adalah aset yang terhubung ke internet karena terdapat kerentanan yang dapat di eksploitasi dari jarak jauh. Berikan pembatasan akses pada aset tertentu, karena semua perangkat, baik itu model lama atau baru, memiliki resiko keamanan yang sama.
3. **Buat Identitas Perangkat yang Kuat:** Setiap perangkat harus memiliki identitas unik yang kuat sebagai dasar untuk autentikasi dan otorisasi. Ini akan membantu mencegah akses yang tidak sah.
4. **Pemantauan Terpusat:** Kumpulkan semua data pemantauan ke dalam satu dashboard. Ini akan memberikan gambaran menyeluruh tentang aktivitas jaringan dan memudahkan deteksi anomali atau ancaman. Notifikasi untuk aktivitas yang mencurigakan juga dapat dibantu dengan mengaktifkan berbagai otomatisasi.
5. **Jangan Percaya Jaringan Lokal:** Anggaplah tidak ada bagian dari jaringan yang sepenuhnya aman. Semua akses harus diautentikasi secara ketat, termasuk akses internal.
6. **Segmentasi Jaringan:** Bagi jaringan menjadi segmen-segmen yang lebih kecil. Jika terjadi serangan, dampaknya dapat dibatasi pada segmen yang terinfeksi.
7. **Verifikasi Berganda:** Jangan hanya mengandalkan kata sandi. Gunakan metode verifikasi tambahan seperti autentikasi dua faktor untuk meningkatkan keamanan akun.
8. **Kebijakan Zero Trust yang Komprehensif:** Buat kebijakan yang jelas dan terukur untuk melindungi aset-aset kritis. Pastikan semua perangkat dan pengguna mematuhi kebijakan tersebut, sehingga lalu lintas jaringan aman dan termonitor.

Kesimpulan

ZTNA menghadirkan cara baru yang lebih aman dan fleksibel dalam mengelola akses jaringan. Prinsip dasarnya sederhana: jangan pernah percaya, selalu verifikasi. Dengan pendekatan ini, ZTNA tidak hanya meningkatkan keamanan jaringan, tetapi juga memberikan fleksibilitas yang lebih tinggi. Meskipun implementasinya mungkin tampak kompleks, manfaat yang didapatkan jauh lebih besar.

Mengadopsi *Zero Trust* adalah langkah cerdas untuk meningkatkan keamanan siber di organisasi Anda. memudahkan pengguna, menyederhanakan pengelolaan, dan memberikan visibilitas yang lebih baik terhadap seluruh jaringan. Dengan *Zero Trust*, Anda dapat dengan mudah memantau dan mengontrol akses dari dalam maupun luar jaringan, sehingga melindungi aset data Anda dari ancaman siber.

Bagi perusahaan yang ingin mengamankan data dan aset berharganya, *Zero Trust* adalah solusi yang tepat. Model ini menjawab tantangan keamanan data yang semakin kompleks dan memberikan ketenangan pikiran bagi bisnis Anda.

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

ACS Group mengucapkan

Selamat memperingati

Maulid Nabi Muhammad ﷺ

12 Robiul Awal 1446 H / 2024

Mari tanamkan keteladanan Nabi Muhammad ﷺ
untuk mencapai kebahagiaan di dunia dan di akhirat.

MENGENAL UEM: SOLUSI TERPADU UNTUK PENGELOLAAN PERANGKAT DI ERA KERJA HIBRID

by **Nopah Hermanto**, AIDC & Security Solutions | ACS Group

Adopsi metode kerja hibrid dan tren BYOD (*Bring Your Own Device*) yang semakin meluas telah mengubah lanskap mobilitas perusahaan. Hal ini menuntut adanya pengelolaan dan pengamanan yang lebih efektif terhadap berbagai perangkat (*endpoints*) yang digunakan untuk mengakses dan memproses data perusahaan. *UEM* hadir sebagai solusi komprehensif untuk mengelola beragam *endpoints* seperti *smartphone*, *tablet*, *desktop*, perangkat *rugged*, dan berbagai sistem operasi lainnya.

UEM adalah pendekatan terpadu untuk mengamankan dan mengelola berbagai jenis perangkat, seperti komputer desktop, laptop, ponsel pintar, dan tablet melalui satu konsol Tunggal yang kohesif.

UEM menyederhanakan manajemen *endpoint* dan meminimalkan potensi risiko dengan menerapkan kebijakan keamanan di setiap perangkat. Hal ini memungkinkan tim TI dalam menghemat waktu dan meningkatkan efisiensi dalam mengelola ribuan perangkat pengguna.

Fungsi UEM

UEM menawarkan solusi komprehensif untuk mengelola beragam perangkat. Dengan UEM, administrator dapat:

- Mengkonsolidasi manajemen: Mengelola perangkat desktop dan seluler dari satu panel.
- Memperbarui perangkat: Mengirimkan pembaruan sistem operasi dan aplikasi secara otomatis.
- Menegakkan keamanan: Menerapkan kebijakan keamanan yang ketat dan menghapus data dari perangkat yang hilang dari jarak jauh.
- Memungkinkan pengguna BYOD mendaftar perangkat mereka sendiri dan mengakses aplikasi perusahaan.

Manajemen aplikasi dalam solusi UEM memberikan fleksibilitas bagi administrator. Aplikasi perusahaan dapat didistribusikan secara paksa ke perangkat pengguna atau pengguna yang berwenang dapat mengaksesnya secara mandiri di toko aplikasi perusahaan.

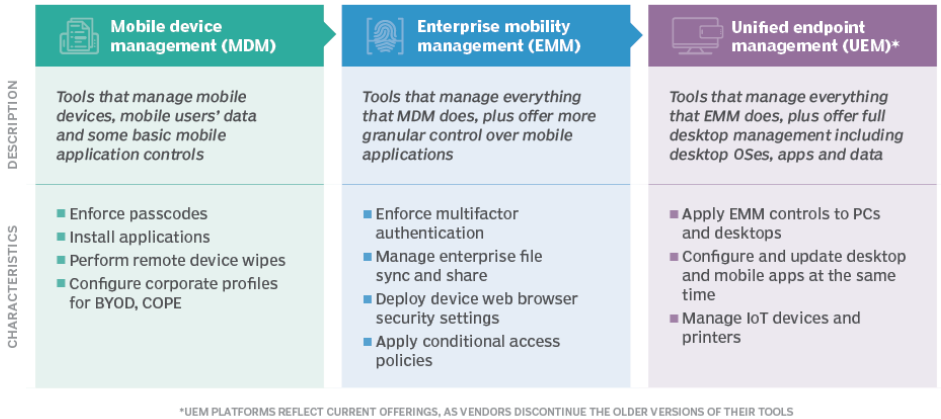
Dengan fitur-fitur yang beragam, solusi UEM menjadi aset yang berharga untuk mengelola beragam perangkat yang berjalan di berbagai platform OS.

Sejarah dan Evolusi UEM

Sejarah evolusi UEM diawali dari pengembangan alat manajemen klien tradisional untuk perangkat seluler, yaitu **MDM *(Mobile Device Management)***. Yang dulunya adalah solusi mandiri yang fokus mengelola perangkat seluler seperti smartphone dan tablet. Kini, fitur MDM menjadi bagian integral dari platform UEM yang lebih komprehensif.

MDM mulai diintegrasikan ke dalam satu platform dengan ***Mobile Application Management* (MAM)**. Dan keduanya berevolusi menjadi ***Enterprise Mobility Management* (EMM)** yang memungkinkan pengelolaan perangkat dan aplikasi secara menyeluruh melalui *Application Programming Interface* (API) MDM, dengan menerapkan protokol khusus dan dukungan untuk mengelola aplikasi.

EMM sendiri kemudian berevolusi menjadi UEM dengan mengintegrasikan manajemen klien tradisional secara lebih mendalam. Pendekatan ini memungkinkan pengelolaan perangkat secara terpadu, baik perangkat seluler maupun desktop.



Dukungan manajemen jarak jauh melalui API dan protokol MDM mempermudah platform UEM untuk mulai mendukung desktop.

Seiring berjalannya waktu, produk-produk ini juga memasukkan lebih banyak elemen manajemen klien tradisional. Platform UEM terus mengintegrasikan berbagai perangkat lunak seperti produk keamanan endpoint, *Identity and Access Management* (IAM), pemantauan kinerja, sinkronisasi file perusahaan, aplikasi berbagi, dan aplikasi mengobrol.

Fitur dan Komponen UEM

Platform Unified Endpoint Management mencakup beberapa komponen:

1. **Manajemen Perangkat**

   UEM memungkinkan pengelolaan perangkat secara terpusat dan fleksibel menggunakan protokol MDM. Dengan protokol ini, perangkat dapat dikonfigurasi, diperbarui, dan diamankan dari jarak jauh, bahkan saat tidak terhubung ke jaringan perusahaan. Protokol MDM bekerja melalui internet, sehingga perangkat tidak perlu masuk ke jaringan perusahaan atau menggunakan VPN. Aktivitas manajemen perangkat meliputi:

   - Mengonfigurasi enkripsi.
   - Mengatur kebijakan kode sandi.
   - Mengelola pembaruan OS dan aplikasi.
   - Mengonfigurasi koneksi Wi-Fi dan VPN.
   - Mengonfigurasi email dan akun lainnya.
   - Melacak lokasi perangkat.
   - Mengunci dan membuka kunci perangkat dari jarak jauh.
   - Mengonfigurasi pengaturan pencegahan kehilangan data (DLP).

2. **Dukungan OS dan Perangkat**

   - **Apple**

     Apple menawarkan protokol MDM yang fleksibel untuk mengelola perangkat iOS, macOS, iPadOS, watchOS, dan tvOS. Layanan manajemen iOS

yang diberikan meliputi Apple Push Notification, membeli aplikasi melalui Apple Business Manager dan Apple School Manager, mengelola Apple ID, dan mendaftarkan perangkat secara massal. Tergantung kebutuhan, Apple MDM memiliki beberapa mode pendaftaran berbeda yaitu pendaftaran pengguna untuk BYOD, pendaftaran perangkat, pendaftaran perangkat otomatis, dan mode supervisi untuk perangkat perusahaan.

- **Android**

Di masa lalu, manajemen Android terfragmentasi. Saat ini, Android Enterprise menyediakan kerangka kerja yang komprehensif untuk mengelola berbagai hal seperti aplikasi kios khusus, perangkat perusahaan, dan perangkat dengan penggunaan campuran antara pekerjaan dan pribadi melalui profil kerja.

- **Perangkat Lainnya**

UEM juga dapat mengelola beberapa jenis perangkat lainnya:

- Chromebook dan perangkat Chrome OS terhubung ke layanan UEM cloud eksklusif yang ditawarkan oleh Google. Meski begitu, beberapa platform UEM lainnya berintegrasi dengan Google sebagai layanan middleware.
- UEM juga dapat mengatur perangkat Rugged dan *wearables* (seperti kacamata pintar dan kacamata virtual reality (VR) atau *augmented reality* (AR)) yang menjalankan OS Android atau memperoleh kemampuan manajemen dari smartphone yang dipasangkan.
- Beberapa platform UEM juga dapat mengelola atau berintegrasi dengan desktop virtual.

3. Deployment dan Enrollment

Tim IT punya dua cara untuk mendaftarkan perangkat karyawan: manual atau otomatis. Untuk cara manual, perangkat didaftarkan satu per satu lewat komputer. Tapi sekarang ada cara yang lebih mudah, yaitu pendaftaran otomatis.

Ketika hampir semua perangkat modern dinyalakan untuk pertama kalinya, perangkat tersebut harus melakukan pendaftaran ke layanan cloud. Jika itu adalah perangkat perusahaan, perangkat tersebut dapat dialihkan ke platform UEM yang sesuai untuk mengkonfigurasinya secara otomatis. Setelah itu, perangkat siap digunakan oleh karyawan.

4. BYOD dan Privacy

Di banyak organisasi, perangkat iOS dan Android pribadi pengguna sering kali digunakan untuk bekerja. Praktik ini menimbulkan tantangan baru di bidang keamanan dan privasi data. Data pekerjaan yang sensitif bercampur dengan data pribadi dalam satu perangkat. Untuk mengatasi hal ini, banyak perusahaan menggunakan solusi UEM.

MAM pada UEM digunakan untuk menerapkan kebijakan perusahaan pada aplikasi dan data tertentu tanpa harus mengontrol seluruh perangkat. Aplikasi tersebut akan langsung terhubung ke server UEM, meskipun perangkat tersebut tidak terdaftar.

Platform UEM juga dapat membatasi peran administrator, sehingga hanya bisa mengakses perangkat yang berkaitan dengan pekerjaan. UEM akan mengeksekusi kebijakan perusahaan mengenai apa yang bisa dan tidak bisa dilakukan oleh pengguna.

Server UEM juga menjaga privasi pengguna dengan tidak menyimpan dan memantau hal-hal yang bersifat pribadi.

5. Manajemen Aplikasi Mobile

Protokol MDM memungkinkan UEM untuk mengelola aplikasi di perangkat secara mendetail. UEM bisa menginstal aplikasi baru, mengatur setting aplikasi, atau mengatur interaksi aplikasi perusahaan dengan aplikasi pribadi. Semua ini bisa dilakukan jika aplikasi tersebut memenuhi standar konfigurasi yang telah ditentukan.

Jika ada perangkat yang belum terdaftar, UEM tetap bisa mengelola aplikasi di dalamnya. Caranya adalah dengan menambahkan fitur manajemen langsung ke dalam aplikasi itu sendiri. Fitur seperti enkripsi, kata sandi, penghapusan jarak jauh, dan pengaturan keamanan lainnya bisa diintegrasikan ke dalam kode aplikasi. Namun, untuk melakukan ini, tim IT harus mengembangkan aplikasi tersebut secara khusus.

Agar proses pengembangan aplikasi lebih mudah, vendor UEM biasanya menyediakan aplikasi dasar seperti email dan browser. Mereka juga menawarkan alat pengembangan (SDK) agar perusahaan bisa membuat aplikasi sendiri yang kompatibel dengan UEM.

Selain itu, UEM menyediakan tempat untuk menyimpan aplikasi yang dibuat sendiri atau mengarahkan pengguna untuk mengunduh aplikasi dari toko aplikasi umum. Untuk mempermudah pengguna, UEM juga menyediakan katalog aplikasi yang bisa diakses sendiri oleh pengguna.

Katalog aplikasi di UEM tidak hanya sebatas daftar aplikasi. Beberapa platform UEM telah berkembang menjadi ruang kerja digital yang lengkap. Pengguna bisa mengakses berbagai aplikasi web dan seluler dengan satu kali login, menggunakan komputer desktop jarak jauh, dan memanfaatkan fitur tambahan seperti aplikasi mini, repositori konten, direktori perusahaan dan asisten virtual.

6. Manajemen Akses dan Identitas

Dengan semakin populernya aplikasi berbasis cloud (SaaS) dan penggunaan perangkat seluler, kebutuhan untuk mengelola akses dan identitas pengguna pun semakin kompleks. Sama seperti UEM hadir untuk mengelola perangkat, solusi manajemen IAM berbasis cloud muncul untuk mengatur identitas pengguna.

Standar seperti *Security Assertion Markup Language* (SAML) dan OAuth telah menjadi kunci dalam menyatukan identitas pengguna di berbagai aplikasi SaaS, memungkinkan fitur *Single Sign-On* (SSO) yang memudahkan pengguna. Seiring waktu, UEM dan IAM semakin terintegrasi. Beberapa platform UEM bahkan telah menyertakan fitur penyedia identitas sendiri.

Ada beberapa cara UEM dan IAM dapat bekerja sama. UEM dapat mendistribusikan sertifikat ke perangkat digital ke perangkat, yang kemudian dapat digunakan untuk memverifikasi identitas pengguna. Ini memastikan hanya perangkat yang terdaftar dan aman dapat mengakses data perusahaan.

Selain itu, SSO sangat penting untuk memberikan pengalaman pengguna yang mulus dan aman, terutama pada perangkat seluler dengan layar yang lebih kecil

UEM bisa memberikan konteks tambahan untuk akses dan autentikasi. Contohnya, kebijakan akses bersyarat dapat mempertimbangkan lokasi perangkat, status manajemen, dan faktor lainnya

sebelum memberikan akses, meminta faktor autentikasi tambahan, memblokir akses, atau melakukan tindakan lain.

7. Keamanan

Sistem operasi seluler memiliki model keamanan yang dari komputer desktop. Selalu terhubung ke internet dan rentan hilang, perangkat seluler memerlukan perlindungan ekstra.

OS seluler bersifat sandbox, dimana aplikasi diisolasi dalam lingkungan terbatas, mencegahnya menggangu aplikasi lain atau sistem operasi. Pengguna mengendalikan izin yang diberikan kepada setiap aplikasi, melindungi data sensitif. Aplikasi umumnya didapatkan dari toko aplikasi resmi yang telah melalui proses verifikasi ketat.

Sebagian besar tugas keamanan seluler adalah masalah pemantauan dan konfigurasi perangkat melalui MDM. MDM memungkinkan IT untuk melakukan berbagai tindakan dari jarak jauh, seperti memeriksa keberadaan aplikasi berbahaya, memastikan sistem operasi dan aplikasi selalu diperbarui, dan mengkonfigurasi pengaturan keamanan seperti enkripsi data dan koneksi VPN. Jika terjadi kehilangan atau pencurian, perangkat dapat dikunci atau dihapus datanya secara remote.

Organisasi juga perlu mengkhawatirkan phishing, rekayasa sosial, dan masalah identitas serta otentikasi lainnya pada perangkat seluler. *Mobile Threat Defense* (MTD) adalah solusi keamanan seluler untuk meningkatkan UEM.

MTD memeriksa integritas perangkat (meliputi jailbreak dan deteksi root), mengamankan jaringan untuk mencegah serangan man-in-the-middle, menganalisis reputasi aplikasi, dan melindungi dari serangan phising.

Pencegahan phishing sangat penting karena tampilan layar yang lebih kecil dan sifat aplikasi chatting yang real-time membuat pengguna lebih sulit mengenali serangan.

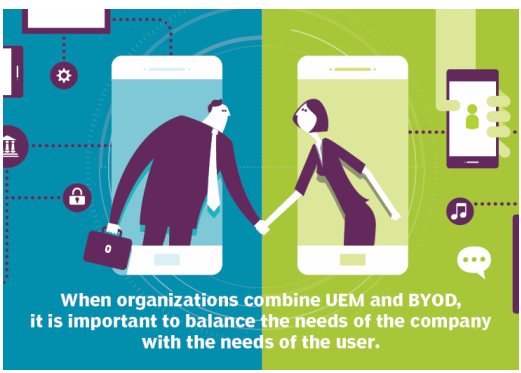
Penerapan MTD sangat diuntungkan dengan integrasi UEM, karena platform UEM dapat memberikan visibilitas yang lebih besar daripada aplikasi agen saja dan menawarkan berbagai cara untuk mengatasi ancaman.

Strategi Penerapan UEM

Menerapkan UEM membutuhkan perencanaan yang cermat, terutama karena melibatkan pengguna akhir, perangkat pribadi (BYOD), dan isu privasi. Sebelum memulai, penting untuk mengkomunikasikan secara jelas kepada karyawan apa saja yang dapat dan tidak dapat dilakukan oleh perusahaan pada perangkat pribadi mereka.

Ketika memperluas UEM ke Windows dan macOS, serangkaian tantangan baru muncul. Perusahaan harus memikirkan cara menerjemahkan kebijakan manajemen tradisional ke dalam kebijakan MDM, sambil mengadopsi platform manajemen perangkat baru.

Penerapan UEM bukanlah proyek yang selesai begitu saja. Ini adalah proses yang terus berkembang. Dengan adanya pembaruan rutin pada sistem operasi seperti iOS, Android, dan lainnya, serta perubahan sikap pengguna terhadap BYOD, perusahaan perlu secara berkala mengevaluasi dan menyesuaikan strategi UEM mereka.



Revolusi Digital di Surabaya: ACS Group Tampilkan Solusi Teknologi Masa Depan

Pada 17 Juli 2024, ACS Group Surabaya menjadi pusat inovasi digital dengan acara "*Go Digital for Optimal Innovation*," yang menyoroti solusi digital terbaru untuk mengoptimalkan kinerja dan inovasi di berbagai sektor industri dari MESPRO, eG Innovations, Huawei, dan Zebra Technologies.

MESPRO hadir dengan aplikasi MES (*Manufacturing Execution System*) yang revolusioner, memberikan kemampuan memantau dan mengontrol proses produksi secara real-time. Solusi ini bertujuan untuk meningkatkan kualitas produk serta mengurangi tingkat cacat, sehingga efisiensi manufaktur semakin optimal.

eG Innovations membuka presentasi dengan teknologi monitoring performa yang canggih, dirancang untuk membantu perusahaan dalam memantau dan mengoptimalkan kinerja aplikasi serta infrastruktur IT mereka. Solusi ini menjamin layanan digital beroperasi dengan lancar dan efisien.

Selanjutnya, Huawei memperkenalkan solusi jaringan inovatif, meningkatkan konektivitas dan fleksibilitas perusahaan. Teknologi ini memungkinkan pembangunan infrastruktur digital yang kuat dan scalable, menjawab kebutuhan masa depan.

Zebra Technologies melengkapi presentasi dengan berbagai solusi seperti tablet, machine vision, dan RFID. Solusi ini dirancang untuk meningkatkan efisiensi operasional dan akurasi, mencakup aplikasi dari manajemen inventaris hingga pelacakan aset.

Acara ini tidak hanya memberikan wawasan tentang solusi digital terbaru, tetapi juga membuka peluang kolaborasi bagi perusahaan yang ingin mengadopsi teknologi terkini. ACS Group Surabaya sukses menghadirkan acara inspiratif dan informatif, menegaskan komitmennya dalam mendukung transformasi digital di berbagai sektor industri.

Optimalkan Manajemen Rumah Sakit dengan Inovasi dari ACS Group di Acara PERSI Jateng

Perhimpunan Rumah Sakit Seluruh Indonesia (PERSI) Jawa Tengah kembali mengadakan acara tahunan yang diselenggarakan pada 22 - 24 Agustus di Grand Rama Patra Hotel & Convention Semarang. Dengan tema "Tantangan & Peluang Digitalisasi Per-rumah Sakit-an di Era *Healthcare* 5.0", acara ini menghadirkan inovasi dari ACS Group.

Dengan memperkenalkan *Laundry Tracking System* (LTS) yang dirancang untuk manajemen linen rumah sakit, mengoptimalkan manajemen linen dan pakaian rumah sakit, dari pencucian hingga distribusi, menggunakan teknologi RFID. Sistem ini menjanjikan efisiensi tinggi dengan meminimalisir kehilangan dan memastikan ketersediaan linen yang selalu siap pakai.

Selain itu, ACS Group bekerja sama dengan Ingram Micro membawa solusi Zebra Technologies yang menghadirkan perangkat keras seperti RFID *Fixed Reader* untuk pelacakan aset rumah sakit secara *real-time*, RFID *Mobile Reader* - Alat portabel yang mempermudah staf rumah sakit dalam melakukan pelacakan dan identifikasi aset di berbagai lokasi secara cepat dan akurat, *Barcode Printer* dan *Scanner* - Memastikan setiap data pasien dan aset dapat ditandai dan diakses dengan mudah, mendukung proses administrasi yang lebih efisien dan minim kesalahan.

Solusi ini dirancang untuk meningkatkan efisiensi operasional rumah sakit, memastikan pelacakan aset yang akurat, dan mengoptimalkan manajemen data, sehingga mendukung kesiapan rumah sakit dalam menghadapi era *Healthcare* 5.0.

Perkuat Jaringan, Perluas Kolaborasi: commIT Indonesia dan HPE Aruba Networking di Ulang Tahun Pertama

Komunitas perkumpulan IT seluruh Indonesia, commIT Indonesia, merayakan ulang tahun pertamanya di Holiday Inn Pasteur, Bandung. Didirikan sebagai wadah para profesional IT dari berbagai segmen, commIT Indonesia terus berupaya untuk memperkuat jaringan dan kolaborasi antar anggotanya, sejalan dengan tema acara tahun ini, "We Connect Better".

ACS Group yang bekerja sama dengan Sistech Kharisma untuk memamerkan solusi jaringan terdepan dari HPE Aruba Networking mewarnai event ini.

Rizwan Hermawan, selaku *Account Manager* dari Sistech Kharisma, menjadi salah satu pembicara utama yang membawakan presentasi mendalam mengenai solusi Instant On dan *Enterprise Solutions* - dipaparkan sebagai solusi jaringan yang mudah diimplementasikan dan sangat cocok untuk usaha kecil hingga *enterprise*, yang menawarkan kinerja tinggi dengan manajemen yang sederhana melalui aplikasi mobile. Beliau juga membahas mengenai implementasi *Security Service Edge* (SSE), bagian dari arsitektur SASE, yang mengintegrasikan keamanan jaringan dengan teknologi cloud untuk memberikan perlindungan maksimal terhadap ancaman siber.

Booth ACS Group menjadi salah satu titik fokus dalam acara ini. Para peserta memiliki kesempatan untuk melihat secara langsung demo unit HPE Aruba Instant On, *Controller*, dan *Switch*, yang dihadirkan untuk memberikan pengalaman langsung.

Dengan adanya kolaborasi antara ACS Group, Sistech Kharisma, dan HPE Aruba Networking, para profesional IT mendapatkan peluang emas untuk memperdalam pengetahuan dan memperluas jaringan, yang pada akhirnya akan memperkuat ekosistem IT di Indonesia.

PRODUCT HIGHLIGHT

FORTINET

FortiPAM

Industri : Semua industri.

Bagaimana ketika kita memiliki banyak vendor produk IT, dan pada waktu ke waktu perlu memberikan akses khusus kepada vendor tertentu? Akses yang bahkan karena sensitif dan sifatnya kritis, pada umumnya tidak diberikan kepada user internal seperti untuk perubahan pengaturan server, akses ke dalam data bisnis, menginstal/menghapus program, menambah/menghapus pengguna, atau mengubah pengaturan jaringan. Akses khusus ini tentunya harus sangat hati-hati diberikan, time-limited, dan perlu dimonitor aktifitasnya secara granular. FortiPAM dari Fortinet dengan konsep ZTNA dapat menjadi solusi komprehensif dan spesifik untuk keperluan ini.

HPE NETWORKING INSTANT ON

Access Point Wi-FI 6: AP22 (Indoor) dan AP27 (Outdoor)

Industri : AP22 - *Reimagined offices, Schools, Retail stores, and Hospitality*.
AP27 - *Education play space, Patios, and Curbside deliveries*.

Dapatkan pengalaman Wi-Fi terbaik dengan HPE Instant On AP22 dan AP27. Kedua perangkat ini dilengkapi teknologi Wi-Fi 6 terbaru, 802.11ax, 2X2:2, yang menawarkan kinerja *roaming* yang lebih baik dan koneksi yang lebih cepat tanpa *gateway* eksternal. AP22 ideal untuk penggunaan di dalam ruangan, sedangkan AP27 yang tangguh dirancang untuk kondisi luar ruangan yang paling menantang. Dirancang dengan IP Rating IP67, perangkat tahan terhadap debu dan kelembapan dalam kondisi yang paling menantang. Mampu menahan suhu dari -40°F hingga 149°F. *Access Point Outdoor* berkecepatan tinggi ini akan membuat Anda tetap terhubung dalam segala kondisi cuaca.

ZEBRA

ZD230TA 4-Inch Desktop Printer

Industri : Manufaktur kecil, Retail, Kesehatan, Transportasi, dan Logistik

Zebra ZD230TA adalah *printer* termal 4 inci yang menonjol dengan kualitas cetak tajam dan jelas, bahkan pada resolusi tertinggi 300 dpi. Dilengkapi fitur yang memudahkan penggunaan dan perawatan, *printer* ini dirancang untuk memberikan kinerja andal dalam jangka panjang. Dengan Zebra ZD230TA, Anda dapat mencetak label dengan kualitas profesional untuk memenuhi kebutuhan bisnis Anda.

INVANTI

Velocity Forms

Industri : *Cross Industry* selama menggunakan aplikasi WMS

Velocity Forms adalah solusi fleksibel untuk mengisi kebutuhan operasional di gudang yang menggunakan WMS. Tanpa perlu mengubah sistem WMS yang ada, Velocity Forms memungkinkan pengguna membuat *custom forms* untuk tugas-tugas seperti penanganan barang rusak atau daftar pemeriksaan awal shift. Formulir ini dibuat dengan mudah melalui Velocity Console lalu dipublikasikan ke *server* Ivanti Neurons untuk IIoT. Data yang terkumpul dapat diakses dan dianalisis secara *real-time*, sehingga memungkinkan otomatisasi berbagai proses. Keunggulan lain dari Velocity Forms adalah tidak memerlukan koneksi internet, tidak membutuhkan keahlian pemrograman, dan dilengkapi dengan lisensi *server* gratis. Selain itu, Velocity Forms juga dapat menampilkan gambar dan menganalisis data secara bebas, menjadikannya solusi yang lebih komprehensif dibandingkan dengan Google Forms atau Microsoft Forms.

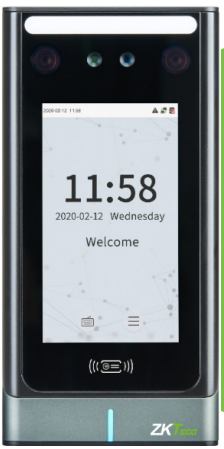
ZKTECO

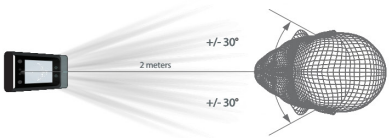
SpeedFace M2

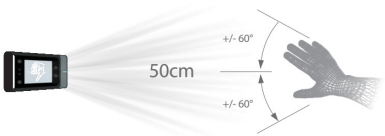
Industri : Semua Industri.

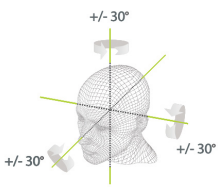
Merupakan perangkat akses kontrol *hybrid-biometrik* berbasis Linux yang menggabungkan teknologi pengenalan wajah dan telapak tangan. Mampu mendeteksi wajah berjarak hingga 2 meter dengan sudut pandang yang lebih luas, memungkinkan identifikasi yang lebih akurat. Selain itu, fitur pengenalan telapak tangan tanpa sentuh juga sangat akurat dengan toleransi sudut yang besar.

Fitur tambahan SpeedFace M2 meliputi pembacaan kartu NFC, pengaturan grup dan level akses, pencatatan kehadiran, serta fitur keamanan seperti alarm anti-perusakan dan verifikasi ganda. Dengan fitur ini, SpeedFace M2 menjadi solusi yang efisien untuk mengelola akses dan kehadiran di berbagai lingkungan.









Untuk penjelasan lebih detail lagi, Anda dapat menghubungi fitur chat kami di www.acsgroup.co.id.

Scan this QRcode

ADVERTORIAL

MESPRO®

The Ultimate Factory Intelligence

Membantu Anda Menuju Kesiapan Industri 4.0

Memberikan Kecerdasan Pabrik Secara Real-Time.

• Kami Memantau • Kami Menganalisa • Kami Mengoptimalkan

Menyajikan Kecerdasan Pabrik Secara *Real-time*.

Apakah Anda siap operasional manufaktur Anda dibawa ke tingkat berikutnya?

Dengan *software Manufacturing Execution System* (MES), kami siap merevolusi cara Anda mengelola proses produksi. Baik Anda sebagai produsen kecil sampai raksasa industri, MES kami dirancang untuk menghadirkan efisiensi, presisi, dan kontrol waktu nyata ke dalam kegiatan operasional Anda.

Dengan interface yang intuitif secara visual, notifikasi Andon secara *real-time*, dan pengukuran OEE yang komprehensif, MES akan membuka gerbang Anda menuju manufaktur yang optimal.

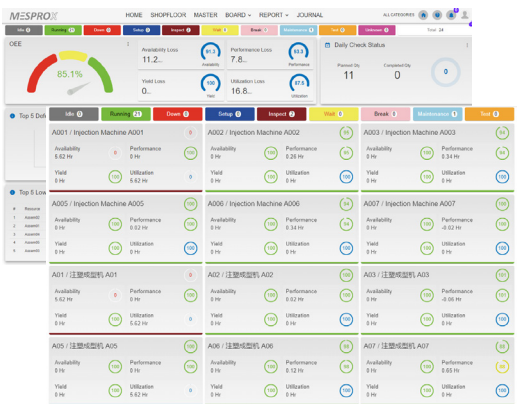
Fitur Utama MES

Visual Production Layout

MES dapat memantau seluruh lantai produksi Anda dengan mudah, lengkap dengan notifikasi Andon yang dinamis untuk mendapatkan update status yang *real-time*.

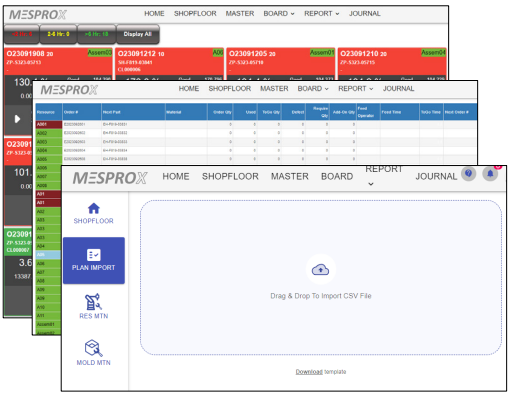
OEE Insights

MES dapat mengukur kinerja manufaktur Anda dengan presisi. Pahami ketersediaan, kinerja, dan kualitas untuk mendorong peningkatan berkelanjutan.



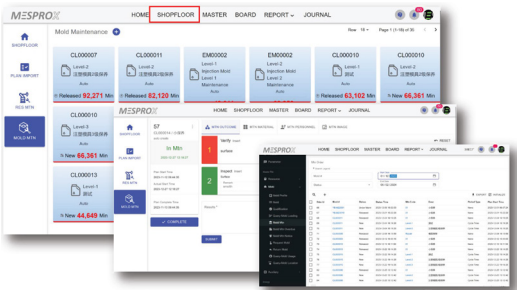
Perencanaan yang Mudah

MES menyederhanakan perencanaan produksi dengan mengimpor *spreadsheet*. Persiapkan kegiatan *shift*, harian, mingguan, atau bulanan dengan mudah.



Pemeliharaan yang Handal

- Membuat order pemeliharaan/perbaikan mesin
- Semua order & status pemeliharaan yang tertunda
- Operasi & pelaporan perintah pemeliharaan
- Log Pemeliharaan, Keterlambatan & Pemberitahuan



Real-time Analytics

Selalu mendapatkan informasi terkini performa proses produksi Anda.

Kami menghubungkan semua jenis mesin:

- CNC
- Injection Molding Die Casting
- Pressing
- Stamping
- Assembly
- Lainnya...

Scan this QRcode

Saksikan Video **MESPRO** dengan pembahasan santai dalam program Podcast **WARTEK (Warung Teknologi)** di channel Youtube kami.

DAN JANGAN LUPA

SUBSCRIBE !

Pameran Ritel Terbesar di Asia Pasifik di Singapura

Pameran ritel terbesar di dunia, NRF (*National Retail Federation*), biasanya diadakan setiap tahun di New York, Amerika Serikat. Namun, pada tahun ini, untuk pertama kalinya, acara bergengsi ini diadakan di Singapura, tepatnya di Marina Bay Sands Convention Center pada tanggal 11-13 Juni 2024. Tim ACS Group berkesempatan menghadiri acara ini untuk menyaksikan langsung perkembangan terkini teknologi yang digunakan dalam industri ritel, baik berupa perangkat lunak maupun perangkat keras.

Acara ini sangat dinantikan oleh para pelaku bisnis ritel di kawasan Asia Pasifik karena lokasinya yang lebih dekat dan mudah diakses. Beberapa hal menarik yang disajikan dalam pameran ini antara lain:

- **Sesi Inovasi:** Lebih dari 24 sesi menghadirkan inovasi terbaru dari para pemain utama di industri teknologi ritel. Inovasi-inovasi ini lahir dari ide-ide kreatif para peserta pameran.
- **Teknologi Terbaru:** Lebih dari 300 penyedia teknologi ritel memamerkan produk-produk terkini mereka, seperti kecerdasan buatan (AI), alat transaksi dengan desain futuristik, kamera otomatis untuk menghitung stok barang, dan masih banyak lagi.
- **Startup Inovatif:** Munculnya banyak startup di industri ritel menghadirkan angin segar dengan teknologi-teknologi yang revolusioner dan pemikiran yang radikal untuk mengubah wajah industri ritel.

PSMF ACS Group: Membangun Kolaborasi dan Inovasi untuk Solusi Terbaik dalam Layanan Profesional

Professional Service Management Forum (PSMF) adalah pertemuan tahunan yang diselenggarakan oleh ACS Group, yang berfungsi sebagai wadah bagi pemimpin *engineer* pusat dan cabang untuk bertukar pikiran, berbagi pengalaman, dan mempelajari teknologi terbaru. Selama dua hari, peserta mendalami materi yang relevan dengan kebutuhan pelanggan, seperti peningkatan kualitas layanan dan pembaruan teknologi, serta berbagi studi kasus untuk menemukan solusi terbaik bagi tantangan masing-masing cabang.

Setiap cabang memiliki karakteristik dan kompleksitas masalah yang berbeda, sehingga diskusi dalam forum ini sangat berharga untuk mengidentifikasi cara-cara paling efektif dan efisien dalam memberikan solusi bagi pelanggan. Forum ini menjadi ajang penting untuk memperkuat kolaborasi antar cabang dan pusat dalam upaya meningkatkan kualitas layanan.

PSMF juga memperkuat kolaborasi antar cabang dan pusat, serta mendorong budaya perusahaan yang dinamis dan kolaboratif. Melalui forum ini, diharapkan para engineer dapat berorientasi pada solusi, bekerja secara sistematis, dan saling bekerja sama untuk memberikan layanan terbaik kepada pelanggan.

Kolaborasi HPE Aruba dan ACS Group: Meningkatkan Kompetensi Partner melalui Sertifikasi

Untuk terus meningkatkan *performance level partner*, pada tanggal 7 Agustus 2024, dari HPE aruba melakukan kunjungan ke ACS Group Gunung Sahari, dihadiri oleh Yusie Mersyana, Partner Business Manager, bersama team Instant On yaitu Eister Corollina Machlon dan Reynard Henderson, Instant On Product Sales dan Product Specialist, disamping itu diperkenalkan juga *new Sales Territory Manager* (SMB), Ricky March. Pada kesempatan tersebut diadakan *enablement portal action* program dan sales sertifikasi yang dihadiri oleh team Markom dan juga team sales ACS, dimana 3 peserta dari sales team ACS berhasil mendapatkan 6 sertifikasi.

CINTA YANG SALAH

Seorang calon istri(CalIs) sedang merasa jengkel dengan calon suaminya(CalSu) karena sebulan lagi mereka akan menikah.

CalIs "Kenapa sih kamu gak bilang dari dulu klo kamu tuh semiskin ini haaahhh..?!"

CalSu "Aku kan udah bilang sayaanngg... Tapi, kamu aja yang gak denger & gak ngerti..!"

CalIs "Emang dulu kamu bilang apa sih ke aku?"(Penuh penasaran)

CalSu "Aku kan bilang, 'Sayang, cuma kamu satu-satunya yang kumiliki dan kupunya di dunia ini..'Eh, kamunya malah jawab 'so sweet'..."

CalIs #!?!%%...Ihhhhh.....

CalSu (Dengan merayu) "Tapi tetap aku sayang ko sama kamu Susan sayang"

KOLOM KETAWA

Tiba2 CalIs menampar CalSu... Plakkkk !!

CalIs "Apa kamu kamu bilang Susannnnnn...."

CalSu "Yakkkkk ampunnnnn... Maafkan daku Wulan sayang, aku keseleo"

CalIs "Youuu and Meee... Endddd.."

CalSu $$##%%&#&^^#

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

TIM PROFESSIONAL SERVICES KAMI TERUS MENINGKATKAN KOMPETENSI TEKNIS UNTUK SENANTIASA MENGHADIRKAN SOLUSI BERKUALITAS TINGGI BAGI PELANGGAN.

CERTIFIED

and many more...

JANGAN BIARKAN BATERAI UNIT ANDA SAMPAI HABIS!

by **Agung Atmoko**, Enterprise IT Solutions Supervisor | ACS Group

Sering ditemukan dari unit-unit yang masuk *repair* di ACS *Service Center* seperti unit *mobile computer* atau *portable printer* dalam kondisi **mati total**, hal ini dapat terjadi diakibatkan karena pengisian yang kurang optimal, baterai mati , ataupun *charger* yang tidak sesuai spesifikasi (*non-original*) atau bukan bawaan dari unit baru. Sebelum unit yang mati total tersebut dikirimkan ke ACS *Service Center,* cobalah langkah-langkah berikut:

1. **Isi Daya Ulang:**
   - Pastikan Anda menggunakan *charger* asli bawaan perangkat. *Charger non-original* bisa merusak baterai.
   - Jika indikator menyala, isi daya minimal selama 2 jam.
   - Setelah itu, nyalakan perangkat.
2. **Ganti Baterai:**
   - Jika perangkat masih tidak menyala, ganti baterainya dengan baterai yang sudah terisi penuh dan diketahui dalam kondisi baik.
   - Jika perangkat tetap tidak menyala, barulah bawa ke ACS *Service Center* terdekat.

Mengapa Baterai Penting Dirawat?

Baterai pada unit *mobile computer* atau *portable printer* memiliki masa pakai terbatas. Penggunaan yang terus-menerus, suhu yang ekstrem, dan usia baterai akan membuat performanya menurun.

- **Siklus Pengisian:** Setiap kali Anda mengisi daya baterai dari 0% hingga 100%, maka disebut satu siklus. Baterai umumnya dirancang untuk bertahan hingga 300-400 siklus.
- **Pentingnya Notifikasi:** Jangan abaikan notifikasi pengisian daya. Keseringan pengisian daya atau sering membiarkan baterai habis dapat merusak kinerja baterai.

Tips Merawat Baterai

- Hindari membiarkan baterai sampai habis total.
- Segera isi battery anda saat kondisi baterai 20%.
- Mengaktifkan mode *Smart Charging* bawaan unit jika ada.
- Simpan perangkat pada suhu ruangan (hindari suhu ekstrem).
- Gunakan *charger* asli.

Merawat baterai dengan baik akan memperpanjang umur perangkat Anda. Dengan mengikuti tips di atas, Anda dapat menghindari kerusakan pada perangkat dan menghemat biaya perbaikan. Jika Anda mengalami masalah dengan perangkat Anda, jangan ragu untuk menghubungi kami ACS *Service Center* terdekat untuk mendapatkan bantuan.

ACS GROUP PT. AUTOJAYA IDETECH PT. SOLUSI PERIFERAL

CORE BUSINESS SOLUTIONS: 4 PILLARS

1 **Automatic Identification & Data Capture (AIDC)**
IT peripherals such as: Barcode/RFID printers, Barcode/RFID readers or scanners, enterprise mobile printers, enterprise mobile computer (handheld, vehicle mount, tablet, wearable).

2 **IT Infrastructure & Cyber Security**
Network Devices (Access Point, Controller, Wired/Wireless), Hyper Converge Data Center, Public & Private Cloud, Cyber Security (Next-Gen Firewall, Network Access Control, Endpoint protection, OT).

3 **Enterprise Security System**
Access Control (+Turnstile, Barrier Gate), Surveillance (Enterprise IP Cam), Alarm system, Unified Command & Control Center.

4 **Enterprise Business Solution**
Software Package, Managed and Professional Services.

Alibaba Cloud · Allied Telesis · BarTender · brother at your side · eG Innovations · Extreme Connect Beyond the Network

FORTINET · Hewlett Packard Enterprise · HID · HIKROBOT · HIKVISION · HPE aruba networking

HUAWEI · Hytera · ivanti · JANZ · MOTOROLA SOLUTIONS · OPT Machine Vision

POINT Mobile · SAMSUNG · Seuic · SOLUM · tp-link · ZEBRA · ZKTeco Indonesia

Jakarta (Head Office)
Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221 - 4208221, 4205187
Email : sales.admin@acsgroup.co.id

Jakarta (Service Center)
Perkantoran Gunung Sahari Permai Blok E No. 3
Jl. Gunung Sahari No. 60 - 63, Kemayoran, Kota Administrasi Jakarta Pusat, DKI Jakarta - 10610
Telp : +6221 - 4208221, 4205187

Cikarang
Cikarang Square Blok E No 62, Jl. Raya Cikarang, Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221 - 29612366, 29612367
Email : adminckg@acsgroup.co.id

Semarang
Grand Ngaliyan Square Blok B No.18, Ngaliyan 50181, Semarang
Telp : +6224 - 76638092, 76638093
Email : adminsmg@acsgroup.co.id

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231 - 8556277, 8556278
Email : adminsby@acsgroup.co.id

Denpasar
Ruko Grand Sudirman Agung Blok B No.29,
Jl. PB Sudirman, Dauh Puri Kelod,
Denpasar Barat, Denpasar - Bali 80114
Telp : +62361 - 4457859
Email : admindps@acsgroup.co.id