NOLSATU

Detak **Transformasi Digital**

by **ACS GROUP**

Buletin Edisi 72
Desember 2025

Untuk
Kalangan
Sendiri

Tingkatkan Kinerja Infrastruktur Jaringan Nirkabel Anda dengan Wireless Network Audit Services

Beyond the Hype:
Introduction to SecOps

Sinergi AIDC dan AI, Membaca Arah Baru Teknologi Industri

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)
- Empianus Eko Putra
- Taufik Maulana Ibrahim
- Kenneth Wira Looho
- Taufiq Rahman
- Gusti Afriansyah
- Bayu Suyantino Putro
- Hendi Fulmansyah
- Jemis Pangaribuan
- Dasa Aprily Ardy
- Angelina Rasta P Ginting
- Agung Atmoko

EDITOR
- Arijanto Hartanto
- Afia Mien
- Angelina R P Ginting

ALAMAT REDAKSI

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

Lihat Lokasi >

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

Hubungi >

Meja Redaksi

Salam Hangat

Empianus Eko Putra

Enterprise Network Solutions

Senior Network Engineer | ACP-CA Certified

Pelanggan yang terhormat,

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat dan karunia-Nya, sehingga kita semua senantiasa diberi kesehatan dan perlindungan.

Di era *high mobility* saat ini, jaringan nirkabel (*Wi-Fi*) bukan lagi sekadar fasilitas pendukung, melainkan sudah menjadi *lifeline* operasional bagi berbagai sektor — mulai dari kantor, pabrik, rumah sakit, hotel, hingga kampus. Konektivitas yang cepat, stabil, dan aman kini menjadi faktor kunci keberhasilan bisnis. Namun, masih banyak organisasi yang bersikap reaktif terhadap masalah jaringan, baru bertindak ketika gangguan sudah terjadi. Pendekatan seperti ini berisiko menimbulkan dampak serius terhadap kinerja dan keamanan.

Melalui Wireless Network Audit Services, kami membantu organisasi melakukan pemeriksaan menyeluruh terhadap ekosistem *Wi-Fi* menggunakan alat analisis profesional. Layanan ini tidak hanya mendeteksi masalah, tetapi juga menjadi langkah preventif yang memastikan jaringan Anda tetap optimal dan terlindungi. Kini saatnya para pengambil keputusan TI menjadikan audit jaringan nirkabel sebagai bagian penting dari rutinitas operasional.

Dalam edisi bulletin kali ini, kami juga mengulas beberapa topik menarik lainnya:

- **Wi-Fi 7**, revolusi konektivitas masa depan yang menjanjikan kecepatan dan efisiensi luar biasa.
- **SOC (*Security Operation Center*)**, pusat kendali keamanan modern yang menjadi garda terdepan pertahanan digital.
- **Sinergi Enterprise Security System dan AI**, kolaborasi cerdas untuk memperkuat keamanan korporasi.
- **Sinergi AIDC & AI**, integrasi antara *Automatic Identification and Data Capture* dengan kecerdasan buatan untuk efisiensi industri.

Sebagai penutup, kami juga menghadirkan berita tentang produk-produk terbaru, kabar internal perusahaan, serta rubrik Tips & Info yang bermanfaat bagi Anda.

Tingkatkan Kinerja Infrastruktur Jaringan Nirkabel Anda dengan Wireless Network Audit Services

Oleh: **Empianus Eko Putra,** Enterprise Network Solutions
Network Engineer | **ACS Group**

Performance & Connectivity

Di era bisnis yang serba terhubung, performa jaringan nirkabel menjadi tulang punggung kelancaran operasional. Namun, sering kali jaringan Wi-Fi tidak berfungsi sebagaimana mestinya — koneksi lambat, sering terputus, sinyal lemah, hingga gangguan yang sulit dijelaskan. Kondisi seperti ini tidak hanya menghambat produktivitas, tetapi juga berpotensi mengganggu kualitas layanan terhadap pelanggan.

Pertanyaannya, **apakah jaringan nirkabel Anda saat ini benar-benar bekerja optimal?**

Menjawab tantangan ini tidaklah mudah tanpa alat yang tepat dan pengalaman mendalam dalam audit jaringan. **ACSGroup** hadir memberikan solusi melalui layanan ***Wireless Network Audit – Performance & Connectivity***, dilengkapi dengan perangkat profesional Ekahau yang telah terbukti andal dalam mendiagnosis serta mengoptimalkan jaringan nirkabel di berbagai industri.

Apa Itu Wireless Network Audit?

Wireless Network Audit atau Audit Jaringan Nirkabel adalah proses evaluasi menyeluruh untuk memastikan jaringan Anda berjalan dengan aman, efisien, dan stabil. Audit ini membantu mendeteksi potensi masalah sejak dini — mulai dari kelemahan sinyal, gangguan (interferensi), hingga konfigurasi keamanan yang tidak tepat — sehingga tim IT dapat mengambil langkah proaktif sebelum masalah berdampak besar pada bisnis.

Beberapa area utama yang menjadi fokus audit meliputi:

1. **Konektivitas :** Menilai/mengevaluasi kekuatan dan stabilitas sinyal di berbagai area.
2. **Kinerja :** Mengukur kecepatan transfer data, latensi, dan kualitas koneksi.
3. **Cakupan :** Mengidentifikasi area “mati” yang tidak terjangkau sinyal.

4 **Interferensi** : Mendeteksi sumber gangguan dari perangkat lain.

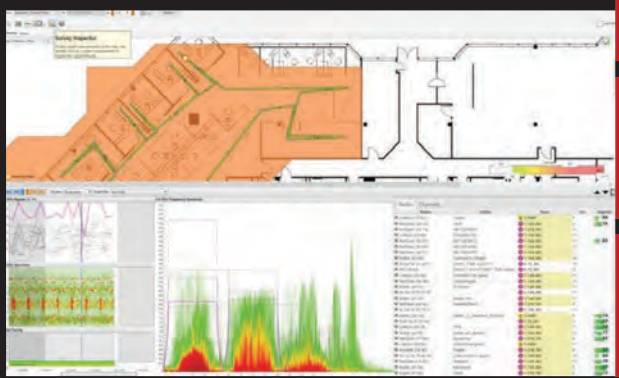
5 **Keamanan** : Mengevaluasi konfigurasi keamanan terhadap risiko akses tidak sah.

6 **Infrastruktur** : Memeriksa perangkat keras dan perangkat lunak jaringan.

Wireless Network Audit Performance & Connectivity

Audit ini merupakan proses evaluasi komprehensif terhadap jaringan nirkabel untuk memeriksa kecepatan, jangkauan, kualitas koneksi, serta potensi interferensi. Tujuannya jelas — menemukan akar masalah, memperbaiki desain dan implementasi jaringan, serta mengoptimalkan performa agar koneksi tetap stabil dan efisien.

Tujuan Audit



- Mendiagnosis jangkauan sinyal, kapasitas, dan performa jaringan nirkabel.
- Mengidentifikasi kesalahan konfigurasi dan penempatan Access Point.
- Memastikan pengaturan SSID, channel, dan power sesuai standar.
- Menganalisis interferensi serta memastikan roaming client berjalan lancar.
- Menjamin seluruh perangkat nirkabel sesuai dengan kebijakan keamanan perusahaan.

Manfaat yang Anda Dapatkan

Optimalisasi Jaringan
Menyesuaikan konfigurasi agar lebih efisien dan stabil.

Peningkatan Kinerja
Menghilangkan hambatan yang menyebabkan koneksi lambat.

Keamanan Maksimal
Memastikan pengaturan jaringan mematuhi standar keamanan industri.

Efisiensi Biaya
Mencegah kerugian akibat downtime atau gangguan berulang di masa depan.

Perangkat & Metode yang Digunakan

ACS Group menggunakan EKAHAU, perangkat profesional kelas dunia yang diakui dalam industri untuk perancangan, analisis, dan troubleshooting jaringan Wi-Fi dengan akurasi tinggi.

Metode yang digunakan adalah ***Active Survey***, yang berfokus pada tiga aspek utama:

Security
Audit keamanan jaringan.

Performance
Evaluasi kecepatan dan stabilitas koneksi.

Configuration
Pemeriksaan dan penyesuaian konfigurasi perangkat.

Tahapan Audit

1 Project Kick-Off

A. Konsultasi awal untuk memahami kebutuhan bisnis dan area kritis jaringan.

B. Meninjau arsitektur jaringan, konfigurasi WLAN controller, serta layout lokasi.

C. Menjadwalkan kegiatan audit agar tidak mengganggu operasional harian.

2 Onsite Wireless Network Audit

A. Pengujian koneksi ke SSID eksisting untuk memvalidasi:

Signal Strength | *Throughput at key zones* | *Data Rate* | *Speed Test and latency* | *Packet loss* | *Round-Trip Time* | *Interference and Noise*

B. Pengujian aplikasi spesifik seperti VoIP, video streaming, aplikasi gudang dan lain-lain.

3 Post-Audit Analysis

A. Analisis hasil survei menggunakan software Ekahau.

B. Identifikasi akar penyebab permasalahan.

C. Pembuatan heatmap report untuk visualisasi kualitas jaringan.

4 Reporting & Recommendation

Penyusunan laporan komprehensif berisi hasil pengukuran, analisis, dan rekomendasi strategis meliputi:

A Heatmaps membantu melihat performa jaringan di seluruh area. Beberapa parameter utama yang kami analisis antara lain:

Signal Strength

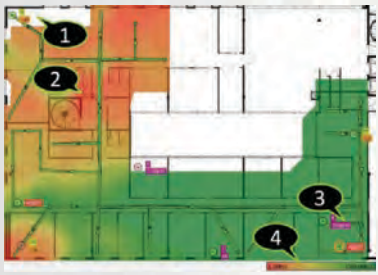
Menunjukkan kekuatan sinyal di berbagai titik, membantu menemukan area lemah atau tanpa sinyal.

1. Signal strength does not meet the requirement. The signal strength is below -65 dBm and the visualization is greyed-out.

2. High signal strength.

Data Rate & Throughput

Mengukur kecepatan dan jumlah data yang benar-benar berhasil ditransfer dalam periode waktu tertentu di area yang berbeda.



1. No data transfer possible

2. Low data rate (Red color)

3. High data rate (Green color)

4. Red = 1Mbps <-> Green = 1300Mbps

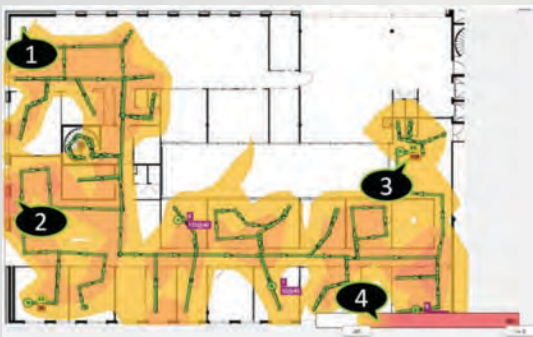
Speed & Latency

Menilai seberapa cepat data berpindah dari sumber ke tujuan pada jaringan.

Notes	Speedtest (9/30/25, 12:58 PM): | 7C:21:0E:7B:04:8F #Speedtest - Download: 56.84 Mbps, Upload: 24.84 Mbps. Ping: 47 ms. Jitter: 11 ms. id: 5A44E015-14B2-428C-A8FD-604BD59C36CZ

Interference / Noise

Mengidentifikasi gangguan dari perangkat lain atau jaringan sekitar yang mengganggu koneksi sehingga menyebabkan penurunan kualitas koneksi, koneksi lambat, dan hilangnya data.

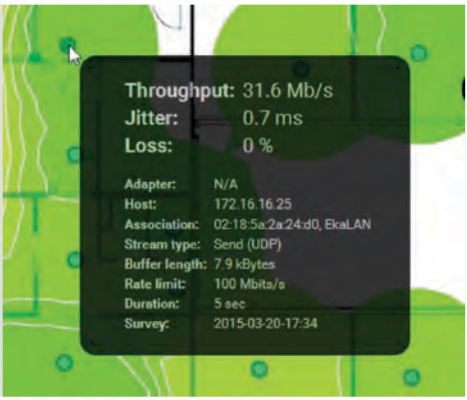


Packet Loss

Mengukur seberapa banyak data hilang selama transmisi.

Round-Trip Time (RTT)

Menunjukkan waktu yang dibutuhkan untuk melakukan transmit dan receive paket ping dan dimunculkan pada layout.



Channel Overlapping

Menemukan saluran frekuensi Wi-Fi yang saling bertumpuk dan menyebabkan interferensi

1. Multiple overlapping channels on 2.4GHz band

2. No overlapping APs

B Daftar Temuan & Akar Masalah.

C Rekomendasi Optimalisasi:

Relokasi Access Point atau perubahan konfigurasi.

Penyesuaian konfigurasi channel dan power.

Pengaturan ulang *band steering* dan *load balancing.*

Mengapa Memilih ACS Group?

Dengan pengalaman panjang dalam solusi jaringan dan teknologi informasi, ACSGroup bukan hanya melakukan audit, tetapi memberikan insight strategis untuk memastikan jaringan nirkabel Anda menjadi lebih tangguh, cepat, dan siap menghadapi kebutuhan bisnis yang terus berkembang.

Percayakan Wireless Network Audit Anda kepada ACSGroup – karena performa jaringan yang stabil berarti efisiensi operasional dan produktivitas bisnis yang lebih tinggi.

HPE Aruba Networking 750 Series Wi-Fi 7 Access Points

Aruba Wi-Fi 7 – Kecepatan Baru untuk Dunia yang Terhubung

Rasakan performa tanpa batas bersama HPE Aruba Networking Wi-Fi 7 Access Points. Seri Aruba 750 dirancang untuk menghadirkan konektivitas ultra-cepat, aman, dan stabil bagi lingkungan kampus, enterprise, hingga industri dengan kebutuhan tinggi.

Dengan kecepatan tri-band hingga 18,7 Gbps, dukungan penuh pada pita 6 GHz, serta kemampuan menghubungkan lebih banyak perangkat *IoT*, Aruba memastikan setiap proses berjalan efisien tanpa jeda.

Didukung fitur keamanan jaringan tingkat lanjut dan presisi lokasi tinggi, Aruba Wi-Fi 7 adalah fondasi cerdas untuk transformasi digital Anda.

Lebih cepat, lebih aman, lebih siap menghadapi masa depan.

Wi-Fi 7 Revolusi Konektivitas Masa Depan dan Dampaknya di Berbagai Industri

Oleh: **D. A. Ardy,** Professional Services Manager | **ACS Group**

Pendahuluan:

Mengapa Wi-Fi 7 Begitu Penting?

Kehadiran Wi-Fi 7, atau yang dikenal juga sebagai IEEE 802.11be, menjadi tonggak baru dalam dunia konektivitas nirkabel. Generasi terbaru ini hadir untuk menjawab tantangan zaman yang serba cepat dan serba digital. Mulai dari aktivitas streaming, game online, hingga sistem otomasi industri — semuanya kini menuntut jaringan yang lebih cepat, stabil, dan efisien.

Di Indonesia, geliat menuju era Wi-Fi 7 juga mulai terasa. Sejak peluncuran resminya pada Februari 2025, Kementerian Komunikasi dan Digital (Kemkomdigi) bersama ***Indonesia Technology Alliance*** (ITA) telah menetapkan pedoman teknis serta regulasi frekuensi bagi penerapan teknologi ini. Langkah tersebut menjadi sinyal kuat bahwa Indonesia siap mempercepat transformasi digital nasional, terutama di bidang industri, pendidikan, dan layanan publik.

Apa Itu Wi-Fi 7 dan Apa yang Membuatnya Berbeda?

Wi-Fi 7 merupakan generasi ketujuh dari teknologi Wi-Fi, diperkenalkan oleh Wi-Fi Alliance pada awal 2024 sebagai penerus Wi-Fi 6 dan 6E. Secara teoritis, Wi-Fi 7 mampu menghadirkan kecepatan hingga 40–46 Gbps, jauh melampaui generasi sebelumnya yang “hanya” mencapai sekitar 9,6 Gbps. Angka tersebut bukan sekadar peningkatan kecil, melainkan sebuah lompatan besar dalam dunia konektivitas nirkabel.

Fitur Unggulan

Beberapa terobosan utama yang dibawa Wi-Fi 7 antara lain:

Bandwidth 320 MHz,
dua kali lebih lebar dibanding Wi-Fi 6E.

4K-QAM (Quadrature Amplitude Modulation),
yang membuat transfer data lebih cepat dan efisien.

Multi-Link Operation (MLO),
memungkinkan perangkat terhubung di beberapa frekuensi sekaligus (2.4, 5, dan 6 GHz) untuk menjaga kestabilan.

OFDMA dan MU-MIMO versi terbaru,
agar performa tetap optimal meski banyak perangkat aktif bersamaan.

Kompatibilitas ke bawah
sehingga perangkat lama Wi-Fi 6 atau 5 masih bisa digunakan.

Keamanan WPA4
untuk perlindungan data yang lebih kuat.

Manfaat yang Dirasakan

Dengan kombinasi teknologi tersebut, Wi-Fi 7 mampu:

- Memberikan kecepatan tinggi (40–46 Gbps), untuk streaming video 8K, *real-time gaming*, hingga AR/VR tanpa gangguan.
- Menurunkan latensi ke tingkat yang hampir tidak terasa — ideal untuk layanan seperti telemedis dan *cloud gaming*.
- Menopang ratusan perangkat secara bersamaan tanpa penurunan performa.
- Memberikan koneksi lebih stabil di area padat, seperti perkantoran atau kampus besar.
- Menjadi fondasi bagi Internet of Things (IoT) dan otomatisasi industri.

Perangkat yang Sudah Mendukung Wi-Fi 7

Agar teknologi ini bisa dimanfaatkan sepenuhnya, tentu dibutuhkan perangkat yang sudah kompatibel.

Smartphone & Tablet

Perangkat dengan Snapdragon FastConnect 7800 (mulai dari Snapdragon 8 Gen 3 ke atas), MediaTek Dimensity 9300, hingga Apple iPhone 16 (chip A18) sudah siap mendukung Wi-Fi 7.

Laptop & PC

Adaptor Intel BE200/BE202(dengan kecepatan maksimal hingga 5.8 Gbps di band 6 GHz), serta chipset Snapdragon X Elite (FastConnect 7800), mulai banyak digunakan di laptop modern seperti ASUS Vivobook S15 OLED, Dell XPS 13/16, Acer Swift Go AI, dan Razer Blade 16.

Access Point (AP)

Beberapa produsen jaringan seperti HPE Aruba (seri 700) dan Cambium Networks (seri X7-35X) telah merilis AP yang siap menyuguhkan kecepatan Wi-Fi 7 sepenuhnya.

Tanpa perangkat access point yang sesuai, kemampuan Wi-Fi 7 tidak akan terasa maksimal, karena koneksi tetap akan turun ke standar Wi-Fi sebelumnya.

Dampak dan Penerapan Wi-Fi 7 di Berbagai Industri

Berikut ini ada beberapa studi kasus hipotetis berdasarkan manfaat Wi-Fi 7, dipadukan dengan situasi nyata di industri teknologi dan manufaktur:

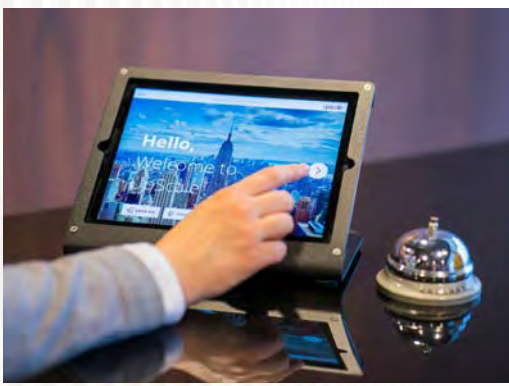
1 Industri Manufaktur: Mendorong Smart Factory

Di lingkungan pabrik modern, ribuan sensor, robot, dan sistem otomatisasi harus berkomunikasi secara real-time. Sedikit saja jeda waktu dapat menimbulkan kerugian besar. Dengan MLO dan OFDMA, Wi-Fi 7 mampu menghubungkan banyak perangkat secara bersamaan dengan latensi sangat rendah. Data dari sensor dan mesin bisa dikirim cepat, mendukung sistem digital twin dan predictive maintenance. Hasilnya: produktivitas meningkat, downtime menurun, dan proses analisis data berjalan lebih akurat.

2 Smart Campus: Pembelajaran Digital Tanpa Gangguan

Kampus modern menuntut jaringan yang tangguh untuk menunjang kegiatan e-learning, konferensi video, hingga laboratorium VR/AR. Wi-Fi 7 memungkinkan ribuan mahasiswa online secara bersamaan tanpa gangguan. Teknologi MLO juga membuat perpindahan antar access point lebih mulus, mendukung pembelajaran berbasis multimedia yang lebih immersive dan efisien.

3 Perhotelan dan Event Venue: Pengalaman Digital Maksimal



Di hotel, stadion, atau arena konser, ribuan pengunjung ingin terhubung ke internet secara bersamaan. Biasanya, sinyal akan melambat atau bahkan terputus. Namun, dengan kanal 320 MHz dan fitur puncturing, Wi-Fi 7 mampu menjaga stabilitas koneksi di area padat. Hasilnya, pengunjung bisa menikmati layanan digital tanpa hambatan, sementara penyelenggara dapat memanfaatkan data real-time untuk meningkatkan pengalaman pelanggan.

4 Rumah Sakit dan Layanan Kesehatan: Kecepatan untuk Menyelamatkan Nyawa

Di dunia medis, koneksi bukan hanya soal kenyamanan, tapi soal keselamatan. Wi-Fi 7 mendukung sistem monitor pasien, transfer hasil imaging, hingga layanan telemedicine dengan latensi sangat rendah.
Kecepatan dan keamanan WPA4 memastikan data pasien tetap terlindungi, sekaligus mempercepat proses diagnosa dan pengambilan keputusan medis.

Wi-Fi 7 dan Masa Depan Konektivitas

Wi-Fi 7 bukan sekadar peningkatan dari versi sebelumnya — ini adalah lompatan besar menuju era baru konektivitas nirkabel. Dengan kecepatan hingga 46 Gbps, latensi ultra rendah, dan kapasitas masif, Wi-Fi 7 menjadi fondasi penting bagi berbagai inovasi: dari industri pintar, kampus digital, hingga rumah sakit cerdas.

Ketika infrastruktur dan perangkat telah siap, Wi-Fi 7 akan membawa dunia menuju kehidupan yang lebih cepat, lebih terhubung, dan lebih cerdas.
Bagi para pelaku industri, perencana TI, dan pengambil kebijakan, inilah saat yang tepat untuk menatap masa depan dan mulai bersiap menyambut revolusi konektivitas nirkabel.

Cinta di Antara Knalpot dan Trotoar

Jupri, driver ojol paling bangga sejagat, jatuh cinta pada Mawar sebagai aktivis lingkungan yang anti banget sama kendaraan bermotor. Karena takut, setiap kali mau ngapel, Jupri selalu parkir motor tiga blok dari rumah Mawar, umpetin jaket hijaunya, dan pura-pura bilang bau bensin di badannya itu **“parfum aroma jalanan donk”.** Namun bikin Mawar curiga.

Puncaknya terjadi saat Mawar menang lomba esai berjudul **“Ancaman Sepeda Motor bagi Eksistensi Trotoar”**, sedangkan Jupri menang penghargaan **“Driver Terbaik Bulan Ini”** — di acara yang sama dan tempat yang sama pula!

Saat MC memanggil nama Jupri, Mawar melongo. **“Kamu driver ojol pri?!”**
Jupri gugup, **“Iya sayang, maap ya?... Tapi plis boleh dong aku antar kamu pulang naik motor?”**

Mawar sedikit kesal, **“Okehh, asal matiin mesin — kita dorong bareng. Biar ramah lingkungan, kan?”**

Cambium Networks X7-35X Wi-Fi 7 Access Points

Cambium Wi-Fi 7 Hadir dengan Performa Unggul Dan Investasi Cerdas

Cambium Networks X7-35X Wi-Fi 7 Access Point menghadirkan kecepatan tinggi dan efisiensi tanpa harus mengorbankan anggaran. Dengan data rate agregat hingga 9,2 Gbps, port 2.5 GbE uplink, dan dukungan tri-band Wi-Fi 7, perangkat ini siap meningkatkan kapasitas dan keandalan jaringan Anda.

Dikelola melalui platform Cambium cnMaestro, pengawasan dan konfigurasi jaringan menjadi lebih mudah, cepat, dan terpusat.

Solusi ideal untuk perusahaan yang ingin beralih ke teknologi Wi-Fi 7 dengan efisien dan *cost-effective.*

Cambium Wi-Fi 7 merupakan produk teknologi yang cepat, tangguh, dan siap untuk pertumbuhan bisnis Anda.

SecOps

Beyond the Hype: Introduction to SecOps

Oleh: **Ken Looho,** FCA, APS-SSE | **ACS Group**

Evolusi SecOps

Istilah Security Operations atau SecOps bukanlah hal baru. Selama bertahun-tahun, konsep ini sudah menjadi topik utama di dunia keamanan siber. Namun, dalam beberapa tahun terakhir, SecOps mendapatkan sorotan yang jauh lebih besar — baik dari sisi industri maupun pengguna akhir.

Mengapa demikian?

Perusahaan kini menghadapi *attack surface* yang terus meluas seiring dengan percepatan digitalisasi. Setiap aplikasi baru, perangkat tambahan, atau sistem yang terhubung memperbesar potensi risiko. Di saat yang sama, banyak organisasi masih kekurangan tenaga ahli keamanan yang mampu menganalisis data log dalam jumlah besar dan menindaklanjutinya secara cepat. Kombinasi kedua faktor inilah yang mendorong kebutuhan akan SecOps.

SecOps bukan sekadar satu alat atau solusi tunggal. Ia adalah sistem terpadu yang menggabungkan berbagai perangkat dan layanan keamanan agar bekerja selaras dalam satu orkestrasi yang solid. Melalui SecOps, seluruh informasi dan laporan keamanan dari beragam sistem — mulai dari *Next-Gen Firewall, Endpoint Security (EDR/Antivirus)*, hingga *Threat Analysis Tools* — dikumpulkan dan dianalisis secara menyeluruh.

Hasilnya? Tim IT mendapatkan visibilitas yang lebih baik terhadap potensi ancaman serta dapat mengambil tindakan cepat dan terkoordinasi. Dengan kata lain, SecOps berfungsi sebagai "pusat kendali" keamanan siber yang membantu mengurangi *alert fatigue* akibat terlalu banyaknya notifikasi dari berbagai alat keamanan yang tidak saling terintegrasi.

Asal-Usul dan Tantangan yang Dihadapi

Pertumbuhan perusahaan sering kali diiringi dengan penambahan alat keamanan yang beragam — setiap alat memiliki fungsi spesifik dan terkadang berjalan sendiri-sendiri.

Kondisi ini menimbulkan silo antara satu sistem dengan lainnya. Akibatnya, tim IT terpaksa menganalisis log dari masing-masing perangkat secara manual, yang memakan waktu dan meningkatkan risiko terlewatnya ancaman penting.

Beberapa tantangan utama yang sering muncul:

1. Keterbatasan waktu dan sumber daya, yang membuat proses penyesuaian dan analisis log tidak optimal.

2. Kurangnya integrasi antar alat keamanan, sehingga visibilitas ancaman menjadi terbatas.

3. Beban kerja tinggi, yang berujung pada kelelahan dan menurunnya efisiensi tim IT.

Solusinya? Mengadopsi pendekatan SecOps dengan dashboard terpadu atau sering disebut *single pane of glass* — yang menampilkan seluruh aktivitas keamanan dalam satu tampilan jelas dan mudah dianalisis.

Tanpa sistem seperti ini, perusahaan berisiko kehilangan visibilitas terhadap ancaman yang sedang terjadi, sekaligus gagal memaksimalkan investasi perangkat keamanan yang sudah dimiliki.

Log Analytics: Awal dari Perjalanan SecOps

Langkah pertama menuju penerapan SecOps biasanya dimulai dari log analysis. Setiap perangkat keamanan menghasilkan data log dalam jumlah besar, dan di sinilah alat seperti FortiAnalyzer dari Fortinet memainkan peran penting.

FortiAnalyzer berfungsi sebagai data lake untuk seluruh log keamanan yang berasal dari berbagai perangkat Fortinet — mulai dari *FortiGate* hingga *FortiClient* dan *FortiSandbox*. Dengan menggabungkan seluruh data tersebut, sistem ini memberikan gambaran menyeluruh tentang kondisi keamanan jaringan perusahaan.

Beberapa keunggulan FortiAnalyzer memudahkan kerja tim IT:

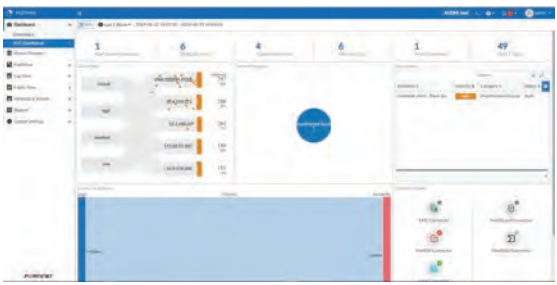
1. **Mengumpulkan dan menganalisis data**
   FAZ mengumpulkan log dalam jumlah besar, lalu mengolahnya menjadi tampilan dan laporan yang mudah dibaca dengan bantuan intelijen dari FortiGuard Labs.

2. **Mendeteksi ancaman lebih cepat**
   Dengan menggabungkan data dari berbagai perangkat, FAZ bisa menemukan serangan berlapis yang sulit terdeteksi. Teknologi AI dan machine learning di dalamnya membantu mengenali aktivitas mencurigakan lebih awal.

3. **Mendukung otomatisasi kerja**
   Fitur Playbook memungkinkan tindakan otomatis, seperti memblokir IP berbahaya, mengarantina perangkat, atau membuat laporan insiden sehingga pekerjaan tim IT jadi lebih ringan dan cepat.

4. **Memenuhi standar keamanan global**
   FAZ sudah tersertifikasi sesuai regulasi internasional seperti GDPR, HIPAA, dan PCI DSS, membantu perusahaan tetap aman dan patuh pada aturan.

5. **Semua terlihat dalam satu tampilan**
   Melalui satu dashboard, tim IT bisa memantau seluruh aktivitas keamanan jaringan dengan lebih mudah dan efisien.



Gambar # SOC Dashboard FortiAnalyzer [reference]

Beberapa vendor lain juga mengadopsi pendekatan serupa. Misalnya, Sangfor menyertakan fitur SOC-Lite langsung di dalam perangkat Athena *NGFW-nya*, memberikan visibilitas instan terhadap potensi ransomware dan memungkinkan *one-click quarantine* terhadap ancaman yang terdeteksi.

SIEM: Integrasi di Dunia Multi-Vendor

Ketika perusahaan menggunakan berbagai merek perangkat keamanan, SIEM (Security Information and Event Management) menjadi solusi utama. Sistem ini bertugas mengumpulkan, mengindeks, dan menganalisis data log dari seluruh vendor keamanan yang digunakan — memberikan pandangan terpadu terhadap status keamanan organisasi.

Fitur penting SIEM mencakup:

1

Analisis Perilaku Pengguna dan Perangkat (UEBA)

SIEM mampu mengenali pola aktivitas normal dari pengguna maupun perangkat. Ketika muncul perilaku yang tidak biasa — misalnya akses ke file sensitif yang jarang dibuka atau komunikasi ke alamat eksternal mencurigakan — sistem akan memberi tanda sebagai ancaman berprioritas tinggi.

2

Pengelolaan Data dalam Skala Besar

SIEM dapat menampung, mengindeks, dan menganalisis data log dari hampir semua sumber dan format. Kemampuannya mengolah data besar ini membantu perusahaan melihat ancaman secara lebih menyeluruh tanpa ada area yang luput *(blind spot)*.

3

Pencarian dan Investigasi Cepat

Analis keamanan bisa melakukan pencarian mendalam untuk menyelidiki insiden, mencari pola ancaman, serta membuat dasbor dan laporan sesuai kebutuhan perusahaan.

4

Deteksi dan Korelasi Ancaman

Dengan aturan korelasi yang canggih dan dukungan *machine learning*, SIEM dapat menghubungkan berbagai peristiwa seperti login gagal, koneksi jaringan mencurigakan, atau unduhan file aneh. Semua ini digabungkan menjadi satu cerita utuh tentang bagaimana serangan terjadi dan apa penyebabnya.

5

Investigasi dan Respon Lebih Cepat

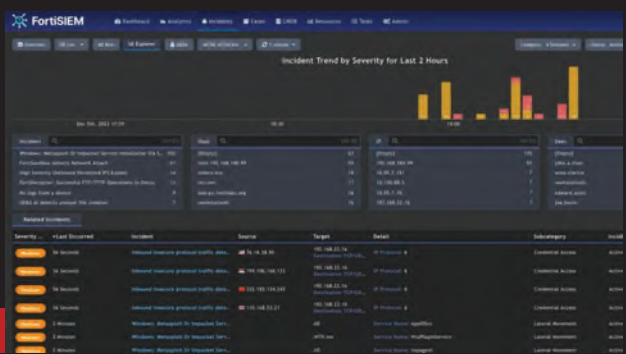
SIEM menyediakan tampilan investigasi yang interaktif, membantu tim keamanan memvisualisasikan jalannya insiden, menemukan sumber masalah, dan merespons ancaman dengan cepat.

6

Peringatan Berdasarkan Risiko (Risk-Based Alert)

Daripada membanjiri tim IT dengan ribuan notifikasi setiap hari, SIEM menyusun peringatan berdasarkan tingkat risiko. Dengan begitu, tim bisa fokus pada ancaman yang benar-benar penting dan berdampak besar.

Dengan pendekatan seperti ini, tim keamanan dapat fokus pada hal yang paling penting — menangani ancaman nyata, bukan sekadar membaca notifikasi.



Gambar# FortiSIEM dashboard [reference]

SOAR: Otomatisasi yang Cerdas

Setelah data terkonsolidasi, langkah berikutnya adalah otomatisasi melalui SOAR (*Security Orchestration, Automation, and Response*). SOAR membantu mengurangi beban kerja manual dengan mengeksekusi tugas-tugas rutin berdasarkan playbook yang telah dirancang.

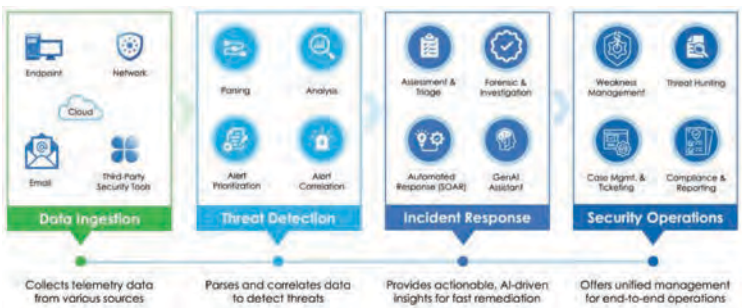
Platform seperti FortiSOAR dari Fortinet, misalnya, sudah mengintegrasikan kecerdasan buatan (*GenAI FortiAI*) untuk membantu analis menyelidiki insiden dan menyusun playbook baru dengan mudah.

Sementara itu, Sangfor Athena NDR menggabungkan modul SOAR langsung ke dalam sistem deteksi ancamannya, memungkinkan respons cepat terhadap aktivitas mencurigakan di jaringan secara real-time.

XDR: Pendekatan Menyeluruh

Jika SOAR berfokus pada otomasi, maka XDR (Extended Detection and Response) berfokus pada visibilitas lintas domain. XDR menggabungkan data dari berbagai sumber — endpoint, jaringan, cloud, email, hingga sistem IAM — dan menganalisisnya menggunakan AI dan machine learning untuk mendeteksi pola serangan yang tidak terlihat secara individual.

Dengan XDR, ribuan alert yang muncul setiap hari dapat disaring dan dikelompokkan menjadi beberapa incident penting dengan konteks yang jelas. Pendekatan ini membantu tim keamanan bertindak lebih cepat dan akurat terhadap ancaman yang tersembunyi.



Gambar# Operasional dari Sangfor Athena XDR

NDR: Melihat Lebih Dalam ke Lalu Lintas Jaringan

Keamanan perimeter dan endpoint saja tidak lagi cukup. Ancaman kini bisa bergerak secara lateral di dalam jaringan internal.
Di sinilah NDR (Network Detection and Response) berperan.

NDR memantau dan menganalisis lalu lintas jaringan *North-South* maupun *East-West*, menggunakan *behavioral analytics* dan *machine learning* untuk mendeteksi aktivitas mencurigakan yang lolos dari lapisan firewall atau EDR.

Teknologi ini sangat efektif dalam menemukan serangan *zero-day* dan komunikasi *command-and-control* yang biasanya tersembunyi dari pengawasan konvensional.

MDR: Solusi Pamungkas yang Dikelola Pihak Ahli

Bagi banyak organisasi, membangun dan mengelola SOC internal 24/7 bukan hal mudah. Di sinilah MDR (Managed Detection and Response) hadir sebagai solusi akhir. Melalui MDR, perusahaan dapat mempercayakan pengawasan dan penanganan ancaman kepada penyedia layanan profesional (MSP).

Layanan ini mencakup pemantauan terus-menerus, investigasi insiden, hingga tindakan mitigasi proaktif — semuanya dilakukan oleh analis SOC yang berpengalaman.

Dengan demikian, tim internal dapat fokus pada prioritas bisnis tanpa mengorbankan keamanan.

Kesimpulan: Perjalanan Menuju SecOps yang Matang

Transformasi digital membawa peluang besar, namun juga tantangan keamanan yang tidak bisa diabaikan. Penerapan SecOps bukanlah proyek sekali jalan — melainkan perjalanan berkelanjutan menuju sistem keamanan yang lebih terintegrasi, otomatis, dan cerdas. Dengan memanfaatkan teknologi seperti log analytics, SIEM, SOAR, XDR, hingga MDR, perusahaan dapat beralih dari pendekatan reaktif menuju strategi proaktif berbasis intelijen ancaman.
Pada akhirnya, keberhasilan SecOps bukan hanya tentang teknologi yang digunakan, tetapi tentang bagaimana kita mengorkestrasi keamanan dengan cerdas, konsisten, dan berkelanjutan.

Sangfor Athena SWG Perlindungan Cerdas untuk Akses Internet Aman

Sangfor Athena Secure Web Gateway (SWG) adalah solusi keamanan modern yang melindungi jaringan perusahaan dari ancaman siber sekaligus menjaga produktivitas di era kerja digital dan hybrid.

Dengan teknologi *AI threat detection, real-time traffic analysis*, dan *advanced web filtering,* Athena SWG mencegah akses berisiko dari malware, unsecured VPN, maupun illegal proxy tools.

Lebih dari sekadar pertahanan, Athena SWG membantu organisasi mengontrol dan memantau aktivitas pengguna agar tetap aman, efisien, dan sesuai kebijakan perusahaan.

Lebih dari sekadar pertahanan, Athena SWG membantu organisasi mengontrol dan memantau aktivitas pengguna agar tetap aman, efisien, dan sesuai kebijakan perusahaan.

Sinergi AIDC dan AI, Membaca Arah Baru Teknologi Industri

Oleh: **Jemis Pangaribuan,** AIDC and Security Technology Manager | **ACS Group**

Di tengah laju transformasi digital yang semakin cepat, istilah seperti automation, real-time data, dan artificial intelligence (AI) makin sering terdengar. Namun, di balik kecanggihan sistem analitik dan pengambilan keputusan otomatis, ada satu teknologi yang menjadi fondasi penting dalam proses pengumpulan datanya — AIDC (Automatic Identification and Data Capture).

AIDC mencakup berbagai metode seperti *barcode*, *RFID*, biometrik, hingga sensor lokasi yang bekerja merekam identitas atau informasi suatu objek dengan cepat dan akurat. Jika AIDC diibaratkan sebagai mata dan telinga yang menangkap data dari lingkungan, maka AI adalah otaknya — yang menafsirkan, menganalisis, dan mengubah data mentah menjadi wawasan yang bermakna.

Ketika keduanya berpadu, terciptalah sistem cerdas yang bukan hanya mampu merekam, tetapi juga memahami dan merespons setiap situasi secara otomatis. Inilah sinergi yang kini sedang mendorong revolusi besar di dunia industri: lebih cepat, lebih aman, lebih efisien, dan lebih adaptif.

Mari kita lihat bagaimana kombinasi AIDC dan AI sudah mengubah wajah berbagai sektor penting — dari transportasi hingga rantai pasok global.

1. Bandara & Transportasi: *Touchless Boarding* untuk Pengalaman Baru

Bayangkan suasana bandara internasional di jam sibuk — antrean panjang, penumpang memegang boarding pass, petugas sibuk memindai tiket. Kini, pemandangan itu mulai berubah.

Berbekal teknologi biometrik yang terintegrasi dengan AI, proses *boarding* dapat berlangsung tanpa sentuhan. Penumpang cukup berdiri di depan kamera beberapa detik, sistem mengenali wajah, dan gerbang terbuka otomatis. Tidak ada tiket kertas, tidak ada antrean panjang — hanya proses cepat dan aman yang memberi pengalaman perjalanan lebih nyaman.

2. Ritel & Smart Checkout: Pengawasan Otomatis yang Lebih Cerdas

Mesin self-checkout di kasir memang praktis, tetapi tidak lepas dari risiko kesalahan — baik karena lupa memindai barang maupun tindakan sengaja.

Di sinilah AIDC dan AI saling melengkapi. Barcode atau RFID memindai barang (fungsi AIDC), sementara kamera AI vision memantau proses transaksi. Jika ada item yang keluar tanpa terdeteksi, sistem segera memberi peringatan. Hasilnya, efisiensi tetap terjaga tanpa mengorbankan keamanan dan akurasi.

3. Gudang & Logistik: *PalletSCAN 360°* yang Hemat Waktu

Dalam dunia logistik, waktu adalah segalanya. Dulu, petugas harus memutar pallet untuk membaca label dari setiap sisi — proses yang memakan waktu dan rawan salah.

Kini, teknologi kamera multi-sisi yang didukung AI mampu membaca semua label sekaligus dalam satu kali lewat di jalur konveyor. Informasi pallet langsung tercatat secara otomatis. Hasilnya: proses lebih cepat, data lebih akurat, dan operasional lebih efisien.

4. Kesehatan & Rumah Sakit: *Smart Bed Management*

Masalah klasik rumah sakit adalah keterlambatan rotasi tempat tidur pasien. Sering kali, bed kosong tidak segera digunakan karena petugas kebersihan belum mendapat informasi.

Dengan smart bed management, setiap tempat tidur dilengkapi RFID atau RTLS tag. Begitu pasien keluar, sistem otomatis mengubah status bed dan mengirim notifikasi ke tim kebersihan. AI memastikan koordinasi berjalan cepat dan lancar, sehingga pelayanan kepada pasien berikutnya bisa segera dilakukan.

5. Pertambangan & Pabrik: *PPE Compliance Monitoring*

Di area industri berat, keselamatan kerja adalah prioritas utama. Namun, memastikan setiap pekerja mengenakan *Personal Protective Equipment (PPE)* dengan benar bukan hal mudah.

Kini, kamera *AI vision* di pintu masuk mampu memverifikasi pemakaian APD secara otomatis.

AIDC memastikan identitas pekerja, sementara AI menilai kelengkapan helm, rompi, atau kacamata pelindung. Sistem ini tidak hanya meningkatkan keselamatan, tapi juga memastikan kepatuhan terhadap standar operasional.

6. Rantai Pasok & Anti-Pemalsuan: Membangun Kepercayaan dengan *Traceability*

Produk palsu menjadi ancaman besar di banyak industri — dari farmasi, elektronik, hingga barang mewah. Untuk mencegahnya, produsen kini memanfaatkan kombinasi *RFID traceability* dan *AI anomaly detection*.

Setiap produk diberi tag unik yang terbaca otomatis di setiap titik distribusi. AI menganalisis pola pengiriman, dan jika ada pergerakan tidak wajar, sistem langsung menandai. Dengan cara ini, transparansi rantai pasok meningkat, dan konsumen terlindungi dari produk tiruan.

Mengapa Sinergi AIDC + AI Penting?

Kombinasi keduanya membawa nilai tambah nyata bagi dunia industri:

Kecepatan & Efisiensi

AIDC menangkap data secara otomatis, sementara AI mempercepat analisis dan pengambilan keputusan hanya dalam hitungan detik.

Akurasi Tinggi

Risiko kesalahan manusia menurun drastis, terutama dalam pencatatan dan pelacakan data.

Keamanan & Kepatuhan

Dari bandara hingga pabrik, sistem terintegrasi ini memperkuat pengawasan dan memastikan standar keselamatan terpenuhi.

Tantangan dan Masa Depan

Meski potensinya besar, adopsi teknologi ini tidak lepas dari tantangan seperti biaya awal yang cukup besar, proses integrasi dengan sistem lama, serta isu privasi data — terutama untuk biometrik.

Namun arah perkembangan industri sudah jelas. *Smart automation* bukan lagi masa depan, melainkan kebutuhan hari ini. Dalam beberapa tahun ke depan, sinergi AIDC dan AI diprediksi akan menjadi standar utama operasional industri global.

Penutup

Sinergi antara AIDC dan AI menjadi bukti nyata bagaimana teknologi mampu mengubah cara kita bekerja, bergerak, dan mengambil keputusan. Dari bandara yang lebih cepat dan aman, toko yang lebih cerdas, gudang yang lebih efisien, rumah sakit yang lebih responsif, hingga pabrik yang lebih patuh terhadap keselamatan — semuanya berawal dari data yang ditangkap dan dipahami dengan cerdas.

Jika dulu AIDC hanya berperan sebagai alat pencatat data, kini bersama AI ia bertransformasi menjadi mesin pengambil keputusan yang mempercepat langkah industri menuju masa depan digital.

Satu kesimpulan jelas: **perusahaan yang mampu mengintegrasikan AIDC dan AI lebih awal akan menjadi pionir di tengah kompetisi global yang semakin ketat.**

Newland N7 Cachalot Pro II – Tangguh di Segala Suhu, Andal di Setiap Misi

Newland N7 Cachalot Pro II dirancang untuk performa tanpa kompromi, bahkan dalam kondisi ekstrem. Beroperasi stabil di suhu antara -20°C hingga 60°C, perangkat ini menjadi solusi ideal bagi industri logistik, pergudangan, maupun operasional *cold storage* yang menuntut ketahanan tinggi.

Dibekali sertifikasi lingkungan tangguh dan *Ingress Protection* (IP) tinggi, N7 memastikan daya tahan optimal terhadap suhu ekstrem, debu, dan kelembapan. Didukung *Wi-Fi 5G, Bluetooth,* dan *NFC,* konektivitas data tetap cepat dan stabil kapan pun dibutuhkan.

Dengan sistem operasi Android 10 dan prosesor Qualcomm, N7 siap menjalankan aplikasi bisnis dengan mulus. Teknologi *Duo Near & Far Scan* memudahkan pemindaian barang dari jarak dekat maupun jauh, sementara kamera 8MP dengan LED dinamis menjamin hasil dokumentasi tetap jelas meski di area minim cahaya.

Baterai 5100mAh yang diisi cepat melalui *USB Type-C* memberikan daya tahan optimal untuk satu siklus kerja penuh

Newland N7 – karena produktivitas tidak mengenal suhu

Sinergi Enterprise Security System dan AI

Oleh: **Jemis Pangaribuan,** AIDC and Security Technology Manager | **ACS Group**

Membangun Keamanan Cerdas untuk Industri Modern

Di tengah transformasi digital yang semakin pesat, keamanan tidak lagi hanya berbicara tentang pagar dan kamera pengawas. Industri modern membutuhkan sistem yang mampu berpikir dan bereaksi cepat terhadap ancaman yang terus berkembang. Membangun keamanan cerdas berarti menggabungkan teknologi *enterprise security system* dengan kecerdasan buatan (Artificial Intelligence) untuk menciptakan perlindungan yang adaptif, prediktif, dan efisien. AI memungkinkan sistem mengenali pola, menganalisis perilaku, serta merespons ancaman sebelum terjadi. Dengan pendekatan ini, perusahaan tidak hanya melindungi aset fisik dan data, tetapi juga meningkatkan efisiensi operasional serta kepercayaan pelanggan. Inilah fondasi baru keamanan industri: cerdas, terintegrasi, dan siap menghadapi tantangan era digital.

A. Bandara dan Transportasi

Proses Bisnis

1. Penumpang memasuki area check-in → sistem biometrik mengidentifikasi wajah secara otomatis.
2. AI melakukan verifikasi identitas terhadap database imigrasi.
3. Kamera vision AI di boarding gate menganalisis pola gerakan penumpang untuk mendeteksi barang tertinggal atau perilaku abnormal.
4. Sistem mengirimkan alert ke petugas keamanan hanya dalam hitungan detik.

Manfaat:

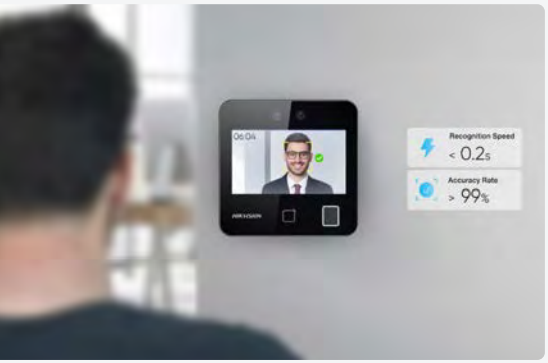
- **Mengurangi antrean imigrasi hingga 40%.**
- **Menekan penyalahgunaan identitas palsu.**
- **Meningkatkan deteksi dini terhadap ancaman.**

Studi kasus:

Sebuah bandara besar di Asia Tenggara menerapkan sistem biometric-AI pada proses imigrasi. Hasilnya, waktu antrean turun 35%, dan penyalahgunaan identitas hampir hilang.

Analisis ROI:

Meski investasi awal besar, efisiensi tenaga kerja dan peningkatan kapasitas penumpang membuat biaya operasional turun 20% dalam tiga tahun.



B. Perbankan dan Keuangan

Proses Bisnis

1. Nasabah masuk ke cabang → kamera AI melakukan *face recognition*.
2. Jika terdeteksi individu dalam daftar hitam, sistem otomatis mengunci area tertentu.
3. Aktivitas cabang diawasi secara *real-time*.
4. Data transaksi dan perilaku dianalisis bersama untuk mendeteksi potensi *fraud*.

Manfaat:

- **Meningkatkan keamanan dengan deteksi dini terhadap aktivitas mencurigakan dan fraud.**
- **Mengurangi ketergantungan pada pemantauan manual, sehingga efisiensi operasional meningkat.**
- **Menghadirkan pengalaman yang lebih aman dan nyaman bagi nasabah, baik di cabang maupun ATM.**
- **Meminimalkan risiko perampokan fisik dan penyalahgunaan identitas.**
- **Mempercepat proses identifikasi nasabah, terutama bagi yang sudah terdaftar.**
- **Memberikan data analitik yang membantu pengambilan keputusan terkait keamanan dan manajemen risiko.**
- **Melindungi reputasi institusi dari kerugian finansial serta potensi pelanggaran regulasi.**

Studi kasus:

Sebuah bank multinasional menggunakan AI untuk mendeteksi perilaku abnormal seperti nasabah yang berulang kali berkeliling tanpa alasan jelas.
AI berhasil memberi *alert* dini dan mencegah perampokan bersenjata.

Analisis ROI:

Kerugian akibat *fraud* perbankan dapat mencapai jutaan dolar per kasus. Dengan sistem AI, potensi kerugian berhasil ditekan hingga 40%, dan ROI tercapai dalam 18–24 bulan.

C. Pabrik dan Pertambangan

Proses Bisnis

1. Pekerja masuk ke area tambang → verifikasi ID dan wajah dilakukan otomatis.
2. Kamera AI memastikan penggunaan *APD* (helm, rompi, kacamata).
3. Sistem memberi peringatan jika pekerja terlalu dekat dengan alat berat atau zona berbahaya.
4. Semua data tersimpan untuk kebutuhan audit K3.

Manfaat:

- **Mengurangi kecelakaan kerja fatal.**
- **Mencegah pencurian material bernilai tinggi.**
- **Memenuhi regulasi keselamatan secara digital.**

Studi kasus:

Perusahaan tambang di Australia menolak akses bagi pekerja tanpa APD lengkap. Hasilnya, tingkat kecelakaan kerja turun 25% dalam satu tahun.

Analisis ROI:

Dengan menekan jumlah insiden, perusahaan memperoleh balik modal dalam dua tahun berkat efisiensi dan penghematan biaya kecelakaan.

D. Rumah Sakit dan Kesehatan

Proses Bisnis

1. Sistem *face recognition* mencatat identitas setiap pasien dan pengunjung.
2. Area sensitif seperti ICU atau farmasi hanya bisa diakses staf berotorisasi.
3. Kamera AI memantau aktivitas abnormal dan memberi peringatan *real-time*.

Manfaat:

- **Melindungi data pasien.**
- **Mengurangi pencurian obat bernilai tinggi.**
- **Meningkatkan rasa aman pasien dan keluarga.**

Studi kasus:

Rumah sakit swasta di Eropa berhasil menurunkan pencurian obat hingga 60% setelah menerapkan sistem keamanan berbasis AI.

Analisis ROI:

Kerugian akibat kehilangan obat dapat ditekan signifikan, dengan pengembalian investasi dalam 12–18 bulan.

E. Retail dan Mall

Proses Bisnis

1. Kamera AI di kasir membandingkan barang yang discan dengan yang keluar.
2. Sistem mendeteksi pencurian atau kelalaian kasir secara otomatis.
3. Notifikasi dikirim ke pusat kontrol untuk tindakan cepat.

Manfaat:

Menekan *shrinkage* hingga di bawah 1%.

Mencegah *fraud kasir.*

Meningkatkan kenyamanan pelanggan.

Studi kasus:

Jaringan supermarket global menerapkan sistem ini di 100 cabang dan berhasil menurunkan *shrinkage* hingga 40% dalam enam bulan.

Analisis ROI:

Dengan rata-rata kehilangan omzet 1,5–2% per tahun, ROI tercapai hanya dalam 12–15 bulan setelah implementasi AI.

F. Energi dan Utilitas

Proses Bisnis

1. Pembangkit listrik dilengkapi sensor perimeter dan kamera *thermal AI.*
2. Sistem mampu mendeteksi intrusi bahkan dalam kondisi gelap total.
3. AI otomatis mengaktifkan alarm dan mengunci akses.
4. Semua data dikirim ke *command center* nasional.

Manfaat:

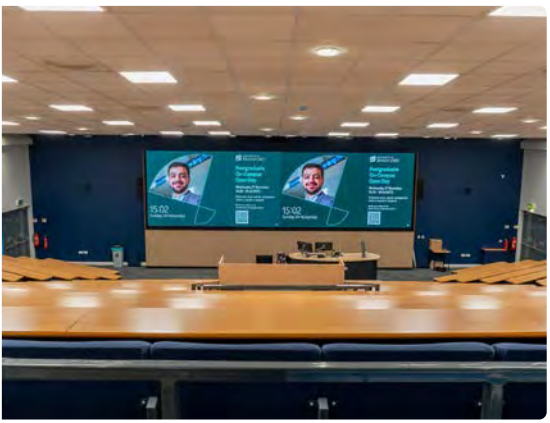
- **Melindungi infrastruktur vital negara.**
- **Mencegah sabotase dan terorisme.**
- **Respon otomatis dalam hitungan detik.**

Studi kasus:

Perusahaan energi nasional menggunakan kamera *thermal* berteknologi AI yang berhasil menggagalkan upaya sabotase di malam hari.

Analisis ROI:

Selain penghematan finansial, nilai ROI juga terletak pada perlindungan reputasi dan stabilitas nasional.



G. Kampus dan Pendidikan

Proses Bisnis

1. Mahasiswa masuk menggunakan ID card dan *face recognition*.
2. Kamera AI mendeteksi kerumunan atau perkelahian.
3. Laboratorium sensitif dibatasi untuk staf resmi.
4. Sistem terhubung langsung ke aparat keamanan jika ada ancaman serius.

Manfaat:

- **Menjamin keamanan lingkungan akademik.**
- **Mengurangi vandalisme dan akses ilegal.**
- **Meningkatkan reputasi kampus.**

Studi kasus:

Universitas di Jepang mencatat penurunan kasus vandalisme hingga 50% dalam satu tahun setelah menerapkan sistem AI security.

Analisis ROI:

Selain penghematan biaya kerusakan, reputasi kampus meningkat signifikan. ROI tercapai dalam 2–3 tahun.

Tren Masa Depan - Ke Mana Arah Security + AI?

1. **AI Predictive Security**
   bukan sekadar mendeteksi, tetapi mampu memprediksi ancaman berdasarkan pola perilaku jangka panjang.

2. **Integrasi Fisik dan Siber**
   keamanan gedung dan data akan menyatu dalam satu sistem terpadu.

3. **Edge AI Security**
   analisis langsung di perangkat (on-device), tanpa tergantung server pusat.

4. **Zero Trust Security**
   setiap akses diverifikasi ulang tanpa ada "akses permanen".

5. **Green Security System**
   teknologi keamanan yang hemat energi dengan sensor pintar berdaya rendah.

Kesimpulan

Sinergi antara *enterprise security system* dan AI bukan lagi masa depan — melainkan kebutuhan saat ini. Dari bandara hingga rumah sakit, bukti menunjukkan bahwa integrasi keduanya meningkatkan keamanan, efisiensi, dan kepercayaan publik.
Lebih dari sekadar kamera atau biometrik, AI menjadikan sistem keamanan berpindah dari reaktif menjadi proaktif bahkan prediktif.

Meskipun investasi awalnya cukup besar, hasil yang diperoleh jelas: penghematan biaya, efisiensi tenaga kerja, penurunan kerugian, serta peningkatan produktivitas — dengan balik modal rata-rata hanya dalam 1–3 tahun.

Rekomendasi:

1. Mulailah dari *pilot project* di area paling kritis.
2. Lakukan integrasi bertahap agar staf beradaptasi dengan sistem baru.
3. Libatkan tim keamanan fisik dan TI dalam satu ekosistem keamanan terpadu.

Dengan strategi yang tepat, perusahaan bukan hanya melindungi aset, tetapi juga membangun fondasi kepercayaan, efisiensi, dan keberlanjutan jangka panjang.

Peran ACS Group dalam Solusi Keamanan Berbasis AI

ACS Group memiliki keahlian dalam merancang dan mengimplementasikan sistem keamanan cerdas berbasis AI, baik menggunakan kamera yang dimiliki pelanggan maupun perangkat baru dari ACS Group. Teknologi AI dapat ditempatkan langsung di dalam kamera (*embedded AI*) atau melalui perangkat eksternal yang disebut AI Box. Fleksibilitas ini memungkinkan sistem beradaptasi dengan kebutuhan dan infrastruktur pelanggan, tanpa harus mengganti seluruh perangkat yang sudah ada.

Dengan pengalaman dan solusi terintegrasi yang dimiliki, ACS Group siap membantu perusahaan membangun sistem keamanan cerdas yang efisien, modern, dan berkelanjutan.

Selamat Hari Natal 2025 *dan* Tahun Baru 2026

Management dan seluruh Staff **ACS Group** mengucapkan selamat merayakan hari Natal yang penuh kasih, damai dan sukacita. Kiranya kehangatan dan kebersamaan di momen ini membawa harapan baru bagi kita semua. Menyongsong tahun 2026, mari kita melangkah dengan semangat baru, tekad yang lebih kuat, dan optimisme untuk terus bertumbuh serta memberikan yang terbaik bagi pelanggan setia, mitra, dan lingkungan sekitar.

Selamat menyambut tahun yang penuh peluang dan keberhasilan.... Amin !!!

Zebra MC9401 - Ketangguhan dan Kecepatan Tanpa Batas

Dirancang untuk lingkungan paling menantang, Zebra MC9401 menghadirkan evolusi terbaru dari seri legendaris MC9000. Dengan dukungan *Wi-Fi 6E* dan *Private & Public 5G,* perangkat ini memberikan konektivitas tercepat, stabil, dan siap mendukung aplikasi industri generasi baru. Pemindaian jarak jauh hingga 30 meter, prosesor lebih cepat, serta ketahanan luar biasa menjadikannya solusi ideal untuk sektor manufaktur, logistik, dan ritel.
Dual SIM (*nano SIM & eSIM*) memberikan fleksibilitas tinggi dalam pengelolaan jaringan, sementara *Bluetooth 5.3* meningkatkan efisiensi dan keamanan koneksi.

MC9401 – performa andal untuk produktivitas tanpa kompromi.

Zebra TC22R - Ringkas, Cepat, dan Efisien untuk RFID Modern

Zebra TC22R menghadirkan kemampuan *UHF RFID* reader terintegrasi dalam desain *all-in-one* yang ringan dan ergonomis. Dengan kecepatan baca hingga 1.300 tag per detik, perangkat ini memungkinkan pelacakan aset dan inventori lebih cepat dan akurat tanpa kelelahan pengguna.
Didukung *Android Enterprise, Wi-Fi 6,* dan *Bluetooth,* TC22R mudah dikelola melalui sistem *Mobile Device Management* yang sudah ada.
Dilengkapi NFC dan aplikasi POS mobile, TC22R memberikan fleksibilitas penuh bagi bisnis modern.

Zebra TC22R – efisiensi tinggi dalam genggaman yang ringan.

Digital Impact for Patient Safety: Through Digital Identification with a Proper Cyber Threat Protection

Dalam rangka memperingati Hari Keselamatan Pasien pada 17 September, ACS Group bersama Zebra Technologies dan HPE Aruba Networking mengadakan Seminar Solution bertema “Digital Impact for Patient Safety: Through Digital Identification with a Proper Cyber Threat Protection” di Binakarna Auditorium, Hotel Bidakara, Jakarta.

Dengan transformasi digital yang semakin kuat, keselamatan pasien harus dijaga melalui akurasi identifikasi dan perlindungan sistem rumah sakit. Zebra Technologies menghadirkan solusi patient identification, specimen tracking, hingga medication administration, termasuk Laundry Tracking System (LTS) berbasis RFID yang mendukung kepatuhan terhadap Permenkes No. 27 Tahun 2017 dalam mencegah penyebaran infeksi pada proses laundry medis.

Sementara itu, Aruba Networking memperkuat keamanan siber rumah sakit melalui pendekatan SASE. ACS Group sekaligus memastikan keamanan fisik sesuai Permenkes No. 40 Tahun 2022 dan Permenkes No. 66 Tahun 2016.

Melalui seminar ini, ACS Group menegaskan komitmennya mendukung sektor kesehatan Indonesia untuk menghadirkan perjalanan pasien yang aman, efisien, dan tetap mengikuti standar keselamatan nasional.

ACS Group & Solum Dukung Transformasi Digital di Hari Ritel Nasional 2025

ACS Group bersama Solum turut hadir dalam rangkaian acara Hari Ritel Nasional (HRN) 2025 yang berlangsung pada 4–6 November serta puncak perayaannya pada 11 November. Kehadiran ACS Group dan Solum tidak hanya melalui booth pameran, tetapi juga melalui sesi presentasi yang memperkenalkan solusi teknologi untuk mendukung percepatan transformasi digital di industri ritel Indonesia.

Hari Ritel Nasional sendiri diperingati setiap 11 November sebagai bentuk apresiasi terhadap kontribusi sektor ritel bagi perekonomian nasional. Diselenggarakan oleh Asosiasi Pengusaha Ritel Indonesia (APRINDO), HRN menjadi momentum sinergi antara pemerintah, pelaku usaha, dan mitra teknologi untuk menghadapi tantangan industri mulai dari regulasi, efisiensi operasional, hingga kesiapan ritel masuk ke pasar global.

Dalam HRN 2025, Solum tampil sebagai salah satu mitra teknologi yang memamerkan solusi Electronic Shelf Label (ESL), menggantikan label harga kertas tradisional dengan sistem digital yang lebih efisien dan akurat. Keikutsertaan Solum selaras dengan tema HRN tahun ini, “Kebangkitan Ritel: Bertumbuh Bersama UMKM, Bergerak ke Pasar Global,” yang menekankan pentingnya inovasi teknologi untuk mendukung modernisasi dan daya saing ritel Indonesia.

Hikvision DS-K1T342MFX - Akses Cepat, Aman, dan Efisien

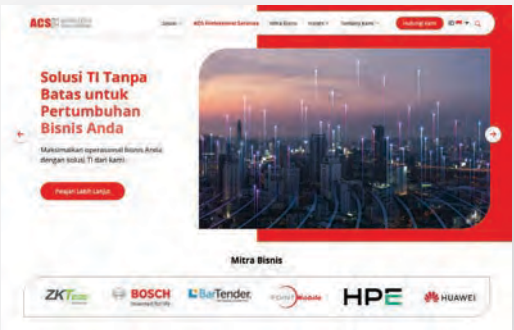
Hikvision DS-K1T342MFX adalah terminal *face recognition* modern yang menghadirkan kemudahan dan keamanan tinggi untuk kebutuhan kontrol akses dan absensi karyawan.

Dengan teknologi pengenalan wajah berkecepatan tinggi dan akurasi tinggi, perangkat ini mampu mengidentifikasi individu hanya dalam hitungan detik, bahkan dalam kondisi pencahayaan yang beragam.

Cocok untuk gedung perkantoran, fasilitas industri, hingga area publik seperti stasiun, perangkat ini memastikan akses yang efisien tanpa kartu atau sentuhan fisik.

Hikvision DS-K1T342MFX – solusi presisi tinggi untuk keamanan dan manajemen kehadiran yang lebih cerdas

Transformasi Digital Website dan Bulletin ACS Group Hadir dengan Tampilan Baru



Dalam rangka memperkuat komunikasi dan mengikuti perkembangan teknologi, ACS Group telah merampungkan proses *revamp website* resmi serta *rebrand* bulletin perusahaan.

Website kami kini hadir dengan tampilan yang lebih modern, navigasi yang lebih intuitif, serta informasi yang tersaji secara lebih terstruktur dan responsif di berbagai perangkat.

Pembaruan ini diharapkan dapat mempermudah pengunjung dalam mengakses informasi seputar solusi yang kami tawarkan untuk mendukung kebutuhan bisnis Anda.

Sementara itu, bulletin ACS Group kini telah berganti nama menjadi Nol Satu: Detak Transformasi Digital, menggantikan nama sebelumnya, *AutoID*. Dengan desain yang lebih segar dan konten yang lebih komunikatif, bulletin ini diharapkan menjadi media yang mencerminkan semangat inovasi serta arah transformasi digital perusahaan.

Melalui langkah ini, ACS Group terus menunjukkan komitmennya dalam menciptakan saluran komunikasi yang relevan, adaptif, dan selaras dengan perkembangan teknologi.

Sangfor SE Summit 2025

Sangfor SE Summit 2025 sukses digelar pada 26 – 28 Agustus 2025 di Mercure PIK Jakarta, menghadirkan lebih dari 80 partner dari berbagai daerah. Selama tiga hari, peserta mengikuti rangkaian sesi ini yang dirancang secara intensif dan eksklusif untuk meningkatkan kompetensi teknis serta pemahaman solusi Sangfor.

Hari I : Memperdalam Solusi Keamanan Siber (Cyber Security Solutions), disertai ujian sertifikasi.

Hari II : Menguasai Solusi Cloud Infrastructure dan inovasi cloud terkini disertai ujian sertifikasi. Pembahasan ini penting karena perusahaan modern kini mengedepankan efisiensi, fleksibilitas, dan ketahanan infrastruktur IT.

Hari III : Menghadirkan Roleplay Session yang interaktif, melatih peserta menghadapi skenario nyata di dunia kerja.

Acara ini tidak hanya menjadi ajang pembelajaran, tetapi juga sarana berharga untuk berbagi pengalaman, memperluas wawasan, dan mempererat kolaborasi antar partner dengan principal.

BMF

ACS Group kembali menggelar Branch Manager Forum (BMF) pada 15–16 Oktober 2025, sebuah agenda rutin setiap semester yang mempertemukan seluruh kepala cabang ACS Group dari Cikarang, Bali, Surabaya, dan Semarang. Forum ini menjadi wadah strategis untuk menyelaraskan visi, mengevaluasi kinerja, dan merumuskan arah pengembangan bisnis ke depan.

Melalui sesi diskusi interaktif dan presentasi capaian, para branch manager berbagi insight, tantangan, serta strategi dalam menghadapi dinamika pasar di masing-masing wilayah. Kegiatan ini juga memperkuat kolaborasi dan membangun budaya kerja yang solid lintas cabang.

Selain menjadi ajang koordinasi bisnis, forum ini juga menjadi momen apresiasi atas dedikasi dan kontribusi seluruh cabang dalam menjaga kualitas layanan. Dengan semangat kebersamaan yang tinggi, ACS Group terus menegaskan komitmennya untuk tumbuh dan berkembang bersama.

Melalui kegiatan ini, diharapkan setiap cabang dapat membawa semangat baru dalam memperkuat posisi ACS Group sebagai mitra solusi teknologi terpercaya di Indonesia. Sinergi yang terbangun di forum ini menjadi fondasi kuat untuk menghadapi tantangan bisnis di masa depan.

Teamwork makes the dream works.

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 Security System

Enterprise Business Solution

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

Pemakaian Unit Mobile Computer di Dalam Warehouse Cold Storage

Oleh: **Agung Atmoko,** ESDA – Services Assurance Supervisor | **ACS Group**

Mengoperasikan perangkat *mobile computer* di lingkungan cold storage memerlukan perhatian khusus agar kinerjanya tetap optimal dan tahan lama. Suhu ekstrem dapat memengaruhi performa perangkat dan daya tahan komponennya, terutama jika tidak disesuaikan dengan prosedur penggunaan yang tepat. Pastikan unit yang digunakan sudah memiliki sertifikasi suhu kerja yang sesuai, misalnya pada rentang –20°C hingga 60°C.

Berikut beberapa tips praktis agar perangkat Anda tetap andal di lingkungan bersuhu rendah:

1. Persiapan Perangkat dan Lingkungan

Aklimatisasi Perangkat

Jangan langsung membawa perangkat dari suhu ruangan yang hangat ke area bersuhu sangat rendah. Biarkan perangkat beradaptasi secara bertahap di area transisi yang lebih sejuk. Langkah sederhana ini membantu mencegah *condensation* yang dapat merusak komponen internal.

Pengisian Penuh Baterai

Baterai akan lebih cepat berkurang di suhu dingin. Pastikan perangkat terisi penuh sebelum digunakan, dan siapkan baterai cadangan yang juga sudah terisi.

Sarung Tangan yang Kompatibe

Gunakan sarung tangan yang mendukung layar sentuh agar pengguna tetap dapat mengoperasikan perangkat tanpa perlu melepasnya. Beberapa unit bahkan memiliki *glove mode* yang bisa diaktifkan pada menu pengaturan.

2. Pengoperasian di Dalam Cold Storage

Minimalkan Kontak dengan Suhu Ekstrem

Hindari menaruh perangkat langsung di permukaan logam atau dinding yang sangat dingin. Gunakan *holster* atau pelindung untuk mengurangi paparan langsung terhadap suhu ekstrem.

Perlindungan dari Kondensasi

Saat keluar dari area dingin ke area hangat, biarkan perangkat beradaptasi di area transisi agar embun menguap alami. Jangan menyeka permukaan perangkat secara langsung; biarkan kering sendiri. Beberapa pengguna menyiasatinya dengan menempatkan perangkat di kantong plastik tertutup rapat saat keluar dari area cold storage untuk menghindari paparan udara hangat secara tiba-tiba.

Aktifkan Mode Tidur atau Hemat Daya

Gunakan *power saving mode* saat perangkat tidak digunakan dalam waktu singkat. Ini membantu memperpanjang masa pakai baterai.

Periksa Suhu Operasional

Selalu pastikan perangkat beroperasi dalam suhu yang direkomendasikan pabrikan. Meskipun dirancang untuk kondisi industri, suhu ekstrem tetap bisa menurunkan performa perangkat.

3. Perawatan dan Pemeliharaan

Pembersihan Teratur

Bersihkan perangkat dari debu atau kotoran menggunakan kain lembut dan kering. Hindari cairan pembersih yang keras karena dapat merusak lapisan pelindung perangkat.

Inspeksi Fisik Rutin

Periksa layar, port, dan area pemindai secara berkala. Aktivitas di gudang yang padat meningkatkan risiko benturan atau kerusakan fisik ringan.

Manajemen Baterai

Ganti baterai jika kapasitasnya mulai menurun signifikan. Penggunaan rutin di suhu dingin dapat mempercepat degradasi sel baterai.

Pembaruan Software dan *Firmware*

Pastikan sistem perangkat selalu diperbarui agar tetap mendapatkan performa terbaik serta peningkatan keamanan dan stabilitas.

4. Tips Tambahan

Berikan Pelatihan kepada Operator

Pastikan setiap pengguna memahami cara mengoperasikan perangkat di lingkungan dingin, termasuk langkah aklimatisasi dan cara merawat unit dengan benar.

Gunakan Aksesori Pelindung

Pertimbangkan penggunaan *rugged case* atau pelindung tambahan yang dirancang khusus untuk area bersuhu ekstrem.

Sistem Pemasangan Aman

Gunakan *holster* atau sistem pemasangan yang kuat dan mudah dijangkau untuk mencegah risiko terjatuh saat perangkat tidak digunakan.

Dengan mengikuti panduan ini, Anda dapat memaksimalkan efisiensi kerja sekaligus memperpanjang usia perangkat di lingkungan gudang *cold storage* yang penuh tantangan.
Sebagai ilustrasi, bayangkan seorang operator dengan pakaian pelindung tebal sedang menggunakan unit Newland N7 di tengah suhu beku — tetap produktif, efisien, dan aman berkat perangkat yang siap menghadapi kondisi ekstrem.

ACS Group Principals

Alibaba Cloud · Allied Telesis · BarTender · brother at your side

BOSCH · Cambium Networks · eG Innovations · Extreme

FORTINET · HID · HIKROBOT · HIKVISION · HPE

Hytera · HUAWEI · ivanti · JANZ · MOTOROLA SOLUTIONS

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

Seuic · SOLUM · ZEBRA · ZKTeco · 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,
Ngaliyan, 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

+62 81 1194 4534 · @acsgroup.co.id · @acsgroup.co.id
acsgroup.official · @acsgroupcoid · acsgroup.co.id

Hubungi ›
Kembali Ke Daftar Isi