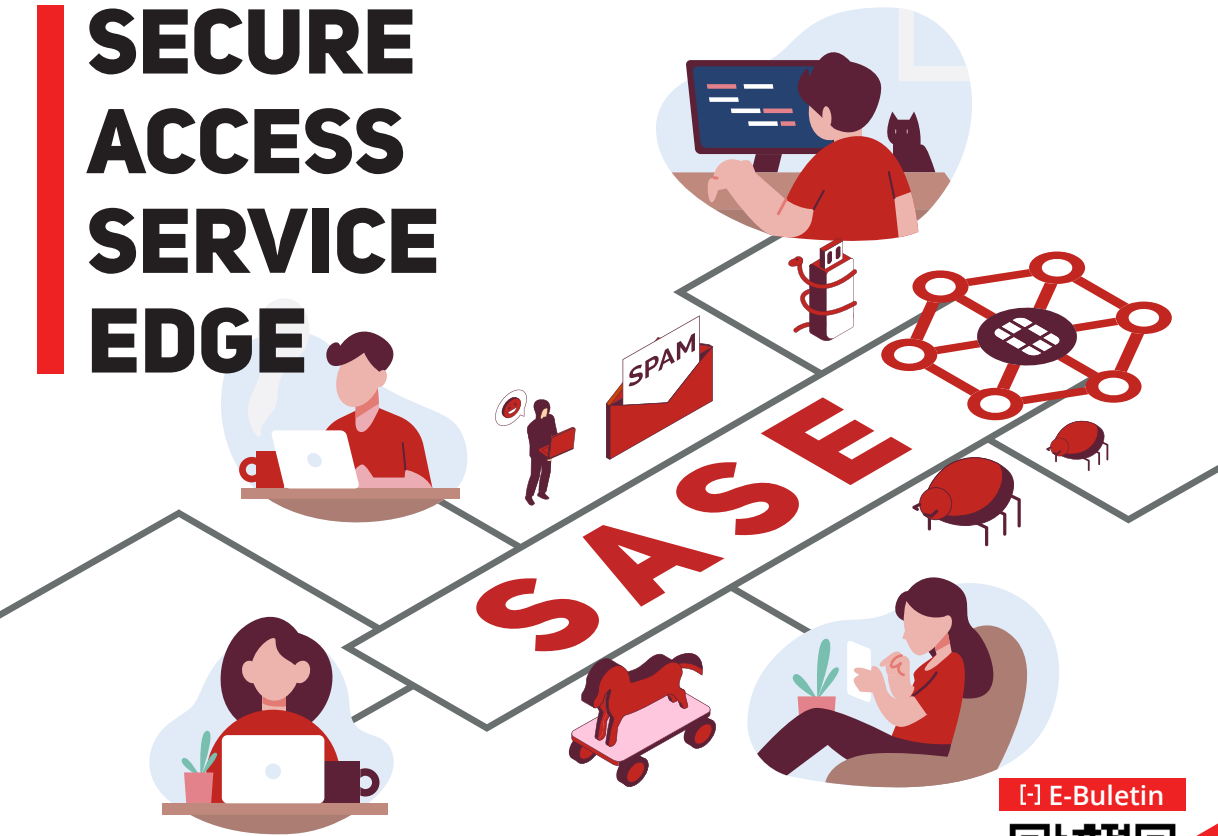


UNTUK KALANGAN SENDIRI

SECURE ACCESS SERVICE EDGE



[-] E-Buletin



**MEDIA KOMUNIKASI
PELANGGAN**

ACS GROUP

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

■ FORTINET ANALYZER

MACHINE VISION

Tips & Info:

Beberapa Cara Efektif Mengamankan Sistem Keamanan Jaringan Komputer Anda



The Ultimate Tool for Improving Efficiency in Workers' Hands

Equip your workers with the right tools to get the job done faster, smarter, and better with Zebra's portfolio of mobile computing hardware and software.

Zebra Technologies provides the Mobile computers **TC15** and **TC26** as reliable and rugged devices, for different environments and for different jobs — from manufacturing, transportation and logistics to retail.

This solution from Zebra uses Wi-Fi or 3G / 4G wireless technology, runs on Windows® or Android™ operating systems and enables workers to do their best, shift after shift.

Additional features, Workforce Connect Push-to-Talk (PTT) Pro2 Mobility DNA - pro licensed, easy-to-deploy and cost-effective.

Contact us, we are ready to help you to provide appropriate solutions for your business activities to make it more efficient and effective.

EDITORIAL

Para pembaca yang budiman,

Kali ini kami membahas 3 solusi yang menjawab tantangan digitalisasi di era *post-pandemic* yang seterusnya akan terus diwarnai WFH/WFA, usaha sentralisasi manajemen dari keamanan data dan jaringan, dan efisiensi otomatisasi dari proses *supply chain*.

Fenomena *Work From Anywhere* yang berlanjut setelah pandemi memerlukan mitigasi keamanan siber yang mumpuni agar komunikasi dan sharing data perusahaan dapat dilaksanakan tanpa menyebabkan *bottleneck*. FortiSASE hadir sebagai solusi konvergensi berbagai *security tools* dengan *cloud-based implementation*.

Banyaknya *security alert* dapat mengakibatkan staf IT kewalahan dan memakan waktu yang tidak sedikit jika harus ditindak satu persatu tanpa adanya sebuah automasi SOP. FortiAnalyzer menyediakan modul automasi administrasi yang dapat memaksimalkan visualisasi laporan dan kemudian membentuk buku pedoman yang komprehensif.

Proses *quality control* membutuhkan mata yang teliti dan jeli untuk mendeteksi dan identifikasi titik spesifik tertentu yang mungkin tidak sesuai dengan spesifikasi yang direncanakan. Teknologi *Machine Vision* dapat memberikan ketepatan

perhitungan dengan tempo yang jauh lebih cepat daripada pemeriksaan manual.

Selamat menikmati ulasan singkat di atas serta berbagai informasi lainnya seperti corporate info, tips & info dan info lainnya. Jangan sungkan untuk melanjutkan diskusi dengan kami jika ada topik yang dapat mengoptimalkan proses bisnis anda, kami siap untuk membantu.

Salam Hangat,

Ken Looho

Professional Services, NSE3

PT. Autojaya Idetech

PT. Solusi Periferal



PEMIMPIN REDAKSI

Andre S.Kouanak

SEKRETARIS REDAKSI

Listya Kartikasari (Jakarta)

Indah Widiyanti (Cikarang)

Luh Wayan Sumariani (Denpasar)

Herdina Septiyaningrum (Semarang)

Sari Wilujeng (Surabaya)

EDITOR

Nuning Kustiawita

Chandra Sari

DESAINER

Oscar Budi Trianto

KONTRIBUTOR (PENULIS)

Ken Looho

Ihdi Arwan

Irvan Kurniawan

ALAMAT REDAKSI

Jakarta (HO)

Perkantoran Gunung Sahari Permai

#C03-05, Jl. Gunung Sahari Raya

No 60-63 Jakarta 10610.

T : +6221-4208221, 4205187

E : acs.marcom@acsgroup.co.id

CONTENT

3 Editorial - **Ken Looho**

4 SASE - Secure Access Service Edge

14 Fortinet Analyzer

16 Machine Vision

18 News & Event

24 Product Highlight

27 Corporate & Principal Info

34 Beberapa Cara Efektif
Mengamankan Sistem Keamanan Jaringan Komputer Anda

ini membutuhkan sebuah solusi yang bisa mempermudah proses bekerja dari mana saja secara lancar dan aman. Dalam hal ini, solusi jaringan tradisional tentu tak lagi bisa memenuhi kebutuhan tersebut yang mengandalkan konfigurasi perangkat yang semakin rumit.

Tantangan lainnya untuk bekerja secara WFA atau *hybrid* adalah faktor keamanan siber yang menuntut disiplin keamanan informatika karena berkaitan dengan perlindungan sistem komputer, jaringan, perangkat lunak, data, dan informasi dari ancaman siber seperti serangan virus, peretasan, pencurian identitas, pencurian data, dan kejahatan siber lainnya. Tujuan dari keamanan siber adalah melindungi informasi yang sensitif dan rahasia serta mencegah kerugian finansial atau reputasi organisasi atau individu. Metode-metode keamanan siber meliputi enkripsi data, firewalls, perangkat lunak keamanan, dan manajemen identitas dan akses.

Tantangan bisnis dan keamanan siber tersebut dapat terjawab dengan menerapkan model jaringan virtual baru seperti **SASE (Secure Access Service Edge)**, di mana teknologi ini dapat diskalakan, fleksibel, dan tentunya aman. Solusi SASE sangat diperlukan sekarang ini dalam bisnis karena memungkinkan perusahaan untuk memungkinkan akses jarak jauh (*remote access*) yang aman ke sumber daya IT. Hal ini terutama dibutuhkan ketika banyak karyawan bekerja yang dari luar kantor atau di lokasi yang berbeda. Solusi SASE menyediakan keamanan *endpoint* dan jaringan yang terintegrasi dengan cara yang signifikan dalam hal **membangun infrastruktur fisik atau biaya tambahan**.

SASE merupakan konsep arsitektur keamanan jaringan modern yang menggabungkan teknologi akses jarak jauh, keamanan internet, dan teknologi jaringan privat virtual (VPN) dalam satu solusi. Tujuannya adalah untuk mempermudah pengelolaan keamanan jaringan dan memberikan akses yang aman, cepat, dan andal ke aplikasi dan sumber daya lainnya, terlepas dari manapun lokasi pengguna. SASE banyak digunakan dalam organisasi yang memiliki banyak karyawan yang bekerja dari jarak jauh (*remote worker*) atau menggunakan aplikasi *cloud*.

Dengan mengadopsi teknologi SASE akan tercipta keamanan dan kecepatan dalam mengatasi isu-isu yang dialami, serta menjadi kunci keberlangsungan bisnis dalam era adopsi mobile dan *cloud*. Istilah SASE pertama kali dicetuskan oleh **Gartner** pada sebuah laporan berjudul **“The Future of Network Security in Cloud”** pada Agustus 2019. Gartner dalam laporan tersebut menyatakan bahwa tren pasar SASE oleh para pelanggan dituntut hal-hal mengenai kesederhanaan, skalabilitas, fleksibilitas, latensi yang rendah dan konvergensi keamanan yang kuat mulai dari jaringan edge, jaringan WAN hingga ke *cloud*.

Masih dalam laporan Gartner yang sama bahwa pada 2023, **20 persen** dari perusahaan akan mengadopsi solusi seperti SWG, CASB, ZTNA, dan FWaaS dari vendor yang sama.



Adapun komponen-komponen dari solusi SASE antara lain:

- 1. Firewall-as-a-service (FWaaS)** adalah solusi firewall dengan layanan berbasis *cloud* yang dapat diskalakan dan menyediakan layanan baru untuk memenuhi kebutuhan yang terus berkembang dan berubah. Pada dasarnya, FWaaS adalah firewall perimeter yang tidak tergantung lokasi untuk akses yang aman. FWaaS memberikan kemampuan firewall generasi berikutnya (NGFW) seperti *web filter*, *advanced threat protection* (ATP), *intrusion prevention system* (IPS), dan keamanan *domain name system* (DNS).
- 2. Zero Trust Network Access (ZTNA)** adalah model keamanan yang membutuhkan verifikasi pada setiap permintaan akses pada jaringan dari semua pengguna, baik yang berada di dalam

Topik

maupun di luar organisasi. ZTNA menggunakan teknologi seperti VPN, firewall, dan enkripsi untuk melindungi data dan aktivitas di jaringan.

- 3. Secure Web Gateway (SWG)** adalah solusi keamanan untuk akses ke internet. SWG melindungi pengguna dari ancaman keamanan seperti *malware*, *phishing* dan jenis ancaman lainnya. SWG memantau, mengontrol dan melindungi akses internet pada organisasi dengan cara memblokir situs web berbahaya atau membahayakan.
- 4. Cloud Access Security Broker (CASB)** adalah solusi keamanan yang membantu organisasi dalam mengelola akses ke layanan *cloud* dan mencegah terjadinya pelanggaran data. CASB melindungi data yang tersimpan di *cloud* dan memastikan keamanan serta kepatuhan aplikasi *cloud* yang digunakan oleh pengguna internal.
- 5. Software-Defined Wide Area Network (SD-WAN)** merupakan sebuah teknologi yang mengintegrasikan dan mengoptimalkan koneksi jaringan WAN *enterprise* dengan menggunakan perangkat lunak atau *software* seperti penyediaan redundansi link dan *load balancing*, penerapan *route traffic* yang cerdas berdasarkan metrik kinerja dan prioritas

bisnis. SD-WAN akan memberikan kontrol, pengelolaan, dan keamanan yang lebih baik terhadap jaringan, serta memungkinkan pemantauan dan manajemen dari jarak jauh (*remote*).

SASE mencakup paket teknologi dengan keamanan ke dalam struktur jaringan global sehingga selalu tersedia di mana pun pengguna berada, di mana aplikasi atau sumber daya diakses atau kombinasi teknologi transportasi apa yang menghubungkan pengguna dan sumber daya.

Solusi SASE memiliki beberapa manfaat antara lain:

- 1. Keamanan yang lebih baik:** Solusi SASE memungkinkan organisasi dan perusahaan untuk mengamankan semua perangkat, jaringan, dan aplikasi mereka dengan memberikan akses hanya kepada entitas yang berwenang. Hal ini melindungi organisasi dan perusahaan dari serangan siber dan upaya yang tidak sah untuk menyusup ke jaringan mereka.
- 2. Efisiensi operasional:** Solusi SASE akan menyederhanakan infrastruktur TI dengan memadukan banyak fungsi keamanan dan jaringan menjadi satu. Hal ini mengurangi biaya dan kompleksitas infrastruktur TI organisasi.
- 3. Penggunaan jaringan yang lebih cepat:** dengan



menggunakan teknologi *edge computing*, SASE memungkinkan akses yang lebih cepat ke aplikasi dan data organisasi.

4. **Skalabilitas yang lebih baik:** SASE memungkinkan organisasi untuk menyesuaikan dan memperluas infrastruktur TI mereka secara lebih mudah dan efisien.
5. **Peningkatan produktivitas:** Dengan memberikan akses yang aman ke aplikasi dan data yang dibutuhkan oleh karyawan, SASE membantu meningkatkan produktivitas dan memberikan pengalaman pengguna yang lebih baik.

perangkat lunak atau perangkat keras mereka. Implementasi SASE membutuhkan waktu dan persiapan yang baik agar dapat memberikan manfaat terbaik bagi organisasi.



Sumber: Gartner. *The Future of Network Security Is in the Cloud.*

Penerapan SASE

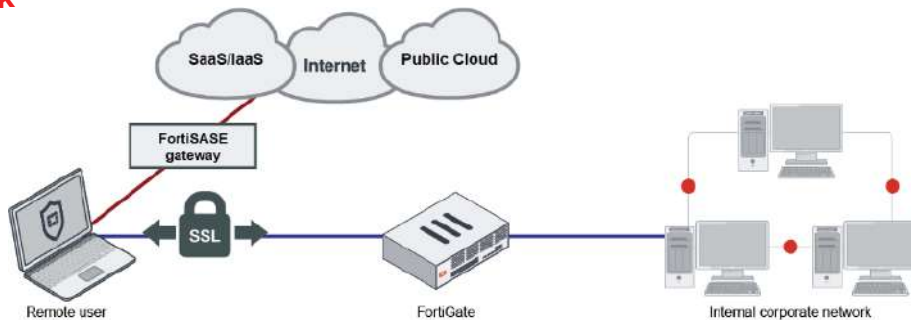
Implementasi SASE dapat dilakukan dengan satu vendor atau dengan beberapa vendor yang berbeda. Jika dengan vendor tunggal maka pilihlah vendor dengan kapabilitas dalam konvergensi jaringan dan keamanan sehingga dapat menghubungkan dan mengamankan pengguna, perangkat, dan lokasi yang terdistribusi ke sumber daya di *cloud*, *edge*, dan lokal. (Sumber Gartner: *Market Guide for Single-Vendor SASE*, <https://blogs.gartner.com/andrew-lerner/2022/09/30/single-vendor-sase/>)

Dalam implementasi SASE, perusahaan mungkin perlu menambahkan tenaga ahli IT atau mengontrak layanan keamanan jaringan. Ada beberapa vendor yang menawarkan layanan SASE dan dapat membantu dalam implementasi dan pengelolaan. Namun, dalam banyak kasus, perusahaan harus mempekerjakan tenaga ahli TI untuk melakukan integrasi dengan sistem internal dan untuk memastikan bahwa sistem aman dan efisien.

Waktu penerapan implementasi SASE akan bergantung pada kompleksitas jaringan dan ukuran perusahaan. Misalnya, perusahaan yang lebih besar dan memiliki jaringan yang sangat kompleks memerlukan waktu lebih lama. Sebelum memulai implementasi SASE, perlu dilakukan audit jaringan dan mempersiapkan infrastruktur yang diperlukan, termasuk kesiapan keamanan data seperti sertifikasi *cloud* dan kepatuhan regulasi. Selain itu, organisasi juga perlu membuat rencana migrasi bagi pengguna agar dapat memperbarui

Berikut beberapa langkah dalam memulai adopsi teknologi SASE:

1. **Penilaian kebutuhan:** Pertama-tama, tim IT dan keamanan dalam organisasi harus mengevaluasi kebutuhan dan tantangan keamanan yang dihadapi oleh organisasi mereka dan menggunakan penilaian risiko untuk mendapatkan pemahaman yang lebih baik tentang area mana yang memerlukan perlindungan maksimum.
2. **Seleksi provider/vendor:** Setelah penilaian risiko selesai, organisasi harus menyeleksi provider SASE yang tepat. Komponen kunci dari provider dan vendor dipilih adalah yang memiliki solusi dan teknologi yang lengkap termasuk firewall, web gateway, CASB, *Data Loss Prevention* (DLP), SD-WAN, serta identitas dan akses manajemen (ZTNA).
3. **Integrasi sistem:** Integrasi dan konsolidasi dari berbagai sistem dan layanan yang dimiliki organisasi menjadi satu platform keamanan tunggal tentunya membutuhkan integrasi agar dapat berjalan lancar. Integrasi ini bisa dilakukan dengan menambahkan peralatan pendukung seperti API (*Application Programming Interface*).
4. **Pelatihan staf:** Setelah platform SASE dikonfigurasi, organisasi akan membutuhkan pelatihan staf agar mereka memahami bagaimana teknologi, kebijakan dan praktik



keamanan digunakan. Informasi otorisasi mengenai opsi-opsi kebijakan keamanan, pengaruh teknologi SASE dan cara mengirim data juga harus dilengkapi untuk staf.

- 5. Penyelarasan kebijakan:** Penerapan SASE diantaranya dengan mempelajari bagaimana menangani kebijakan pengelolaan keamanan untuk perangkat, khususnya perangkat bergerak (mobile) serta para karyawan yang menggunakan *Virtual Private Network* (VPN) atau yang di jaringan internal perusahaan. Hal ini penting karena organisasi ada dalam faktor yang mengalami perkembangan yang sangat cepat.
- 6. Evaluasi kinerja:** Kinerja platform SASE harus terus dinilai untuk memastikan bahwa Solusi SASE yang telah diterapkan tetap berjalan dengan efisien dan efektif. Perubahan kebutuhan keamanan dan bisnis harus digariskan dan ditinjau secara berkala.

Adopsi SASE untuk penerapan dalam bisnis yang terbaik adalah dengan pendekatan **hybrid**, seperti menggunakan sistem keamanan dan jaringan yang ada, sambil secara bertahap mengimplementasi teknologi SASE yang secara fleksibel dapat menskalakan jumlah perangkat, pengguna WFA dan sumber daya yang di-hosting cloud dalam jumlah yang besar.

Biaya investasi SASE pun bervariasi tergantung pada ukuran perusahaan dan kebutuhannya. Biaya Investasi penerapan SASE ini akan lebih efisien jika dibandingkan dengan membangun sistem keamanan *endpoint* dan *jaringan* secara terpisah.

Dapatkan solusi SASE dan penerapannya melalui ACS Group yang menghadirkan

produk portofolio yang lengkap mulai dari perangkat *endpoint* hingga infrastruktur IT dan teknologi terkini seperti mobile, cloud dan IoT. Dengan cakupan layanan yang luas di seluruh Indonesia, ACS Group siap untuk mendukung dan mengembangkan bisnis para pelanggannya, serta menyederhanakan kompleksitas baik jaringan dan keamanan dalam satu *platform* dengan solusi yang terintegrasi.

FORTISASE dari Fortinet - Solusi Akses yang Aman dan Fleksibel

SASE adalah strategi baru dalam menggabungkan fungsi jaringan dan keamanan dengan kemampuan *wide-area network* (WAN) untuk mendukung kebutuhan akses yang dinamis dan aman pada organisasi sekarang ini. Secara konseptual, SASE menggabungkan *Software Defined WAN* (SD-WAN) dan layanan keamanan jaringan seperti *Next-Generation Firewall* (NGFW), *Secure Web Gateway* (SWG), *Zero-Trust Network Access* (ZTNA), dan *Cloud Access Security Brokers* (CASB) ke dalam satu model layanan.

Solusi **FortiSASE** memungkinkan organisasi untuk menerapkan akses yang aman (*secure access*) dan lokasi para pengguna, *workload*, perangkat, ataupun lokasi aplikasi tidak menjadi masalah. Hal ini menjadi suatu kelebihan yang sangat penting khususnya untuk para pengguna yang bekerja secara *remote*, aplikasi-aplikasi SaaS (*software as service*) yang sangat cepat, pergerakan data sangat masif di berbagai *data center*, kantor-kantor cabang, serta pada lingkungan *hybrid-cloud* maupun *multi-cloud*.



Gambar 1. Cloud Delivered SASE

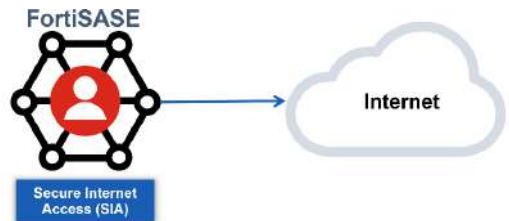
FortiSASE adalah solusi keamanan *cloud* dari Fortinet (Single-Vendor SASE) dengan skalabilitas yang tinggi sebagai layanan yang memungkinkan untuk akses yang aman dan fleksibel, kapan saja dan dimana saja untuk para pengguna yang bekerja di mana saja.

Dengan dukungan FortiOS dan Fortinet Security Fabric, FortiSASE menyediakan orkestrasi tanpa hambatan NGFW (Next-Generation FireWall) di *cloud*, dengan fitur-fitur: Antivirus, Web Filter, intrusion prevention system (IPS), DNS, file filter, Data Leak Prevention (DLP) dan SSL inspection. Secara bersamaan semua aspek tersebut memungkinkan Fortinet untuk memberikan layanan SASE dengan fleksibilitas dan konsumsi model (OPEX - operation expense) yang dibutuhkan oleh *enterprise*.

Fortinet memungkinkan organisasi menerapkan keamanan yang tepat di setiap tahap dalam era transformasi digital. Dengan inovasi selama lebih dari 20 tahun, Fortinet telah memberikan solusi keamanan dan jaringan yang handal dan terpercaya.

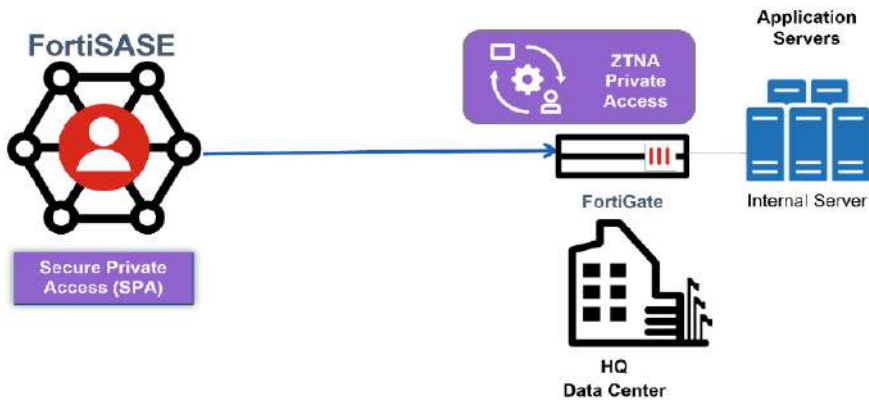
Beberapa Contoh Penggunaan dan Penerapan FortiSASE

1. Secure Internet Access (SIA) - Akses ke internet dengan aman



Gambar 2. Secure Internet Access (SIA)

Internet telah memberi banyak manfaat seperti sebagai sumber informasi, memudahkan dalam komunikasi, bekerja dan belajar hingga untuk mendukung kegiatan bisnis, namun perlu waspada karena akses ke internet yang tidak aman dapat disusupi oleh penjahat *cyber-crime* mulai dari pelanggaran privasi pengguna, pencurian data hingga mengenkripsi file atau data pengguna yang mengakibatkan file tidak dapat dibaca dan perangkat tak dapat digunakan sehingga harus memberikan uang tebusan (*ransom*) untuk bisa mendapatkan kode enkripsi tersebut.



Gambar 3. Secure Private Access (SPA) Access (SIA)

Untuk itu, para pengguna WFA dengan mobilitas yang tinggi (*remote user*) ataupun lokasi cabang yang tidak terlindungi oleh perangkat perimeter keamanan perusahaan, akses internet secara langsung meningkatkan resiko dan potensi serangan siber. FortiSASE dengan kemampuan **Secure Web Gateway (SWG)** dan **Firewall-as-a-Service (FWaaS)** yang komprehensif dapat mengamankan akses dan melindungi pengguna dan perangkat mobile yang terhubung dengan internet secara konsisten sehingga tidak perlu takut lagi ketika mengakses internet dengan koneksi jaringan public.

2. Secure Private Access (SPA) - Akses ke jaringan privat dengan aman

Dengan fleksibilitas tempat dan waktu dalam bekerja sekarang ini, organisasi perlu mengambil langkah-langkah untuk memastikan karyawan dapat bekerja secara produktif dan aman bagi mereka berada di kantor, di rumah, atau di perjalanan. Yang bagian terpentingnya adalah memungkinkan akses yang aman dan terjamin ke jaringan privat, sumber daya IT, dan aplikasi organisasi. Pastikan akses ke dalam jaringan privat organisasi memenuhi persyaratan dan kebijakan keamanan yang telah ditetapkan.

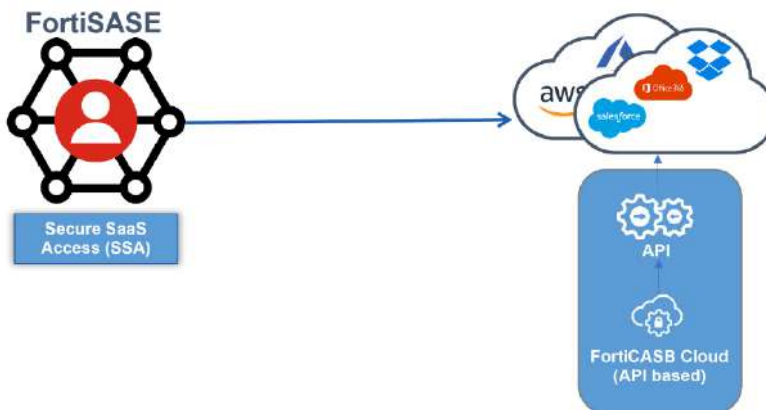
FortiSASE dengan **Zero Trust Network Access (ZTNA)** menghubungkan pengguna di lokasi mana pun berada yang melakukan

akses jarak jauh ke jaringan privat organisasi mendapatkan keamanan yang konsisten. ZTNA akan melakukan verifikasi terhadap identitas pengguna, postur perangkat, dan otorisasi pengguna sebelum mengakses suatu aplikasi. Akses yang diberikan pun hanya terhadap aplikasi tertentu, hanya untuk satu sesi. Dengan demikian ZTNA memastikan hanya pengguna dan perangkat yang sesuai saja yang dapat melakukan akses ke jaringan privat organisasi. Prinsip keamanan *Zero Trust* diterapkan dan terus memantau aktivitas pengguna selama sesi, dan setelah terkoneksi pun, ZTNA akan meminta proses otentikasi ulang secara berkala atau saat koneksi diam selama beberapa waktu.

FortiSASE Secure Private Access juga memberi manfaat lainnya untuk organisasi dengan integrasi jaringan **SD-WAN (Software-Defined WAN)** yang lancar untuk akses aplikasi-aplikasi perusahaan dengan secara otomatis menentukan jarak yang terpendek (*shortest path*) dalam komunikasinya karena didukung adanya kemampuan *intelligent steering* dan *dynamic routing* di FortiSASE.

3. Secure SaaS Access (SSA) – Akses ke aplikasi SaaS dengan aman

Layanan SaaS (*software as a service*) telah banyak menghasilkan aplikasi-aplikasi modern yang memberi banyak kemudahan dan dapat beroperasi dengan baik. Tersedia 24 jam tanpa batas lokasi, tidak perlu repot mengurus



Gambar 4. Secure SaaS Access (SSA)

infrastruktur atau ketersediaan aplikasi karena layanan SaaS umumnya sudah menjanjikan SLA (*Service Level Agreement*) yang baik. Di sisi lain, layanan SaaS menghadirkan tantangan, seperti bagaimana keamanan data yang disimpan di *cloud*, apakah hanya pengguna yang diberikan keistimewaan saja yang dapat mengakses aplikasi guna mencegah *security breach*, lalu apakah kebijakan keamanannya dapat diadopsi di lingkungan *on-premise* organisasi? Diperlukan perantara untuk keamanan akses ke *cloud*, atau dikenal dengan **CASB - Cloud Access Security Broker**, adalah titik penerapan kebijakan keamanan yang diposisikan antara pengguna perusahaan dan penyedia layanan *cloud*. CASB dapat menggabungkan beberapa kebijakan keamanan yang berbeda, mulai dari autentikasi dan pemetaan kredensial hingga enkripsi, deteksi adanya program jahat (*malware*), dan menawarkan solusi yang fleksibel guna membantu memastikan keamanan aplikasi *cloud*.

FortiSASE Secure SaaS Access, adalah *Dual-Mode* CASB generasi berikutnya yang menggunakan *API-based* CASB (FortiCASB) dan *Inline* CASB dengan ZTNA dan SASE yang memberikan visibilitas yang komprehensif dengan mengidentifikasi aplikasi-aplikasi SaaS dan akses ke data yang sensitif di *cloud* serta melaporkannya atau kemampuan Shadow IT dalam menentukan perilaku abnormal dari

akses ke aplikasi yang tidak disetujui. Dengan FortiSASE Secure SaaS Access maka 4 pilar keamanan CASB mengenai visibilitas (*visibility*), kepatuhan (*compliance*), keamanan data (*data security*), dan perlindungan terhadap ancaman (*threat protection*) dapat tercapai dan dipenuhi dengan baik.

Penutup

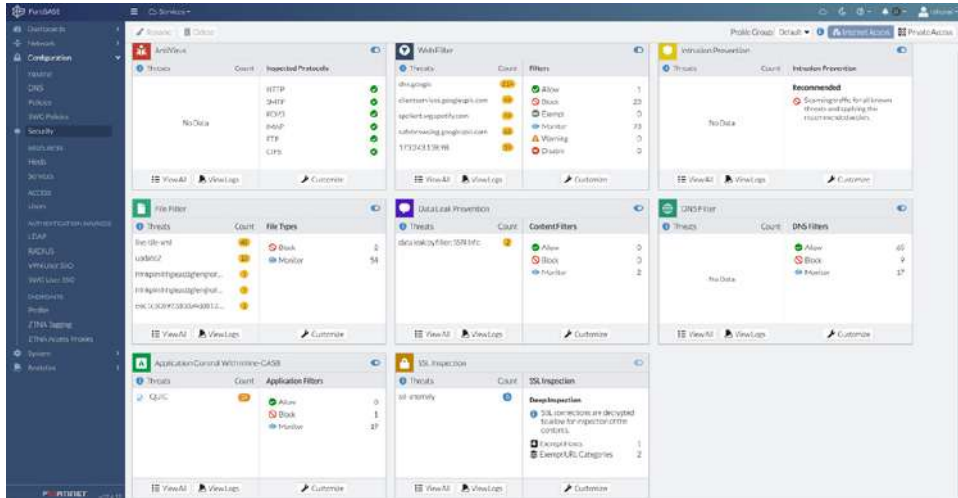
FortiSASE adalah layanan *Software as a Service* (SaaS) yang menjaga klien dalam akses ke internet secara aman. FortiSASE dapat memastikan pekerja hybrid atau yang bekerja dari mana saja baik di kantor, di rumah, di café atau di perjalanan dapat bekerja dengan aman ketika memanfaatkan akses jaringan internet. FortiSASE memiliki fitur-fitur keamanan yang handal dalam melindungi kliennya melakukan akses yang memanfaatkan internet sebagai penghubung.

Dapatkan layanan FortiSASE dan penerapannya dengan ACS Group yang menghadirkan produk portofolio yang lengkap mulai dari perangkat *endpoint* hingga infrastruktur IT dan teknologi terkini seperti mobile, *cloud* dan IoT. Dengan cakupan layanan yang luas di seluruh Indonesia, ACS Group siap untuk mendukung dan mengembangkan bisnis para pelanggannya, serta mengurangi kompleksitas terkait jaringan dan keamanan dalam satu *platform* dengan solusi yang terintegrasi.

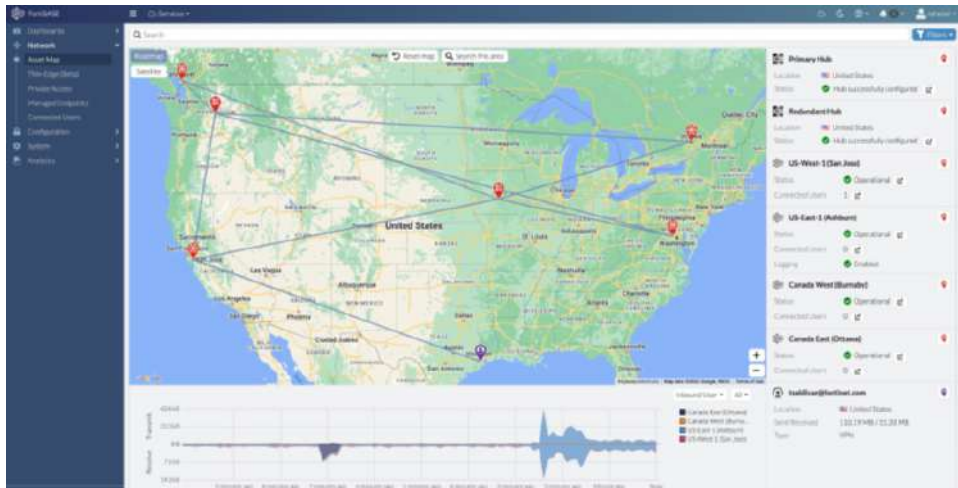
Topik

Referensi:

- Fortinet FortiSASE Concept Guide Version 23.1.17
- Fortinet FortiSASE Architecture Guide Version 23.1.21
- Gartner: The Future of Network Security Is in the Cloud. Introducing the Secure Access Service Edge - Neil MacDonald
- Gartner: Market Guide for Single-Vendor SASE



Gambar 5. Konsol FortiSASE dengan fitur-fitur keamanan



Gambar 6. Tampilan FortiSASE Secure Private Access dengan SD-WAN sebagai jembatan akses pengguna dengan ke aplikasi privat



Saksikan Video terbaru kami,
yang membahas ACS Care di
channel Youtube kami.

Jangan lupa **SUBSCRIBE** !

Scan this
QRcode



ANTUSIAS

[KOLAM KETAWA]

Wagimin adalah seorang sales vacuum cleaner yang sukses menjual ribuan unit di kotanya.

Melihat tingkat kesuksesan penjualannya yang tinggi, managernya mengirim Wagimin bukan ke kota yang lebih besar seperti ke ibu kota melainkan ke pedesaan untuk menawarkan vacuum cleaner ke masyarakat desa.

Sesampainya di desa, Wagimin mencoba memutar otak bagaimana cara menjual produk tersebut agar dapat diterima orang-orang yang ada di area pedesaan. Dia coba menghampiri sebuah rumah yang cukup besar dan mengetuk pintu. Seorang ibu-ibu membukakan pintu untuknya dan Wagimin mulai mempromosikan barang dagangannya.

"Bu, berapa lama yang Ibu butuhkan untuk menyapu rumah ibu?"

"Butuh waktu lama mas, bahkan butuh sehari untuk membersihkan rumah dan juga peternakan di belakang"

"Baik bu, kalau untuk membersihkan sofa dan kasur, Ibu butuh waktu berapa lama bu?"

"Wahhh itu juga sama butuh waktu yang lama juga mas, karena di sini sangat berdebu dan kami punya kucing yang suka tiduran di sofa"

"Nah kalau begitu saya punya solusinya bu!" kata Wagimin dengan antusias."Oh ya !!" sahut sang Ibu.

"Ibu tidak perlu berlama-lama, dengan Vacuum Cleaner ini, seluruh rumah Ibu bisa dibersihkan dalam waktu 5 menit saja!" ujarnya sambil memperlihatkan vacuum cleaner yang dibawanya.

Meskipun begitu, sang Ibu tidak begitu terkesan dan tertarik. Namun demi menarik minat si Ibu, Wagimin kemudian mengeluarkan sekantong tanah dan menyebarkannya di lantai rumah itu dan menyiramnya dengan air.

Sang ibu sangat terkejut, "Waduhhhh...." namun ketika ia mulai membuka mulutnya untuk protes, Wagimin buru-buru menyelaknya "Sabar Bu, kalau vacuum cleaner ini tidak bisa membersihkan seluruh tanah ini, saya akan membersihkannya dengan tangan saya sendiri bu... tenang saja!!"

Ibu itu mendengus dan berseru "Kalau begitu, siap-siap pegel ya! Di rumah kami tidak ada listrik !!!"



FortiAnalyzer

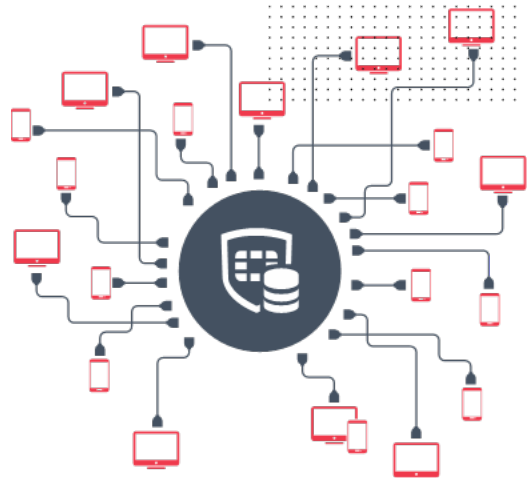
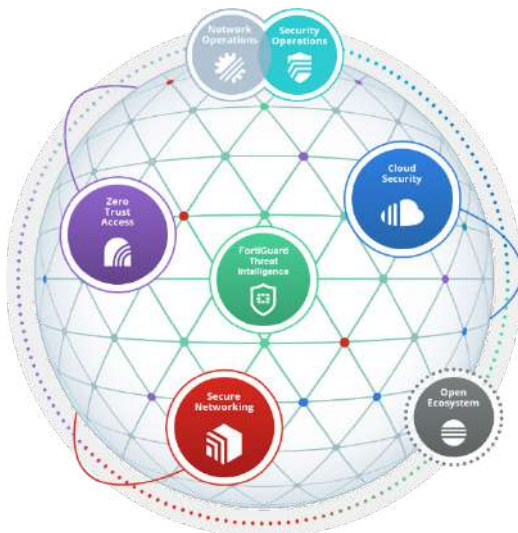
by Ken Loohe, Professional Services ACS Group

Security Operations Center [SOC] common issue:

- Too many cyber security vendors.
- Too many alerts.
- Require a time-consuming manual respond each time an incident occurs.
- Lack of trained people to keep up with current technology.

Dengan meningkatnya intensitas digitalisasi dan banyaknya perangkat yang terhubung, bagaimana kita dapat melakukan pemeriksaan yang komprehensif dalam laporan yang *visually-pleasing*? Bagaimana kita mengautomasi respon, untuk mengurangi *administration-fatigue*?

FortiAnalyzer bukan sekedar laporan-laporan "cantik". Perangkat ini dapat mengurangi alert yang notabene tidak perlu, dengan mengoptimalkan fungsi otomatisasi operasional. Sebagai bagian dari pilar SOC dalam Fortinet



Security Fabric, FortiAnalyzer memberikan dashboard komprehensif yang dapat dengan mudah digunakan untuk mempelajari *user habit* dan *tendencies*.

Salah satu highlight laporan adalah ID dari device-device yang perlu dilakukan update/patch.

Untuk keperluan presentasi, tersedia laporan-laporan yang secara detail mengupas kondisi jaringan, user yang beresiko, dan tindakan yang telah dieksekusi FortiGate.

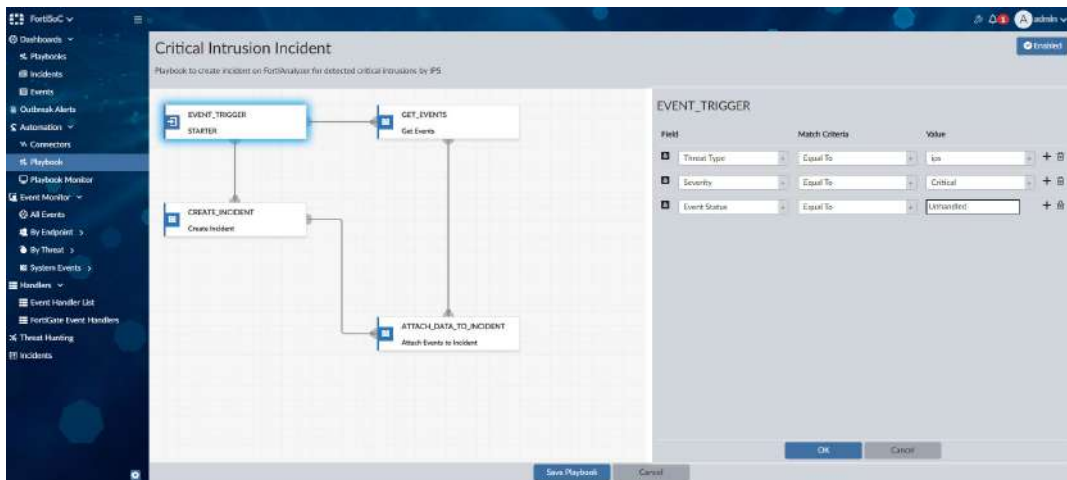
Lisensi Indicator of Compromise memberikan *threat intelligence* harian yang berisi daftar dari host yang kemungkinan terimplikasi ancaman, disajikan dalam bentuk table dan grafik.



Fitur *Centralized Storage Log* mengaktifkan Security Rating Service yang memberikan penilaian pada url mencurigakan dengan update per ½ jam.

Rating ini dapat mengupdate FortiGate untuk memblokir potensi serangan *malware*.

Visibilitas yang diberikan FortiAnalyzer juga termasuk SD-WAN summary (NOC, performance, dan SLA issue) serta laporan Sandbox. Visibilitas ini dapat dilanjutkan ke fitur *Event Handler*, dimana ada pengukuran konsistensi *log* untuk dapat



dilakukan simplifikasi *workflow* yang akan lebih didefinisikan dengan fitur *Playbook: Response & Remediate*.

Form Factor FortiAnalyzer tersedia dalam bentuk:

1. Appliance / hardware box
2. VM
3. Cloud pada cloud provider marketplace seperti Alibaba Cloud, AWS, Azure
4. Hosted pada Data Center Fortinet

Fitur FortiAnalyzer:

- Reporting
- Centralized Log Management
- Event Dashboard
- Event List
- Incidents
- Playbooks
- Event Handlers
- FortiGate Event Handlers
- CLI Script Automation

Available in:



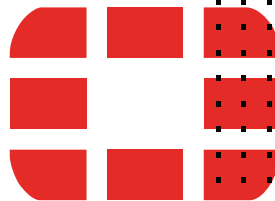
Appliance



Virtual Machine



Cloud



Machine Vision

Apa itu Machine Vision dan Penerapannya dalam Bisnis?

by Ardy, AIDC & Security Solution Manager ACS Group



Bayangkan bila mesin mempunyai mata? Akankah ia seperti mata manusia yang melihat untuk menganalisa kemudian memutuskan sesuatu atasnya?

Jawabannya adalah ya, mesin saat ini diberikan 'penglihatan' agar ia bisa menginspeksi dan menganalisis suatu benda kemudian menentukan keputusan/tindakan untuk benda tersebut.

Definisi Machine Vision

Machine Vision adalah teknologi dan metode yang digunakan untuk melakukan inspeksi dan analisis otomatis yang berbasis pencitraan, misalnya pada kontrol proses dan panduan oleh robot yang biasanya digunakan dalam skala industri.

Machine Vision sendiri melibatkan banyak sekali teknologi, misalnya perangkat lunak dan perangkat keras, sistem yang terintegrasi, beragam aksi, metode, dan keahlian. *Machine Vision* berusaha untuk mengintegrasikan beragam jenis teknologi ke dalam sebuah cara baru dan menerapkannya untuk menyelesaikan beragam masalah.

Machine Vision banyak digunakan untuk kebutuhan manufaktur dan industri, misalnya untuk mendeteksi adanya defect atau cacat pada produk.

Cara kerja Machine Vision

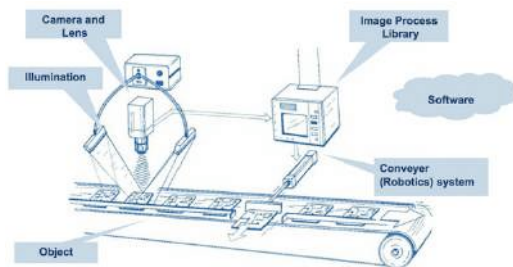
Machine Vision adalah sebuah teknologi ataupun metode yang mengkombinasikan banyak jenis teknologi lainnya, seperti sensor pintar,

kamera pintar, software dan hardware, algoritma, dan beberapa teknologi lain untuk menghasilkan output yang diharapkan.

Machine Vision umumnya digunakan untuk skala industri misalnya dalam industri manufaktur untuk mendeteksi adanya kecacatan pada produk. *Machine Vision* melibatkan sensor-sensor untuk mendeteksi keberadaan produk. Sensor ini kemudian akan memicu sumber cahaya untuk menerangi area produk dan kemudian sebuah kamera untuk menangkap gambar produk tersebut.

Frame grabber (perangkat pendigitalan) kemudian akan menerjemahkan gambar dari kamera menjadi sebuah output digital. File digital tersebut kemudian akan disimpan di komputer agar bisa dianalisis oleh perangkat lunak (*software*).

Perangkat lunak (*software*) lantas akan membandingkan file digital tersebut dengan rangkaian kriteria yang telah ditentukan sebelumnya. Jika perbandingan dihasilkan bahwa produk ada kecacatan, maka produk tersebut tidak akan lolos inspeksi.



Penggunaan Teknologi Machine Vision

Contoh penggunaan teknologi *Machine Vision* untuk inspeksi otomatis berdasarkan image, misalnya pada:

- Pengontrolan proses industri
- Pendeteksi nomor plat kendaraan
- *Wood quality inspection*
- *Final inspection of sub-assemblies*
- *Engine part inspection*
- *Label inspection on products*
- *Checking medical devices for defects*
- *3D model building (photogrammetry)*
- Surveillance (monitor penyusup, analisa trafik jalan tol dan lainnya)
- Interaksi manusia dan robot (*Human Robot Interaction*)

Perbedaan antara Machine Vision dan Computer Vision

Computer Vision dan *Machine Vision* adalah teknologi yang tumpang tindih. Sistem *Machine Vision* membutuhkan komputer dan perangkat lunak khusus untuk pengoperasiannya, sedangkan *Computer Vision* tidak perlu diintegrasikan dengan mesin. *Computer Vision* dapat, misalnya, menganalisis gambar atau video online digital serta “gambar” dari detektor gerakan, sensor inframerah, atau sumber lain, bukan hanya foto atau video. *Machine Vision* adalah sub-kategori dari *Computer Vision*.

Penerapan Machine Vision dalam Bisnis

Machine Vision saat ini telah banyak digunakan untuk keperluan *Quality Control*. Di samping manfaatnya yang besar untuk *Quality Control* produk dalam skala besar, *Machine Vision* juga dikembangkan untuk keperluan-keperluan lainnya.

Di bawah ini adalah contoh-contoh penerapan *Machine Vision* untuk keperluan bisnis:

- *Machine Vision* untuk Pertanian

Dalam bidang pertanian, *Machine Vision* terutama digunakan dalam perkebunan anggur. Mesin pemanen dilengkapi dengan teknologi *machine vision* agar bisa mendeteksi lokasi anggur. Berkat adanya *machine vision*, robot pemanen bisa memanen tanpa merusak buah anggur. Selain itu, *machine vision* juga bisa digunakan untuk memonitor tanaman dan mendeteksi penyakit tanaman.

- Kontrol dan Pengelolaan Stok

Machine vision bisa digunakan untuk secara cepat membaca barcode dan label pada produk. Pada sektor manufaktur, penting untuk memastikan bahwa mesin mengambil komponen yang tepat sementara produk terus bergerak menuju perakitan.

- Pelacakan Produk

Dalam industri yang sangat ketat diatur dan diawasi, misalnya industri farmasi, sangat penting untuk bisa melacak bahan-bahan, nomor serial produk, serta tanggal kadaluarsa. Untuk keperluan tersebut, *machine vision* bisa melakukannya dengan mudah dan cepat.

- Pengukuran dan Kalibrasi

Machine vision juga bisa digunakan untuk mengukur celah di busi untuk memastikan apakah ia sesuai dengan spesifikasi atau sekedar mengidentifikasi alat ukur yang perlu dikalibrasi. Penggunaan *machine vision* dalam bidang ini cukup efisien.

- Keamanan dan Keselamatan

Machine vision bisa meningkatkan keamanan dan keselamatan terutama pada site konstruksi dengan banyak peralatan berat.

Dengan semakin berkembangnya teknologi, penggunaan *Machine Vision* akan semakin banyak dari hari ke hari. Apakah Anda siap untuk mengimplementasikannya sendiri di dalam bisnis proses Anda?

Seminar **Secure your Operational Technology Environment from Cyber Attacks** bersama Fortinet

ACS Group bersama dengan Fortinet Indonesia dan Exclusive Networks Indonesia [ENID] menyelenggarakan event Secure your Operational Technology Environment from Cyber Attacks pada tanggal 9 Maret 2023 dan bertempat di Ciputra World Hotel, Surabaya.

Acara yang dihadiri para perwakilan dari berbagai perusahaan manufaktur ini dibuka oleh Boedijanto Linardi selaku Branch Manager ACS Group cabang Surabaya. Kemudian dilanjutkan sambutan oleh Yulita Ongkowidjaja-Inside Sales Representative Fortinet Indonesia.

Acara ini menargetkan para pelaku industri agar waspada atas munculnya ancaman terhadap Operational Technology(OT) yang terus membayangi, serta bagaimana teknologi Fortinet dapat memberikan solusi akurat untuk melindungi HMI, SCADA, PLC yang diakses dari jarak jauh.

Kemajuan teknologi memungkinkan user melakukan pekerjaan dari mana saja, di mana kemudahan konektivitas sejalan dengan resiko intrusi yang dibawanya. Gangguan operasional pabrik dapat menjadi bencana besar bagi kesehatan perusahaan manapun, oleh karena itu tindakan pengamanan yang memadai perlu



dilakukan. Salah satu komentar yang mencolok dari peserta yaitu protokol dan perangkat OT biasanya membingungkan TI karena ketidaktahuan dan perbedaannya. Salah satu perbedaan tersebut adalah kondisi umum dari OS yang usang di lingkungan OT, karena memiliki permukaan serangan yang besar jika tidak memiliki DMZ yang tepat untuk bertindak sebagai pertahanan perimeter. Fortinet menggunakan pendekatan Model Purdue yang komprehensif untuk memitigasi risiko, sebagaimana diuraikan panjang lebar oleh Bella Nurhasanah (Konsultan Keamanan Fortinet Indonesia) dalam sesi tanya-jawab dan berlanjut sampai ke booth.

Ahmad Karrubi (Presales Engineer ENID) memaparkan Secure SD-WAN, dimana selain percepatan koneksi yang dimungkinkan SD-WAN dan diamankan FortiGuard Labs, penghematan biaya TCO menjadikan Fortigate pilihan produk yang tepat guna untuk memaksimalkan investasi dengan fitur keamanan yang mumpuni.



Seminar **Digitize your Physical Security** bersama Hytera, ZKTeco, & Uniview



ACS Group terus memberikan pengetahuan bagi para pelanggan setia dalam memberikan update teknologi dalam bentuk seminar. Acara seminar kali ini bertajuk “Digitize Your Physical Security” yang diselenggarakan pada hari Rabu, 15 Maret 2023 di Holiday Inn, Jababeka Cikarang. Momen ini merupakan acara tatap muka pertama kali semenjak tiga (3) tahun ACS Group melaksanakan seminar secara daring. Bersama dengan principal Hytera, ZKTeco, dan Uniview, acara ini dihadiri oleh peserta dari berbagai perusahaan dengan lini bisnis yang berbeda.

Acara ini dibuka dengan kata sambutan oleh Suprianto Kusman selaku Branch Manager ACS Group Cikarang dengan menekankan empat (4) pilar penting ACS Group. Dilanjutkan dengan sesi pertama dari Hytera tentang “Make Connections Lead the Future” oleh Krisna Dhian W - Hytera Country Channel Manager dilanjut dengan memperkenalkan solusi HT analog yaitu Push to Talk Over Cellular (POC Hytera) oleh Richard Andrian - Hytera Product Specialist.

Suandi Tennece selaku ZKTeco Product Manager kemudian mengisi sesi selanjutnya dengan topik bahasan “ZKTeco Introduction for Hardware and Software” dengan memperkenalkan solusi terbaru *hardware* dan *software*, seperti: *time attendance*, *access control*, *thermal product*, *ZKBio Security*, dan *ZKBioAccess IVS*.

Sesi berikutnya pemaparan materi “UNIVIEW For Manufacturing, Logistics & Transportation Solution” oleh Murjianto - Uniview Technical Support yang memperkenalkan CCTV pintar untuk bidang bisnis manufaktur, logistik, dan transportasi. CCTV yang diperkenalkan oleh Uniview adalah produk yang lebih efisien dalam hal *bandwith* dan penyimpanan.

Pengenalan produk terbaru dari Hytera, ZKTeco, dan Uniview yang mumpuni dapat memberikan solusi lengkap dalam menunjang kebutuhan komunikasi dan koordinasi. Memberikan efisiensi biaya, kemudahan dalam mengatur infrastruktur, memantau setiap informasi yang beredar di setiap orang yang menggunakannya.



Technology Update Smart Hospital with Connected Healthcare bersama Zebra Technologies



Rumah sakit cerdas ditandai dengan adanya otomatisasi dalam menjawab tantangan cepat dalam kebutuhan tanpa mengorbankan perawatan pasien. Pengembangan konsisten dalam transformasi digital sudah dilakukan oleh Siloam Hospital bekerjasama dengan ACS Group dan Zebra Technologies.

Melalui kerja sama yang sudah terjalin selama ini maka pada tanggal 13 April 2023 diadakan acara pertemuan dengan tema “Smart Hospital with Connected Healthcare”. Acara yang dihadiri oleh tim IT Siloam Hospital dan beberapa rekan yang turut serta melalui daring ini menyajikan update teknologi di bidang kesehatan.

Sambutan awal oleh Arijanto Hartanto - Sales and Marketing Director ACS Group dan dilanjutkan presentasi oleh Khoirul Ummah - Zebra Senior Territory Account Manager.

Perkembangan teknologi khususnya bidang kesehatan ditandai dengan lahirnya Internet of Things (IoT) yang semakin canggih. Teknologi tepat guna ini akan mampu meningkatkan efisiensi dan efektivitas jika diterapkan di rumah sakit, dalam hal seperti: pergerakan staf, pasien, peralatan termasuk ketersediaan kamar serta pasokan rumah sakit.

Sebelumnya, beberapa lembaga kesehatan memperlengkapi karyawannya menggunakan mobile saat bekerja dimana beberapa diantaranya dengan mobile dan *tablet* konsumen. Namun saat

menguji aplikasi mobile di lingkungan klinis mereka menyadari bahwa perangkat konsumen tersebut tidak memenuhi standar perawatan pasien yang membutuhkan penanganan segera.

Khoirul Ummah menjelaskan bahwa TC51-HC adalah mobile computer berukuran saku yang cocok digunakan Siloam Hospital. Produk OS Android ini dilengkapi dua kamera bawaan untuk membantu staf klinis mengambil foto kondisi pasien saat konsultasi sebagai dokumentasi medis. Solusi lain untuk rumah sakit ini yaitu: ET4x-HC Series, printer label, scanners, sampai barcode wristbands untuk pasien.

TC51-HC tahan terhadap sanitasi dan sterilisasi yang harus dilakukan secara teratur untuk membantu mengurangi risiko infeksi, yang menjadi perhatian utama di antara dokter dan manajer rumah sakit.



Pererat Kebersamaan, ACS Group adakan Buka Bersama dengan HITA Banten



Dalam rangka menyemarakkan bulan suci Ramadhan 1444 H, ACS Group dan HITA Chapter Banten menggelar acara buka puasa bersama dengan thema “Together We Go Beyond” yang diadakan pada hari Jumat, 14 April 2023 di Mint and Pepper Mercure Alam Sutera.

Acara buka puasa bersama ini dihadiri oleh jajaran top management dan managerial dari divisi IT berbagai hotel yang menjadi anggota HITA Banten. Momen ini sekaligus merupakan media perkenalan ACS Group dan sekaligus momentum untuk *update* berita mengenai Aruba Instant On dan Hytera Push-To-Talk over Cellular (PoC).

Dalam sambutannya, Slamet Riyadi - ketua HITA Banten, mengatakan bahwa acara buka puasa ini sangat diapresiasi sebagai terjalannya hubungan baik antara ACS Group dan HITA Banten. Dalam acara tersebut turut hadir pula Arijanto Hartanto

- Sales & Marketing Director ACS Group.

Acara ini dibuka dengan perkenalan yang dibawakan oleh Kevin Fernando - Account Executive ACS Group dan dilanjutkan pemaparan solusi Hytera PoC oleh Richard Andrian - Hytera Product Specialist. Dalam pemaparannya ditekankan mengenai perubahan yang dilakukan oleh Hytera, kelebihan yang ditawarkan, hingga cara penggunaannya di bidang perhotelan. Hytera adalah perangkat radio digital dua arah yang kompak dengan performa yang luar biasa dan value besar.

Acara ini ditutup dengan presentasi mengenai Aruba Instant On oleh Empianus E. Putra - Network Engineer Aruba Specialist. Agenda yang diberikan meliputi ringkasan mengenai Aruba HPE, tren dan tantangan bisnis, hingga jaminan serta servis yang ditawarkan.



Mengoptimalkan Kebersamaan dalam Tradisi Halal Bihalal dengan ExtremeCloud IQ (XIQ)

Pada momen yang penuh kehangatan dan kebersamaan di bulan Ramadhan, ACS Group bersama Extreme Networks, perusahaan teknologi terkemuka dalam solusi jaringan, mengadakan acara Halal Bihalal pada Rabu, 10 Mei 2023 di Greyhound Cafe, Menteng. Didampingi dengan pendekatan yang inovatif menggunakan platform mereka yang terbaru, ExtremeCloud IQ (XIQ).

Acara ini dihadiri oleh mitra bisnis Extreme Networks yaitu 8 perusahaan besar yang bergerak di bidang hospitality, percetakan & media, courier dan F&B.

Sambutan awal disampaikan oleh Direktur Sales dan Marketing ACS Group, Arijanto Hartanto, dan dilanjutkan dengan sambutan dan ucapan terima kasih dari perwakilan Blue Power Technology selaku distributor, Natasha Eunike.

ExtremeCloud IQ adalah platform manajemen jaringan berbasis cloud yang disediakan oleh Extreme Networks. Platform ini memungkinkan pengelolaan dan pemantauan jaringan secara sentral, serta memberikan analitik dan kecerdasan buatan (AI) untuk meningkatkan efisiensi dan kinerja jaringan.



ExtremeCloud™ IQ

Menuju Era IKN: ACS Group bersama Aruba Networks membuka Jalan untuk **Perkembangan Teknologi Perhotelan** melalui HITA Kaltim

Dalam persiapan menghadapi masa depan IKN (Ibu Kota Negara Nusantara), industri perhotelan di propinsi Kalimantan Timur semakin membutuhkan perancangan teknologi dan infrastruktur yang memadai. Untuk memperkenalkan teknologi terkini kepada para pelaku bisnis perhotelan, ACS Group bekerja sama dengan Sistech Kharisma membawa solusi Aruba Networks memperkenalkan solusi Access Point pada acara HITA Kaltim pada 20 Mei 2023 di Maxone Balikpapan.

Acara ini dibuka dengan doa dan menyanyikan lagu Indonesia Raya sebagai cerminan persatuan. Dilanjutkan dengan pembukaan kata sambutan dari Chairman HITA Kaltim - Pramono, dilanjutkan oleh Chairman HITA Indonesia - Andy Aries, dan IHGMA Balikpapan - M. Zuwaini.

Dalam acara ini, HITA Kaltim memberikan kesempatan bagi para peserta untuk berdiskusi dan berbagi pengetahuan dengan para ahli dan praktisi di bidang teknologi perhotelan melalui presentasi dan pameran teknologi.

Melalui booth yang disediakan, Aruba Networks berbagi inovasi teknologi yang dapat meningkatkan efisiensi dan pengalaman pelanggan dalam industri perhotelan, misalnya Aruba Instant On dengan Aruba AP-505 nya untuk keperluan lobby dan ruang konferensi; AP-515 cocok mengatasi kebutuhan di aula; AP11D handal di area publik seperti lobby, restoran, atau lounge hotel; AP17 menghadirkan keandalan dan fleksibilitas tinggi untuk are outdoor dengan kondisi ekstrim; dan AP11 cocok untuk hotel dengan skala kecil hingga menengah, dan area yang membutuhkan konektivitas dasar seperti kamar tamu atau ruang rapat kecil.



Aruba Networks terus berinovasi untuk memberikan solusi yang andal dan mendukung perkembangan teknologi dalam industri perhotelan di Kalimantan Timur. Dukungan Aruba Networks, Sistech Kharisma, dan ACS Group sebagai sponsor dan mitra acara ini menunjukkan komitmen untuk memajukan industri perhotelan melalui penerapan teknologi terkini.

PRODUCT HIGHLIGHT

ARUBA HPE

Aruba Fabric Composer

Industri : All Industries

Dashboard View

Includes information about fabrics, switches, hosts, VMs, and Security

Workflow Automations and Guided Setup

Point and click GUI network and security services automation



Network and Switch Visualization

Hosts, MAC, Neighbors, Switch inventory, health status

API level integrations with various environments

Including HPE, Aruba, VMware vSphere, ESX, NSX and Nutanix

Aruba Fabric Composer adalah sebuah *software orchestration* atau perangkat lunak yang berfungsi sebagai orkestrasi dalam pengelolaan perangkat data center yang menggunakan perangkat switch Aruba OS-CX sehingga memudahkan dalam pengoperasian jaringan karena menghadirkan otomasi dan analitik yang terdistribusi baik di jaringan campus, cabang dan data center. Orkestrasi digunakan untuk mengotomasi proses konfigurasi dan pengelolaan perangkat jaringan, sehingga lebih mudah untuk mengelola jaringan berskala besar.

Fabric Composer memungkinkan administrator mengkonfigurasi jaringan *leaf-spine* dari satu konsol daripada harus masuk ke setiap perangkat switch satu per satu. Fabric Composer mengatur konfigurasi perangkat switch menggunakan alur kerja yang interaktif dengan mengotomasi tugas yang berulang dan manual, seperti penyediaan/*provisioning*, konfigurasi, dan penyebaran sumber daya TI.

Fabric Composer terintegrasi dengan platform infrastruktur populer lainnya untuk memastikan beban kerja komputasi dan penyimpanan (*compute & storage workloads*) terhubung dengan mudah ke VLAN, *port groups*, dan elemen jaringan

lainnya sehingga mengurangi kesalahan manual. Fabric Composer juga memberikan visibilitas yang jelas tentang konektivitas *end-to-end* untuk pemantauan dan pemecahan masalah.

Kombinasi Aruba Fabric Composer dan Aruba OSCX juga mendukung lingkungan non-HPE seperti VMware Cloud Foundation, VMware vSphere, VMware NSX, Nutanix Prism, dan lain-lainnya, sehingga pelanggan menikmati manfaat proses-proses otomasi dari *fabric provisioning*, *workflow* berbasis event, optimisasi lalu-lintas dari media penyimpanan (*storage*) serta manajemen kebijakan keamanan (*security policy*).



ARUBA HPE

Aruba CX 10000 Switch Series

Industri : All Industries

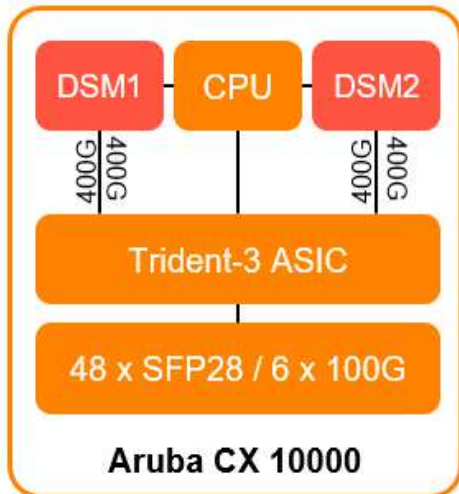
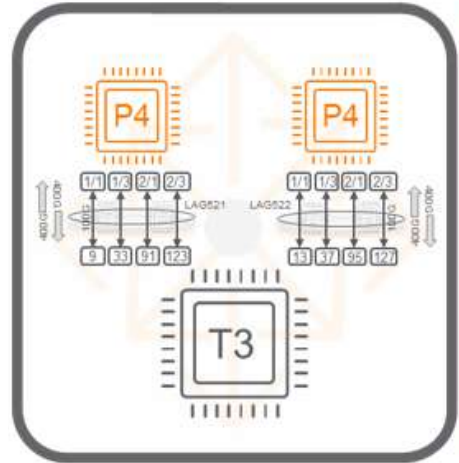


Perangkat switch Aruba CX 10000 Series adalah perangkat switch generasi baru yang dirancang untuk menyederhanakan arsitektur jaringan dengan platform *switching* berkinerja tinggi dan berkemampuan layanan terdistribusi. Perangkat switch Aruba CX 10000 Series merupakan pioneer teknologi **Distributed Services Switch (DSS)** yang mengkombinasikan teknologi *routing* dan *switching* Aruba (layer 2-3) dengan teknologi **AMD Pensando** yang berjalan di layer 4-7 meliputi *stateful firewall*, *DDoS protection*, NAT, *load balancer*, dan *deep flow-based session-level telemetry* dengan *logging* serta layanan enkripsi.

Aruba CX 10000 Switch Series memiliki kapasitas hingga **3.6 Tbps bidirectional switching** dan 2,000 Mpps *forwarding*, dilengkapi konektivitas 48 ports *line rate* 10/25GbE (SFP/SFP+/SFP28) dan 6 ports 40/100GbE (QSFP+/QSFP28) serta merupakan perangkat switch 800G *ultra-high-speed network*.

Aruba CX 10000 Switch Series berbasiskan AOS-CX, merupakan *database-driven operating system* modern yang dapat melakukan proses otomatisasi dan mempermudah tugas-tugas dalam jaringan yang kritikal dan kompleks. Dengan *built-in database*-nya memungkinkan pelanggan dan developer aplikasi menggunakan *software scripts* untuk keperluan *historical troubleshooting*, *past trends analysis*. Hal ini tentu membantu dalam prediksi dan menghindari masalah di masa mendatang terkait skalabilitas, keamanan, dan kinerja yang *bottlenecks*.

Arsitektur dari perangkat switch Aruba CX 10000 series adalah arsitektur jaringan agnostic yang sangat fleksibel ketika diterapkan sebagai perangkat *access switch*, sebagai perangkat switch leaf Top of Rack (ToR) atau End of Row (EoR) dalam data center, serta memungkinkan sebagai *aggregation layer switch* di lingkungan kampus.



PRODUCT HIGHLIGHT

ZEBRA

ZT111 Industrial Printer

Industri : Manufacturing, Healthcare, Retail, Transportation and Logistics.

Merupakan tipe printer industri yang dapat menjadi pilihan dan andalan Anda dengan harga hemat dan mampu memberi Anda LEBIH, yaitu “lebih banyak fitur, lebih tahan lama, lebih aman, dan lebih banyak waktu aktif(uptime). Penggunaannya mudah dengan kecepatan cetak yang tinggi dengan bentuk dimensi yang hemat ruang, sebagai pilihan yang tepat untuk memajukan bisnis Anda. Disamping itu printer ini sangat mudah untuk diintegrasikan ke dalam jaringan Anda yang sudah ada karena kompatibel dengan versi sebelumnya dan menampilkan Emulasi Printer untuk menggantikan merek lain tanpa harus mengubah format label atau menulis ulang kode.



ZEBRA

RFD90 Ultra-Rugged UHF RFID Sleds

Industri : Manufacturing, Government, Transportation and Logistics.

Zebra RFD90 adalah RFID reader ultra rugged yang memiliki pilihan daya baca standar dan daya baca dengan jangkauan jauh tanpa henti. Produk ini mampu mempertahankan pergerakan rantai pasokan dan melacak tag pada aset serta inventaris Anda. Ultra-Rugged UHF RFID Sleds ini dirancang untuk bekerja di lingkungan yang ekstrim. Teruji tahan benturan jatuh setinggi pada jarak 1,8 meter di atas beton dan memiliki peringkat IP65 serta IP67 untuk tingkat industri. Perangkat ini mampu beradaptasi dengan teknologi baru bahkan yang sedang berkembang. Sudah dilengkapi dengan Wi-Fi 6 enables easy over-the-air (OTA) device management. Kami siap membantu dalam menerapkan solusi teknologi RFID untuk kelancaran alur proses bisnis Anda.



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

Scan this
QRcode



Buka Bersama Helios Netventure Series untuk Partner Bisnis

Aruba HPE bersama Helios Informatika Nusantara menggelar kegiatan buka bersama dengan partner bisnis, salah satunya ACS Group, di Jakarta Aquarium, Neo Soho Lantai LG 10, Jakarta, Rabu (05/04). Acara ini merupakan wujud kebersamaan, meningkatkan silaturahmi antara Aruba dengan partner bisnis.

Momen ini sekaligus sebagai media mempelajari bagaimana Aruba dapat menyediakan fondasi jaringan yang aman untuk *Zero Trust* dan *Secure Access Service Edge* (SASE). Dalam pembahasan Episode 3: Aruba ClearPass and Edgeconnect for Zero Trust Security, pembahasan ini memberikan



kualitas pengalaman dan keamanan tingkat lanjut. Dengan Aruba Edgeconnect, akan memudahkan pengerjaan operasional bisnis seperti: *Simplify WAN architecture, Agile, Business Driven, Simplified IT Ops Edge platform*, hingga lisensi keamanan.

Selanjutnya, pada saat ini serangan bukan hanya dari luar ke internal namun saat ini serangan dimungkinkan terjadi dari internal sendiri. Oleh sebab itu, untuk akses internet dapat diatur melalui Network Access Control Clearpass Aruba yang sudah dilengkapi dengan fitur tambahan seperti: *Onboard, Guest, hingga Onguard*.

Sosialisai APTISI: Kolaborasi dan Inovasi dalam Pengembangan Teknologi Identifikasi di Indonesia

APTISI atau Asosiasi Pengusaha Teknologi Identifikasi Seluruh Indonesia adalah Asosiasi ini dibentuk dengan tujuan menjadi wadah komunikasi yang efektif dan sarana pertukaran informasi yang saling memberikan manfaat dan saling menguntungkan antar sesama Pengusaha yang menjadi anggota perkumpulan.

APTISI dibentuk dan disahkan pada bulan November 2022 lalu dan pada tanggal 16 Mei 2023 bertempat di Holiday Inn Kemayoran telah mengadakan acara perdana sekaligus sosialisasi yang dihadiri kurang lebih 50 perusahaan yang bergerak dibidang Teknologi Identifikasi.

Dalam kata sambutan pertama, Indra Tjahjadi (Pembina APTISI) dan Basuki Surodjo (Ketua

Umum APTISI) menekankan pentingnya kerja sama antara pengusaha dalam menghadapi tantangan dan peluang di bidang teknologi identifikasi. Mereka menyampaikan bahwa kolaborasi antara pengusaha adalah kunci untuk mengembangkan industri ini secara berkelanjutan. Kerja sama yang baik akan memperkuat daya saing APTISI.

Selanjutnya, Wisnu Wahyudin (Wakil Ketua Kadin), menekankan peran penting APTISI dalam menjadi solusi dari permasalahan teknologi identifikasi, bahkan mengenai permasalahan regulasi. Beliau menggarisbawahi bahwa APTISI memiliki komitmen untuk menghadirkan inovasi teknologi. Dengan demikian, APTISI berperan sebagai penyeimbang dalam menghadapi tantangan di era digital.



CORPORATE INFO

Training Product Seuic di kantor ACS Group

Service Center ACS Group berkomitmen penuh untuk memberikan kepuasan pelayanan purna jual(after sales) secara prima kepada para pelanggan setia.

Demi tercapainya tujuan tersebut, team Engineer ACS Group selalu dibekali pelatihan(training) oleh para principal kami sehingga mereka memiliki kompetensi yang baik dalam hal perawatan, perbaikan, konsul dan pelayanan lainnya secara prima.

Pada tanggal 22 May 2023, Mr. Gexinjie dari SEUIC, salah satu principal kami memberikan pelatihan, upgrade skill & transfer knowledge serta tanya jawab seputar issue-issue di lapangan dan info ketersediaan stock spare part.



Melihat pengalaman, kompetensi dan perlunya dukungan purna jual tersebut, SEUIC juga telah menunjuk ACS Group sebagai **Authorized Service Center SEUIC** di Indonesia, itu sebabnya ACS Group bersama SEUIC terus memberikan tambahan skill & knowledge produk kepada para engineer sehingga dapat melakukan proses troubleshooting & solving secara akurat, tajam dan efisien.

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

BEING CERTIFIED MEANS WE ARE QUALIFIED TO RUN HIGHER-QUALITY JOB FOR YOU AS OUR VALUED CUSTOMER.



and many more...

Gathering Seru ACS Group di Taman Bukit Palem Resort Setelah 3 Tahun Pandemi



ACS Group mengadakan gathering penuh kegembiraan di Taman Bukit Palem Resort - Bogor. Acara ini menjadi pertemuan pertama kali setelah 3 tahun sejak pandemi COVID-19 melanda, dan menghadirkan momen yang sangat ditunggu-tunggu bagi seluruh karyawan.

Gathering ACS Group di Taman Bukit Palem Resort menjadi ajang untuk mempererat hubungan antar karyawan baik Jakarta dan seluruh cabang-cabang ACS Group dalam merayakan kebersamaan setelah masa-masa pandemi. Acara ini dihadiri oleh lebih dari 100 karyawan ACS Group yang penuh semangat.

Pada pembukaan acara, Singgih Prabawa (Ketua Panitia) dan Indra Tjahjadi selaku Managing Director, menyampaikan apresiasi kepada seluruh tim atas dedikasi mereka dalam menghadapi



tantangan pandemi dan memberikan kebahagiaan kepada karyawan untuk menikmati gathering selama 2 hari 1 malam.

CORPORATE INFO

Selama gathering, berbagai permainan dan kompetisi seru diadakan untuk mempererat hubungan tim. Semua karyawan ACS Group turut berpartisipasi dalam games tim yang melibatkan kerjasama dan strategi. Tidak hanya itu, ada juga kegiatan offroad yang menantang dan memacu adrenalin, memberikan kesempatan bagi karyawan untuk menghadapi tantangan dengan semangat yang tinggi.

Malam hari, suasana fun night menghiasi acara dengan penampilan menarik, mulai dari

pertunjukan musik, tarian, hingga drama dari karyawan baru. Semua karyawan berbaur dalam kegembiraan, tertawa, dan menikmati momen kebersamaan yang lama ditunggu-tunggu.

Outing ACS Group kali ini menjadi peringatan penting bahwa ACS Group telah mengatasi masa-masa sulit dan tetap bertahan dalam menghadapi tantangan yang tak terduga. Semangat dan kebersamaan yang terbentuk di acara ini akan menjadi modal berharga untuk mencapai kesuksesan di masa depan.



Alibaba Cloud Indonesia Partner Bootcamp



Alibaba Cloud mengadakan bootcamp untuk partner mereka di Indonesia, dihadiri 23 partner T1 dan T2.

Dr. Anthon Hutabarat (Head of Channel) membuka acara ini dengan memberikan gambaran market cloud Indonesia yang terus berkembang pesat, didasari kebutuhan akan skalabilitas dan efisiensi biaya yang diberikan oleh teknologi cloud computing.

Event utama diawali dengan pemaparan Safeguarding Cloud Security oleh **Jerry Ye** (Utility Products Business Unit - Security Service) yang menunjukkan berbagai macam cara dan tools yang disediakan oleh Alibaba Cloud untuk mengamankan resource Alibaba Cloud, multi-cloud dan juga on-premise. Portfolio Alibaba Cloud Security dibagi dalam 3 kategori: Account, Business, dan Monitoring Operation. Level yang paling mendasar adalah Anti-DDoS yang dapat memitigasi serangan layer 7, difasilitasi dengan scrubbing center yang dedicated sudah ada di lokasi Indonesia.

Christina Ding (Utility Products Business Unit - Storage Service) melanjutkan pembahasan dengan tema Store & Data Access, membahas solusi Storage yang fleksibel dan dinamis. Perkembangan pesat Alibaba Cloud membuatnya

sudah ranking #3 dalam waktu yang singkat, didasari kebutuhan global dari group yang memiliki DNA e-commerce ini. Point penting yang perlu dipertimbangkan dalam adopsi cloud untuk data adalah Volume, Velocity, Variety, Veracity, dan Value dimana peningkatan signifikan kelima unsur itu dengan keberadaan dari perkembangan teknologi mewajibkan organisasi perlu mengadopsi pendekatan cloud untuk penyimpanan data dan tools komputasi mereka.

Menutup sesi oleh pembicara regional, Shin Lip **Chok** (Partner Support) memaparkan Cloud Service Offering & After-sales Support yang bisa ditelusuri untuk mendukung keberhasilan onboarding end-user. Edukasi yang esensial ini membuka wawasan terhadap Service Level yang dapat diberikan untuk kelancaran operasional.

Andre Onggara (Senior Channel Development) kemudian memberikan sales pointers untuk mempelajari kebutuhan customer dengan seksama, dilengkapi oleh M. Rohibun (Solution Architect) yang memaparkan poin-poin spesifik agar partner dapat memberikan solusi yang tepat guna. Use case seperti critical app, high-availability, security leveling, database, beserta Reliable and responsive support dipertajam lebih lanjut kemudian lewat group role play yang mensimulasikan request dari end-user.

PRINCIPAL INFO

ACS Group meraih penghargaan Services Partner Of The Year dari Zebra Technologies di acara APAC Channel Partner Summit 2023 di Bali

ACS Group telah meraih penghargaan Services Partner Of The Year dari Zebra Technologies di acara APAC Channel Partner Summit 2023, 9 Maret 2023. ACS Group adalah satu-satunya perusahaan dari Indonesia bahkan se-Asia Pasifik yang memperoleh penghargaan tersebut, dan kami boleh mengucapkan syukur karena ini merupakan Anugerah Tuhan yang besar bagi ACS Group. Penilaian penghargaan ini diraih atas komitmen untuk pelayanan/service dan komitmen ACS Group dalam bidang Identification dan Data capture.

ACS Group yang diwakili oleh Arijanto Hartanto – Sales & Marketing Director menerima penghargaan tersebut dalam bentuk plakat yang diserahkan oleh Christanto Suryadarma Southeast Asia(SEA) Sales Vice President & Channel Lead Sales for APAC dan George Pepes APAC Vertical Solutions Lead, Healthcare and Retail, Zebra Technologies Asia Pasific.

Kami ACS Group sangat menghargai kepercayaan yang diberikan dan akan terus



mempertahankan serta meningkatkan service/pelayanan kami kepada para pelanggan setia. Kami mengucapkan terima kasih atas kepercayaan para pelanggan yang terus mempercayai kami untuk bekerjasama dan kami akan menjaga tetap kemitraan ini untuk kemajuan bersama.

ACS Group mengucapkan

Selamat hari raya

Idul Adha 1444 H

Semoga kita dapat
meneladani pengorbanan
serta ketaqwaan Nabi
Ibrahim AS dan Ismail AS.

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



PRINCIPAL INFO

ACS Group menerima 3 Penghargaan sekaligus dari Zebra Technologies



ACS Group di tahun 2023 ini telah memperoleh 3 Award sekaligus dari Zebra Technologies, antara lain “Top Revenue Contribution”, “Strategic Win (EVM) Partner” dan “RFID Partner Of The Year”.

Award ini diberikan pada acara tahunan “Zebra ID Partner Summit 2023” yang berlangsung pada tanggal 8-9 Mei 2023 di The Village Resort Bogor. Acara ini diikuti oleh para partner, disti, serta vendor yang bekerja sama dengan Zebra Technologies.

Penghargaan yang kami peroleh ini merupakan sebuah pengakuan tertinggi dari principal terhadap ACS Group sekaligus menjadi cambuk bagi kami untuk lebih inovatif lagi dalam menghadirkan berbagai pelayanan yang berkualitas dan tepat guna.

Namun semua yang telah ACS Group terima juga tak lepas dari kerjasama yang baik dengan para pelanggan setia yang telah dibangun dengan baik pula.



Penghargaan “Top Revenue Contribution”*kiri* dan “RFID Partner Of The Year”*kanan* dari Zebra Technologies yang diterima oleh Ibu Nuning Kustiawita, Sales Manager ACS Group.



Penghargaan “Strategic Win (EVM) Partner” dari Zebra Technologies yang diterima oleh Harry Sugiarto, Senior Account Executive ACS Group.



Beberapa Cara Efektif Mengamankan Sistem Keamanan Jaringan Komputer Anda

by Jemis Pangaribuan,
AIDC and Security Technology Manager



1. Menggunakan Password yang benar.

Gantilah password secara berkala. Jangan menggunakan nama, tanggal lahir, kota, dan lain sebagainya. Hindari menggunakan *password* dengan kata-kata yang ada di kamus bahasa apapun. Selalu gunakan kombinasi angka, huruf, dan karakter lain.

2. Hindari atau tidak mengklik link yang tidak jelas sumbernya.

Saat ini, banyak orang tertipu oleh link yang tidak jelas sumbernya. Link tersebut mengatasnamakan perusahaan atau instansi yang kredibel. Tetapi alamat internet di balik link tersebut menuju ke sebuah situs untuk memancing atau mengelabui pengguna. Misalnya, ada sebuah link mengatasnamakan Internet Banking Bank BCA. Lalu setelah pengguna mengklik link tersebut, maka pengguna akan diminta untuk mengganti *user name* dan *password*. Padahal, link tersebut adalah palsu. Jika Anda ragu dengan link tersebut, pastikan Anda minta tolong ke *network administrator* atau orang yang ahli di bidang tersebut.

3. Gunakan Software resmi.

Gunakan selalu *software* resmi. Saat ini, banyak *software* gratis yang bisa di *download* lewat internet. Tetapi, *software* tersebut belum tentu aman dari virus, *ransomware* atau *malware* yang bisa menyerang *system* komputer Anda. Pelaku kejahatan akan meminta tebusan agar si korban bisa kembali mengakses data miliknya.

4. Gunakan Antivirus terpercaya dan perangkat Internet/Intranet Security.

Saat ini, banyak *software* antivirus dan perangkat internet dalam 1 box. Jangan lupa untuk selalu meng-update fitur dari box tersebut.

5. Jika perlu, gunakan jasa Cyber Security.

Sebagai sebuah perusahaan profesional, tentu Anda mengetahui akan pentingnya data-data pelanggan Anda. Jika Anda tidak dapat melindunginya, maka perusahaan bisa terkena sanksi serta kehilangan kepercayaan dari pelanggan.

Untuk menghindari hal tersebut, maka Anda dapat menggunakan jasa cyber security untuk membantu mengamankan data-data Anda.



Amankan Jaringan Anda dengan Platform Universal Extreme



ExtremeCloud™ IQ dari Extreme Networks adalah platform manajemen jaringan berbasis cloud yang memberikan visibilitas, analitik canggih, dan kecerdasan buatan untuk mengoptimalkan kinerja jaringan mulai dari penerapan hingga pemeliharaan. Dengan fitur adaptif dan kemampuan manajemen yang terpusat, ExtremeCloud IQ memungkinkan pengelola jaringan untuk mengontrol perangkat dengan efisien, mengambil keputusan yang cerdas, dan memastikan keamanan jaringan yang optimal. Platform ini merupakan solusi inovatif yang membantu perusahaan meningkatkan efisiensi, mengoptimalkan penggunaan sumber daya, dan menghadapi tantangan transformasi digital.

Kami siap membantu Anda untuk keamanan dan kelancaran bisnis Anda.

Need More Info? Contact us at today: marketing@bluepowertechology.com

PT Blue Power Technology

Centennial Tower 12th Floor
Jl. Jend. Gatot Subroto Kav 24-25, Jakarta - Indonesia
Ph. +6221 806 22278

CORE BUSINESS SOLUTIONS: 4 PILLARS



- 1 Automatic Identification & Data Capture (AIDC)**
IT peripherals such as: Barcode/RFID printers, Barcode/RFID readers or scanners, enterprise mobile printers, enterprise mobile computer (handheld, vehicle mount, tablet, wearable).
- 2 IT Infrastructure**
Network Devices (Access Point, Controller, Wired/Wireless), Hyper Converge Data Center, Public & Private Cloud, Cyber Security (Next-Gen Firewall, Network Access Control, Endpoint protection, OT).
- 3 Enterprise Security System**
Access Control (+Turnstile, Barrier Gate), Surveillance (Enterprise IP Cam), Alarm system, Unified Command & Control Center.
- 4 Enterprise Business Solution**
Software Package, Managed and Professional Services.

BUSINESS PARTNERS

Alibaba Cloud

HPE aruba networking

BarTender
BY SEAGULL SCIENTIFIC

BOSCH
Invented for life

brother
at your side

Extreme
Connect Beyond the Network

FORTINET

Hewlett Packard
Enterprise

HID

HIKVISION

HUAWEI

Hytera

ivanti

JANZ

POINT Mobile

SAMSUNG

Seuic

ZEBRA

ZKTeco
Indonesia

Jakarta (Head Office)

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

Jakarta (Service Center)

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

Cikarang

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

Semarang

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

Surabaya

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