NOLSATU

Buletin Edisi 70
April 2025

Untuk Kalangan Sendiri

Detak **Transformasi Digital**

by **ACS GROUP**

EMS & PAM dalam ZTNA

Pengamanan Akses **WFA ke Aplikasi** dan **Data Perusahaan**

E-BULETIN

MEDIA KOMUNIKASI
PELANGGAN

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

Daftar Isi

PEMIMPIN REDAKSI
- Andri S Kouanak

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

KONTRIBUTOR (PENULIS)
- Gusti Afriansyah
- Jemis Pangaribuan
- Julyani
- Arijanto Hartanto
- D. A. Ardy
- Nopah Hermanto
- Angelina Rasta P Ginting
- Agung Atmoko

EDITOR
- Arijanto Hartanto
- Afia Mien
- Angelina Rasta Perbina Ginting

ALAMAT REDAKSI

Jakarta (HO)
Perkantoran Gunung Sahari Permai
C # 03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.

T : +6221-4208221, 4205187
W: +628111 944 534
E : acs.marcom@acsgroup.co.id

Lihat Lokasi >

Hubungi >

Meja Redaksi

Salam,

Andri S Kouanak

Pemimpin Redaksi

PT. Autojaya Idetech

PT. Solusi Periferal

Para Pelanggan yang Terhormat,

Di tahun 2025 ini, kami menerbitkan buletin edisi-70, dengan nama yang baru yaitu NOL SATU. Nama ini merupakan dasar dari semua sistem komputer dan mencerminkan filosofi pertumbuhan yang dimulai dari sesuatu yang kecil hingga menciptakan dampak yang besar. Dengan harapan buletin dengan penampilan baru ini dapat membangun perubahan besar dari awal yang kecil, namun dengan pondasi yang kuat serta memberi pemahaman yang lebih lagi mengenai perjalanan teknologi TI. Mulai tahun 2025 ini, buletin kami akan terbit setiap 4 bulan sekali dalam setahun.

Pada era digital saat ini, kemudahan transaksi data menjadi tren baru dalam sistematika teknologi informasi. Data menjadi aset yang sangat berharga baik data personal maupun data perusahaan. Meskipun memberikan banyak kemudahan, namun hal ini patut diwaspadai. Karena disamping akses yang lebih gampang didapat, akan berdampak dengan potensi celah keamanan yang semakin terbuka, jika tidak dibarengi dengan sistem perlindungan keamanan data yang kuat.

Endpoint Management Server (EMS) dalam Zero Trust Network Access (ZTNA) serta Solusi Privileged Access Management (PAM) akan menjadi pembahasan utama pada buletin ini. Dengan EMS, organisasi dapat memiliki visibilitas yang lebih baik terhadap aktivitas jaringan dan merespons ancaman dengan lebih cepat, serta Privileged Access Management (PAM) membantu organisasi untuk mengontrol dan memantau aktivitas akun istimewa, mencegah penyalahgunaan, dan mengurangi risiko kebocoran data.

Dalam edisi 70 ini kami juga membahas Machine Vision, sebagai teknologi yang memungkinkan peralatan industri untuk melihat dan mendeteksi fitur atau cacat, sehingga memberikan panduan operasional ke perangkat. Sistem machine vision dapat menggunakan gambar yang diperoleh untuk membuat keputusan cepat untuk keputusan terbaik produksi, berdasar tangkapan visual machine vision.

Kami juga mengulas berbagai informasi kegiatan internal dan eksternal kami. Dengan harapan Buletin NOL SATU ini dapat memberikan informasi, pengetahuan serta masukan baru sehingga bisa membuka ruang kolaborasi kami bersama rekan - rekan bisnis sekalian di masa mendatang.

ZTNA

EMS ZTNA Dan PAM

Solusi Terpadu Untuk Mengamankan Aset Penting Perusahaan Di Era Digital

Pada masa digital saat ini, ancaman siber bukan sekedar isapan jempol belaka. Bahkan ancaman ini semakin besar dan canggih. Model konvensional *“trust but verify”* sudah tidak mampu lagi menjadi pelindung yang baik bagi data anda.

Perubahan dalam lanskap keamanan digital ini, memerlukan adanya pendekatan yang lebih baik lagi. Dalam dunia keamanan siber modern yang semakin komplek, konsep *Zero Trust Network Access (ZTNA)* sudah semakin populer. Teknologi ini menjadi makin diminati, karena menawarkan pendekatan yang lebih aman, dalam pengelolaan akses ke jaringan dan aplikasi, tanpa mengedepankankan kepercayaan implisit. Anda tentu penasaran bukan tentang bagaimana ZTNA lebih dalam, serta manfaatnya bagi organisasi? Mari ikuti ulasan berikut ini:

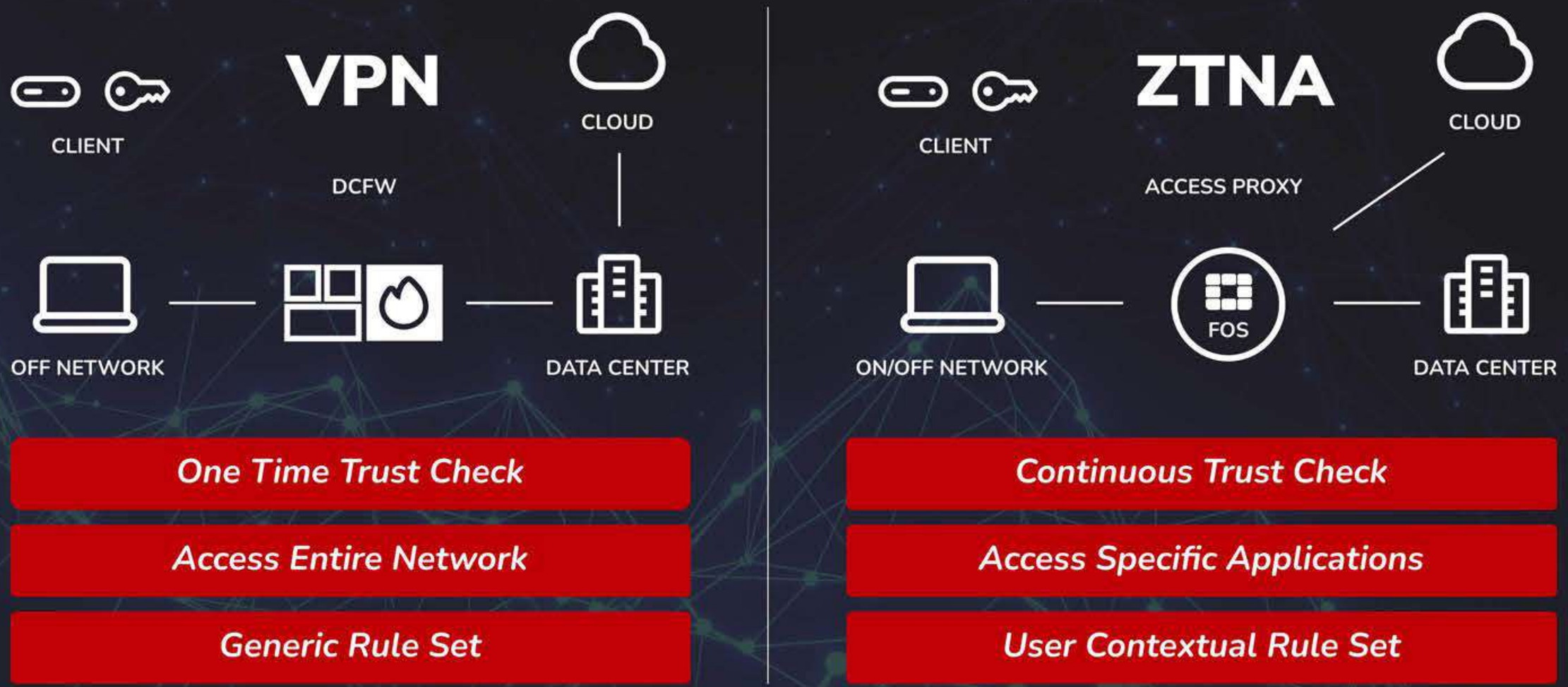
Mengenal Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) adalah pendekatan keamanan jaringan yang tidak menganggap ada entitas yang dapat dipercaya secara otomatis, baik di dalam maupun di luar jaringan. ZTNA mengharuskan setiap pengguna (internal maupun external) dan perangkat untuk diverifikasi secara berulang dan konsisten sebelum diberikan akses ke dalam jaringan.

Perbedaan ZTNA Dengan System Keamanan Tradisional

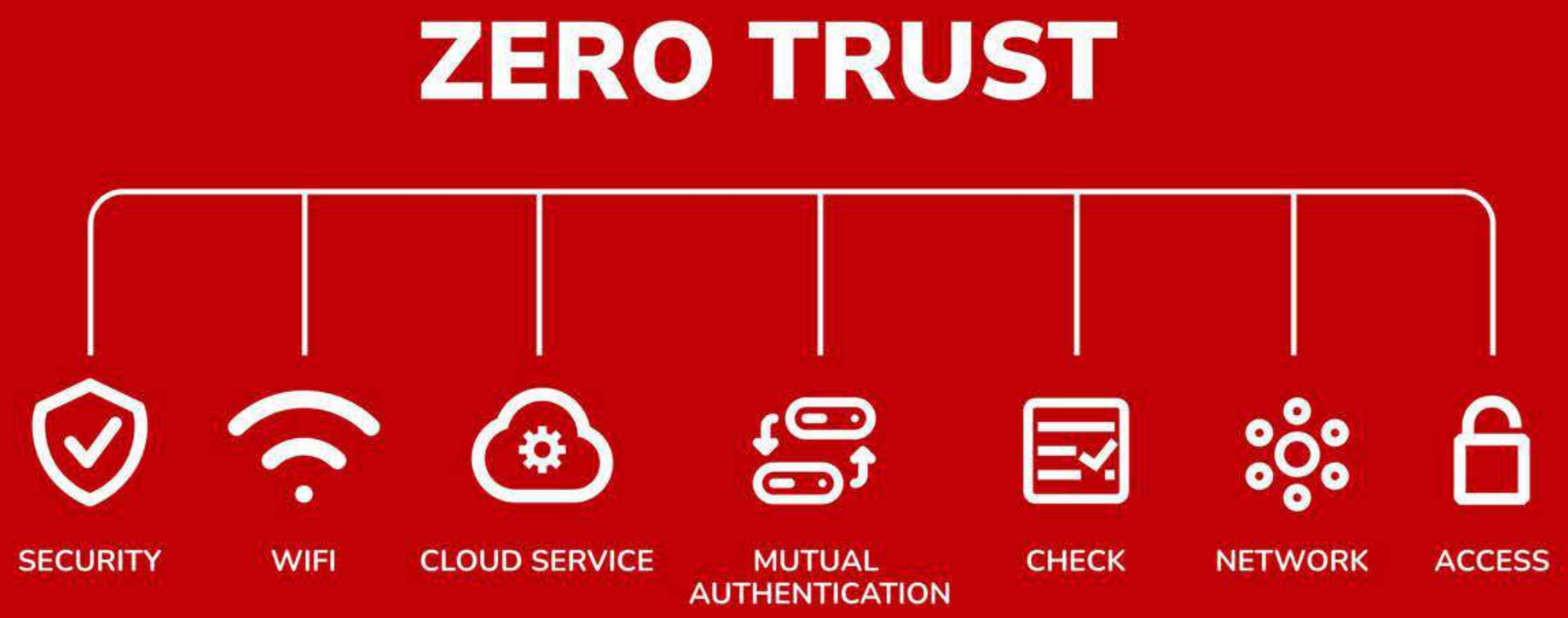
Sistem keamanan siber tradisional seringkali mengandalkan perimeter jaringan yang dikendalikan dengan Firewall, dalam model tradisional ini ancaman dari dalam jaringan bisa luput dari perhatian, sebaliknya ZTNA mengadopsi model dimana tidak ada kepercayaan yang diberikan kepada pengguna atau perangkat, hingga mereka berhasil diverifikasi. Hal tersebut membuat ZTNA lebih unggul dalam menangkal ancaman dari dalam jaringan. ZTNA memberikan batasan akses dan segmentasi jaringan, dimana pengguna hanya diberikan ijin untuk mengakses aplikasi dan data yang relevan, hal tersebut dapat mengurangi resiko penyalahgunaan akses dan serangan siber.

Dalam menghindari ancaman eksternal dan internal, ZTNA mewajibkan setiap akses untuk menjalani otentikasi dan otorisasi, terlepas dari lokasi pengguna atau lingkungan jaringan baik pengguna yang berasal dari dalam jaringan ataupun pengguna yang berasal dari luar jaringan. Hal tersebut bisa dijalankan dengan *Work From Home (WFH)* ataupun *Work From Anywhere (WFA)*



Bagi organisasi atau perusahaan yang memiliki lingkungan jaringan yang dinamis, dimana diperlukan solusi yang fleksibel serta dapat diskalakan, ZTNA menawarkan fleksibilitas ini untuk mengadaptasi perubahaan dan memperluas jaringan tanpa mengurangi tingkat keamaman.

Dengan berkembangnya perubahan atau tren dalam mengakses jaringan, ZTNA dapat memberikan pengalaman pengguna akses yang lebih aman , serta tidak mengurangi kecepatan akses. ZTNA memungkinkan pengguna bisa mengakses jaringan mereka dengan lebih cepat. Sebagai informasi, bahwa ZTNA merupakan bentuk evolusi dari tradisional akses yang kita kenal dengan *VPN (Virtual Private Network)*.



Manfaat Dari Penerapan ZTNA?

ZTNA tidak hanya memberi perlindungan tambahan tetapi juga meningkatkan efisiensi operasional. Berikut ini beberapa manfaat utama dari ZTNA:

1 Meningkatkan Level Keamanan

ZTNA akan mampu meningkatkan rasio keamanan dengan mengurangi resiko akses ilegal. Setiap akses didasarkan pada otentifikasi ketat, sehingga meminimalisir ancaman atau adanya anomali di dalam jaringan model adaptif dari ZTNA. Dimana kepercayaan tidak pernah diberikan secara implisit, menjadikan keamanan lebih kuat.

2 Menambah Keamanan Akses Jarak Jauh

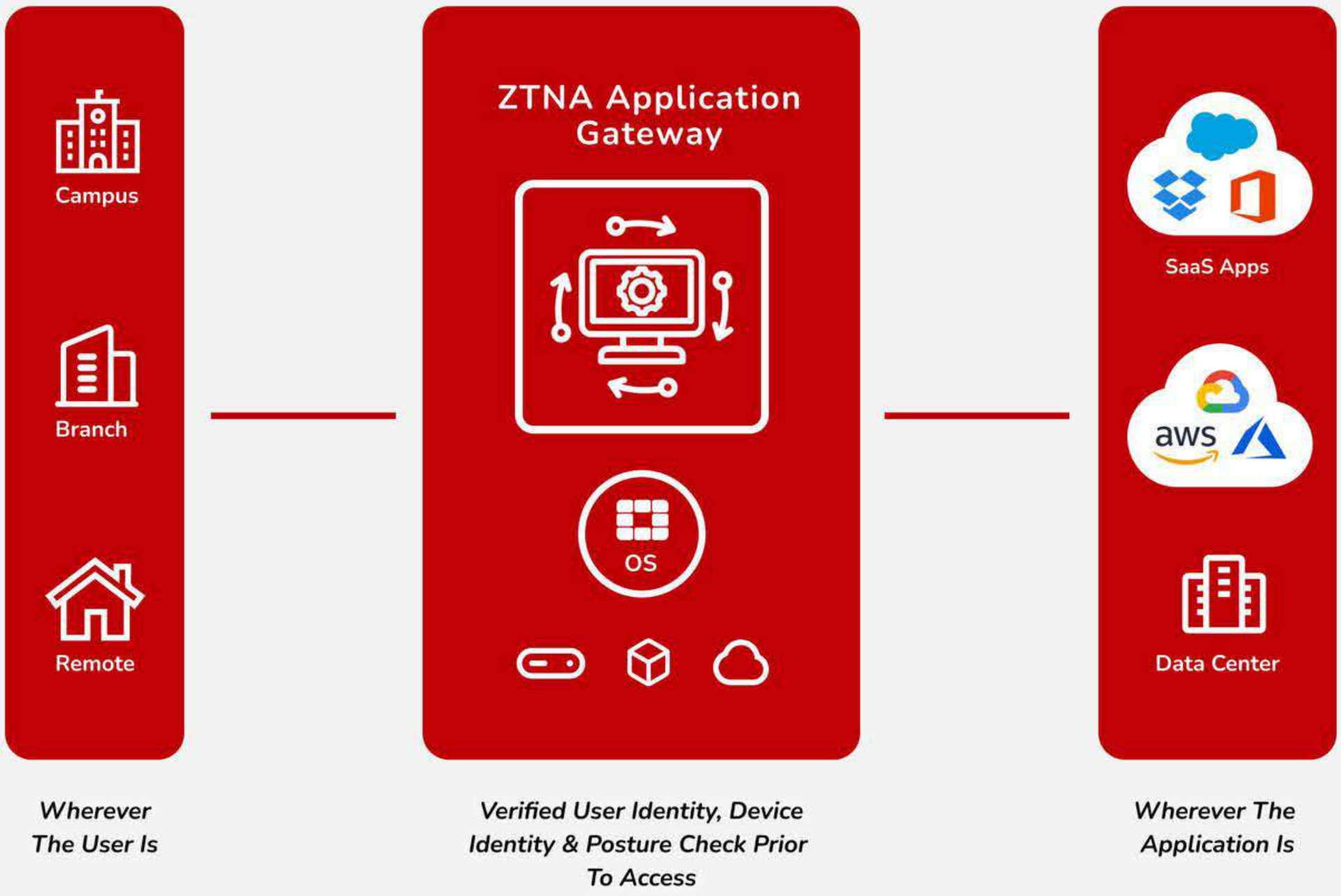
ZTNA juga memastikan akses yang aman bagi pengguna jarak jauh. Berbeda dengan VPN tradisional, ZTNA bekerja dengan memberikan akses hanya kepada aplikasi yang dibutuhkan, tanpa membuka seluruh jaringan. Hal ini menambah lapisan keamanan yang sangat diperlukan di era kerja jarak jauh (*remote*) sekarang ini.

3 Pengelolaan Akses Yang Lebih Baik

Dengan ZTNA, pengelolaan akses menjadi lebih baik dan cepat. Setiap permintaan akses dikendalikan berdasarkan identitas dan konteks, memungkinkan kontrol yang lebih tepat dan sesuai kebutuhan. Ini membantu dalam mengurangi risiko dan meningkatkan standar keamanan keseluruhan.

Bagaimana Cara Kerja **ZTNA?**

Prinsip dan strategi keamanan *Zero Trust* beroperasi dengan penerapan, bahwa akan selalu ada ancaman konstan baik dari luar maupun di dalam jaringan, ZTNA juga berasumsi bahwa setiap upaya untuk mengakses jaringan atau aplikasi adalah ancaman. Filosofi keamanan jaringan ini menyatakan bahwa tidak seorangpun di dalam atau di luar jaringan bisa dipercaya sampai identitas mereka diverifikasi secara penuh. **Asumsi ini menjadi dasar strategi administrator jaringan, yang mengharuskan untuk merancang langkah-langkah keamanan yang ketat, dengan prinsip tidak pernah percaya atau *zero trust*.**



Perangkat lunak yang berfungsi sebagai penghubung, yang dipasang di jaringan perusahaan dengan demikian setiap koneksi yang berjalan dalam jaringan tersebut bisa dipastikan bersih dari ancaman. Karena dengan keberadaan teknologi tunneling yang terenkripsi untuk kebijakan akses baik yang berasal dari dalam jaringan itu sendiri maupun dari luar jaringan. Di sinilah poin dari akses *zero trust* dan bertanggung jawab untuk:

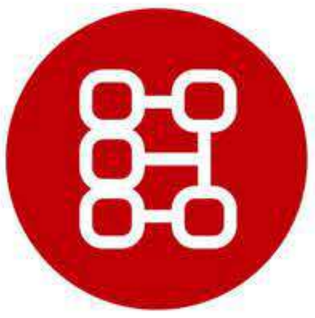
Users, sebagai langkah pertama dalam upaya keamanan menggunakan strategi ini memerlukan autentikasi identitas pengguna yang kuat dan verifikasi integritas perangkat pengguna.

Applications, konsep dasar dari penerapan strategi ini adalah bahwa aplikasi tidak dapat dipercaya sehingga butuh pemantauan berkelanjutan saat runtime untuk memvalidasi perilaku dari aplikasi tersebut

Infrastructure, segala sesuatu yang berhubungan dengan infrastruktur seperti *router, switch, cloud, IoT* yang harus ditangani dengan pendekatan ini

Verify Users

Validate Devices



Limited Priveleged Access

Pengelolaan Akses Yang Lebih Baik

Karena koneksi outbound atau koneksi yang terjadi “dari dalam ke luar”, ke layanan ZTNA, network administrator tidak perlu lagi membuka port Firewall Inbound untuk akses aplikasi, hal ini dapat melindunginya dari paparan terhadap virus atau malware yang ada di internet publik, serta mengamankan dari serangan D-Dos dan serangan lainnya.

ZTNA juga dapat melayani atau mengcover perangkat yang dikelola, atau yang tidak dikelola secara traffic, untuk perangkat yang dikelola oleh ZTNA, mengikuti pendekatan berbasis klien. Dimana klien atau agen yang dimiliki perusahaan dipasang pada perangkat. Pada hal ini, Klien bertanggung jawab untuk mengambil informasi terhadap perangkat -

tersebut dan membagikan detailnya dengan layanan ZTNA. Koneksi dibuat dengan aplikasi pada validasi identitas pengguna dan postur keamanan perangkat.

Penerapan prinsip zero trust tidak selalu harus memulai atau membangun jaringan dari awal, karena merancang strategi zero-trust adalah bagaimana kita memasang kerangka kerja yang tepat dengan alat yang tepat sebagai solusi keamanan.
Sebagai organisasi atau perusahaan juga perlu berkomitmen untuk mengubah cara akses yang selama ini diterapkan, serta bagaimana cara menjaga keamanan di seluruh lingkungan atau jaringan internal perusahaan.

Sebagai contoh, bagaimana ZTNA bekerja adalah dimulai dari sebuah perangkat user yang akan mencoba melakukan akses terhadap server atau aplikasi tertentu yang ada di dalam lingkungan jaringan sebuah organisasi atau perusahaan. Yaitu, sebelum perangkat diterima masuk ke dalam area network ZTNA, perangkat yang dimaksud akan diperiksa terlebih dahulu, apakah perangkat tersebut sudah memenuhi level keamanan perangkat user yang sudah diterapkan sebelumnya oleh ZTNA hal ini yang sering disebut rule tagging atau tidak.

Jika perangkat user tersebut sudah memenuhi level keamanan yang diterapkan oleh rule tagging ZTNA, maka perangkat tersebut akan diperbolehkan masuk dan mengakses server atau aplikasi yang dituju lebih lanjut. Namun, apabila perangkat tersebut tidak dapat memenuhi level keamanan yang sudah diterapkan ZTNA maka akses tersebut akan di *drop*, atau tidak diberikan akses lebih lanjut.

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

Langkah selanjutnya adalah, dengan memahami siapa penggunanya, aplikasi mana yang mereka gunakan dan bagaimana mereka terhubung? Penggunaan sistem keamanan ini akan mendorong proses verifikasi yang sangat ketat. Verifikasi ini dilakukan untuk setiap user dan device yang berupaya mengakses jaringan.

Endpoint Management Server Dalam **ZTNA**

Apa itu *Endpoint Management Server (EMS)*? Implementasi ZTNA yang efektif membutuhkan sistem yang dapat mengelola dan mengamankan semua titik awal akses, yaitu apa yang disebut dengan endpoint. Disinilah peran *Endpoint Management Server (EMS)* menjadi sangat penting. EMS memungkinkan organisasi untuk mengelola penuh akses serta aman dari perangkat endpoint seperti laptop, smartphone, dan tablet yang terhubung ke jaringan.

Sistem EMS yang baik menawarkan berbagai kemampuan yang memperkuat keamanan jaringan dan menyederhanakan manajemen endpoint. Berikut adalah beberapa fitur utama yang dimiliki endpoint:

1 Visibilitas Dan Kontrol Yang Komprehensif

Inventarisasi Perangkat
EMS secara otomatis mendeteksi dan menginventarisasi semua perangkat yang terhubung ke jaringan, memberikan visibilitas penuh atas aset Teknologi Informasi (TI) organisasi.

Penilaian Kerentanan
EMS ini mampu melakukan pemindaian kerentanan pada endpoint untuk mengidentifikasi dan mengatasi potensi risiko keamanan.

Manajemen Patch
EMS dapat mengotomatisasi proses patching perangkat lunak untuk memastikan endpoint selalu diperbarui dengan patch keamanan terbaru.

2 Otentikasi Dan Kontrol Akses Yang Kuat

Multi-Factor Authentication (MFA)
EMS secara otomatis mendeteksi dan menginventarisasi semua perangkat yang terhubung ke jaringan, memberikan visibilitas penuh atas aset Teknologi Informasi (TI) organisasi.

Kontrol Akses Berbasis Peran
Akses ke sumber daya jaringan diberikan berdasarkan peran pengguna, memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi sensitif. Dalam hal ini EMS mengarahkan akses ke suatu tujuan yang spesifik, seperti contohnya, tim Marketing tidak diizinkan mengakses aplikasi tim *finance*. Meski begitu, EMS dapat terintegrasi dengan manajemen identitas seperti *LDAP (Lightweight Directory Access Protocol) atau Active Directory)*

Posture Assessment
Sebelum memberikan akses, EMS dapat memeriksa postur keamanan perangkat, seperti status antivirus, firewall, dan enkripsi disk.

3 Manajemen Aplikasi Dan Perangkat Lunak

Deployment Aplikasi
EMS memungkinkan administrator TI untuk mendistribusikan dan menginstal aplikasi secara remote ke endpoint.

Pembatasan Aplikasi
Sistem ini dapat membatasi penggunaan aplikasi tertentu pada endpoint untuk mencegah eksekusi program yang tidak sah.

Kontrol Perangkat
EMS dapat mengontrol penggunaan perangkat periferal seperti USB drive dan printer untuk mencegah kebocoran data.

4 Keamanan Data Yang Terintegrasi

Enkripsi Data
EMS dapat mengenkripsi data sensitif pada endpoint untuk melindungi informasi dari akses yang tidak sah.

Data Loss Prevention (DLP)
Sistem ini dapat mencegah kebocoran data dengan memantau dan memblokir transfer data sensitif.

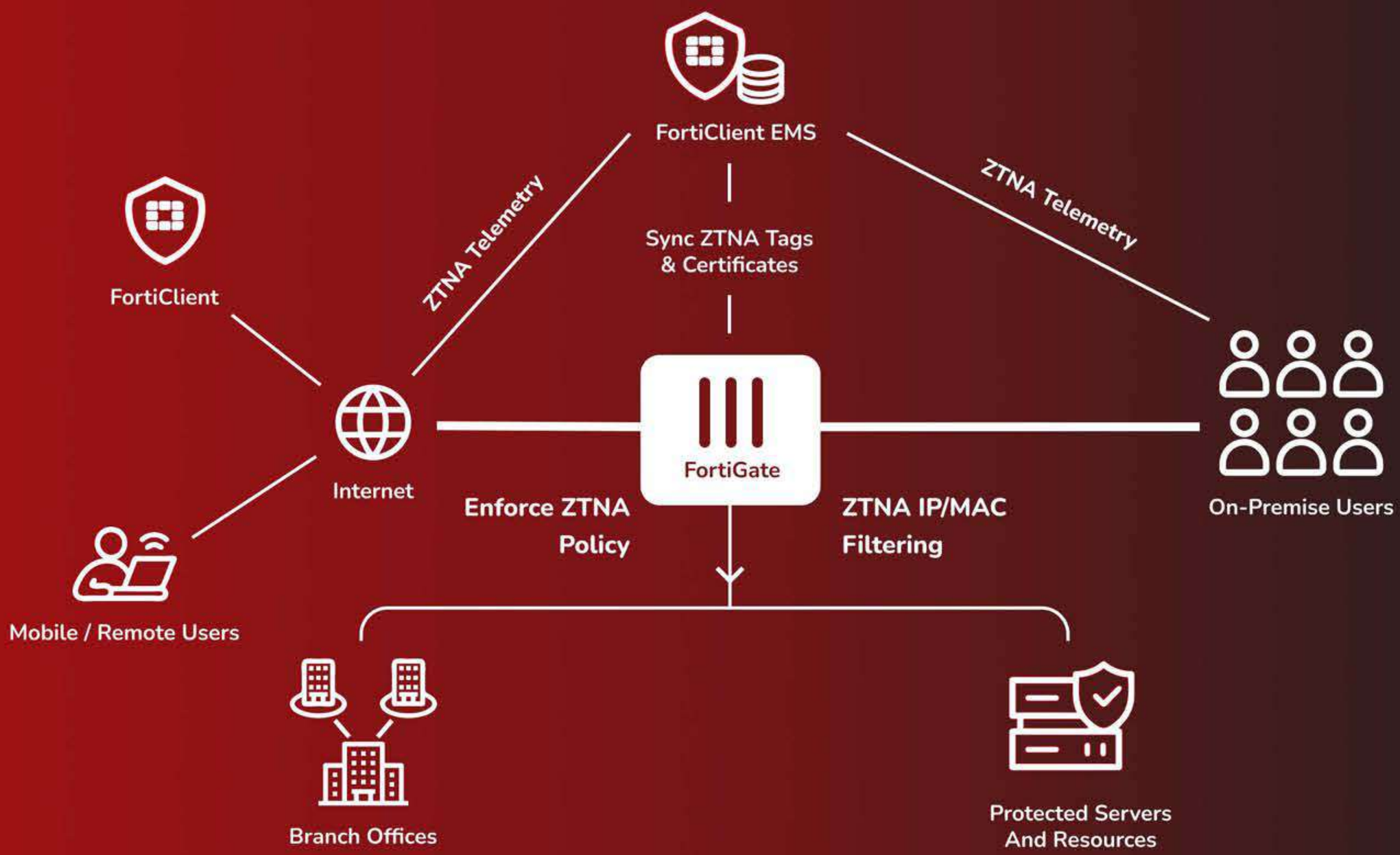
Mobile Device Management (MDM)
EMS menyediakan fitur MDM untuk mengamankan dan mengelola perangkat mobile seperti smartphone dan tablet.

5 Kemudahan Penggunaan Dan Otomatisasi

Deployment Aplikasi
EMS memungkinkan administrator TI untuk mendistribusikan dan menginstal aplikasi secara remote ke endpoint.

Pembatasan Aplikasi
Sistem ini dapat membatasi penggunaan aplikasi tertentu pada endpoint untuk mencegah eksekusi program yang tidak sah.

Kontrol Perangkat
EMS dapat mengontrol penggunaan perangkat periferal seperti USB drive dan printer untuk mencegah kebocoran data.



EMS Manage ZTNA Traffic

Bagaimana **EMS** Berhubungan Dengan **ZTNA?**

ZTNA, seperti yang telah kita bahas sebelumnya, adalah model keamanan yang sangat bergantung pada status dan keamanan perangkat (*endpoint*). EMS berperan kunci dalam mewujudkan prinsip ZTNA dengan menggunakan pendekatan:

Inventarisasi Perangkat
EMS memberikan daftar lengkap semua perangkat yang terhubung ke jaringan. Ini memungkinkan organisasi untuk mengetahui perangkat mana yang perlu dilindungi dan diatur.

Pengelolaan Kebijakan
EMS memungkinkan administrator untuk menetapkan kebijakan keamanan yang berbeda-beda untuk setiap jenis perangkat atau kelompok pengguna. Kebijakan ini dapat mencakup persyaratan patch, antivirus, firewall, dan lainnya.

Pemantauan Keamanan
EMS akan secara kontinu memantau status keamanan perangkat, seperti adanya malware, konfigurasi yang tidak aman, atau perangkat lunak yang tidak diperbarui.

Pengelolaan Remote
EMS memungkinkan administrator untuk mengelola perangkat dari jarak jauh, seperti menginstal perangkat lunak, memperbaiki masalah, atau menghapus data jika diperlukan.

Enforce ZTNA Policies
EMS dapat terintegrasi dengan solusi ZTNA untuk memastikan bahwa hanya perangkat yang memenuhi persyaratan keamanan yang dapat mengakses sumber daya jaringan.

Fitur Utama **EMS** Dalam Konteks **ZTNA?**

ZTNA, seperti yang telah kita bahas sebelumnya, adalah model keamanan yang sangat bergantung pada status dan keamanan perangkat (endpoint). EMS berperan kunci dalam mewujudkan prinsip ZTNA dengan menggunakan pendekatan:

Inventarisasi Perangkat yang Komprehensif
Memetakan semua perangkat yang terhubung, termasuk perangkat yang tersembunyi atau tidak dikenal.

Pengelolaan Patch
Memastikan semua perangkat memiliki patch keamanan terbaru.

Pengelolaan Antivirus
Memastikan semua perangkat dilengkapi dengan antivirus yang aktif dan diperbarui.

Pengelolaan Konfigurasi
Menerapkan konfigurasi keamanan yang konsisten di seluruh perangkat.

Pemantauan Perangkat
Melacak aktivitas perangkat dan mendeteksi anomali.

Pengelolaan Aset
Melacak siklus hidup perangkat dari awal hingga akhir.

Integrasi dengan ZTNA
Berkomunikasi dengan solusi ZTNA untuk memastikan bahwa hanya perangkat yang memenuhi persyaratan keamanan yang dapat mengakses sumber daya.

Privilege Access Management **(PAM)**

Industri manufaktur modern sangat bergantung pada teknologi informasi, mulai dari sistem kontrol produksi hingga manajemen rantai pasokan. Seiring dengan meningkatnya konektivitas dan otomatisasi, risiko keamanan siber juga semakin besar. Salah satu aspek krusial dalam mengamankan infrastruktur TI adalah *Privilege Access Management*.

PAM adalah pendekatan keamanan yang berfokus pada pengelolaan dan perlindungan akses istimewa, yaitu akses yang dimiliki oleh pengguna dengan hak istimewa tinggi seperti administrator IT. Pengguna ini memiliki akses ke sistem dan data yang kritis, sehingga penyalahgunaan akses mereka dapat mengakibatkan dampak yang sangat merugikan bagi organisasi.

Apa Itu Privilege Access Management (PAM)?

PAM adalah serangkaian kebijakan, prosedur, dan alat yang digunakan untuk mengelola, mengontrol, dan memonitor akses ke akun-akun dengan hak istimewa dalam sebuah organisasi. Akses ini mencakup akun yang memiliki kontrol penuh terhadap sistem dan aplikasi, seperti akun administrator (admin), akun root di sistem berbasis Unix/Linux, dan akses yang digunakan untuk melakukan perubahan besar pada infrastruktur TI (misalnya, database, jaringan, dan aplikasi kritikal). PAM berfokus pada:

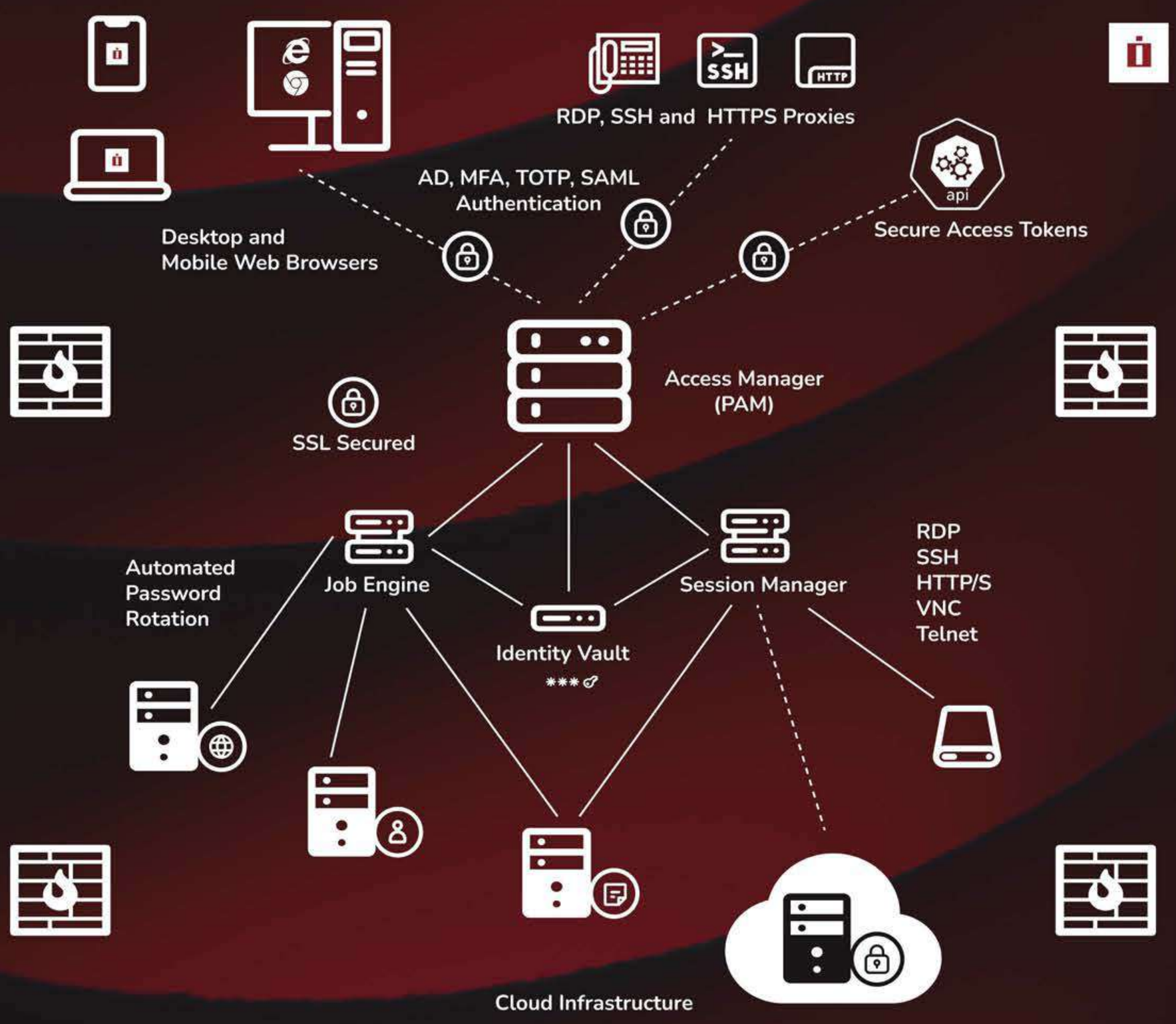
1 Mencegah Penyalahgunaan Akses

Akun-akun dengan hak istimewa memberikan kemampuan untuk mengubah konfigurasi sistem, mengakses data sensitif, dan bahkan menginstal perangkat lunak berbahaya. Jika tidak diawasi dengan baik, akun-akun ini bisa dieksploitasi, baik oleh pihak internal yang tidak bertanggung jawab maupun oleh penyerang eksternal.

2 Mengurangi Risiko Keamanan

Banyak pelanggaran data besar yang terjadi akibat akses yang tidak sah ke akun-akun privileged. PAM bertujuan untuk mengurangi risiko ini dengan memberikan kontrol ketat terhadap siapa yang dapat mengakses akun tersebut, bagaimana mereka dapat mengaksesnya, dan apa yang dapat mereka lakukan setelah mendapatkan akses.

Arsitektur Priviledge Access Management



Komponen Utama Dalam PAM

Untuk mengimplementasikan PAM yang efektif, ada beberapa komponen utama yang harus dimiliki dalam sistem manajemen akses istimewa, di antaranya:

1 Manajemen Akun Privileged

Akun *privileged* adalah akun dengan hak akses penuh terhadap sistem dan aplikasi, yang biasanya hanya diperlukan oleh administrator atau pemelihara sistem. PAM berfungsi untuk:

- **Mendeteksi dan mencatat akun privileged di seluruh infrastruktur.**
- **Membatasi siapa yang dapat membuat atau mengelola akun *privileged*.**
- **Mengelola siklus hidup akun tersebut, termasuk pembuatan, penghapusan, dan rotasi kata sandi.**

2 Manajemen Kata Sandi (Password Management)

Manajemen kata sandi yang kuat sangat penting dalam PAM. Karena kata sandi yang digunakan pada akun privileged sering kali menjadi target utama bagi penyerang. Beberapa praktik yang digunakan dalam manajemen kata sandi pada PAM seperti halnya:

Securely Encrypted Vault

Penyimpanan digital yang dilindungi dengan enkripsi kuat untuk menyimpan data sensitif, seperti kata sandi, informasi pribadi, atau data penting lainnya. Vault ini memastikan bahwa hanya pengguna yang sah yang dapat mengakses informasi tersebut dengan menggunakan kunci enkripsi atau kata sandi master. Enkripsi yang digunakan di vault ini mencegah akses dari pihak yang tidak berwenang, bahkan jika data tersebut dicuri atau disusupi.

Master Key for Access

Kata sandi atau kunci utama yang digunakan untuk membuka atau mengakses sistem keamanan yang lebih besar, seperti *password manager*, vault terenkripsi, atau aplikasi yang menyimpan informasi sensitif. Master key ini berfungsi sebagai "pintu gerbang" untuk mendapatkan akses ke seluruh data yang disimpan dalam sistem yang dilindungi, dan hanya individu yang sah yang memiliki akses ke kunci ini.

Sufficient amount of storage

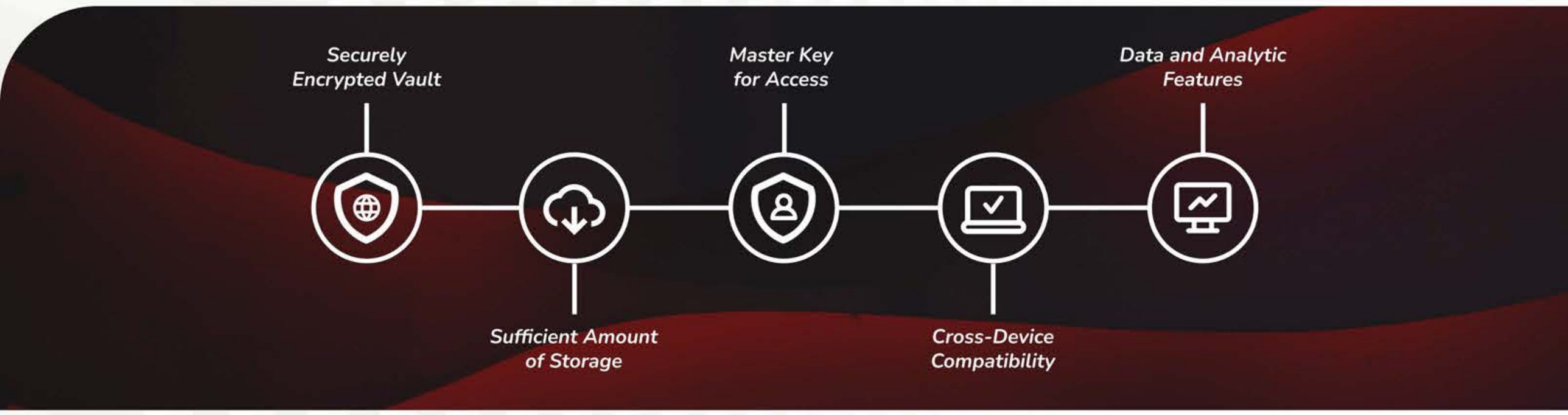
Merujuk pada jumlah ruang penyimpanan yang cukup untuk menyimpan data atau informasi yang dibutuhkan oleh sistem atau aplikasi, tanpa mengalami masalah keterbatasan kapasitas yang dapat mengganggu kinerja atau fungsionalitasnya.

Cross-device compatibility

Merujuk pada kemampuan sebuah aplikasi, sistem, atau perangkat untuk berfungsi dengan baik di berbagai perangkat atau platform yang berbeda, seperti komputer desktop, laptop, smartphone, tablet, atau bahkan perangkat lain seperti smartwatch atau perangkat IoT.

Data and Analytics Features

Kemampuan PAM dalam mengelola kata sandi dengan mengumpulkan, menganalisis, dan menyajikan data yang relevan terkait penggunaan kata sandi, keamanan, dan aktivitas pengguna. Fitur ini memungkinkan pengguna atau administrator untuk memperoleh wawasan tentang pola keamanan, penggunaan kata sandi, dan potensi risiko.



3 Kontrol Akses Berdasarkan Kebutuhan *(Least Privilege)*

Prinsip Least Privilege mengharuskan bahwa pengguna atau aplikasi hanya diberikan akses yang diperlukan untuk melaksanakan tugas mereka. Dalam konteks PAM, hal ini berarti:

Pembatasan akses
ke aplikasi atau sistem hanya pada pengguna yang benar-benar membutuhkan akses tersebut.

Pembatasan durasi akses
Menggunakan hak istimewa hanya untuk waktu yang diperlukan, setelah itu akses tersebut dicabut.

Segmentasi akses
Mengelompokkan pengguna ke dalam kategori berdasarkan level akses yang diperlukan.

4 Pemantauan Dan Pencatatan Aktivitas *(Session Monitoring And Logging)*

Pemantauan kontinu terhadap sesi akses privileged sangat penting untuk mendeteksi aktivitas yang mencurigakan. Komponen ini mencakup:

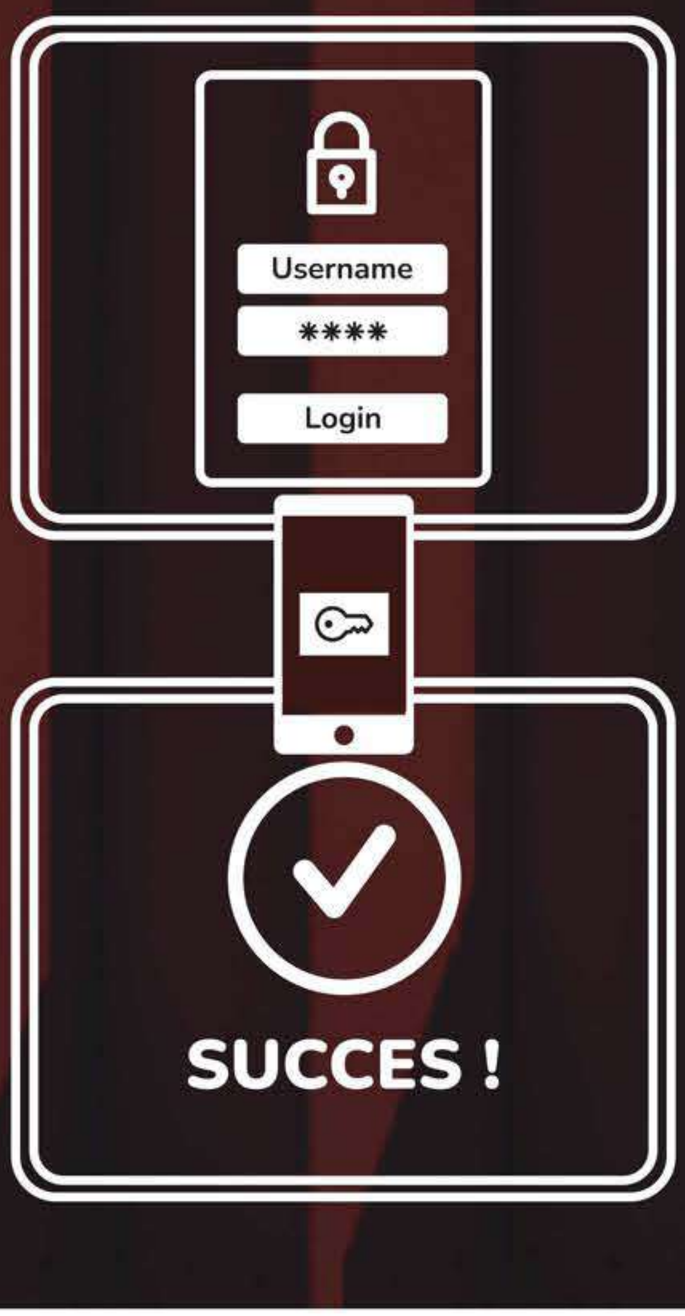
Pencatatan aktivitas
(audit logs) yang merekam semua tindakan yang dilakukan oleh pengguna dengan akses istimewa.

Pemantauan *real-time*
yang memungkinkan administrator untuk mendeteksi dan merespons potensi penyalahgunaan dengan cepat.

Rekaman sesi
untuk memungkinkan analisis forensik setelah kejadian insiden.

5 Autentikasi Multi-Faktor (MFA)

MFA menambah lapisan keamanan tambahan dengan meminta pengguna untuk memverifikasi identitas mereka menggunakan dua atau lebih faktor autentikasi. Ini bisa melibatkan:



- **Kombinasi dari sesuatu yang diketahui** (kata sandi)
- **Sesuatu yang bersifat biometrik** (sidik jari, pemindaian wajah).
- **Sesuatu yang dimiliki** (token perangkat atau aplikasi autentikasi),

PAM yang efektif akan mengintegrasikan MFA untuk akses ke akun-akun privileged.

6 Kontrol Akses Dinamis

Kontrol akses yang berbasis risiko dan waktu semakin menjadi bagian dari PAM. Hal ini memungkinkan organisasi untuk mengubah level akses secara dinamis berdasarkan faktor-faktor seperti:

Lokasi pengguna
Apakah pengguna mencoba mengakses sistem dari lokasi yang tidak dikenal?

Waktu dan kondisi aktivitas
Misalkan, apakah pengguna mencoba mengakses sistem di luar jam kerja atau di luar kebiasaan?

Manfaat Implementasi PAM

Dengan menerapkan PAM dalam sistem keamanan siber anda, maka beragam manfaat pun bisa didapatkan perusahaan/ organisasi, seperti berikut ini:

1. Mengurangi Resiko Penyalahgunaan Akses

Dengan membatasi akses istimewa hanya untuk pihak yang berwenang dan melakukan pemantauan yang cermat, PAM mengurangi kemungkinan penyalahgunaan akses oleh pengguna internal atau penyerang eksternal.

2. Memastikan Kepatuhan Dengan Regulasi

Banyak regulasi dan standar industri, seperti GDPR, HIPAA, dan PCI DSS, mengharuskan pengelolaan akses yang ketat terhadap data sensitif dan sistem kritis. PAM membantu organisasi untuk memenuhi standar kepatuhan ini dengan menyediakan kontrol akses yang lebih kuat dan audit trail yang dapat dilacak.

3. Meningkatkan Keamanan Sistem

Implementasi prinsip Least Privilege dan pemantauan aktivitas pengguna dengan hak istimewa membantu mencegah serangan siber dan insiden yang bisa merusak integritas dan kerahasiaan data.

4. Meningkatkan Efisiensi Operasional

Dengan mengotomatisasi pengelolaan kata sandi, rotasi akses, dan pemantauan sesi, PAM mengurangi beban administratif pada tim TI dan memungkinkan organisasi untuk lebih fokus pada prioritas bisnis lainnya.

Tantangan Dalam Implementasi PAM

Meskipun PAM terlihat sebagai solusi dalam sistem keamanan, namun penerapannya juga tidak lepas dari tantangan, seperti berikut ini:

1. Kompleksitas Infrastruktur Dan Integrasi	Organisasi besar dengan infrastruktur yang kompleks mungkin menghadapi tantangan dalam mengintegrasikan sistem PAM ke dalam jaringan TI yang sudah ada. Solusi PAM harus mampu beradaptasi dengan berbagai sistem yang digunakan, termasuk server, aplikasi, perangkat jaringan, dan lainnya.
2. Pengelolaan Dan Pemeliharaan Sistem Yang Terus Berubah	Dalam lingkungan yang dinamis, di mana pengguna dan perangkat sering berubah, menjaga agar kebijakan PAM tetap relevan dan efektif membutuhkan upaya yang berkelanjutan.
3. Biaya Dan Sumber Daya	Solusi PAM, baik yang berbasis perangkat keras maupun perangkat lunak, seringkali memerlukan investasi yang signifikan. Organisasi harus menilai biaya vs manfaat dalam hal peningkatan keamanan dan pengurangan risiko.
4. Resistensi Terhadap Perubahan	Pengguna internal berpotensi merasa terhambat oleh kebijakan baru yang diberlakukan oleh sistem PAM, seperti rotasi kata sandi atau prosedur autentikasi multi-faktor. Oleh karena itu, penting untuk melibatkan semua pemangku kepentingan dalam proses perencanaan dan pelaksanaan untuk mengurangi resistensi terhadap perubahan.

Cambium Access Point
cnPilot E410 - Indoor

Cambium Access Point
Outdoor cnPilot e510

Cambium Access Point

Cambium Access Point cnPilot E410 Indoor memiliki fitur bracket terintegrasi yang mudah dipasang dan merupakan enterprise-grade 802.11ac Wave 2. Produk ini memiliki desain industrial yang cocok di perusahaan atau bisnis apa pun. Access Point ini dapat dikelola oleh cnMaestro cloud, on-premise cnMaestro atau sebagai standalone Access Point.

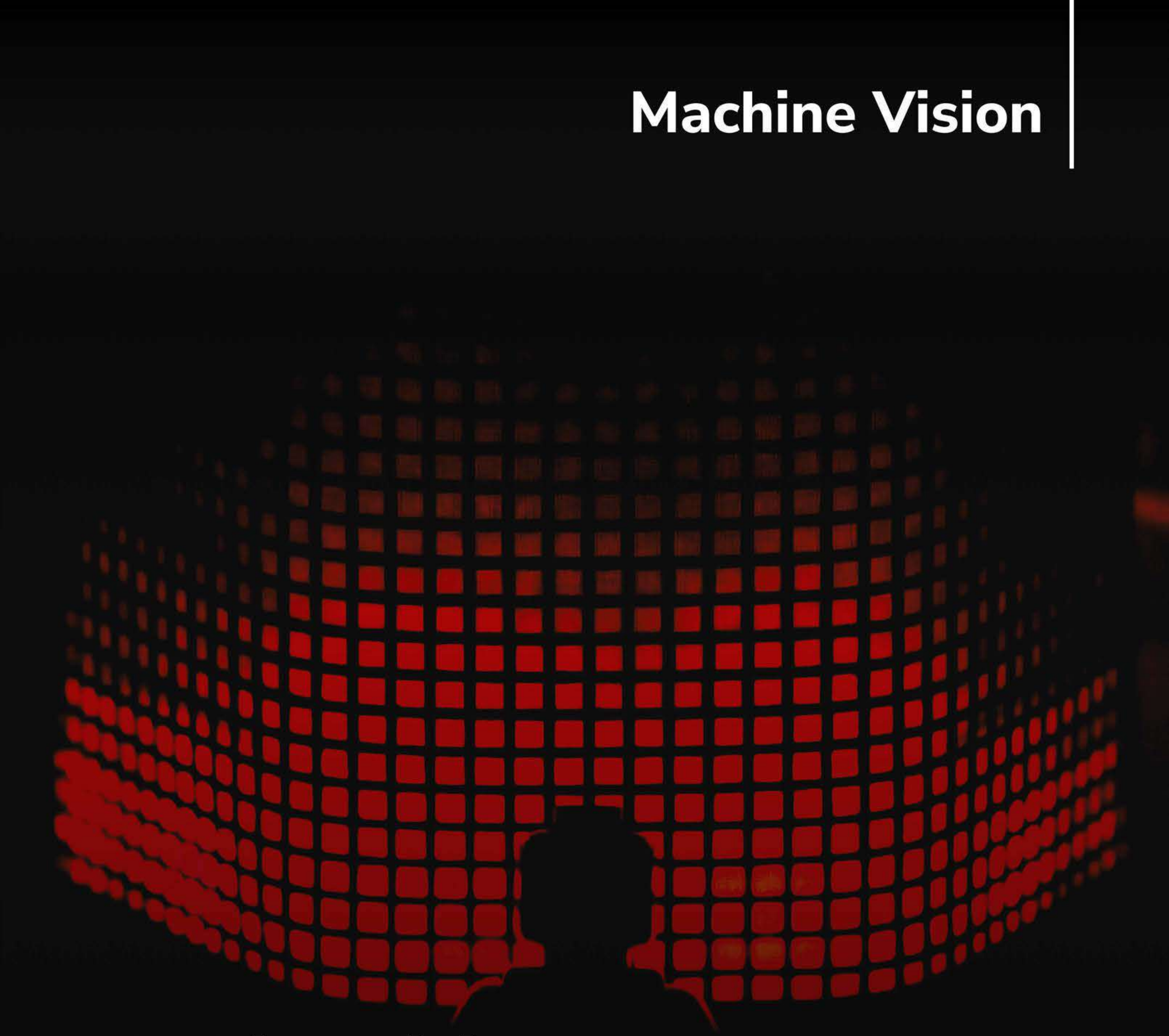
Cambium Access Point cnPilot E410 - Indoor

Cambium Access Point cnPilot E410 *Indoor* memiliki fitur bracket terintegrasi yang mudah dipasang dan merupakan enterprise-grade 802.11ac Wave 2. Produk ini memiliki desain industrial yang cocok di perusahaan atau bisnis apa pun. Access Point ini dapat dikelola oleh cnMaestro cloud, on-premise cnMaestro atau sebagai standalone *Access Point*.

Cambium Access Point Outdoor cnPilot e510

Ideal untuk perusahaan dan komunitas yang banyak beraktifitas di luar ruangan, Wi-Fi publik, atau Wi-Fi perusahaan. Access Point Outdoor cnPilot e510 dengan antenna omni-directional dari Cambium ini dirancang untuk aplikasi baik low, medium dan high-density. Masing-masing dirancang dengan bracket pemasangan terintegrasi & antena internal untuk memudahkan pemasangan yang dapat diulang dari satu site ke site yang lain.

Machine Vision



Machine Vision Membuat Produksi Anda Lebih Cepat & Cerdas

Machine Vision, merupakan sebuah inovasi dengan basis *Artificial Intelligence (AI)*, atau kecerdasan buatan. Inovasi baru ini diciptakan untuk bisa meningkatkan kapasitas serta kemampuan peralatan industri, dengan melihat dan menganalisa tugas dari mesin produksi secara cerdas. Serta mampu melakukan quality control, dan memberikan jaminan peningkatan keselamatan kerja.

Bisa disimpulkan, teknologi ini memberikan peralatan-peralatan industri kemampuan untuk dapat melihat dan membuat keputusan yang tepat berdasarkan apa yang dilihat. Kegunaan *Machine Vision* dalam industri adalah untuk melakukan inspeksi visual, penentuan posisi, dan pengukuran bagian, hingga identifikasi dan pelacakan produk.

Sebagai salah satu teknologi pendiri otomasi industri, teknologi ini membantu meningkatkan kualitas produk. Bukan itu saja, teknologi ini juga mempercepat produksi dan mengoptimalkan manufaktur dan logistik selama beberapa dekade. Sekarang, teknologi ini adalah salah satu inovasi yang memimpin transisi menuju Industri 4.0

Kegunaan *Machine Vision*

1. Mengurangi Kesalahan Manusia (*Human Error*)

Manusia memang dianugerahi mata oleh Tuhan Yang Maha Esa, namun belum bisa dikatakan sempurna. Meskipun mata manusia sangat ideal untuk interpretasi kualitatif, akan tetapi *Machine Vision* mampu mengukur kuantitas produk dengan sukses. Berkat keakuratan, pengulangan, dan kecepatannya.

Contoh: Aplikasi untuk dunia kedokteran

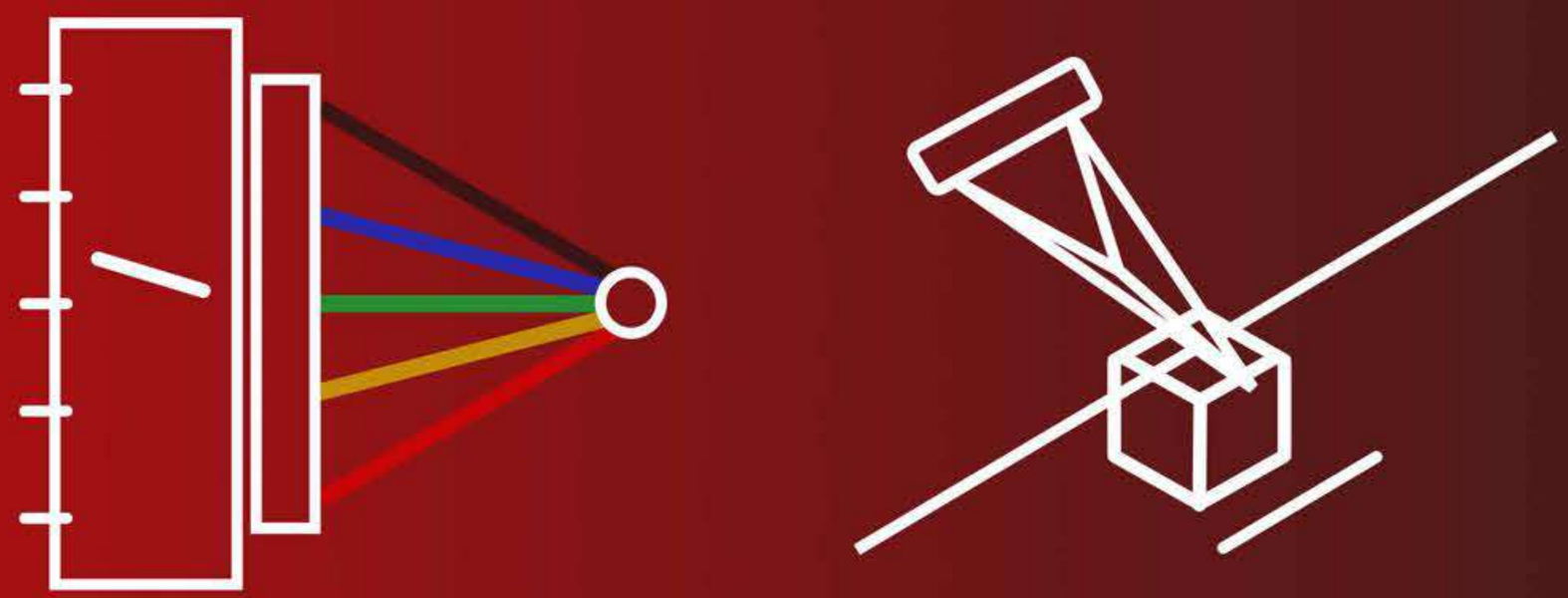
Sistem ini digunakan untuk melakukan inspeksi terhadap obat atau pil ke bungkusnya. Apakah obat/pil tersebut sudah benar masuk secara jumlah. Apakah posisi obat/pil tersebut miring?. Apakah obat/pil tersebut pecah?. Apakah bungkus obat/pil nya masih kosong? Dan sebagainya.

2. Mengidentifikasi Cacat Cetak.

Mungkin sulit untuk mengidentifikasi anomali pencetakan, termasuk corak warna yang salah. Seperti misalnya, cetakan yang tidak tepat (*miss*), atau huruf yang hilang. Namun kehadiran *Machine Vision,* membuat tugas ini terasa begitu mudah. Cara aplikasi *Machine Vision* pada industri cetak adalah, dengan gambar master yang dimasukkan ke dalam sistem. Kemudian Gambar tersebut digunakan sebagai pembanding untuk semua cetakan/ komponen yang diproduksi. Setiap penyimpangan dari master segera ditandai untuk diperbaiki.

3. Menemukan dan Mengukur Dengan Akurat

Machine Vision juga melibatkan penentuan dimensi objek secara akurat. Aplikasi ini dapat menemukan dan mengukur titik-titik tertentu pada gambar, termasuk diameter, radius, jarak, dan kedalaman. Untuk keperluan praktis, aplikasi ini dapat digunakan untuk mengidentifikasi diameter dalam lubang silinder mesin atau mengukur tingkat pengisian cairan botol. Data tersebut diperoleh dengan menggunakan kamera 2D atau 3D.



4. Mendeteksi Warna

Sistem *Machine Vision* juga dapat digunakan untuk mendeteksi dan membedakan warna. Misalkan, Cat mobil bodi mobil dengan kaca spion yang dipasang belakangan. Kemudian mendeteksi urutan kabel yang dipasang pada konektor. Apakah urutan kabel sudah benar, untuk menghindari korsleting listrik.

5. Mendeteksi Cacat Produksi

Seperti yang terlintas dalam benak pikiran kita, *machine vision* dapat mendeteksi kelainan produk seperti penyok dan goresan pada permukaan. Dengan memanfaatkan batasan deteksi secara hati-hati untuk memastikan cacat yang dapat diterima dapat dibedakan dari cacat yang tidak dapat diterima, machine vision mampu mendeteksinya. Sehingga anda tidak perlu khawatir, machine vision sangat ideal untuk tugas-tugas semacam ini,karena sistem akan beroperasi berdasarkan contoh (master), bukan aturan yang ketat.

Beberapa Contoh Solusi Produk *Machine Vision*

SC3000 SERIES

MV-ID3016PM-08M-WBN

OPT-IDG1-16L06P-31

Sehingga, jika perusahaan Anda membutuhkan solusi produk melalui m*achine vision*, yang sudah kami ulas di atas, anda bisa menghubungi kami, kami siap untuk bekerja sama, berdiskusi dan mengimplementasikannya untuk mendukung efisiensi dan efektivitas kegiatan operasional di perusahaan Anda.

ZEBRA

ZEBRA Kiosk Computer KC50

Desain yang mengundang konsumen

KC50 diciptakan agar pelanggan dapat berinteraksi dengan layar yang terang, mudah dilihat di lingkungan apa pun. Hadir dengan opsi layar 15” dan 22” memiliki lapisan layar anti-noda/anti sidik jari serta body yang tahan terhadap debu serta cipratan air. Memiliki konektor Z-Flex untuk menghubungkan periferal, seperti *scanner barcode* dan bilah lampu notifikasi.

Produk ini siap digunakan sebagai terminal pembayaran dan dapat membaca kartu pembayaran apapun karena didukung oleh Zebra PayTM.

ZEBRA TD50

Dirancang untuk ruang publik

TD50 adalah komponen inti dalam Sistem Kios Zebra. Cocok digunakan untuk layanan mandiri seperti di ritel, perhotelan, perbankan, pemerintahan, dan banyak lagi. Ketika transaksi kios mengharuskan pelanggan atau karyawan Anda diminta untuk melihat atau memverifikasi atau dapat juga memasukkan informasi, TD50 ini akan mempermudahnya. Komputer Kios Android™ KC50 yang menjadi inti dari setiap Kios Zebra akan memberikan informasi yang tepat ke TD50.

Stand SC-2000

SC-2000 adalah dudukan untuk pemasangan komputer kios KC50 dan monitor sekunder layar sentuh TD50.

Managed Service

Memahami **Managed Service** ACS Group, Solusi Cerdas Mengelola Aset TI

Bisnis yang mampu bertahan dan berkembang dengan baik saat ini, tidak lepas dari bagaimana pengaplikasian infrastruktur Teknologi Informasi (TI) dalam sistem. Akan tetapi, untuk bisa memberikan jaminan keamanan atas infrastruktur TI berjalan terus dengan baik, diperlukan perawatan, pemantauan dan pengelolaan yang kontinu dan berkelanjutan. Maka dari sinilah *Managed Service* TI, akan mengambil peran, sehingga perusahaan akan bisa berfokus dalam pengembangan kebijakan bisnis nya.

1 Apa Itu *Managed Service*?

Secara umum "*Managed Service*" atau "Layanan yang Terkelola" didefinisikan sebagai model bisnis di mana sebuah organisasi atau perusahaan mendelegasikan tanggung jawab dan fungsi terkait pengelolaan dan pemeliharaan berkelanjutan kepada penyedia pihak ketiga *(third-party company)*. Dalam konteks bisnis, *Managed Service* seringkali berkaitan dengan bidang TI, di mana perusahaan mempercayakan pengelolaan infrastruktur TI mereka kepada penyedia layanan pihak ketiga.

2 Manfaat *Managed Service*

Managed Service menawarkan berbagai manfaat bagi perusahaan, terutama dalam meningkatkan efisiensi operasional dan memberikan kesempatan kepada perusahaan untuk fokus pada pertumbuhan bisnis inti. Berikut penjelasan terperinci, tentang manfaat *Managed Service*

Fokus Pada Bisnis Inti

Dengan mengalihkan tugas-tugas pengelolaan TI, perusahaan dapat internal, seperti pemeliharaan staf TI internal, pelatihan, serta pemeliharaan perangkat keras dan perangkat lunak. Model biaya berlangganan yang umum dalam Managed Service memungkinkan perusahaan untuk memprediksi pengeluaran TI dengan lebih baik. Penyedia *Managed Service* memiliki sumber daya yang ahli di bidangnya sehingga pengelolaan TI bisa lebih efisien dan mengurangi pemborosan sumber daya.

***Support* Yang Tidak Dibatasi Waktu**

Perusahaan tidak perlu khawatir akan ketersediaan layanan support karena penyedia Managed Service menawarkan fleksibilitas 24/7, bahkan pada hari libur nasional apabila dibutuhkan.

***Point of Contact* yang dapat diandalkan**

Pada saat perusahaan bermitra dengan penyedia *Managed Service*, perusahaan tidak perlu kuatir adanya perputaran / rotasi dari tenaga ahli. Penyedia Managed Service akan menyiapkan jalur eskalasi maupun kontak pengganti yang siap turun untuk membantu menyelesaikan permasalahan yang ada.

3 *Managed Service* ACS

ACS Group adalah perusahaan integrator sistem yang berdiri sejak tahun 1992. Kami memfokuskan keahlian kami pada 5 (lima) pilar, yaitu: *Internet of Things (IoT)*, Infrastruktur TI, Keamanan Siber, Sistem keamanan Perusahaan, dan Solusi Bisnis Perusahaan yang mencakup Layanan Profesional dan Layanan Terkelola.

ACS Managed Service adalah sebuah layanan yang ditawarkan oleh ACS Group untuk mengelola sistem atau infrastruktur TI perusahaan mulai dari operasional perangkat *IoT, wired / wireless network system, access control system* sampai ke *cyber security* untuk pengamanan terhadap sistem / infrastruktur TI perusahaan. Layanan-layanan dalam ACS *Managed Service* dirancang dan dipersiapkan untuk mendukung kelima pilar ACS yang ada.

4 Ruang Lingkup *Managed Service* ACS

ACS Managed Service memiliki ruang lingkup layanan yang mengutamakan *Customer Business* diantaranya:

- ***Proactive Monitoring***
  Adalah layanan yang ACS tawarkan untuk selalu siap siaga merespon setiap permasalahan atau permintaan atas suatu layanan dengan cepat. Layanan bisa disesuaikan dengan kebutuhan pelanggan, salah satunya
  - ***24×7 Support***
    Layanan yang selalu tersedia untuk pelanggan sepanjang waktu, 24 jam sehari, 7 hari seminggu. Dengan layanan ini respon terhadap permasalahan menjadi lebih cepat sehingga meminimalkan waktu henti (downtime) dan gangguan.

- ***Problem Handling***
  Adalah layanan dimana ketika problem yang berhubungan dengan sistem TI memerlukan penanganan masalah, pelanggan akan menghubungi ACS *Helpdesk* untuk meminta layanan perbaikan. Permintaan akan diproses dengan ticket sebelum dieksekusi. Layanan problem handling bisa dilakukan dengan 2 cara:
  - ***On Site / Breakfix***
    Adalah layanan perbaikan di tempat, jadi ketika terjadi masalah pada perangkat maka perbaikan bisa langsung dilakukan di lokasi / site dimana perangkat itu berada. Layanan breakfix dimungkinkan karena selain Service Center yang tersebar di beberapa lokasi strategis, ACS juga memiliki Service Hubs yang tersebar di seluruh Indonesia.

Remote Service.
Adalah layanan untuk melakukan pekerjaan seperti konfigurasi sistem, pemantauan atau perbaikan sistem dari jarak jauh melalui jaringan internet.

Preventive Maintenance
Adalah pemeliharaan perangkat hardware yang dilakukan oleh ACS engineer agar sistem tetap berjalan dengan baik dan meminimalkan terjadinya kerusakan perangkat ketika sistem sedang berjalan.

Patch Management
Adalah layanan dimana ACS engineer akan selalu memonitor patch dan update version dari sistem perangkat lunak (*software*) maupun dari supporting software. Selanjutnya ACS *engineer* akan mengirimkan rekomendasi *pre-patch* report kepada pelanggan dan kemudian melakukan eksekusi patch sesuai dengan persetujuan pelanggan.

Service Center
Merupakan layanan perbaikan *(repair service)* yang dikhususkan untuk beberapa jenis perangkat IoT ACS engineer yang handal dan berpengalaman akan menganalisa permasalahan pada perangkat, melakukan perbaikan serta penggantian *spare-parts* apabila diperlukan agar perangkat dapat kembali berfungsi normal. ACS *Service Center* tersebar di beberapa lokasi strategis di Indonesia yaitu Jakarta, Cikarang, Semarang, Surabaya, dan Denpasar. Tim ACS engineer bahkan memiliki pengalaman layanan hingga ke luar negeri.

Backup Unit
Merupakan layanan untuk menjaga agar operational downtime terukur dan tidak melewati *maximum downtime* yang diinginkan pelanggan. Perangkat TI yang rusak akan digantikan dengan perangkat pengganti *(Back-up Unit)* yang mempunyai fungsi yang sama.

Rental Unit
Adalah layanan penyewaan perangkat baik itu perangkat yang sudah ada dan siap digunakan atau perangkat baru sesuai dengan kebutuhan pelanggan.

Pickup and Delivery
Merupakan layanan untuk pengambilan perangkat TI yang rusak di lokasi / site dimana pelanggan berada, maupun untuk penyerahan perangkat penggantinya.

Report and Recommendation
Adalah laporan yang berisi performa / kinerja dari perangkat / infrastruktur TI, rekomendasi apabila dibutuhkan (bisa dilakukan dalam periode bulan / kuartal), perpindahan perangkat TI dari suatu lokasi ke lokasi lainnya, termasuk juga posisi inventori dari perangkat TI dan perangkat penggantinya. Selain itu ada juga laporan mengenai pencapaian *SLA (Service Level Agreement)* sesuai dengan yang telah disepakati bersama dengan pelanggan.

- ***Extended Warranty (ACS Care)***
  Merupakan bentuk perlindungan tambahan terhadap produk-produk tertentu dengan memperpanjang masa garansi standar produk.

ACS *Managed Service* dilengkapi dengan aplikasi yang mumpuni sesuai kebutuhan customer untuk mendukung berjalannya layanan-layanan yang ada. aplikasi ini dibangun dan dikembangkan sendiri oleh ACS Group.

5 Apa Yang Membedakan A*CS Managed Service* Dengan Yang Lain?

Layanan *Managed Service* mungkin memang ada di tempat lain, akan tetapi Layanan yang diberikan oleh *ACS Managed Service*, memiliki berbagai keunggulan, seperti:

- Tim Support TI yang telah memiliki banyak pengalaman profesional dan terlibat langsung dalam proses implementasi proyek TI serta memiliki sertifikasi profesional yang dikeluarkan oleh Principals. Tim Support TI mempunyai beragam spesialisasi teknologi TI dan tingkat kualifikasi skill (tier-1, tier-2, tier-3 dan consultant).

- Service Center merupakan layanan perbaikan perangkat TI yang dapat diperbaiki oleh team Service Center lokal kami yang berada di seluruh kota besar wilayah indonesia.

- *Call Center* sebagai single point of contact dari perusahaan dengan menggunakan *Hotline Number*. Perusahaan dapat menentukan kebutuhan waktu operasi dari *Call Center*, 8×5 maupun sampai 24×7 termasuk hari libur nasional.

- *Escalation Management System*, *ACS Managed Service* dalam proses penyelesaian masalah TI memiliki *System Operating Procedure* yang menjamin permasalahan dipahami, dapat diselesaikan dan ditangani oleh tenaga ahli yang tepat.

- Layanan *Managed Service* tidak dapat dilepaskan dari *SLA (Service Level Agreement)*. Perusahaan perlu menginventarisasi faktor-faktor yang bisa menghambat kelancaran proses bisnis yang diakibatkan oleh tidak berjalannya infrastruktur TI dengan baik dan kemudian menyusun beragam SLA sesuai faktor-faktor tersebut. ACS Managed Service menawarkan standard *SLA (response time dan resolution time)* maupun SLA lainnya yang perlu dibicarakan sebelumnya dengan perusahaan.

6 Pentingnya *Managed Service*

Managed Service TI menjadi sangat penting dalam dunia bisnis modern karena kemampuannya dalam mengatasi kompleksitas dan tantangan yang dihadapi perusahaan dalam mengelola infrastruktur TI. Produk dan Layanan *Managed Service* TI terbukti telah membantu perusahaan meningkatkan efisiensi dan produktivitas, mengurangi resiko serta memastikan infrastruktur TI yang andal dan aman sehingga perusahaan bisa fokus pada pertumbuhan inti bisnis.

Sehingga bisa dipastikan, dengan menggunakan layanan dari *ACS Managed Service*, akan mampu memberikan jaminan keberlangsungan bisnis anda, melalui dukungan layanan terbaik dalam menjaga infrastruktur TI anda, tanpa harus mengganggu kinerja produksi perusahaan secara umum.

Janji Sang Peramal

Kolom Ketawa

Seorang wanita mendatangi seorang peramal untuk menanyakan masa depannya.

"Pak! Saya ingin melihat tentang garis usia saya, menurut Anda sampai usia berapa saya hidup?"

"Wah ibu bertanya tentang usia harga konsultasinya murah 10 juta saja, ibu bersedia?".

Karena penasaran sang ibu membayarnya, kemudian sang peramal dengan santai bermeditasi dan membaca heksagramnya serta berkata:

"Hasil heksagram menunjukkan ibu dapat hidup sehat hingga usia 100 tahun!"

"Haaahhh.. bapak yakin dengan apa yang bapak katakan?"

"Pasti terjadi dong!.. siapa yang ga kenal saya" **dengan sombongnya.**

"Pak!", **wanita tua itu ragu-ragu** "Bagaimana jika itu salah?"

"Tenang kalau meninggal sebelum umur 100 tahun, datang saja ke sini, saya garansi 100 persen uang kembali!"

!?!%%&###

PM84 adalah enterprise mobile device yang dilengkapi fitur-fitur seperti Octa-core, RAM 4 GB/ROM 64 GB, Corning Gorilla Glass serta baterai 4.950 mAh yang kuat dan mudah diganti(opsional 7.020 mAh) sehingga dapat digunakan sepanjang hari. PM84 dilengkapi kamera belakang 13 MP dan depan 5 MP serta memiliki sertifikasi AER untuk memenuhi persyaratan ketat Google, termasuk pembaruan perangkat lunak dan keamanan yang teratur dan konsisten. Memiliki mesin pemindai untuk membaca semua simbologi 1D/2D untuk mendukung layanan pengiriman, transportasi, dan manajemen gudang. Tahan jatuh dari ketinggian 1,8 m (6 kaki) dan beroperasi dalam kisaran suhu -20 °C hingga 60 °C (-4 °F hingga 140 °F).

PM84

ACS Group siap bekerjasama menghadirkan solusi Point Mobile PM84 di perusahaan Anda untuk menunjang kegiatan operasional di perusahaan anda agar lebih efektif.

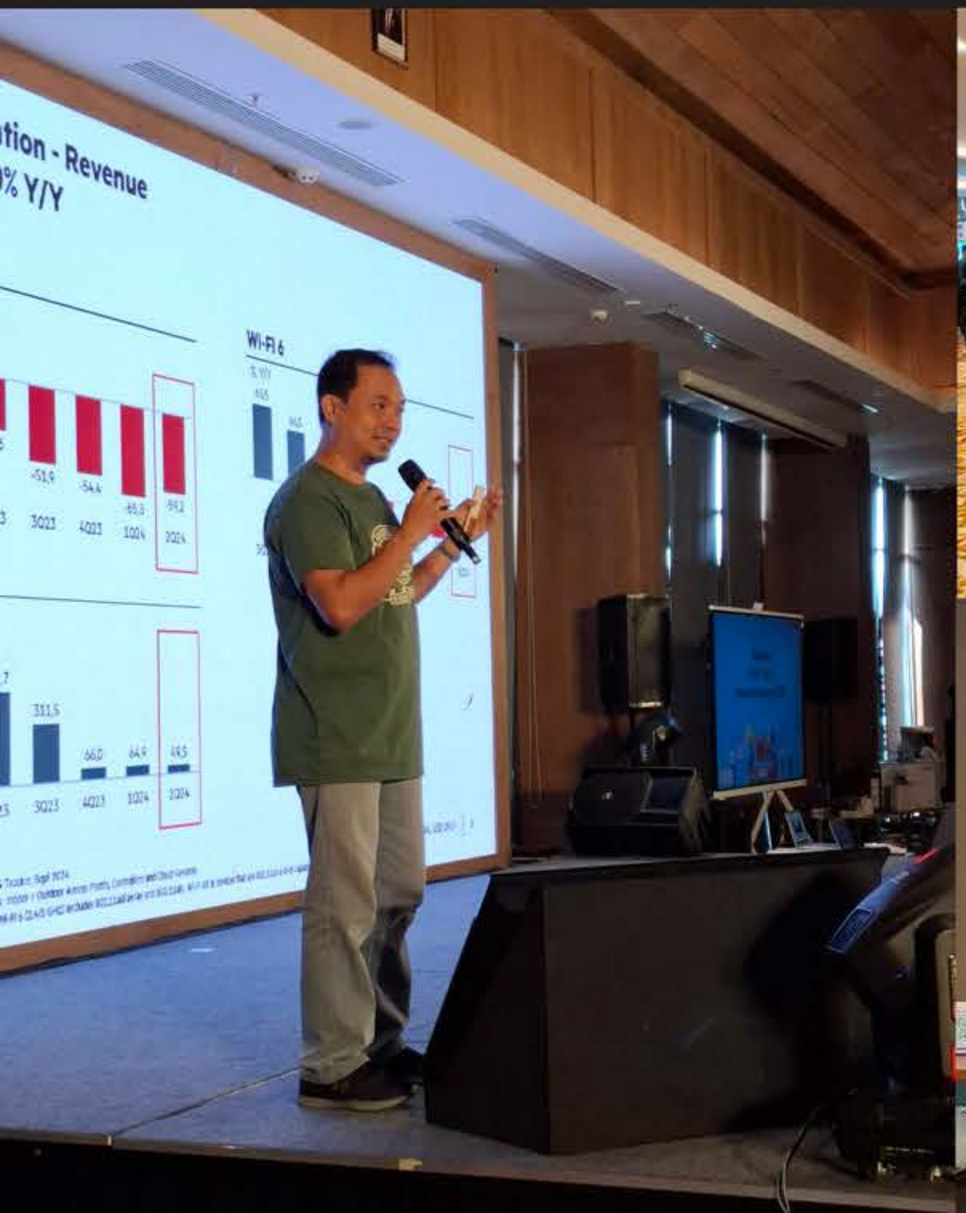
15th Bali Annual Gathering 2025: Sebuah Inovasi WiFi Terbaru dari HPE Aruba Networking

15th IT Bali Annual Gathering 2025, yang digelar pada 15 Februari 2025, sukses digelar dengan dukungan penuh dari HPE Aruba Networking dan ACS Group. Event bergengsi yang digelar di Harris Hotel Bali ini, menghadirkan beragam inovasi terbaru dari dunia digital dan jaringan.

Salah satu booth yang banyak mendapat decak kagum dari para pengunjung dan peserta, adalah *Booth Exhibition* Aruba, yang menampilkan portofolio lengkap dari solusi industri jaringan. Sesi presentasi dari Presales Manager HPE Aruba Networking, Denny, yang membahas tentang WiFi-6E mendapat sambutan hangat dari audiens yang hadir. Dengan pilihan On-Prem dan Cloud (seri 610,630, dan 650), teknologi terbaru dari HPE Aruba *Networking* ini, menawarkan jaringan dengan kecepatan tinggi, kapasitas besar, namun dengan latensi yang rendah.

Event kali ini juga menampilkan demo produk, jejaring antar profesional, pelaku bisnis dan praktisi IT, serta sesi diskusi berkaitan dengan kondisi terkini, tantangan, serta solusi jaringan modern. Dimana beragam sesi ini mendapatkan antusiasme tinggi dari para peserta 15th IT Bali Annual Gathering 2025. Hal tersebut membuktikan bahwa kolaborasi dan inovasi sudah menjadi bagian penting dalam industri teknologi dan informasi dewasa ini.

Ucapan terima kasih dihaturkan kepada HPE Aruba Networking dan ACS Group, beserta seluruh peserta yang terlibat. Sampai berjumpa di IT Bali *Annual Gathering* selanjutnya!



Corporate Info

ACS Group: Bersyukur di 2024.
Bersinar Untuk 2025

Mencatatkan beragam torehan positif di 2024, menjadi modal bagi ACS Group dalam mengarungi tantangan di 2025. Hal tersebut terwujud dalam event tutup tahun ACS Group pada 20 Desember 2024. Bertemakan "Bersyukur di 2024, Bersinar di 2025", acara tahunan yang diadakan di Kantor Pusat ACS Group ini, menjadi refleksi dan apresiasi atas kerja keras seluruh tim, serta momentum tepat untuk persiapan hadapi tantangan di 2025.

Dalam suasana penuh kehangatan dan kebersamaan, event tutup tahun ACS Group ini diisi dengan sesi makan bersama, ucapan penuh syukur, serta penyambutan dan pengenalan anggota tim baru. Kehangatan acara semakin bertambah dengan kehadiran para alumni ACS Group, yang turut memeriahkan acara. Kesempatan ini juga digunakan untuk bisa saling mengenal lebih dekat antar anggota tim dan karyawan, serta berbagi pengalaman kerja selama ini bersama ACS Group.

Dengan semangat kebersamaan, ACS Group optimis menghadapi tahun 2025 dengan penuh harapan dan inovasi. Semoga tahun mendatang membawa lebih banyak peluang dan keberhasilan bagi seluruh tim. Terima kasih kepada seluruh tim ACS Group yang telah berkontribusi sepanjang tahun ini.

Mari terus bersinar dan bersyukur dalam setiap langkah ke depan!

Vrensly Albert Lilipory -
Engineer, Zebra Certified.
Implementasi di **Singapura**

Hendi Fulamnsyah -
Senior Engineer, Zebra Certified.
Implementasi di **Beijing, China**

Nopah Hermanto -
Senior Engineer, Zebra Certified.
Implementasi di **Tokyo, Jepang.**

Gigih Setiawan - Engineer, Zebra Certified. Implementasi di **London Inggris**

Ari Prasetia - Senior Engineer, Zebra Certified. Implementasi di **New York, USA**

ACS Group sukses melaksanakan proyek implementasi **di 5 Negara (Singapura, China, Jepang, Inggris dan Amerika Serikat).**

ACS Group telah berhasil dengan sukses menjalankan pekerjaan implementasi produk Zebra *Mobile Computer* MC33 dan Zebra Printer ZD231, untuk proyek instansi pemerintahan di 5 kantor cabang luar negeri diantaranya: **Singapura, Tokyo, Beijing, London dan New York(USA)**. Dan juga implementasi untuk kantor cabang mereka yang tersebar di **42 kota di Indonesia.**

Semua pekerjaan implementasi tersebut diselesaikan dalam periode waktu Oktober 2024 sampai dengan Februari 2025.





Raker ACS Group 2025: **Teamwork Makes The Dream Work**

Sebuah harapan besar didasarkan kerjasama tim yang solid, menjadi semangat utama yang dihasilkan ACS Group dalam Rapat Kerja 2025. Raker yang diadakan pada 20-22 Februari 2025 tersebut, diikuti oleh seluruh karyawan ACS Group dari cabang **Tangerang, Cikarang, Bali, Semarang, Surabaya, dan Yogyakarta.**

Sinergitas demi keberhasilan bersama menjadi tema yang diangkat dalam rapat kerja ACS Group 2025 kali ini. Dimana kegiatan utamanya meliputi, review pencapaian di tahun 2025, serta rencana kegiatan (*action plan*) untuk tahun 2025. Presentasi sendiri dilakukan oleh seluruh divisi dari ACS Group, termasuk juga *back office*, serta *professional service*, sales & marketing, serta banyak divisi lainnya.

Momen raker ini benar - benar mampu dimanfaatkan oleh seluruh tim dan divisi di ACS Group, untuk bisa melakukan evaluasi strategi di tahun sebelumnya, serta merancang langkah yang lebih baik untuk perjalanan ACS Group yang lebih baik di tahun 2025.

Disamping juga menghadirkan sesi spesial motivasi bertajuk “8 Etos Kerja Profesional” yang diberikan oleh Saut Sitompul. Sesi ini mampu memberikan wawasan berharga dan sudut pandang baru, dalam peningkatan kapasitas serta kualitas kerja di lingkungan ACS Group.

Sebagai penutup, malam kebersamaan Fun Night: ACS Got Talent menghadirkan pertunjukan kreatif dari para karyawan, menciptakan suasana yang penuh semangat dan kekompakan.

Dengan semangat kolaborasi dan inovasi, ACS Group siap menghadapi tantangan 2025 dan terus berkembang. Terima kasih kepada seluruh tim yang telah berpartisipasi.

Sampai jumpa di Rapat Kerja berikutnya!

Training Produk **SEUIC Q9**

Pada tanggal 5 Maret seluruh *engineer* mendapatkan *training update* produk dari SEUIC yaitu produk Q9 yang dibawakan oleh Rizky Hidayat-Presales and *Technical Engineer* SEUIC.
SEUIC Q9 adalah produk terminal genggam yang tangguh yang dirancang untuk kelas industri dan produk ini juga sudah digunakan oleh salah satu customer kami yang bergerak di bidang logistik.

PT. Solusi Periferal **"Top Achiever Partner 2024"** HPE Aruba Networking .

Pada acara Partner Awarding Night HPE Aruba Networking Indonesia 2024, di Mantra PIK - 11 December 2024 ACS Group, **PT. Solusi Periferal mendapat penghargaan Top Achiever Focus Partner 2024 dari HPE Aruba Networking Indonesia**, atas keberhasilan mengeksekusi beberapa proyek *enterprise* WLAN di sektor Hotel Bintang lima. Atas pencapain penjualan solusi Aruba Networking di 2024 tersebut menjadikan Solusi Periferal kembali sebagai Platinum Partner Aruba Networking.

Sertifikasi

Tim Professional Services ACS Group Terus Meningkatkan **Kompetensi Teknis** Untuk Menghadirkan **Solusi Berkualitas Tinggi** Bagi Pelanggan.

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

5-Pillars Of Core Competency

Internet of Things

Mobile Computing (Handheld, Vehicle, Tablet, Cold Storage-Rated), Bar/QR-Code Scanner & Label Printer, Mobile Printers, RFID, and Machine Vision Peripherals.

Network Audit, Wired & Wireless, SDWAN, Data Center Networking, HyperConverged DC/Private Cloud, and Public Cloud.

IT Infrastructure

Cyber Security

NGFW & Secure Switching, IT/OT visibility, ZeroTrust Access, Edge hardening,

App integrity, Centralized Command & Analytics, Persistent Threat Mitigation, and Unified SASE

Surveillance and Comms, Barrier Gate, & Access Control, Intelligent Alarm, and Unified Command Control Center.

Enterprise Business Solution

Enterprise Security System

Professional Services, Application (WMS, Asset Management & Tracking, MES), Unified Endpoint Management, and Managed Service

Perlunya **Grounding Kelistrikan** Pada Pemasangan Printer Barcode

Printer Barcode sangat penting dalam berbagai industri. Sehingga kontinuitas pemakaian nya sehari - hari sangat diperlukan. Salah satu bentuk perlindungan kepada printer barcode adalah dengan mengaplikasikan grounding listrik.

Penggunaan grounding listrik yang baik, kepada printer barcode akan memberikan banyak manfaat seperti berikut ini:

1. Mengurangi Resiko Konsleting/ Tersengat Arus Listrik

Grounding membantu mengalirkan arus listrik yang tidak diinginkan ke tanah, sehingga mengurangi risiko korsleting yang dapat merusak printer atau menyebabkan user cedera tersengat listrik saat menyentuh body dari logam pada printer barcode tersebut.

2. Mengurangi Gangguan Elektromagnetik (EMI)

Grounding membantu mengurangi gangguan EMI yang dapat mempengaruhi kinerja printer atau peralatan elektronik lainnya di sekitarnya.

3. Mengurangi Risiko Petir

Jika printer terhubung ke jaringan listrik yang tidak memiliki grounding yang baik, maka risiko kerusakan akibat petir menjadi lebih tinggi. Grounding yang baik dapat membantu mengalirkan arus petir ke tanah, sehingga mengurangi risiko kerusakan.

4. Meningkatkan Kinerja Printer

Grounding yang baik dapat membantu meningkatkan kinerja printer dengan mengurangi gangguan EMI dan mengurangi risiko korsleting.

5. Mengurangi Risiko Kerusakan Pada Komponen Elektronik

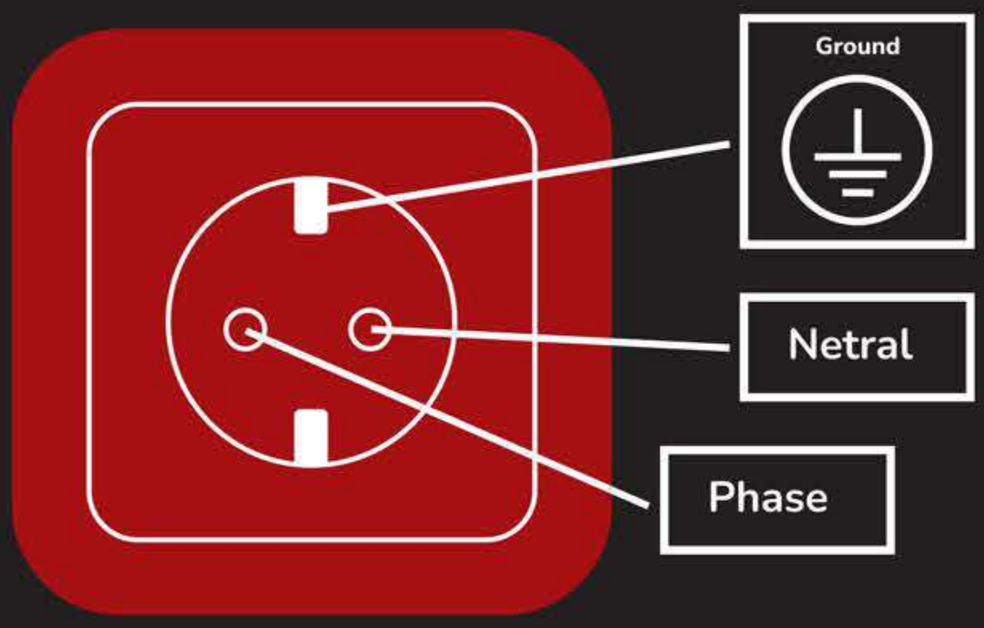
Grounding yang baik dapat membantu meningkatkan kinerja printer dengan mengurangi gangguan EMI dan mengurangi risiko korsleting.

Cara Memastikan Grounding Yang Baik

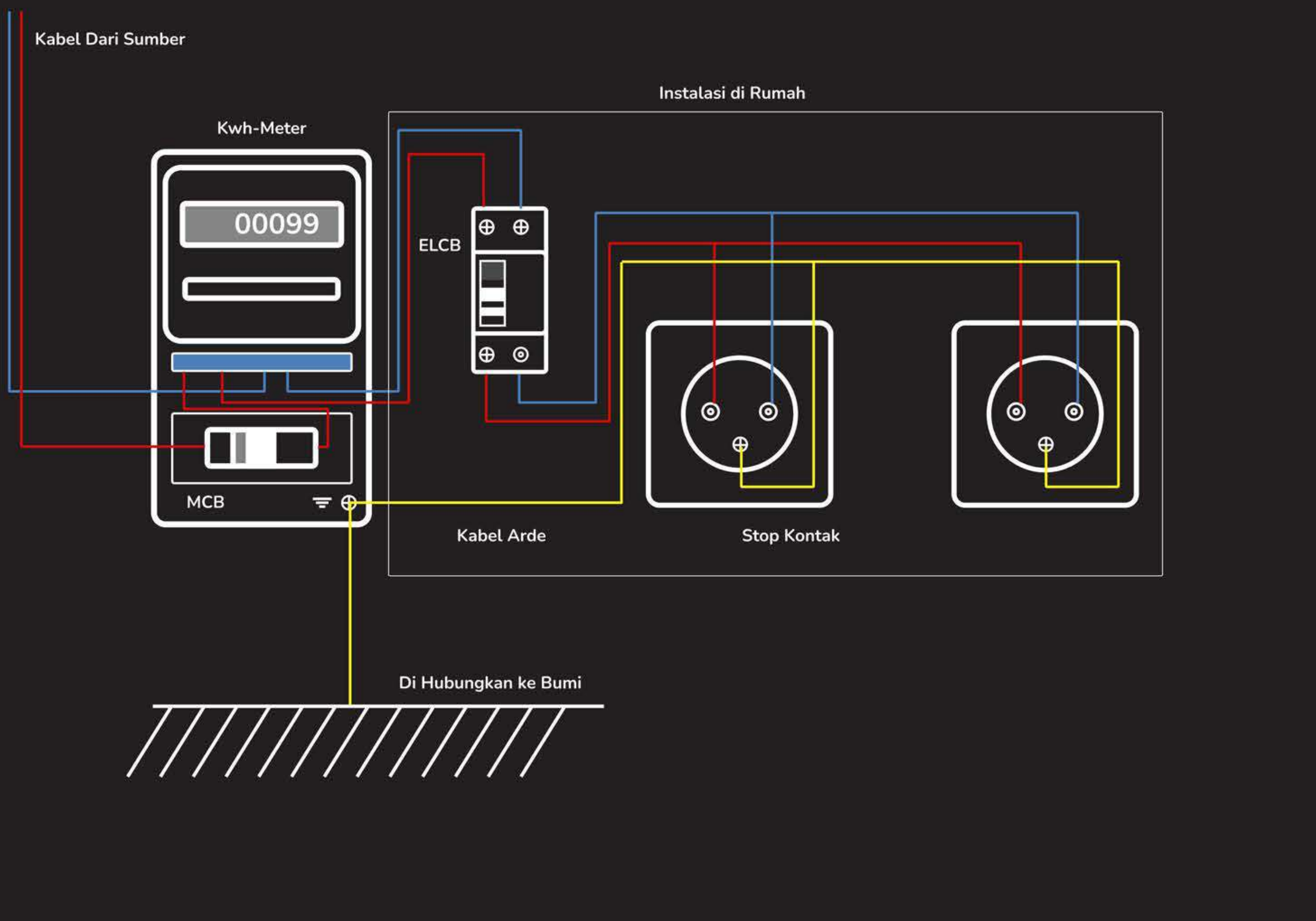
1. Pastikan Kabel Daya Terhubung Dengan Benar Sumber Daya Listrik Dan Memiliki Grounding Yang Baik.
2. Periksa Kondisi Kabel Daya Secara Teratur Dan Pastikan Bahwa Tidak Ada Kerusakan Atau Keausan Yang Dapat Mempengaruhi *Grounding*.
3. Gunakan Pengaman Listrik Yang Memiliki Grounding Yang Baik Untuk Melindungi Printer Dari Korsleting Atau Gangguan EMI.
4. Pastikan Instalasi Listrik Di Tempat Printer Terpasang Memiliki Grounding Yang Baik Dan Memenuhi Standar Keselamatan Listrik.

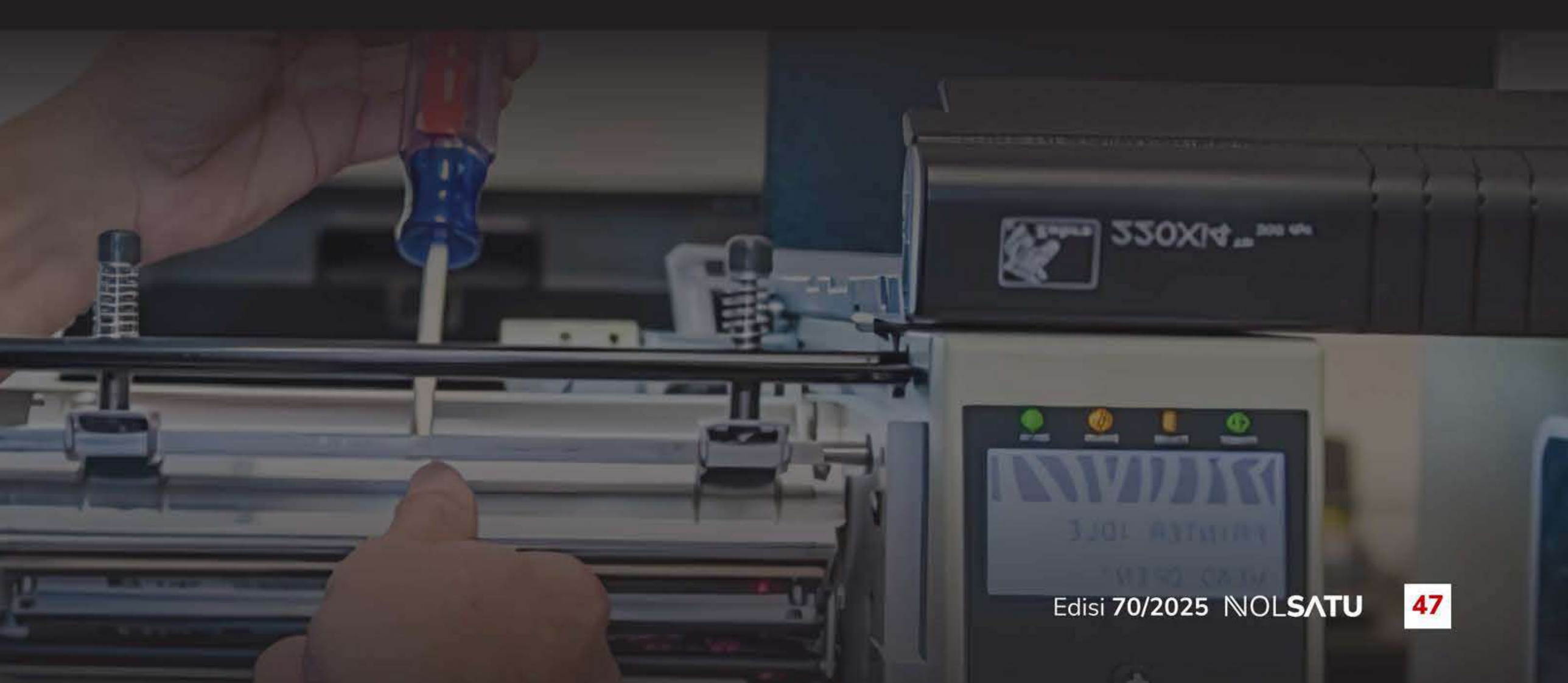
Cara Memastikan Grounding Yang Baik

Tegangan grounding ideal adalah kurang dari atau sama dengan 5V AC jika diukur dengan Voltmeter antara titik netral dengan grounding pada outlet/stop kontak listrik PLN.
Dengan memastikan grounding yang baik, Anda dapat mengurangi risiko kerusakan pada printer barcode dan memastikan kinerja yang optimal.



Installasi Kabel Grounding Di Rumah





ACS Group Principals

Alibaba Cloud · Allied Telesis · BarTender by Seagull Scientific · brother at your side

BOSCH · Cambium Networks · eG Innovations · Extreme Connect Beyond the Network · FORTINET

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

ivanti · Hytera · HUAWEI · JANZ · MOTOROLA SOLUTIONS

OPT Machine Vision · omada · POINT Mobile · SAMSUNG · SANGFOR · Seuic

SOLUM Solution provider. · ZEBRA · ZKTeco Indonesia · 42GEARS

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

Jakarta (HO) & Service Center
Perkantoran Gunung Sahari Permai #C
No. 03-05 & #E No. 3, Jl. Gunung Sahari
Raya No 60-63 Jakarta 10610
Telp : +6221 - 4208221(H), 4205187(H)
Email : sales.admin@acsgroup.co.id

Cikarang
Cikarang Square Blok E No 62,
Jl. Raya Cikarang Cibarusah Km 40, Cikarang
Barat, Bekasi, Jawa Barat 17530
Telp : +6221 - 29612366, 29612367
Email : adminckg@acsgroup.co.id

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

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo, Jawa Timur 61254
Telp : +6231 - 8556277(H); 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

MORE INFO

acsgroup.co.id
PT Autojaya Idetech &
PT Solusi Periferal
autojayasolusi
+62 811 1194 4534
(Chat Only)

Hubungi ›
Kembali Ke Daftar Isi