GEBYAR

BULETIN EDISI 54/MARET 2021

AUTO-ID

UNTUK KALANGAN SENDIRI

MAXPRO® CLOUD

Media Penyimpanan dan Pengelolaan Video di Internet

Drivelock :
Ayo, Lakukan Enkripsi Pada Data Penting Anda!

TIPS & TRIK :
Tips Dalam Menghentikan Serangan Phishing

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

EDITORIAL

Para Pembaca yang budiman,

Salam sejahtera bagi kita semua.

Puji serta Syukur kita panjatkan ke Hadirat Tuhan Yang Maha Esa atas segala berkat, karunia dan perlindungan-Nya lah kita masih diberikan kekuatan dan kesehatan. Kiranya di Tahun 2021 ini kita semua senantiasa berada dalam perlindunganNya dan semua yang kita rencanakan dapat tercapai serta semoga pandemi covid-19 ini segera berakhir.

Pembaca yang kami hormati, topik yang kita pilih di awal penerbitan tahun 2021 ini adalah tentang Maxpro Cloud dan Drivelock, dimana di era digital dan di masa pandemi covid-19 seperti ini sangat mempengaruhi bagaimana cara kita bekerja dan berbisnis. Dua topik kita kali ini sangat erat bersentuhan dengan keamanan data atau Data Security. Saat ini semua bisnis dipaksa untuk melakukan transformasi digital dan tentu saja perlu kewaspadaan agar supaya data/informasi perusahaan kita aman tersimpan tanpa harus mengorbankan asset perusahaan yang tidak ternilai harganya. Semoga pilihan topik kami kali ini dapat memberikan pencerahan bagi para pembaca yang budiman.

Seperti biasa, di edisi ini juga dapat anda temukan info-info yang menarik diantaranya info product highlight, tips dan info, kegiatan ACS Group dan info lainnnya.

Akhir kata, saya mewakili tim ACS Group mengucapkan selamat membaca, semoga bermanfaat dan semakin sukses di tahun yang baru ini, Amin.

Salam Redaksi,

Ihdi Arwan
Professional Services Supervisor
ACS Group
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
Usadi Sastra Atmadja

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Ihdi Arwan
Jemis Pangaribuan
Irvan Kurniawan

ALAMAT REDAKSI
Jakarta (HO)
Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
Telp : +6221-4208221, 4205187
Fax : +6221-4207903, 4207904, 4205853

CONTENT

2 Editorial - **Ihdi Arwan**
3 Media Penyimpanan dan Pengelolaan Video di Internet by Maxpro® Cloud
8 Ayo, Lakukan Enkripsi Pada Data Penting Anda!
12 Events
18 Product Highlight
22 Corporate & Principal Info
25 Tips Dalam Menghentikan Serangan Phishing

Media Penyimpanan dan Pengelolaan Video di Internet by Maxpro® Cloud

by **Jemis Pangaribuan**, AIDC and Security Technology Manager ACS Group

MAXPRO® Cloud adalah Suatu Platform security atau keamanan yang terintegrasi berbasis Internet yang dirancang khusus untuk bisnis skala kecil-menengah. MAXPRO® Cloud di hosting atau ditempatkan di dalam Media Microsoft Azure, dengan mengintegrasikan hak akses, intrusi pelanggaran, pengawasan video ke dalam satu user interface atau aplikasi pengguna. Aplikasi ini mendukung pengawasan untuk satu atau beberapa lokasi area pengawasan. MAXPRO® Cloud juga menyediakan teknologi baru untuk mengamankan fasilitas area sekaligus menyederhanakan operasional keamanan.

MAXPRO adalah sistem platform yang fleksibel, dapat diskalakan, dan memungkinkan pelanggan atau pengguna untuk mendapatkan tingkat keamanan dan keselamatan yang efisien karena mengurangi biaya infrastruktur IT, dan merampingkan operasional perusahaan dengan memberdayakan pemilik usaha kecil hingga menengah untuk secara efisien mengoperasikan dan mengakses data dari akses, intrusi, dan sistem video mereka.

Misalnya, sebuah bisnis dengan banyak situs dapat menggunakan MAXPRO® Cloud untuk membuat keputusan tentang kontrol akses dari jarak jauh dari smartphone. Daripada harus menghabiskan waktu mengakses komputer desktop di satu lokasi tertentu. Selain itu, karena sistem ini di-host yang ada di cloud, tidak ada server atau perangkat lunak tambahan yang harus dibeli dan dikelola. Inilah yang dimaksud dengan penyederhanaan infrastruktur IT. MAXPRO® Cloud memberi kemungkinan kepada para penggunanya untuk menciptakan pendapatan baru setiap bulan dari sistem yang dihosting di cloud, sambil menyediakan platform keamanan terintegrasi dengan biaya pemasangan dan layanan yang lebih rendah.

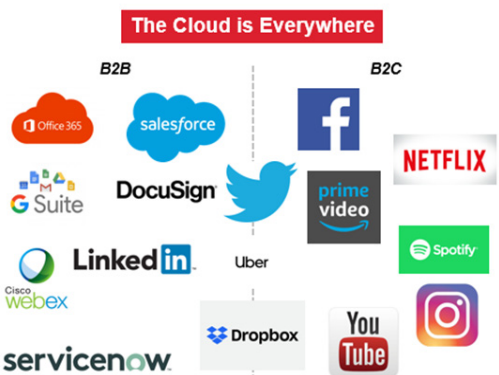
Dengan manajemen akses jarak jauh, pebisnis atau pengguna tidak lagi harus menghadapi down-time yang mahal untuk menunggu dan membayar engineer yang tepat menghidupkan atau memperbaiki system keamanan dan keselamatan ini.

Hal ini memungkinkan pelanggan untuk memantau lingkungan mereka dari jarak jauh melalui cloud dengan Microsoft Azure, bisnisman dapat melindungi aset-aset berharga mereka melalui solusi yang hemat biaya ini.

Selain itu, untuk para Pengembang Aplikasi, antarmuka pemrograman aplikasi (API) MAXPRO® Cloud akan tersedia di Portal Pengembang Honeywell yang memungkinkan komunitas pengembang Honeywell membuat aplikasi khusus. Portal Pengembang Honeywell menyediakan lingkungan pengembangan yang komprehensif, dengan alat dan API tercanggih untuk mengaktifkan dan mempercepat pembuatan layanan baru dan aplikasi inovatif yang terintegrasi penuh dengan platform Honeywell.

WHY CLOUD ?

1. 97% perusahaan besar di dunia menggunakan layanan cloud untk sektor public, private atau kombinasi dari keduanya, Menurut Mc.Afee
2. Pendapatan Infrastruktur TI Cloud Melampaui Pendapatan Infrastruktur TI Tradisional untuk Pertama Kalinya pada Kuartal Ketiga 2018, Menurut IDC



MIGRASI KE CLOUD

Di bawah ini, ada beberapa trigger dan benefit yang menyebabkan migrasi sistem tradisional ke cloud.

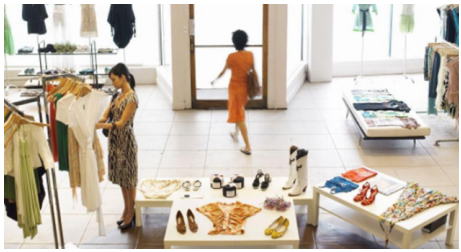
1. Aktivitas kriminal yang sering terjadi di toko-toko, terutama yang buka 24 jam sehari. Yang menjadi perhatian disini adalah personal dan peralatan keamanannya. Dengan menerapkan sistem ini, kita dapat **mencegah penyusup** dengan memiliki perangkat keamanan di lokasi
2. Produk keamanan yang berbeda dari beberapa vendor dan merek. Issue disini adalah, integrasi antara CCTV, Access Control, Alarm tidak saling terkoneksi. Dengan Honeywell System, anda telah mempunyai sistem yang handal secara **End-to-End Solutions for Connected Security**.
3. Sesuaikan dengan strategi perusahaan untuk menjangkau cakupan secara geografi. Concern disini adalah masalah **Flexibility & Future proof**. Dengan menggunakan Honeywell Cloud, anda hanya perlu membayar apa yang anda gunakan, karena sistem Honeywell mempunyai skalabilitas di masa yang akan datang.
4. Mengelola bermacam-macam properti di beberapa lokasi. Hal ini akan memperlambat pekerjaan dan menaikkan biaya operasional. Dengan Honeywell Cloud, hal ini akan di dikelola dengan cara yang simple, yang tentunya akan **menaikkan efisiensi operasional** perusahaan.

CONTOH PENERAPAN

Berikut ini adalah Contoh Penerapan dari MAXPRO® Cloud:

1. Retail

MAXPRO® Cloud meningkatkan keselamatan dan keamanan, meminimalkan kehilangan inventaris dan barang-barang jualan di lingkungan ritel, mengurangi biaya infrastruktur TI, dan merampingkan operasional dengan memberdayakan pemilik untuk membuat keputusan yang tepat dan real-time.



2. Commercial Offices

Melalui notifikasi secara real-time, dan dashboard aplikasi operasional intuitif yang dikirimkan ke perangkat seluler apa pun, MAXPRO® Cloud memungkinkan Anda sebagai pemilik atau pengelola perusahaan melindungi orang, properti, dan aset Anda secara efektif dan efisien.

3. Franchises

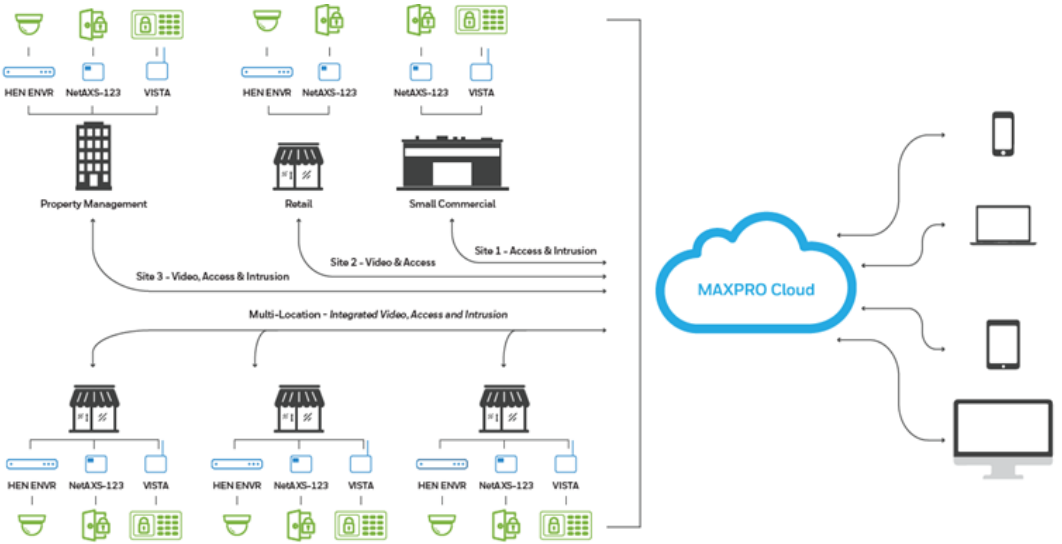
Menghubungkan lokasi waralaba secara regional atau nasional tidak pernah mudah dilakukan. Tetapi dengan MAXPRO® Cloud, anda dengan mudah dapat memantau dan mengelola kontrol akses dan sistem keamanan dari jarak jauh hanya dengan satu klik.

4. Property Management

Tingkatkan daya jual properti Anda dan tingkatkan hunian serta retensi penyewa dengan memanfaatkan sistem manajemen keamanan berbasis cloud yang dapat diskalakan dan memberikan situasi secara real-time nyata ke perangkat seluler apa pun.

SYSTEM ARCHITECTURE

Topology atau System Architecture dari MAXPRO® Cloud adalah seperti di bawah ini.



AWARD

Beberapa Penghargaan yang didapat dari Teknologi ini.

Seluruh Staff dan Management ACS GROUP mengucapkan

SELAMAT MEMPERINGATI

ISRA MI'RAJ NABI MUHAMMAD ﷺ 1442 H

11 Maret 2021

SELAMAT HARI RAYA

NYEPI

14 Maret 2021

SELAMAT MEMPERINGATI

JUMAT AGUNG

2 April 2021

PASKAH

4 April 2021

ACS GROUP

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

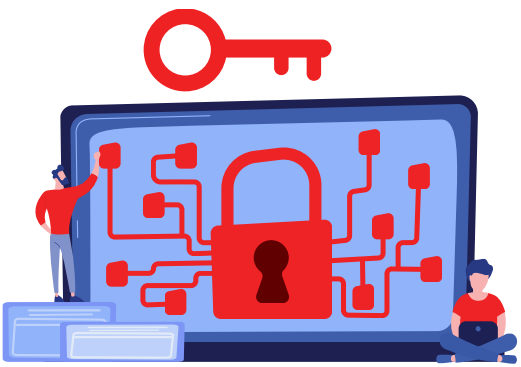
Ayo, Lakukan Enkripsi Pada Data Penting Anda!

by **Ihdi Arwan**, Professional Services Supervisor ACS Group

Data memiliki sejarah yang lebih pendek daripada emas, tetapi ternyata berdampak lebih besar pada bisnis global sekarang ini. Dimana dapat disaksikan bahwa perusahaan yang telah menemukan cara untuk mengumpulkan, mengolahnya dan menggunakan data yang dapat mengungguli pesaing mereka. Lihat saja *Google*, *Facebook*, *Amazon* misalnya, aplikasi yang mereka buat terutama ditujukan untuk mengumpulkan data.

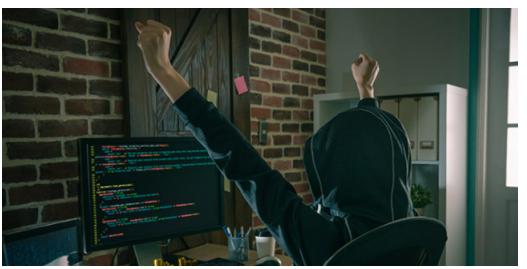
Jadi apakah data adalah emas baru? Data adalah komoditas seperti emas. Perlu pemurnian untuk mendapatkan hasil maksimal, seperti emas. Tetapi terdapat pula data yang tidak berharga, dan itu ada dimana-mana. **Nilai data adalah wawasan yang dapat dibuatnya**. Wawasan yang diperoleh dari penggunaan data yang berkualitas baik dan secara cerdas akan sangat berguna. Merek dan perusahaan yang mampu mengembangkan wawasan tersebutlah yang dapat ditindaklanjuti, dan akan menjadi pemenang.

Namun data yang bernilai tersebut dan tersimpan secara digital baik di *local machine*, *database* perusahaan dan di *server cloud* menjadi incaran sehingga terjadilah pelanggaran, pencurian dan pembobolan data pada perusahaan bisa secara sangat sederhana ataupun kompleks tergantung dari cara kita memberikan akses kepada orang yang berhak mengaksesnya.



Bagaimana pencurian atau pembobolan data terjadi?

Pencurian data terjadi ketika seseorang menyusup ke sumber data dan mengekstrak atau menggandakannya *copy file* yang sifatnya rahasia. Hal ini dapat dilakukan dengan cara mengakses komputer target secara langsung atau dengan melewati keamanan jaringan dari jarak jauh.



Pelaku dari pencurian data ini bisa dilakukan oleh orang luar atau bahkan orang dalam itu sendiri (internal perusahaan). Serangan pada dunia maya yang paling umum digunakan dalam pelanggaran data antara lain:

1. **Malware**

   Malware untuk kependekkan dari "*Malicious Software*" adalah istilah yang menjelaskan program yang berisi kode-kode yang dirancang

untuk merusak file computer, sistem aplikasi atau perangkat lunak. Contoh *malware* seperti *virus*, *worm*, *key logger*, *spyware*, *backdoor*, *trojan horse*, *rootkit*, *exploit* dan lain-lain.

Jadi dampak dari *malware* antara lain adalah merusak file dan sistem aplikasi sehingga tidak dapat mengakses data. Kemudian penyusupan dan pengintaian oleh *malware* dengan tujuan mencuri data atau kredensial akses (*username* dan *password*) sehingga dapat menembus ke sumber daya informasi yang bersifat rahasia dan pribadi.

2. Ransomware

Ransomware adalah *malware* yang paling berbahaya karena bertujuan memeras dan meminta uang tebusan (*ransom*) dimana cara kerjanya adalah hasil kolaborasi yang terstruktur, sistematis dan massif dari beberapa *malware* yang mungkin dimulai dengan *adware*, kemudian *spyware* yang didalamnya menyusup *trojan horse*, ditambah lagi pengintaian *key logger* hingga terjadi *backdoor* dan dikendalikan dari jarak jauh oleh mesin *botnet* (*robot* dan *network*) dan ini semua ada ulah para siber kriminal yang telah bersatu menjadi kelompok sindikat. Korbannya pun telah banyak dan tak tanggung-tanggung mulai dari lembaga pemerintahan hingga perusahaan swasta, lembaga perbankan, lembaga kesehatan dan pendidikan. Untuk mengakses atau membuka file yang telah ter-enkripsi biasanya pelaku akan meminta tebusan berupa mata uang *cryptocurrency*.

Beberapa gangguan dan serangan yang terjadi mungkin saja dikarenakan kurangnya pemahaman dan kesadaran para pengguna komputer dan sistem informasi akan bahaya dan resiko yang mungkin terjadi seperti hal-hal kecil berikut ini:

Penggunaan USB stick, kadang dengan mudahnya menggandakan *file-file* penting didalamnya yang mungkin berisi hasil karya pemikiran, data dan informasi yang sensitive (daftar harga, data pelanggan/pemasok, data pribadi, dan sebagainya, dan mungkin hingga karya desain proyek atau data *intellectual property* - IP).

Resikonya adalah jika USB stick ini hilang atau jatuh lalu kebetulan ditemukan oleh pihak atau oknum yang tidak bertanggung jawab, sehingga perlu dipertimbangkan penggunaan enkrispi data pada USB stick ini agar walaupun secara fisik hilang namun data-data didalamnya tidak dapat dicuri karena telah di enkripsi.

Enkripsi (*encryption*) adalah suatu langkah untuk mengamankan data/file/informasi dengan cara mengubahnya ke dalam sistem kode dengan algortima tertentu yang jika dibaca/diakses tanpa alat pemecahan atau dekripsi (*decrypt*) terlebih dahulu akan menjadi hal yang tidak bermakna. Baik enkripsi dan deskripsi adalah bagian dari ilmu kriptografi yang telah ada sejak jaman Romawi Kuno di masa Julius Caesar.

Masih dengan USB stick yang juga berpotensi terhadap penyebaran *virus*, *worm* dan *malware* dari satu perangkat komputer ke perangkat komputer lainnya melalui port-port USB yang terbuka dan merupakan antarmuka atau *interface* yang umum sekarang ini, baik pada perangkat laptop, desktop hingga perangkat mobile. Dan tentu saja semua port tersebut tidak mungkin seketika ditutup dan dikunci serta merta tetapi tentunya dapat dilakukan dengan pengaturan yang baik, misalnya:

a. Aktivitas buka dan tutup port USB dengan mekanisme otorisasi atau *authentication*, sehingga dapat teridentifkasi siapa yang mengakses, port USB mana yang digunakan, dan kapan waktunya dan jika diperlukan tambahkan apa alasan atau *reason* nya.

b. Perangkat USB stick tertentu saja yang di-*authorize* atau yang diperbolehkan beroperasi di lingkungan perusahaan karena setiap USB stick memiliki identifikasi khusus dan perangkat USB stick yang beroperasi ini sudah divalidasi dan dapat dipastikan kebersihan dan kesehatannya.

c. Transaksi file yang terjadi baik *copy*, *cut*, *delete*, *move* dari file tersebut dari satu lokasi ke USB stick akan tercatat *log* dan *history* nya beserta shadow file nya. *Shadow file* adalah backup atau duplikasi dari file data tersebut. Hal ini tentu saja sangat penting dalam hal pelacakan kembali terkait forensik mengenai lalu lintas file tersebut atau

hilangnya file yang bernilai, penting, dan bersifat rahasia.

Sedikit contoh-contoh pengamanan USB stick di atas, dapat diimplementasikan dengan perangkat lunak **Drivelock**, sebuah perusahaan top penyedia jasa layanan solusi keamanan data dan IT dari Jerman yang sudah melindungi ribuan perusahaan di seluruh dunia dari ancaman keamanan siber dengan platform '**zero trust**'-nya.

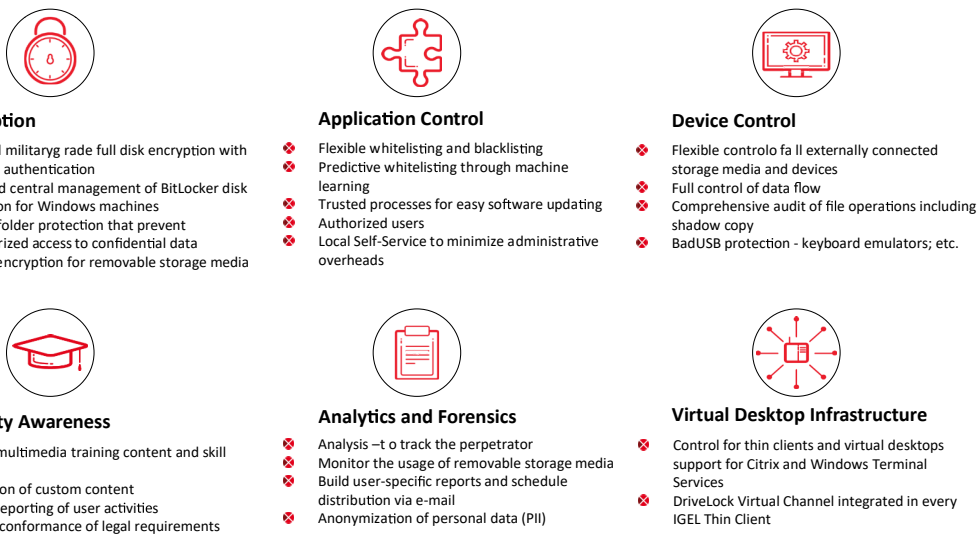
Dari berbagai solusi endpoint yang ada, Drivelock memposisikan solusinya dengan sangat menarik untuk melindungi setiap komputer di perusahaan. Ada enam hal dasar yang sangat penting yang menjadi bagian dari solusi Drivelock yaitu

1. Enkripsi
2. Pengaturan setiap aplikasi yang ada di computer
3. Pengaturan setiap perangkat yang terkoneksi ke computer
4. Pemberian notifikasi keamanan data terkini ke setiap pengguna
5. Pengamanan *thin clients*, *monitoring*
6. Data forensik setiap pengguna.

Berbagai fitur pada gambar 1 ketika dilakukan implementasi, maka akan dapat tercapai keamanan data dan IT di perusahaan yang semakin dibutuhkan terutama dimasa WFH (*Work From Home*) seperti sekarang ini dimana pengguna sangat tersebar baik di luar kantor yang mana kebijakan atau *policy* keamanan sulit diterapkan tanpa adanya solusi seperti Drivelock.

Solusi DriveLock ini telah diimplementasikan oleh salah satu pelanggan ACS Group di Indonesia yang berada di area Jawa Tengah dimana banyak berdiri industri *textile*, *garment* dan *apparel*, mulai dari skala kecil hingga besar. Banyak dari *brand-brand* terkenal internasional yang mempercayakan produknya diproduksi di pabrikan Indonesia.

Data-data dari material dan desain produk dari *brand-brand* ternama ini sangat rentan untuk dicuri, pencurian tidak saja melalui jaringan jarak jauh tapi bisa saja terjadi justru berasal dari oknum internal perusahaan yang mengakses langsung ke sumber daya sistem informasi dalam perusahaan untuk mengambil data yang sensitif dan rahasia tersebut dan mungkin juga menyangkut hak karya cipta atau *intellectual property.* Dan pencurian data tersebut mungkin saja dapat terjadi dengan mudahnya melalui proses meng-*copy file* data rahasia melalui USB stick!



Gambar 1. DriveLock Endpoint Protection

Contoh pencurian data ini dapat terjadi mulai dari dalam lingkup kecil hingga terjadi pada perusahaan besar. Data-data yang berisikan informasi harga, informasi material, desain produk terbaru bisa saja bocor dan diperjualbelikan kepada pihak-pihak yang ingin mengambil keuntungan dari bocornya rahasia data ini.

Asal Tahu Saja

USB Rubber Ducky adalah *keystroke injection attack tool*, yang berbentuk seperti USB Stick atau *Flashdisk*, namun berfungsi layaknya *keyboard*.

Lalu mengapa device ini disebut sebagai Bad USB dan di sisi lain dapat membantu pentester?

Jadi cara kerja Bad USB Rubber Ducky adalah sebelum melakukan serangan, maka terlebih dahulu menuliskan *payload* berupa inputan *keyboard* yang nantinya akan dijalankan oleh Bad USB Rubber Ducky, sebagai contoh untuk menambahkan pengguna (Windows) sesuai keinginannya melalui inputan *keyboard*, maka Bad USB akan diprogram untuk menjalankan perintah:

```
+R > cmd.exe > net user username password /add
```

Lalu script tersebut di-*compile* dan tinggal di-*plug* saja ke mesin target. Itu hanya salah satu contoh, masih banyak hal lain yang bisa dilakukan dengan Bad USB Rubber Ducky atau bisa dibilang tak terbatas!

Dan yang lebih parah adalah karena perangkat ini dikenali sebagai USB HID (*Human Interface Device*) oleh komputer, maka antivirus akan sangat sulit mendeteksi Bad USB Rubber Ducky ini bahkan mungkin tidak bisa, karena terbaca sebagai *keyboard normal*.

Jadi amankan USB port anda dengan Solusi **DriveLock**!

Sumber : https://hackernoon.com/low-cost-usb-rubber-ducky-pen-test-tool-for-3-using-digispark-and-duck2spark-5d59afc1910

Event Virtual ACS Group

Kegiatan update product lewat webinar bagi para pelanggan setia terus dilakukan oleh ACS Group. Kegiatan webinar ini bekerja sama dengan para principal,

Webinar #MakeItVan

Vorsta Product

15 Desember 2020

VOSTRA (PT Vostra Internasional) merupakan rekanan strategis dari ACS yang bergerak dalam bidang teknologi informasi dengan 3 pilar bisnis salah satunya yaitu produk MDM/EMM (Mobile Device Management/Enterprise Mobility Management).

Produk MDM/EMM inilah yang diangkat pada webinar kali ini, sebagaimana kita ketahui Mobility sebagai salah satu trend technology selain Cloud, Big Data, AI/ML yang saat ini tingkat adopsinya di Indonesia meningkat cukup pesat. Pesatnya adopsi teknologi Mobility ini dikarenakan business benefit yang dirasakan secara langsung bagi perusahaan yang telah menerapkannya yaitu peningkatan produktivitas kerja.

Lalu, apa kaitannya produk Vanguard MDM dengan penerapan teknologi Mobility?

Ketika perusahaan mengadopsi teknologi Mobility dengan memberikan berbagai perangkat mobile kepada karyawan (seperti smartphone atau tablet) dan telah mengembangkan aplikasi mobile yang berjalan di perangkat tersebut maka dibutuhkan sistem MDM(mobile device management) untuk memberikan kemudahan dan proteksi agar penerapan teknologi tersebut tepat sasaran yaitu untuk meningkatkan produktivitas kerja.

Berbagai fitur yang dapat memberikan kemudahan pengelolaan perangkat dan aplikasi mobile diantaranya adalah:

1. Fitur Zero Touch untuk mempercepat waktu implementasi dengan menghilangkan proses manual seperti konfigurasi perangkat dan instalasi aplikasi bisnis yang dibutuhkan.
2. Remote devices untuk menghilangkan kunjungan teknisi dengan fitur remote terminal yang dapat digunakan bahkan dalam kondisi bandwidth rendah.
3. Location tracking untuk melihat historis pergerakan perangkat sebagai indikasi produktivitas tim di lapangan.
4. Geofence(Pagar Digital) dengan konfigurasi Geofence per grup perangkat yang dapat melakukan tindakan tertentu pada perangkat saat perangkat berada di dalam dan atau di luar area yang telah ditentukan.
5. Map(peta) yang dapat menampilkan lokasi semua perangkat di dalam satu peta. Tampilan holistik untuk semua perangkat di semua lokasi dengan informasi yang memadai seperti pengguna, email, IMEI, grup.
6. Kemampuan kustomisasi yang dapat dengan mudah menambahkan fitur baru untuk mendukung berbagai use cases. Misalnya: kehadiran online yang diintegrasikan ke dalam

sistem HC pelanggan, kebutuhan pelaporan, manajemen tamu(e-visitor), dan lain-lain.

7. Kemampuan integrasi dengan REST API dan webhook untuk mendukung berbagai kasus penggunaan(use cases). Misalnya: pergerakan historis perangkat yang disimpan dalam big data pelanggan, integrasi dengan sistem CI/CD, integrasi dengan LDAP, dan lain-lain.
8. Berbagai fitur untuk memudahkan pengelolaan perangkat dan aplikasi, juga fitur proteksi untuk pengamanan informasi sensitif dapat dipelajari lebih lanjut pada knowledge base Vanguard MDM pada tautan berikut ini https://vanguard-kb.vostra.co.id

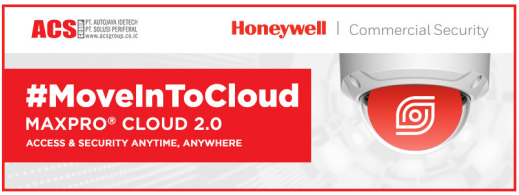
EMM atau MDM atau Mobile Security adalah solusi aman bagi enterprise untuk penerapan teknologi mobile. Solusi ini menyediakan fitur pengamanan informasi sensitif serta pengelolaan penggunaan perangkat dan aplikasi untuk kebutuhan operasional perusahaan. Pengelolaan cukup melalui satu dashboard yang telah terintegrasi, sehingga memudahkan operasionalisasi dari implementai teknologi mobile.

Peningkatan produktivitas dapat terwujud karena karyawan dapat menggunakan aplikasi dan data yang disediakan oleh perusahaan dari mana saja, kapan saja, dan dari berbagai perangkat secara aman, sehingga bisa menghasilkan efisiensi biaya dan tercapainya peningkatan produktivitas kerja.

Webinar #MoveInToCloud

Honeywell Security Product

9 Februari 2021



Honeywell Security pada event ini menjelaskan bahwa MAXPRO® Cloud merupakan Honeywell cloud based integrated connected building platform yang dirancang untuk para pelanggan bisnis kecil-menengah. Solusi yang memberikan kontrol akses waktu secara nyata, pengawasan video, dan deteksi intrusi ke perangkat seluler apapun yang menghubungkan para pelanggan ke gedung mereka dan memungkinkan pengguna untuk membuat keputusan bisnis secara tepat kapan saja dan dimanapun.

Lebih dari sekadar sistem keamanan, MAXPRO® Cloud adalah alat bisnis dinamis yang memberikan wawasan yang dapat ditindaklanjuti yang dapat Anda gunakan untuk meningkatkan layanan dan menghemat biaya. Secara lengkap tentang MAXPRO® Cloud ini dapat anda baca pada topik utama di halaman depan.

Anda dapat menyaksikan video Podcast "Eps. 5 Honeywell Maxpro® Cloud" di channel Youtube kami.

Scan this QRcode

Eps. 5
Honeywell
Maxpro® Cloud

SUBSCRIBE
ACS Group Youtube Channel
PT Autojaya Idetech & PT Solusi Periferal (ACS Group)

Things that will you discover.

- Podcast
- Case Study
- Product Highlight
- Unboxing & Tutorial
- ... etc.

SOLUSI HONEYWELL UNTUK OPERASIONAL MANUFAKTUR MODERN

Operasional manufaktur sekarang ini melampaui lebih dari sekedar jalur produksi di pabrik. Ini dimulai dari saat bahan mentah diterima hingga tahap di mana barang jadi atau sub-perakitan mulai dibuat dan siap untuk dikirim. Dengan demikian, proses pembuatan meliputi pergudangan, fabrikasi dan perakitan suku cadang, pengujian, pengawasan terhadap kualitas, pengemasan akhir, penyimpanan dan pengiriman. Semua ini membutuhkan sistem, aplikasi perangkat lunak dan sejumlah perangkat untuk bekerjasama secara terkontrol dan terkoordinasi. Honeywell menyediakan solusi otomatis yang memberdayakan produsen untuk mendorong efisiensi di sepanjang kegiatan operasional tersebut dan mengendalikan alur kerja yang kritikal.

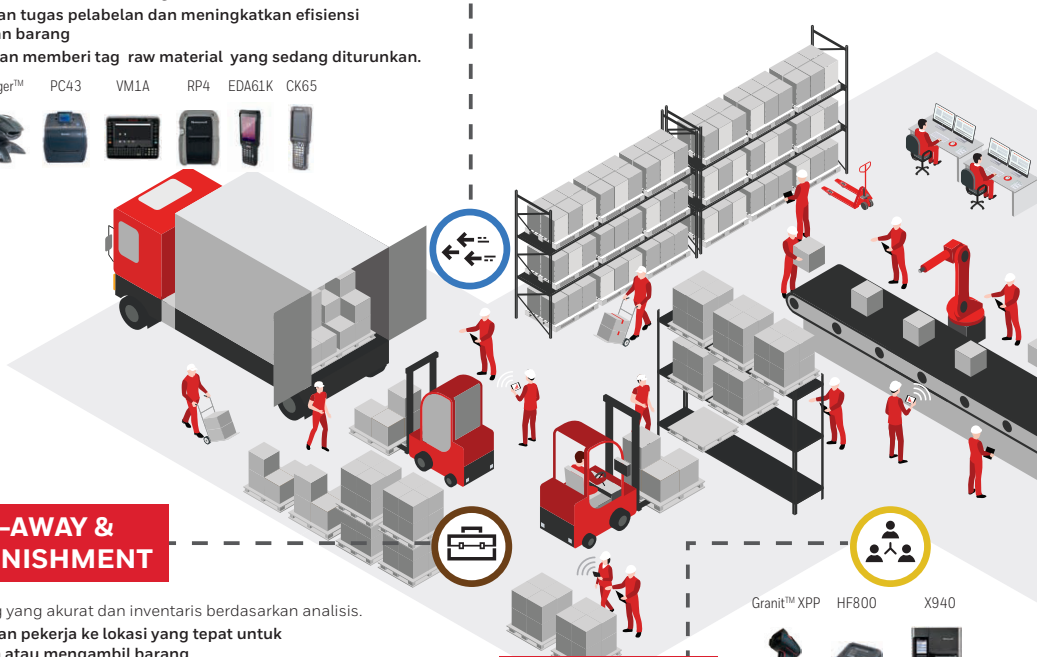
GOODS RECEIVING

PENERIMAAN / PENGIRIMAN BARANG

Proses pemilahan (sortir) bahan yang masuk secara cepat untuk disimpan dan ditempatkan dalam proses put-away

- **Membaca barcode high density, proses masuk dan keluar gudang tanpa jaringan WiFi**
- **Meng-capture data untuk meningkatkan efisiensi dan produktivitas**
- **Memudahkan tugas pelabelan dan meningkatkan efisiensi pengambilan barang**
- **Mencetak dan memberi tag raw material yang sedang diturunkan.**

Xenon™ XP | Voyager™ | PC43 | VM1A | RP4 | EDA61K | CK65



PUT-AWAY & REPLENISHMENT

Proses picking yang akurat dan inventaris berdasarkan analisis.

- **Mengarahkan pekerja ke lokasi yang tepat untuk menyimpan atau mengambil barang.**
- **Proses Cycle Counting dapat disisipkan dengan proses put-away**
- **Melacak tingkat inventarisasi dan mengaktifkan proses replenishment (pengisian ulang) selanjutnya.**

Granit™ XP | 8670 Ring Scanner | VM1A | Guided Work (Voice)

PRODUCTION

Granit™ XPP | HF800 | X940

Informasi waktu yang realtime untuk kegiatan produksi

- **Memperbarui status WIP bersama proses produksi**
- **Meningkatkan produktivitas dan efisiensi tenaga kerja melalui pemindaian yang cepat dan mempercepat pelaksanaan pekerjaan.**
- **Mencetak dengan presisi tinggi pada label serial number.**
- **Melacak dan menelusuri hingga ke individual part atau level produk.**

HONEYWELL SMART TALK

Sarana komunikasi tim yang cerdas, constant dan instant untuk para pengguna perangkat seluler.

HONEYWELL OPERATIONAL INTELLIGENCE

Real Time Data Analytics

Untuk IT Asset Management

PACKING

Proses dimana pesanan pelanggan dikemas dan diberi tag/label secara akurat:

- **Memandu para pengemas barang tentang apa saja yang harus disiapkan dan dikemas**
- **Mencetak label pengiriman yang sesuai**
- **Verifikasi barcode untuk memastikan 100% dapat dibaca oleh pihak penerima**

Granit™ XP PX940 EDA61K CK65 VM1A Guided Work (Voice)

SHIPPING

Menyelesaikan pesanan dengan cepat dan tepat sekalipun kondisi pemesanan sedang tinggi.

- **Menghilangkan loading manual pada proses verifikasi**
- **Mencetak label yang akurat.**
- **Memindai item yang akan diproses dan dikirim.**

Granit™ XP PX940 EDA61K CK65 VM1A

QUALITY CONTROL

Inspeksi atau pemeriksaan terhadap produk guna memastikan bahwa produk telah memenuhi standar kualitas yang disetujui.

- **Menandai dan memberi label pada produk yang tidak memenuhi standard kualitas.**
- **Membantu memastikan semua sudah sesuai dengan standard yang ditentukan.**

PM SeriesC Granit™ XP K65

Honeywell

Webinar #GeniusOnEdge

Zebra Technologies, Poly & Samsung Product

3 Maret 2021

Perkembangan teknologi baik perangkat IT (Information Technology) dan juga IOT (Internet of Things) yang sangat cepat, membuat perusahaan di semua bidang harus menerapkan transformasi digital dalam mendukung bisnis perusahaan, agar tidak tertinggal dalam kompetisi di dunia usaha. Tanggal 3 Maret 2021 lalu ACS Group bekerja sama dengan Zebra Technologies dan Ingram Micro Indonesia mengadakan acara webinar dengan thema #GeniusOnEdge. Pada acara ini Zebra Technologies membawakan beberapa update produk mobile computer dan label printer serta produk RFID sedangkan Ingram Micro menyampaikan produk solusi Samsung dan Poly Camera.

PRODUK ZEBRA TECHNOLOGIES

Teknologi AIDC (Automatic Identification and Data Capture) sudah menjadi kebutuhan di beberapa industri berkembang di era sekarang dan terus berkembang disesuaikan dengan kebutuhan di lapangan.

Zebra Technologies pada event ini menyampaikan solusi AIDC nya yang sudah terbukti keandalannya di berbagai sektor industri.

Dengan enterprise mobile computer dari Zebra, para pekerja dapat mengakses informasi, aplikasi serta orang, yang mereka butuhkan untuk menyelesaikan pekerjaan mereka. Hasilnya mampu meningkatkan produktivitas serta pelayanan yang semakin baik kepada para pelanggan. Zebra juga menyediakan portofolio RFID yang tersebar di berbagai industri dan telah teruji, konsisten dan andal di lapangan dengan akurasi dan interoperabilitas yang tak tertandingi. Printer label dari Zebra memiliki kualitas cetak, kecepatan cetak, dan pengelolaan yang tercepat di kelasnya demikian pula dengan printer RFID yang mampu menghasilkan pengkodean pada label, tag, dan kartu RAIN RFID secara akurat di mana pun dan kapan pun Anda membutuhkannya.

Para pemain industri ritel, produsen, perusahaan transportasi dan logistik terbesar di dunia kemudian organisasi penjualan dan layanan lapangan, serta penyedia layanan kesehatan mengandalkan teknologi Zebra setiap hari untuk meningkatkan bisnis mereka.

PRODUK SOLUSI POLY

Platform video conference menjadi alat komunikasi utama yang digunakan untuk menjaga produktivitas selama pandemi ini, baik sektor bisnis, pemerintah, hingga pendidikan memanfaatkan video conference. Karena kebutuhan inilah banyak perusahaan yang menawarkan platform video conference dengan segala keunggulan yang bisa dinikmati. Teknologi yang dimanfaatkan harus membantu seluruh karyawan bekerja lebih pandai, pastikan Anda memilih video conference terbaik untuk mendukung WFH (Work From Home) atau WFA (Work From Anywhere). Karena video conference merupakan solusi komunikasi yang relatif baru bagi perusahaan di Indonesia, perlu adanya riset terkait kualitas platform yang akan Anda gunakan. Pilihan berbagai platform video conference saat ini sangat bervariasi, jangan sampai perusahaan Anda salah memilih.

Poly (Polycom+Plantronics) merupakan perusahaan yang bergerak dalam Audio Video Conference ternama di dunia. Poly hingga saat ini masih merupakan perusahaan yang paling terdepan dengan berbagai macam penghargaan yang telah di dapat, dan tingkat kepuasan yang tinggi dari para pelanggan.

Melalui webinar ini, Poly membagikan pengalaman serta saran yang terbaik, untuk perusahaan anda dalam menerapkan solusi video conference terbaik untuk mendukung WFH atau WFA. Saat ini adalah kondisi yang tidak memungkinkan bagi karyawan untuk melakukan interaksi fisik dengan rekan kerja dan pelanggan. Oleh sebab itu, para pemimpin perusahaan harus pintar memilih video conference terbaik agar perusahaan dapat tetap beroperasi dan karyawan tetap bekerja

secara produktif. Solusi video conference terbaik bagi perusahaan akan terus berkembang sebagai solusi yang berguna untuk berkomunikasi bahkan hingga pandemi COVID-19 berakhir, karena perusahaan akan terus merasakan efisiensi dari pemanfaatan teknologi Poly ini.

PRODUK SOLUSI SAMSUNG

Digital signage merupakan media display elektronik yang oleh banyak enterprise digunakan untuk menyampaikan informasi mereka secara dinamis dan menarik. Dengan memanfaatkan teknologi LCD, LED dan Plasma, digital signage dapat menyampaikan informasi secara satu arah dan dua arah menggunakan dukungan interaktif. Pada umumnya digital signage ini digunakan untuk menampilkan informasi produk, promosi, branding, navigasi, iklan, jadwal dan masih banyak lagi.

Samsung pada event kali ini menyampaikan Samsung Smart Signage nya yang memberikan kemudahan untuk kebutuhan promosi Anda sekaligus menayangkan tontonan program TV favorit untuk para konsumen. Smart signage TV ini mudah dipasang tanpa memerlukan alat-alat tambahan karena memiliki player internal dan bisa digunakan sekaligus untuk menonton TV. Fitur inilah yang membedakannya dari media promosi tradisional. Desain tipis, fashionable dan modern sesuai dengan gaya kontemporer masa kini serta didukung doleh format video, gambar dan teks dengan layout split screen dan mampu beroperasi hingga 16 jam / hari, 7 hari / minggu.

Samsung Smart Signage dapat digunakan kapan saja / di mana saja dan memiliki akses berbasis cloud ke portal konten. Dengan satu platform, tim yang menjalankan sistem hanya memiliki satu layanan dan saluran dukungan pelanggan. Dengan satu sistem, staf IT dan manajer konten dapat memperoleh manfaat dari satu interface, yang dapat dengan mudah mengontrol seluruh jaringan layar saat mengaktifkan konten yang disesuaikan untuk khalayak tertentu berdasarkan lokasi layar.

Sistem yang paling canggih menawarkan akses backend melalui perangkat yang terhubung – fitur penting untuk menyebarkan pesan darurat atau pemberitahuan. Penggunaan interface berbasis cloud yang aman dan kolaboratif juga menyederhanakan pengelolaan tingkat izin dan akses pengguna untuk beberapa tempat di area office, pabrik atau kampus/sekolah. Sistem dengan fleksibilitas tinggi memungkinkan administrator dari berbagai departemen untuk mengakurasi informasi yang relevan dengan target audiens mereka, seperti pengaturan konten khusus untuk mereka yang ada di gedung tertentu atau beberapa tempat tertentu.

KUIS AITEE 54

Menangkan 10 voucher belanja untuk 5 orang pemenang !!!

Pertanyaan :

1) Apa tu Maxpro® Cloud?
2) Sebutkan serangan pada dunia maya yang paling umum digunakan dalam pelanggaran data?
3) Apa itu USB Rubber Ducky?

Caranya :

1) Jawaban dapat anda cari di dalam Buletin Vol 54 ini.
2) Silahkan Anda isi Form sekaligus menjawab pertanyaan anda melalui link **bit.ly/KUISAITEE54**
3) Peserta wajib mengisi dengan lengkap dan benar, kesalahan pengisian form pribadi menjadi tanggung jawab pengisi form jika Anda memenangkan KUIS ini.
4) Pemenang KUIS akan ditetapkan apabila memenuhi syarat dan ketentuan dari AITEE
5) KUIS ditutup sampai 30 Mei 2021.
6) Pengumuman KUIS akan diumumkan di Buletin Edisi 55 Juni 2021

Aruba Networks

AP560 dan AP570 Series

Access Points Outdoor

aruba
a Hewlett Packard Enterprise company

Aruba Access Point (AP) seri 560 dan 570 adalah seri Access Point dengan teknologi WiFi terbaru 802.11ax atau bisa disebut WiFi-6 dengan peruntukan khusus area outdoor yang berarti AP ini sudah memiliki rating tahan air dan debu untuk digunakan di area luar ruang tanpa takut rusak karena debu maupun hujan. Selain debu dan hujan, AP tipe ini juga memiliki daya tahan yang sangat baik terhadap suhu ekstrim baik ekstrim dingin seperti cold storage ataupun ekstrim panas seperti sengatan matahari terik.

Dengan teknologi 802.11ax-nya maka kedua tipe AP ini memiliki banyak kelebihan dibanding AP tipe lain dimana akan memiliki banyak kelebihan seperti OFDMA, MU-MIMO, Advanced Cellular Coexistence, Intelligent Power Monitoring. Seperti yang dijabarkan di whitepaper mengenai 802.11ax dengan judul "802.11ax white paper", WiFi-6 AP juga memiliki kekhususan lain seperti teknologi Target Wake Time (TWT) untuk perangkat IOT, peningkatan keamanan nirkabel baru WPA3, operasi yang lebih baik di area high-density, transmit beamforming, dan lain-lain.

Beberapa area yang sangat cocok untuk menggunakan AP tipe ini adalah:

- Warehouse dengan suhu ekstrim,
- Area produksi yang banyak getaran, panas, atau bahkan dingin,
- Cold-storage sampai dengan suhu 40 derajat celcius di bawah 0,
- Area luar ruang sangat panas seperti pinggir pantai atau area pabrik dengan suhu 70 derajat celcius di atas 0,
- Area ekstrim dengan standar khusus seperti Class 1 Division 2 atau ATEX Zone 2,
- Area parkir luar ruang dengan banyak debu dan panas.
- Area pelabuhan kontainer yang sangat panas dan kadar korosi garam yang tinggi.
- Dan berbagai area ekstrim lainnya.

AP-575 Outdoor

AP-565 Outdoor

Perbedaan utama dari kedua tipe di atas adalah kapasitas nya dengan seri 570 yang memiliki kapasitas lebih tinggi sehingga sangat cocok untuk implementasi di area yang memiliki banyak pengguna sedangkan seri 560 cocok untuk implementasi yang lebih ekonomis.

ACSGroup siap membantu bapak/ibu untuk memberikan konsultasi lebih lanjut untuk kebutuhan sinyal WiFi di area outdoor perusahaan bapak/ibu.

Aruba Networks

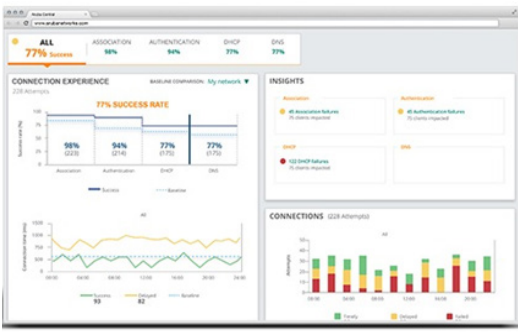
Aruba Central

Cloud Network Management and Operations

aruba
a Hewlett Packard Enterprise company

Cloud adalah solusi IT yang sangat strategis dan cocok untuk perusahaan-perusahaan kecil maupun besar. Melihat kondisi negara kita yang sangat luas maka solusi cloud sangatlah baik untuk diterapkan terutama dari sisi simplifitas dan fungsi, dan efisiensi-nya.

Salah satu solusi cloud yang dimiliki oleh ACS Group adalah Aruba Cloud Central dari Aruba Networks HPE dimana solusi Cloud dari Aruba ini bertujuan untuk melakukan tiga fungsi utama pengaturan infrastruktur di perusahaan kita, keamanan siber, dan teknologi kecerdasan buatan (AI).0



Kemudahan implementasi perangkat juga menjadi salah satu fitur Aruba Central dimana implementasi menggunakan prinsip zero touch provisioning (ZTP) dimana dengan teknologi ini ketika kita ingin melakukan implementasi, cukup mengirimkan perangkat dalam keadaan factory default atau tidak perlu ada config apapun juga dan ketika dinyalakan, perangkat akan secara otomatis melakukan konfigurasi sendiri atas perintah dan pantauan dari Aruba Central.

Seringkali ketika setelah melakukan implementasi infrastruktur jaringan di perusahaan, kita jarang melakukan pemantauan secara berkala yang biasanya terjadi karena tampilan dari aplikasi monitoring yang terlalu rumit dan kurang informatif. Aruba Central dibuat atas dasar simplifitas ini sehingga dapat semudah mungkin melihat hanya data-data penting yang perlu kita ketahui tapi di sisi lain sangat informatif serta dapat melihat banyak jenis perangkat sehingga kita tidak memerlukan beragam aplikasi yang perlu dipantau. Hanya 1 aplikasi, 1 tampilan, untuk melihat semua perangkat infrastruktur kita secara simple dan informatif.

Setelah kemudahan pemantauan, Aruba Central juga memiliki keamanan siber yang sangat baik dimana kita dapat melakukan implementasi Intrusion Prevention System (IPS) dan Intrusion Detection System (IDS) yang dapat di-implementasikan secara menyeluruh di jaringan kita melalui Aruba Central.

Melalui Aruba Central, kita dapat memanfaatkan teknologi masa depan jaringan menggunakan AIOps (AI for IT Operations) dimana ketika muncul sebuah masalah di jaringan kita, Aruba Central dengan AIOps nya dapat memberikan sebuah solusi yang tepat untuk kita untuk dapat secepat mungkin dan secara efisien mengatasi masalah tersebut.

Yang tidak kalah pentingnya dalam mengelola jaringan adalah dengan adanya fitur membuat laporan atau reporting atas jaringan kita dimana dengan Aruba Central kita dapat membuat laporan secara komprehensif tentang konektivitas semua perangkat, kesehatan dari jaringan kita, dan aktivitas semua user di jaringan. Laporan dapat diatur untuk dibuat secara otomatis secara berkala ataupun secara manual kapanpun ketika dibutuhkan.

Fortinet

FortiSASE

Edge Security for Distributed Networks

Secure Access Service Edge (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.

Dengan solusi SASE maka memungkinkan organisasi untuk menerapkan akses yang aman (secure access) dan tidak menjadi masalah dengan lokasi dimana para pengguna, workload, perangkat, ataupun aplikasi berada. Hal ini menjadi suatu kelebihan yang sangat penting khususnya bagi para pengguna yang bekerja secara remote, aplikasi-aplikasi SaaS (software as service) yang bersifat rapid adoption, serta pergerakan data sangat cepat di berbagai data center, kantor-kantor cabang, serta pada lingkungan hybrid-cloud maupun multi-cloud.

FortiSASE adalah solusi keamanan cloud yang highly scalable dari Fortinet sebagai layanan yang memungkinkan untuk akses yang aman dan fleksibel, kapan saja dan di mana saja untuk para pengguna/ pekerja berada.

Memanfaatkan kekuatan dari FortiOS dan Fortinet Security Fabric, FortiSASE menyediakan orkestrasi yang tanpa hambatan antara NGFW di cloud, Web Security, intrusion prevention (IPS), DNS, dan Sandboxing. Dan secara bersama semua aspek tersebut memungkinkan Fortinet untuk memberikan layanan SASE dengan fleksibilitas dan konsumsi model yang dibutuhkan oleh modern enterprise.

FortiSASE memungkinkan organisasi menerapkan keamanan yang tepat di setiap tahap dalam transformasi digital mereka. Dengan inovasi selama lebih dari 20 tahun, Fortinet telah memberikan solusi keamanan dan jaringan yang benar-benar dinamis yang dihadirkan sebagai layanan.

Seluruh Staff dan Management
ACS GROUP mengucapkan

SELAMAT MENYAMBUT

BULAN SUCI

RAMADHAN 1442 HIJRIAH

13 April 2021

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

Beda Keyakinan

Won-Shik, seorang pemuda yang setelah sekian lama hidup sendiri menemukan Eun-Hye kekasih pujaan hatinya, tetapi pernikahan mereka tidak berlangsung lama karena perbedaan keyakinan.

Jung-Hwa yang merupakan sahabat Won-Shik mempertanyakan perihal penyebab perpisahan mereka.

Jung-Hwa: Kenapa broo sampai kalian bercerai seperti ini, apa masalahnya?

Won-Shik : Kita berbeda keyakinan bro, aku dah ngga tahan lagi.

Jung-Hwa: Bukannya kalian seagama ya?

Won-Shik : Memang...

Jung-Hwa: Lantas kenapa sampai bercerai karena perbedaan keyakinan, apa yang dipermasalahkan?

Won-Shik : Selama ini aku selalu yakin bahwa aku ini ganteng, tapi Lina tidak bisa menerima keyakinanku itu dan selalu mempermasalahkannya.

Jung-Hwa: ?@#$%&*$W%^W&E*

KOLOM KETAWA

#ACSNATIONS2021

KICK OFF ACS Group

January 11th, 2021

ACS Group mengadakan acara Kick Off pada tanggal 11 Januari 2021 secara online by ZOOM, kegiatan ini diikuti oleh seluruh staf termasuk cabang ACS baik Cikarang, Semarang, Surabaya dan Denpasar.

Acara Kick off ACS Group ini dibuka oleh Indra Tjahjadi selaku Managing Director, dilanjutkan dengan "Success Spirit" yang disampaikan oleh Arijanto Hartanto - Sales & Marketing Director.

Pada acara ini beberapa staf ACS Group mendapatkan apresiasi sebagai **THE BEST PERFORMER 2020** dan terpilih 4 orang staff antara lain:

1. **Deny Irawan**, Enterprise IT Solutions – Engineer, Jakarta
2. **R.A. Maycieanne**, Logistik Supervisor, Jakarta
3. **Gigih Setiawan**, Enterprise IT Solutions – Junior Engineer, Jakarta
4. **M. Wawan Wahyudin**, Account Executive, Jakarta

Disamping The Best Performance yang diberikan, ACS Group juga memberikan Penghargaan Kesetiaan sebagai karyawan ACS Group berupa sertifikat dan pin emas kepada 3 staff dengan masa jabatan 20 tahun yaitu

- **Ir. Heru Wahyudi** - Sales General Manager, Jakarta
- **Andri S Kouanak, S.Kom** - Media Lead, Jakarta
- **Devi Andriani, SE** - Finance Supervisor, Jakarta

Sedangkan untuk masa jabatan 25 tahun ada 4 staff yaitu

- **Arijanto Hartanto**, Sales & Marketing Director, Jakarta
- **Sofie Su**,Logistic & Procurement Director, Jakarta
- **Sudarsono,SE, M.Ak**, Senior Acct and Tax, Jakarta
- **Saryono**, Logistic Staff, Jakarta

Fortinet Mengakuisisi Panopta

Network Monitoring and Remediation Innovator

Panopta https://www.panopta.com/ adalah platform pemantauan infrastruktur hibrid dan diagnostik yang berbasis SaaS (*Software as Service*) untuk memastikan bahwa jaringan para pelanggan Fortinet yang berkinerja tinggi dan aman melalui operasi NetSec (*Network Security*) yang otomatis.

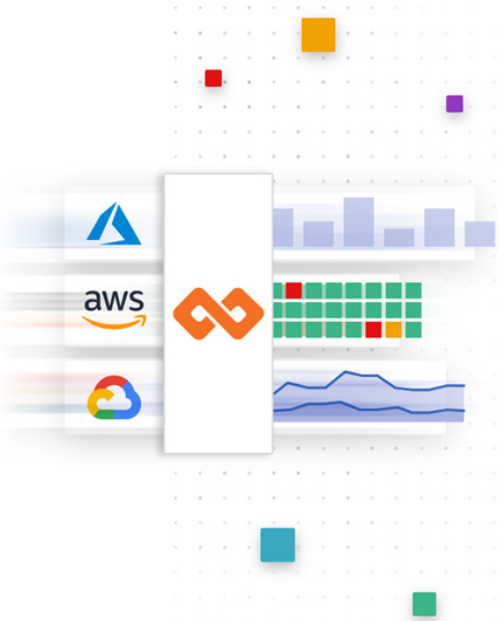
Fortinet® (NASDAQ: FTNT), vendor global dan pemimpin dalam hal solusi keamanan siber yang luas, terintegrasi, dan otomatis, per 8 Desember 2020 mengumumkan telah mengakuisisi Panopta, inovator platform SaaS yang menyediakan visibilitas *full stack* dan manajemen otomasi akan kesehatan jaringan perusahaan, termasuk *server*, perangkat jaringan, *containers*, aplikasi, *database*, *virtual appliances*, dan infrastruktur *cloud*.

Memastikan infrastruktur digital dengan waktu operasional yang penuh atau 100% adalah hal yang sangat penting bagi perusahan saat ini. Solusi berbasis *cloud* Panopta memberikan gambaran yang lengkap tentang setiap layanan, perangkat jaringan, dan aplikasi dalam penerapannya, baik itu dalam *container*, *cloud*, *on-premise*, atau *hybrid*. Fortinet's Security Fabric, dikombinasikan dengan platform Panopta yang berskalabiltas, pemantauan jaringan dan perangkat diagnostik, memungkinkan Fortinet untuk menawarkan solusi jaringan dan manajemen operasi keamanan yang paling komprehensif untuk perusahaan atau penyedia layanan.

Dengan akuisisi Panopta, Fortinet akan menghadirkan platform jaringan berbasis keamanan yang terlengkap di industri dengan menambahkan kemampuan baru dalam hal pemantauan jaringan, deteksi, dan respons terhadap insiden.

Fitur-fiturnya meliputi:

- Pemantauan yang terpadu dan manajemen insiden secara otomatis yang mengurangi waktu respons dan resolusi untuk tim NOC (*Network Operation Center*) maupun SOC (*Security Operation Center*) serta komitmen terhadap SLA (*Service Level Agreement*).
- Lebih dari 50 titik global (*global points of presence - PoPS*) dengan *low-cost probes* untuk mensimulasikan kinerja aplikasi dan latensi yang berpengaruh terhadap *end user experience* atau yang dikenal dengan istilah *synthetic transaction monitoring*.
- *Cloud native monitoring* untuk *workload* pada Kubernetes dan PaaS di AWS dan Azure.
- *Alerting workflows* yang sepenuhnya dapat di konfigurasi dengan integrasi siap pakai untuk perusahaan pihak ketiga dan penerapannya dengan alat komunikasi yang modern.
- Layanan *first-class partner-friendly* dari Fortinet yang berkelanjutan dan komitmen kepada mitra-mitranya.



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.

- Aruba Certified Edge Professional (ACEP)
- Aruba Certified Mobility Professional (ACMP)
- Aruba Certified Design Professional (ACDP)
- Aruba Certified ClearPass Professional (ACCP)
- Aruba Certified Switching Professional (ACSP)
- Aruba Certified Mobility Associate (ACMA)
- Aruba Certified Switching Associate (ACSA)
- Cambium Networks ePMP Certified
- Extreme Sales Specialist in Extreme Wireless
- Extreme Design Specialist in Wireless Core
- Honeywell Gold Performance Partner
- ICSI | CNSS Certified Network Security Specialist
- Microsoft Certified: Azure Fundamentals
- Microsoft Certified Professional (MCP)
- NCP Nutanix Certified Professional
- NSE 1 Network Security Associate
- NSE 2 Network Security Associate
- NSE 3 Network Security Associate
- Nutanix Certified Systems Engineer: Level 1
- NCSR Nutanix Certified Sales Representative
- Project Management Professional Certified
- Samsung Knox Certified
- Zebra Mobile Computing Sales Professional Certification
- Zebra Advanced Data Capture Technical Professional Certification
- Zebra RFID Technical Professional Certification, etc.

Tips Dalam Menghentikan Serangan Phishing

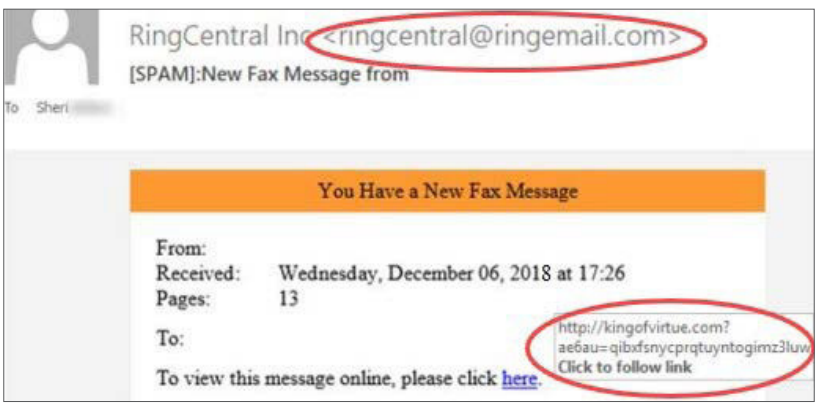
Phishing, adalah salah satu bentuk serangan di dunia maya yang berdasarkan pada rekayasa sosial atau *social engineering*, adalah risiko keamanan yang teratas bagi organisasi saat ini. Teknik phishing berkisar dari *blast email* secara massal dan pesan teks hingga serangan yang bertarget (*targeted attacks*) terhadap individu dengan informasi yang sangat berharga.

Serangan phishing dapat melalui email, pesan teks, postingan media sosial, komunikasi suara, dan media lainnya. Seringkali, kontennya adalah berisi tautan ke situs web palsu yang dirancang untuk mengelabui agar mengungkapkan informasi sensitif seperti nama pengguna, kata sandi, nomor akun, data perbankan, dan detail informasi kartu kredit.

Situs web palsu memainkan peran penting dalam eksploitasi phishing, meniru situs web yang resmi dari perusahaan-perusahaan yang tepercaya untuk menanamkan kepercayaan pada calon korban.

Hampir semua organisasi yang menggunakan email, SMS, pesan instan, media sosial, atau pun komunikasi suara adalah calon korban phishing. Di masa lalu, penyerang mengirimkan ribuan atau jutaan email phishing dengan harapan menjerat beberapa korban. Dalam beberapa tahun terakhir ini telah terlihat pergeseran ke teknik yang lebih bertarget seperti *spear phishing* dan *voice phishing* (*vishing*).

Saat ini, serangan phishing semakin menargetkan eksekutif, baik karena informasi kontak mereka sering kali dapat diakses publik, dan mereka cenderung memiliki data yang berharga. Penjahat dunia maya kemudian menggunakan kredensial email curian dari para eksekutif untuk mengirim pesan yang tampaknya otentik yang meminta staf atau karyawannya untuk mentransfer sejumlah uang ke rekening di luar negeri atau melakukan jenis penipuan lainnya adalah salah contoh modus operandi dari phishing.



Gambar 1. Email phishing dengan tautan URL palsu. Perhatikan perbedaan antara tautan URL sumber yang diklaim ringemail.com (atas) dan URL sumber sebenarnya kingofvirtue.com (bawah).

Gambar 2. Situs web palsu. Perhatikan keberadaan ikon gembok dan https://.

Agar efektif, program anti-phishing perlu menyertakan tiga komponen utama:

1. *Cybersecurity awareness and training*, atau pelatihan dan kesadaran akan keamanan siber
2. *Email security* atau keamanan email
3. *Web address filtering*, atau pemfilteran alamat situs web.

Untuk mencegah serangan phishing yang berhasil, beberapa tindakan berikut sangat disarankan:

- Melakukan program untuk kesadaran akan keamanan (*security awareness*) dan pelatihan keamanan siber kepada para karyawan dan terus mengukur efektivitasnya
- Pengamanan dengan perangkat *Secure Web Gateway* (SWG) yang dapat mengetahui adanya serangan web dengan teknik pemfilteran URL, adanya visibilitas, dan inspeksi terhadap lalulintas data baik *Secure Sockets Layer* (SSL) dan *Transport Layer Security* (TLS)
- Memastikan bahwa sistem keamanan email divalidasi oleh penguji independen pihak ketiga
- Menginformasikan pada para karyawan dengan segera setelah mengetahui adanya eksploitasi phishing tertentu yang terdeteksi

Cybersecurity awareness and training

Berikut adalah beberapa area utama yang perlu untuk dievaluasi oleh para *security leader* dalam mengevaluasi mengenai program *cybersecurity awareness* mereka, antara lain:

- Menetapkan metrik untuk perubahan perilaku seperti jumlah tiket *help-desk* terkait masalah keamanan dan pengguna yang mengalami skema phishing
- Survei ataupun kuis terhadap para pekerja untuk mengukur motivasi, kemampuan, dan pemicu guna mengetahui apa yang sebenarnya diketahui para karyawan dan seberapa besar kecenderungan mereka untuk bertindak berdasarkan pengetahuan tersebut.
- Ulangi survei secara berkala untuk mengukur tren

Email security

Perangkat keamanan email harus menyediakan tiga kemampuan dasar untuk menghentikan serangan phishing, yakni:

- Kemampuan untuk mengatasi risiko yang ditimbulkan oleh lanskap ancaman (*threat landscape*) yang terus berubah dan semakin cepat
- Kemampuan untuk membantu organisasi beralih dari postur keamanan yang reaktif ke postur keamanan yang lebih proaktif
- Memberikan informasi mengenai *Return of Investment* (ROI) yang dapat diukur

Web Address Filtering (WAF)

Dengan *Web Address Filtering* (WAF) atau pemfilteran alamat situs web, maka akan membatasi akses ke alamat web berdasarkan basis data informasi yang diketahui tentang situs web tertentu. Solusi WAF akan mengizinkan akses ke situs yang diketahui aman (*white-list*) atau melarang akses ke situs yang berbahaya karena mengandung serangan phishing dan malware (*black-list*). Dan karena demikian dinamisnya situs-situs yang web berbahaya, maka solusi dari perangkat WAF *top-tier* tentunya menggunakan metode pembelajaran mesin (*machine learning*) dan layanan langganan intelijen ancaman (*threat intelligence subscription services*) agar tetap terkini.

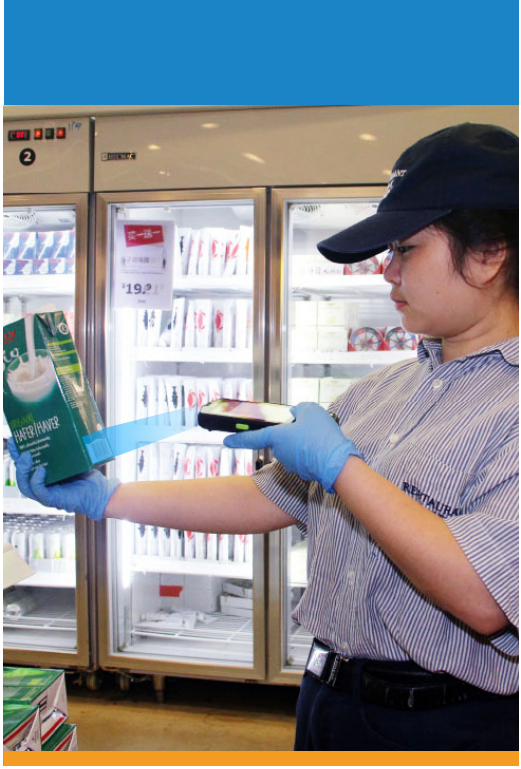
Sumber: https://www.fortinet.com/content/dam/fortinet/assets/education/eg-guide-on-phishing.pdf

*/ Penulis : Irvan Kurniawan(irvan@acsgroup.co.id)

Seuic

AUTOID Q9

Leading A New Standard of Durable Capture Tools



Features

- 8-core 2.0GHz
- Android 10.0(GMS)
- RAM+ROM: 3+16GB
- 4.0'' IPS Screen
- 4G/Dual-band WIFI
- IP67/1.8m Drop

Industry Use

- Distribution Center
- Warehouse Management
- Store Management
- Picking

Jiangsu Seuic Technology Co., Ltd. didirikan sejak tahun 2002 dan selalu fokus untuk melakukan R&D secara independent dan inovasi berkesinambungan. Saat ini, SEUIC memiliki lini produk termasuk terminal genggam kelas industri (PDT/Barcode Device), identifikasi visual (Fix Scanner) dan produk UHF RFID (Mobile RFID).

Setelah sukses dengan penjualan SEUIC AutoID9 di pasar Indonesia, kini SEUIC meluncurkan salah satu produk terbarunya dilengkapi dengan Android 10, IP67, kapasitas baterai 5,200mAh dengan ketebalan hanya 16.2mm, memiliki kapasitas memori 4GB/64GB, kamera depan 5MP dan kamera belakang 13MP dan versi BT 5.0 yang dinamakan dengan "AUTOIDQ9".

Seluruh perangkat barcode SEUIC termasuk AUTOIDQ9 dapat dikombinasikan dengan Mobile Device Management dari SEUIC sehingga pengguna dapat mengontrol seluruh perangkat secara real time dan melindungi keseluruhan data yang ada didalamnya jika menggunakan MDM SEUIC ini.

Untuk info lebih lanjut silahkan hubungi kami
di website: https://en.seuic.com/ atau https://www.acsgroup.co.id/ .

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

CORE BUSSINESS SOLUTIONS : 4 PILLARS

Automatic Identification & Data Capture (AIDC) — 1
- Label (Barcode) Printer & Supplies
- Card Printer & Supplies
- RFID Printer & Supplies (RFID Tag)
- Barcode Scanners
- RFID Reader
- Enterprise Mobile Computers
- Enterprise Tablet

IT Infrastructure — 2
- Data Center Solutions
- Hyper Converge Infrastructures
- Enterprise IT Networks Wired & Wireless
- Cyber Security Solutions

Enterprise Security System — 3
- Access Control - Single ID Management
- Alarm System
- IP CCTV

Enterprise Business Solution — 4
- AMTS - Asset Management and Tracking System
- LTS - Laundry Tracking System
- GAS-V - Gate Access System - Vehicle
- ABS - Agriculture Plantation and Mill Management

BUSINESS PARTNERS

aruba a Hewlett Packard Enterprise company · BarTender by Seagull Scientific · brother at your side · Cambium Networks · DriveLock · Extreme Connect Beyond the Network
FORTINET · Hewlett Packard Enterprise · HID · HIKVISION · Honeywell · ivanti
JANZ · NUTANIX Your Enterprise Cloud · POINT Mobile · SAMSUNG · Seuic · ZEBRA

Jakarta (HO)
Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221-4208221, 4205187
Fax : +6221-4207903, 4207904, 4205853

Cikarang
Cikarang Square Blok E No 62, Jl. Raya Cikarang,
Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221-29612366, 29612367
Fax : +6221-29612368

Semarang
Grand Ngaliyan Square Blok B No.18,
Ngaliyan 50181, Semarang
Telp : +6224-76638092, 76638093
Fax : +6224-76638096

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231-8556277; 8556278
Fax : +6231-8556279

Denpasar
Ruko Grand Sudirman Agung Blok B No.29,
Jl. PB Sudirman, Dauh Puri Kelod,
Denpasar Barat, Denpasar - Bali 80114
Telp : +62361-4457859
Fax : +62361-4746526