GEBYAR
BULETIN EDISI 52/SEPTEMBER 2020

AUTO-ID

UNTUK KALANGAN SENDIRI

MENGATASI ANCAMAN SIBER DI TENGAH PANDEMI COVID-19

#AssetOnTrack

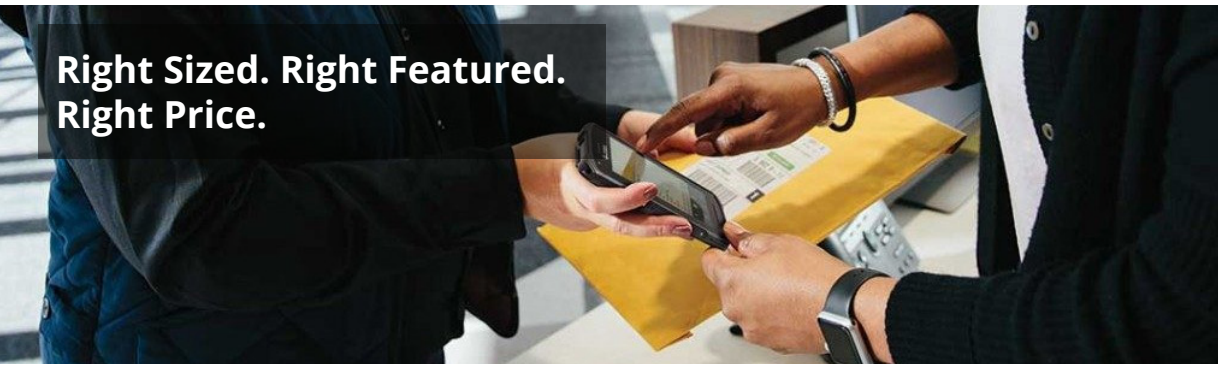
AMTS ENTERPRISE EDITION V.6

Manage your General Affairs' assets more effectively, faster, with better precision

TIPS & INFO :
10 Steps to Cyber Security

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

ZEBRA CAPTURE YOUR EDGE



TC21/TC26 Touch Computer

THE ULTIMATE COST-EFFECTIVE TOUCH COMPUTER BUILT FOR INSIDE THE FOUR WALLS

Step up to the business-class durable TC21/TC26 Touch Computers — without stepping up in price. Choose the connectivity your workers need – the WiFi-only TC21 or the WiFi/cellular TC26. Then choose the features that will allow your workers to improve task accuracy and on-the-job efficiency. And you can protect it all with the affordable optional Zebra OneCare™ SV support plan, which covers normal wear and tear and much more.

Markets and Applications

Inside the four walls	Outside the four walls
• Retail	• Field service
• Hospitality	• Direct Store Delivery (DSD)
• Light warehouse	• Postal
	• Courier
	• Route accounting

PEMIMPIN REDAKSI
Andre S.Kouanak

SEKRETARIS REDAKSI
Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
Luh Wayan Sumariani (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Chandra Tjahjadi

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Ketut Gede Turangga
Kenneth Lohoo
Irvan Kurniawan

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

CONTENT

EDITORIAL

Para Pembaca dan Pelanggan yang terhormat,

Salam Sejahtera. Puji syukur pada Tuhan yang Maha Esa, atas segala berkat, karunia, dan perlindungan-Nya di masa pandemi COVID-19 ini yang tentunya menjadi masa-masa sulit bagi kita semua. Semoga kita semua senantiasa berada dalam lindungan-Nya dan pandemi ini segera berakhir.

Sebagaimana kita ketahui bersama, pandemi COVID-19 telah mengubah banyak hal dalam tatanan kehidupan kita. Pada lima bulan terakhir banyak perusahaan yang memberlakukan karyawannya untuk bekerja dari rumah (WFH) dalam rangka meminimalisir penyebaran virus ini. Transisi dari WFO (bekerja dari kantor) ke WFH yang dialami oleh para pekerja yang secara tradisional bekerja dari kantor fisik dapat menjadi tugas yang berat bagi suatu perusahaan. Hal ini juga bersamaan dengan transisi akses data perusahaan dan sumber daya jaringan, ke tempat kerja alternatif. Selain mempertimbangan infrastruktur jaringan yang akan diakses oleh seluruh karyawan, perusahaan juga harus menyadari bahwa penjahat siber siap untuk mengeksploitasi kelemahan dan celah keamanan yang sering muncul selama proses tersebut. Baik pengguna maupun sistem yang tidak siap dan kurang aman, dapat dengan cepat menjadi celah bagi penjahat siber dan aktivitas berbahaya lainnya. Penurunan drastis pada pemasukan yang diterima oleh perusahaan tentu akan berdampak buruk pada keuangan perusahaan dan tidak menutup kemungkinan terjadinya *Financial Distress*, terlebih apabila badan usaha mereka terpaksa ditutup dalam rentang waktu yang tidak pasti. Hal ini akan berdampak pada konsentrasi perusahaan untuk melakukan perawatan terlebih pembaharuan pada infrastruktur jaringan dan sistem informasi perusahaan khususnya. Dibutuhkan suatu solusi yang ideal untuk menjawab tantangan tersebut, baik dari segi biaya (TCO) dan segi keamanannya.

Topik utama buletin pada terbitan ketiga tahun ini akan membahas solusi dari permasalahan tersebut yang berjudul "Mengatasi Ancaman Siber Di Tengah Pandemi COVID-19".Pada edisi kali ini kami juga menghadirkan topik AMTS(Asset Management Tracking System), info *product highlight*, tips & info serta berbagai kegiatan ACS Group seperti *solution* seminar, *training*, dan info-info lainnya. Akhir kata, saya mewakili tim buletin ACS mengucapkan selamat membaca dan semoga bermanfaat.

Salam Redaksi,

Ketut Gede Turangga
Enterprise Network Solutions Engineer
ACS GROUP
PT. Autojaya Idetech
PT. Solusi Periferal

Mengatasi Ancaman Siber di Tengah Pandemi COVID-19

by **Ketut Gede Turangga**,
Enterprise Network Solutions Engineer ACS Group cabang Denpasar

Pandemi COVID-19 dapat dikatakan sebagai sebuah disrupsi pada peradaban manusia yang tidak pernah diprediksi akan terjadi pada abad ke-21 oleh para analis dan pakar kesehatan di seluruh dunia bahkan oleh para pegiat *big data* serta *artificial intelligence* (AI). Hingga kini belum ada satu negara pun yang mengakui bahwa mereka memiliki tindakan yang tepat pada penanganan COVID-19. Setiap negara saling belajar dari praktik terbaik negara lainnya untuk mendapatkan formula tindakan yang tepat untuk menangani pandemi tersebut. Protokol kesehatan yang diberlakukan saat ini masih terus diperbarui menyesuaikan dengan situasi dan kondisi pandemi yang terus berubah setiap saat. Kini teknologi informasi dan komunikasi memiliki peran dalam upaya penanganan sekaligus salah satu jawaban dari tantangan untuk bertahan hidup semasa pandemi COVID-19. Demi melindungi warganya dan meminimalisir penyebaran virus ini, pemerintah di berbagai negara pun mengambil langkah-langkah penanganan. Di antara opsi yang banyak dibahas adalah kebijakan isolasi atau lockdown dan pembatasan sosial. Dalam upaya mendukung program pemerintah tersebut, para pelaku bisnis maupun perusahaan-perusahaan melakukan penyesuaian sistem kerja karyawannya untuk menjaga stabilitas maupun produktivitas perusahaan. Salah satu penyesuain yang dilakukan oleh banyak perusahaan adalah menerapkan kebijakan kepada karyawannya untuk dapat bekerja dari rumah (WFH) atau menjadi pekerja jarak jauh.

"TAHUKAH ANDA? Sejak April 2020, Sekitar 1.25 Juta Orang di Jakarta, Bekerja Dari Rumah (WFH)"[1]

Berdasarkan konferensi pers Presiden Joko Widodo pada tanggal 15 Maret 2020, masyarakat dihimbau agar bekerja dari rumah (WFH) sebagai langkah agar penyebaran virus COVID-19 dapat diminimalisir. Dinas Tenaga Kerja, Transmigrasi dan Energi DKI Jakarta pada bulan April 2020 mencatat setidaknya jumlah pekerja yang WFH ada sebanyak 1.25 juta orang. Para pekerja ini berasal dari 3.788 perusahaan. Meski jumlah pekerja yang WFH mulai menurun per 14 April 2020 yaitu sebanyak 1.01 juta pekerja dari 3.653 perusahaan, angka tersebut bukanlah jumlah yang kecil. Perusahaan yang menerapkan WFH secara penuh terdata sebanyak 1.273 perusahaan dengan total jumlah pekerja sebanyak 177.509 pekerja.

Gambar 1. Ilustrasi Kondisi WFH
(Photo by Ketut Subiyanto from Pexels)

Perlahan bekerja dari rumah (WFH) telah menjadi normal baru untuk sebagian besar tenaga kerja di Indonesia bahkan di dunia. Hal ini diperkirakan akan terus berlanjut bahkan ketika beberapa pekerja kembali bekerja dari kantor setelah pandemi COVID-19. Sebagian besar perusahaan saat ini telah menemukan cara untuk memungkinkan karyawan mereka dapat terhubung kembali ke pusat informasi, aplikasi, dan aset yang mereka butuhkan untuk melakukan pekerjaan mereka dari rumah. Salah satu contohnya yaitu rapat virtual jarak jauh yang kini menjadi hal biasa dan aktivitas ekonomi telah meningkat di berbagai *platform* digital.

Transisi dari WFO (bekerja dari kantor) ke WFH yang dialami oleh para staff seperti administrasi, tim dukungan teknis, SDM, departemen pemasaran, dan pekerja lain yang secara tradisional bekerja dari kantor fisik dapat menjadi tugas yang berat bagi suatu perusahaan. Hal ini

[1] *https://mediaindonesia.com/read/detail/304349-jumlah-pekerja-yang-wfh-di-jakarta-menurun*

juga bersamaan dengan transisi akses data perusahaan dan sumber daya jaringan, ke tempat kerja alternatif. Selain mempertimbangan infrastruktur jaringan yang akan diakses oleh seluruh karyawan, perusahaan juga harus menyadari bahwa penjahat siber siap untuk mengeksploitasi kelemahan dan celah keamanan yang sering muncul selama proses tersebut. Baik pengguna maupun sistem yang tidak siap dan kurang aman, dapat dengan cepat menjadi celah bagi penjahat siber dan aktivitas berbahaya lainnya. Karena waktu adalah esensi, keamanan harus menjadi elemen *integral* dari setiap strategi *teleworker*.

Selain kesehatan, pandemi COVID-19 juga berdampak pada perekonomian secara global. Penurunan drastis pada pemasukan yang diterima oleh perusahaan tentu akan berdampak buruk pada keungan perusahaan dan tidak menutup kemungkinan terjadinya *Financial Distress*, terlebih apabila badan usaha mereka terpaksa ditutup dalam rentang waktu yang tidak pasti. Hal ini akan berdampak pada konsentrasi perusahaan untuk melakukan perawatan terlebih pembaharuan pada infrastruktur jaringan dan sistem informasi perusahaan khususnya.

"TAHUKAH ANDA? Dalam Tiga Bulan Pertama 2020 ada 854.441 Halaman *Phishing* dan Palsu Yang Dikonfirmasi"[2]

Sebuah laporan dari Bolster, penyedia platform yang bertugas sebagai identifikator aktivitas penipuan melalui analisis algoritma mendalam, mengkonfirmasi dalam tiga bulan pertama di tahun 2020 terdapat 854.441 halaman *phishing* dan palsu dengan 4 juta halaman web lainnya dianggap mencurigakan. Sekitar 30% dari semua halaman tersebut berkaitan dengan COVID-19. Secara keseluruhan ditemukan jumlah halaman *phishing* dan palsu yang ditayangkan naik dari 3.142 pada Januari menjadi 8.342 pada Maret. Di bulan Maret, Bolster mengklaim bahwa ditemukan 102.676 situs web yang terkait dengan penipuan medis, dengan 1.092 situs web yang menjual *hydroxychloroquine* atau menyebarkan informasi yang salah tentang penggunaannya untuk menyembuhkan COVID-19. Bolster juga menemukan lebih dari 145.000 pendaftaran domain mencurigakan yang mencakup kata-kata, "stimulus stimulus." Jumlah situs web yang mengklaim menawarkan pinjaman usaha kecil juga melonjak 130% dari Februari hingga Maret. Menurut laporan Bolster, peretas memutar 60.707 situs web penipuan bank untuk menyedot dana stimulus. Situs kolaborasi dan komunikasi *phishing* mengalami peningkatan 50% dari Januari hingga Maret. Situs *streaming phishing* juga mengalami peningkatan 85% dari Januari hingga Maret, dengan lebih dari 209 situs web dibuat per hari. Bolster bahkan menemukan beberapa situs *web phishing* menjajakan *cryptocurrency* COVID-19 palsu dan dompet *crypto*.

Shashi Prakash, kepala ilmuwan Bolster, dalam laporannya mengatakan dengan begitu banyak fokus pada penjahat *cyber* pandemi COVID-19 telah berhasil mengeksploitasi situasi. Dengan begitu banyak karyawan yang bekerja dari rumah untuk membantu memerangi penyebaran virus COVID-19, banyak dari mereka lebih cenderung menjadi mangsa serangan *phishing* dan penipuan terkait lainnya. Sayangnya, sebagian besar karyawan tersebut juga menggunakan perangkat pribadi yang tidak memenuhi standar keamanan perusahaan. Awalnya, banyak organisasi mengasumsikan kebutuhan untuk bekerja dari rumah hanya akan berlangsung beberapa minggu. Namun, hingga sekarang belum ada kejelasan kapan mayoritas karyawan akan kembali ke kantor. Bahkan, setelah belajar cara bekerja dari jarak jauh, beberapa organisasi mungkin memutuskan untuk tidak meminta karyawan mereka kembali ke kantor sama sekali.

"TAHUKAH ANDA? Ada Tiga Aspek Penting Dalam Menjaga Keamanan Informasi"

Dalam menjaga keamanan informasi suatu perusahaan atau organisasi, ada 3 aspek penting yang perlu diperhatikan yaitu kerahasiaan, integritas, dan ketersediaan, yang lebih dikenal sebagai trias CIA (*Confidentiality, Integrity, Availability*). Sederhananya, *confidentiality* ini bisa berarti sama dengan privasi. Hal ini merupakan serangkaian langkah-langkah yang perlu dilakukan untuk mencegah terekspos nya informasi sensitif dari jangkauan tangan orang-orang yang tidak berwenang. Selain itu harus dipastikan bahwa orang yang tepat sudah benar-benar mendapatkan data yang dibutuhkan. Dengan demikian, pembatasan akses perlu diterapkan agar data hanya dapat ditunjukkan pada pihak yang berwenang. Menjaga kerahasiaan data juga dapat dilakukan dengan mengadakan pelatihan khusus bagi mereka yang mengetahui adanya dokumen tersebut. Pelatihan tersebut biasanya akan mencakup edukasi terkait risiko keamanan yang dapat mengancam informasi/data penting yang ada. Aspek selanjutnya dari pelatihan ini dapat mencakup edukasi pembuatan kata

[2] *https://bolster.ai/reports (Q1 FY 2020 State of phishing & Online Fraud)*

sandi yang kuat serta praktik-praktik keamanan sejenis yang lainnya.

Gambar 2. Trias CIA

Aspek kedua merupakan *Integrity* yang berarti menjaga konsistensi, akurasi, dan kepercayaan terhadap data untuk setiap waktu hingga seterusnya. Data tidak boleh diubah pada saat proses transit dari satu perangkat ke perangkat lain. Kemudian langkah-langkah tertentu perlu dilakukan untuk memastikan bahwa data tidak bisa diubah-ubah oleh orang yang tidak punya kepentingan sejalan (misalnya, para peretas yang ingin melakukan manipulasi data dsb). Langkah-langkah tersebut juga termasuk izin dalam mengakses file dan batasan kontrol bagi akses pengguna. Kontrol ini dapat digunakan untuk mencegah perubahan yang keliru atau penghapusan tidak disengaja dari pengguna resmi yang berpotensi menimbulkan masalah. Sehingga pada intinya *backup/ redundant* harus tersedia untuk memulihkan data yang sudah terdampak masalah agar bisa kembali ke keadaan yang semula. *Checksum hashing* dapat digunakan untuk memverifikasi integritas data selama transfer. Sebuah *checksum* digunakan untuk memverifikasi integritas file, atau rangkaian karakter, setelah mereka ditransfer dari satu perangkat ke perangkat lain di jaringan lokal Anda atau Internet. *Checksum* dihitung dengan fungsi *hash*. Beberapa *checksum* yang umum adalah MD5, SHA-1, SHA-256, dan SHA-512. Fungsi *hash* menggunakan algoritma matematika untuk mengubah data menjadi suatu nilai dengan panjang yang tetap. Nilai *hash* hanya ada untuk perbandingan. Dari nilai *hash*, data asli tidak dapat diambil secara langsung. Misalnya, jika Anda lupa kata sandi, kata sandi anda tidak dapat dipulihkan dari nilai *hash*. Kata sandi harus diatur ulang.

Aspek ketiga yaitu *availability*. Memastikan sumber daya yang ada siap diakses kapanpun oleh *user*, *application*, maupun sistem yang membutuhkannya. Sama seperti aspek *integrity*, rusaknya aspek *availability* dari sistem juga bisa diakibatkan karena faktor kesengajaan dan faktor *accidental* (kecelakaan). Faktor kesengajaan bisa dari serangan *Denial of Service* (DoS), maupun *hacker/cracker*. Untuk faktor accidental (kecelakaan) bisa karena *hardware failure* (rusak atau tidak berfungsi dengan baiknya *hardware* tersebut), korsleting listrik, kebakaran, banjir, gempa bumi, dan bencana alam lainya.

Pandemi COVID-19 telah menciptakan lingkungan yang ideal bagi para penjahat dunia maya untuk meluncurkan kampanye *phishing* yang dimaksudkan untuk memungkinkan kegiatan- kegiatan kriminal mulai dari pencurian kredensial sederhana hingga penipuan langsung. Namun, kedalaman aktivitas terlarang itu, kini mencapai tingkat yang belum pernah terjadi sebelumnya. Ancaman terhadap keamanan jaringan semakin berkembang dan kompleks setiap harinya sehingga dibutuhkan suatu teknologi yang kompleks pula untuk melawannya. Muncul paradigma baru yang tadinya mungkin hanya mengamankan di salah satu titik dalam suatu jaringan, contohnya aspek *end-client* atau *user*-nya, menjadi bagaimana mengamankan keseluruhan aspek di dalam jaringan perusahaan.

Salah satu fitur teknologi dalam pencegahan ancaman keamanan jaringan yang semakin kompleks itu diantaranya melebur fungsi *firewall* konvensional dan aplikasi antivirus ke dalam satu perangkat *gateway* di dalam jaringan, dimana perangkat tersebut akan memindai baik trafik transfer file maupun traffik *mail attachment* yang ada, terhadap berbagai bahaya yang dapat mengancam keamanan jaringan perusahaan itu sendiri. Teknologi ini terus dikembangkan dengan fitur-fitur baru seperti URL *filtering*, *application control*, *anti-spam*, *anti-phishing* hingga mengamankan aset jaringan perusahaan seperti *web* maupun *database server*. Dari berbagai teknologi baru pengamanan keamanan jaringan inilah muncul juga istilah-istilah baru.

Saat ini, salah satu istilah dalam industri keamanan jaringan yang sedang populer adalah *Advanced Persistent Threat* (APT). Secara umum APT adalah ancaman akses tidak sah terhadap suatu jaringan secara terus menerus, yang tujuan utamanya untuk mencuri informasi berharga. Dalam menanggulangi

APT, dibutuhkan ketelitian maupun kejelian kita saat mengamankan perangkat dan aset jaringan perusahaan. Sifat APT yang dalam satu waktu dapat menggabungkan serangan terhadap sektor-sektor tertentu hingga eksploitasi bermacam *vulnerabilities* pada sisi teknis maupun manusianya dalam suatu organisasi. Hal ini mengakibatkan kesulitan dalam proses deteksi maupun pencegahannya. Diperlukan suatu sistem keamanan jaringan yang terintegrasi. Pendekatan tradisional dengan mengintegrasikan berbagai macam vendor keamanan jaringan terbaik di segmen fiturnya, tentu tidak cukup untuk ancaman yang terkoordinasi dan secara terus menerus mengancam dalam satu waktu yang bersamaan.

Mencegah '*Known*' *Threats*

Sistem keamanan jaringan modern yang ada saat ini mempunyai konsep pertahanan seperti mekanisme sistem imun tubuh manusia dimana memiliki banyak lapisan pertahanan yang bekerjasama melawan gangguan yang tidak diinginkan, sistem keamanan jaringan modern yang ada saat ini mempunyai konsep pertahanan berlapis-lapis dalam mencegah ancaman keamanan jaringan yang mungkin terjadi.

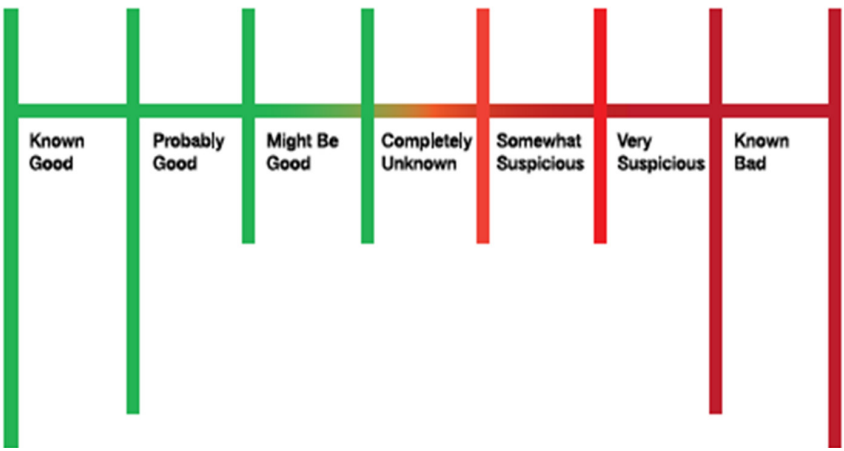
Sebuah analogi yang dapat menjelaskan kesamaan antara sistem imun tubuh dan *software* antivirus adalah proses vaksinasi terhadap patogen yang telah diketahui (*known*), dimana patogen/virus komputer dideteksi dan dianalisis oleh pihak eksternal yang kemudian membuat sebuah vaksin/antivirus *signature* untuk mengatasinya. Vaksin/antivirus *signature* inilah yang akan digunakan kembali ketika terjadi infeksi patogen/virus komputer yang sama di kemudian hari.

Dampak penerapan mekanisme tersebut akan berbeda apabila menyangkut gangguan pada jaringan komputer, dimana '*signature*' yang dimaksud sebelumnya juga bisa merujuk kepada pola akan perilaku akses jaringan yang mencurigakan dibanding hanya sebagai sebuah potongan *code* yang berbahaya. Hasil akhirnya tetap sama, gangguan maupun ancaman yang sudah diketahui '*signature*'-nya tetap dapat dicegah sebelum terjadi.

Mendeteksi '*Unknown*' *Threats*

Untuk kedua mekanisme baik imun tubuh dan jaringan perusahaan yang dijelaskan sebelumnya, gangguan dari ancaman yang belum dikenal atau belum ada vaksin/antivirus sayangnya tidak dapat dihindarkan. Efek gangguan yang dihasilkannya tergantung dari seberapa cepat dan efektif gangguan itu dideteksi, dikarantina lalu diberantas.

Sama seperti sistem kekebalan tubuh manusia yang setiap waktu secara terus menerus mengawasi gangguan yang mungkin masuk kedalam tubuh, begitu juga seharusnya dengan sistem keamanan jaringan pada perusahaan, harus tetap waspada terhadap perilaku akses jaringan yang tidak biasa ataupun *malicious*



Gambar 3. Known VS Unknown Threats

code. Agar sistem keamanan dapat dijalankan, jaringan perusahaan harus mengandalkan perangkat teknologi yang tidak hanya melakukan analisa perilaku akses jaringan namun juga dapat melakukan *sandboxing*.

Monitoring yang dilakukan secara terus menerus serta membandingkan perilaku akses jaringan dengan parameter dasar 'normal' yang ada, dimungkinkan dapat mendeteksi lebih awal akan tanda-tanda dari sebagian besar gangguan ancaman jaringan. Kombinasi dengan database pengetahuan yang terperinci tentang bagaimana beberapa ancaman terjadi, dapat mendeteksi secara akurat dan cepat untuk sebagian besar ancaman yang sama sekali tidak dikenal sebelumnya.

Mendeteksi sebuah *malicious code* yang tidak dikenal sebelumnya (belum ada *signature* antivirus/ penanganan) yang mungkin saja merupakan sebuah ancaman keamanan jaringan, sebaiknya dilakukan dengan 2 cara. Langkah pertama, meskipun *malicious code* tersebut mungkin adalah dalam 'bentuk' yang baru, namun biasanya terdapat parameter-parameter *coding* yang sudah umum digunakan dan dapat dikenali melalui teknik *deep packet inspection* dengan '*signature*' yang *up-to-date*. Namun lain halnya untuk *malicious code* yang memang benar-benar baru baik secara *coding* maupun bentuknya yang lebih dikenal dengan istilah *zero-day threats*. Langkah terbaik yang dapat dilakukan saat ini yaitu dengan menggunakan perangkat keamanan jaringan yang dikenal dengan sebutan Sandbox. Sandbox digunakan bertahun-tahun oleh tim peneliti ancaman keamanan jaringan, hanya saja baru-baru ini teknologi sandbox diperkenalkan untuk digunakan dalam lingkungan keamanan jaringan perusahaan. Ide dasar dari teknologi sandbox ini adalah menyediakan lingkungan terisolasi yang aman, dimana nantinya digunakan untuk menguji setiap file mencurigakan yang akan memasuki jaringan. File seperti ini dapat dieksekusi tanpa harus membahayakan jaringan utama operasional perusahaan itu sendiri. Proses ini dapat dimonitor dan hasilnya menentukan apakah file yang dicurigai tersebut benar-benar sebuah ancaman keamanan atau tidak.

Langkah yang kedua adalah dengan tidak membiarkan teknologi sandbox tertipu oleh teknik-teknik menghindari deteksi seperti *logic bombs*, *rootkits* atau *bootkits*, dan lainnya. Meningkatnya penggunaan teknologi sandbox di dalam suatu jaringan perusahaan, menyebabkan para penjahat dunia maya untuk lebih mengembangkan berbagai teknik menghindari deteksi yang lebih kompleks, sebagian besar memanfaatkan kelemahan dari teknologi sandbox dimana lingkungan virtual yang ada di sandbox tidak sama dengan kondisi operasional jaringan sebenarnya. Mereka mengeksploitasi kelemahan sandbox itu dengan mengembangkan yang lebih canggih yang akan aktif apabila dijalankan di kondisi operasional jaringan sesungguhnya, sehingga sandbox tidak dapat mendeteksinya diawal. Satu-satunya cara untuk membalikkan teknik tersebut adalah melalui *advanced code emulation analysis*, dimana instruksi berbahaya terhadap keamanan jaringan seperti itu dapat dikenali/dideteksi, bahkan sebelum instruksi *code* tersebut dijalankan.

Meminimalisir Dampak Dari '*Unknown*' *Threats*

Apabila kita mendeteksi adanya gangguan pada jaringan dari ancaman yang tidak dikenal, ada 2 hal yang bisa kita lakukan:

- Segmentasi Area. Membatasi potensi kerusakan dari gangguan tersebut dengan sesegera mungkin melakukan segmentasi (karantina) terhadap area yang terdeteksi ancaman. Perkecil ruang geraknya agar tidak menginfeksi/memasuki sumber daya jaringan yang lain.
- Proses Analisa (transisi dari '*unknown*' menjadi '*known*'). Setelah dibatasi ruang geraknya, gangguan ancaman tersebut haruslah dianalisis lebih lanjut untuk mengetahui potensi dampak dan resiko yang ditimbulkan, hingga proses dimana akhirnya gangguan tersebut menjadi '*known*' oleh perangkat-perangkat jaringan lainnya.

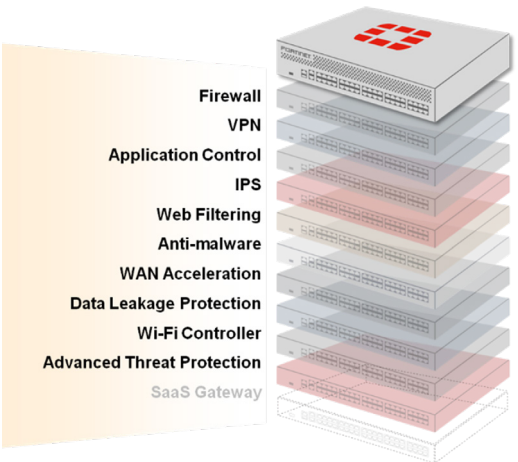
Proses akhir dari kedua langkah tersebut adalah membuat ancaman yang tidak dikenal tersebut dapat diingat oleh sistem jaringan kita sebagai database 'imun' dalam penanganan ancaman gangguan yang sama di kemudian hari.

Solusi Dari Fortinet

Fortinet sebagai salah satu vendor keamanan jaringan yang ternama, mempunyai 2 kelebihan unik dibanding kompetitor di segmen *market*-nya.

Yang pertama adalah keunikan dari perangkat lunaknya yang menjadi inti dari semua segmen produk dari Fortinet, kesatuan inilah yang mampu memberikan respons keamanan berlapis, integrasi, kolaborasi serta otomasi di setiap lini keamanan di dalam jaringan dalam menghadapi gangguan ancaman keamanan yang terus berkembang dan semakin kompleks setiap harinya.

Kelebihan Fortinet dibanding kompetitor yang kedua adalah FortiGuard, yang merupakan sebuah jaringan riset global untuk ancaman keamanan jaringan, menyediakan "vaksin" bagi known maupun *unknown zero-day threat* diseluruh dunia selama 24 jam, 365 hari secara *realtime*. Sebagai member dari *Cyber Threat Alliance* dan lembaga-lembaga riset *threat* lain, Fortinet dengan FortiGuard-nya bertukar informasi akan segala ancaman keamanan jaringan baik yang *known* ataupun *unknown* yang sedang maupun akan terjadi di jaringan global dunia. Hal ini dimaksudkan untuk dapat melakukan penanganan terhadap ancaman keamanan yang ada menjadi lebih cepat, efektif, dan terotomasi secara pintar.



Gambar 4. FortiGate Security Features

Atas ancaman *Advanced Persistent Threat* (ATP) yang sudah kita bahas sebelumnya, Fortinet mempunyai solusi *Advanced Threat Protection System*, dimana kerangka solusi ATP dari Fortinet adalah sebagai berikut.

- **Aspek LAN/WAN/Internet/*Cloud via* FortiGate**

  Pada aspek ini, identik dengan solusi untuk memfilter semua trafik *Ingress*, *Egress*, maupun Internal didalam suatu jaringan. Fortinet dengan FortiGate-nya, mempunyai peran sentral yaitu sebagai *firewall* generasi berikutnya atau lebih dikenal dengan istilah *Next Generation Firewall* (NGFW). Fortigate dapat memfilter lalu lintas jaringan untuk melindungi organisasi dari ancaman eksternal dengan mempertahankan fitur "*firewall stateful*" seperti *packet filtering*, dukungan VPN, pemantauan jaringan, dan fitur pemetaan IP. Fortigate juga memiliki kemampuan inspeksi yang lebih dalam sehingga perangkat ini memiliki kemampuan unggul untuk mengidentifikasi serangan, dan ancaman lainnya.

  Dengan fitur-fitur mumpuni dari Fortigate, suatu perusahaan dapat melakukan kontrol aplikasi, pencegahan intrusi, dan visibilitas tingkat lanjut di seluruh jaringannya. Fortigate juga dapat difungsikan sebagai internal *segmentation firewall* maupun *unified threat management*. Ada 3 hal yang membuat FortiGate lebih unggul dibanding kompetitor dan menjadi yang teratas dalam laporan Gartner di segmen UTM (*Unified Threat Management*) selama tiga tahun berturut-turut.

  1. **Perlindungan tanpa henti**

     FortiGate bersama FortiGuard dalam hal layanan keamanannya mendapat peringkat teratas dari berbagai lembaga independen seperti NSS Labs dan Top Virus Bulletin Reactive & Proactive AntiMalware.

  2. **Kemudahan *monitoring* dan konfigurasi**

     Dengan sistem operasi FortiOS dan FortiView, melakukan konfigurasi hingga *monitoring* terhadap semua trafik jaringan yang terjadi menjadi sangat mudah.

  3. **Performa yang tidak tertandingi**

     Dengan processor FortiASIC-nya, yang dibuat secara khusus untuk menangani algoritma jaringan, membuat performa *throughput* dalam hal proses *filtering* konten maupun paket deep inspection jauh mengungguli kompetitornya.

- **Aspek *Email Server via* FortiMail**

  Di masa pandemi ini banyak email-email *spam* berusaha menarik perhatian pengguna internet dengan misalnya, menjual produk-produk dengan permintaan tinggi seperti masker, pembersih tangan atau vitamin dan bahkan mereka dapat memicu teori konspirasi pandemi. Penipuan *phishing* yang dibuat mirip dengan email dari organisasi pemerintahan atau Organisasi Kesehatan Dunia (WHO). Para *scammer* telah merancang email yang tampaknya berasal dari pihak-pihak berwenang tersebut yang

Gambar 5. Fortinet Berada Pada Posisi Leader (Network Firewalls) - Gartner Magic Quadrant

tentunya mengandung tautan *phishing* berbahaya atau lampiran berbahaya. Ada juga email yang mengklaim memiliki daftar kasus virus corona 'baru' atau 'diperbarui' di daerah Anda. Dengan solusi *Email Server* dari Fortinet, FortiMail, data sensitif perusahaan tentu akan dilindungi dan membuat semua konten email bebas dari *spam*/virus/ dan sejenisnya, sehingga produktivitas operasional karyawan juga akan meningkat.

Gambar 6. Proses Email Filtering FortiMail

- **Aspek *Web Server via* FortiWeb**

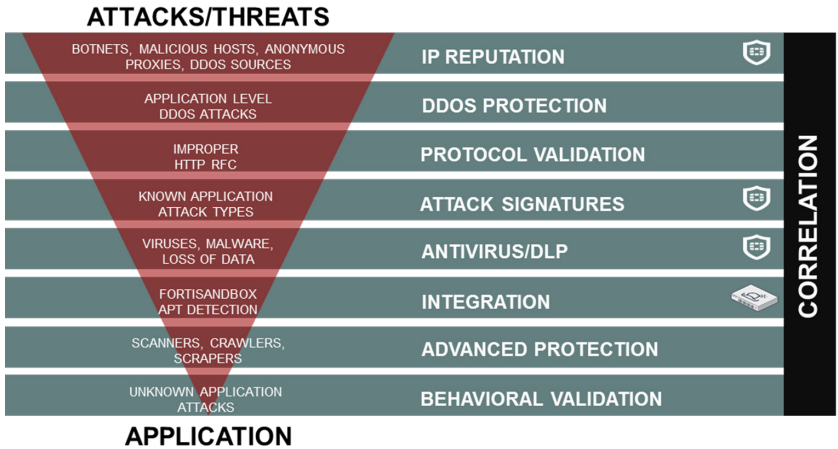
FortiWeb, *Web Application Firewall* dari Fortinet. Melindungi *web* dan aplikasi *server* dari kemungkinan celah keamanan yang dapat di-*exploit* oleh *hacker*. Dengan mekanismenya yang melindungi semua lapisan keamanan dari aplikasi maupun *web server*, sehingga dapat meminimalisir semua gangguan ancaman keamanan yang mungkin terjadi.

FortiWeb mengambil pendekatan komprehensif untuk melindungi aplikasi *Web*, termasuk reputasi IP, perlindungan DDoS, validasi protokol, *signatures* suatu serangan aplikasi, mitigasi *bot*, dan banyak lagi untuk mempertahankan aplikasi Anda terhadap berbagai ancaman, termasuk OWASP Top 10.

- **Aspek *End Points via* FortiClient**

Terkadang kita melupakan aspek paling penting yang menjadi tujuan utama awal dari sebuah serangan yang terjadi, yakni aspek *end-points* (PC/ *Smartphones*/*Tablets*).

FortiClient memberikan perlindungan terhadap ancaman '*known*' maupun '*unknown*' baik ketika *end-*



Gambar 7. All Layers Protection dari FortiWeb

points berada di 'dalam' maupun di 'luar' jaringan perusahaan, hingga menyediakan konektivitas yang aman di semua perangkat.

Solusi *end-points* dari Fortinet melalui FortiClient-nya memiliki beberapa keunggulan sebagaimana berikut ini.

- Mudah digunakan dan dikelola.
- *Patch Management*. Sebagai bagian dari Fortinet *Security Fabric*, FortiClient mendapat manfaat perlindungan terhadap ancaman '*known*' maupun '*unknown*' yang didukung oleh FortiGuard Labs dan integrasi dengan sandbox-nya
- FortiClient dapat mengkarantina suatu objek yang berbahaya dan mengakhiri, kill prosesnya secara *real-time*.

- **Aspek *Network* Sandbox *via* FortiSandbox**

Elemen yang menjadi sentral dari kerangka *advanced threat protection system* dari Fortinet ini bertugas menganalisa setiap perilaku aktivitas jaringan secara dinamis, tidak hanya berpaku pada atribut-atribut statis saja, dalam mengidentifikasi yang tadinya sebagai *unknown threat*. Beberapa APT mempunyai teknik untuk menghindari deteksi keamanan (*Advanced Evasion Techniques*) seperti sandboxing, diantaranya:

- ***Logic Bombs***

  Merupakan *code* yang tidak aktif setelah terinstalasi sampai adanya *action* tertentu yang memicunya untuk aktif.

- ***Rootkit dan Bootkits***

  Malware dengan *level* tingkat lanjut sering mengandung komponen *rootkit* yang menumbangkan sistem operasi dengan *kernel-level code* untuk mengendalikan sistem secara penuh.

- **Sandbox *Detection***

  Teknik penghindaran tingkat lanjut lainnya adalah kesadaran akan lingkungan sandbox itu sendiri.

- ***Botnet Command* dan *Control Window***

  Aktivitas *botnet command* & *control* (*botnet* C&C) biasa dimulai dengan sebuah *dropper*. *Dropper* merupakan *code* yang benar-benar bersih dalam struktur *coding*-nya, namun mempunyai rutinitas terhubung ke URL atau alamat IP tertentu untuk mengunduh file yang berisi perintah.

- ***Network Fast Flux***

  Malware dengan *level* tingkat lanjut dapat menggunakan teknik *fast flux* atau *domain generation algorithm* (DGA) untuk mengubah alamat URL maupun IP yang akan digunakan oleh *host* yang terinfeksi dalam menghindari fitur identifikasi berbasis reputasi *server botnet* C&C.

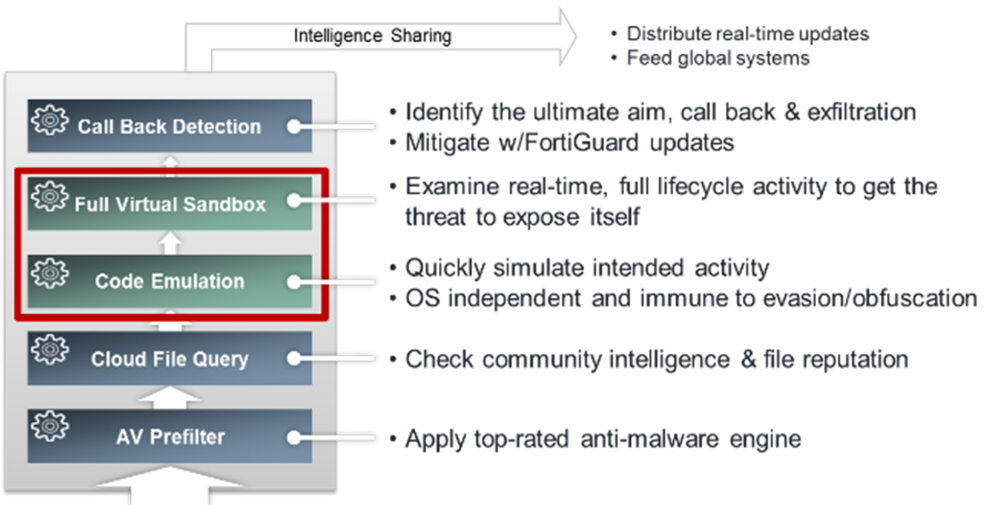
- ***Encrypted Archives***

  Satu trik yang ketinggalan jaman metodenya namun masih sangat efektif adalah menyembunyikan ke dalam arsip yang terenkripsi, yang berarti file tidak dapat dibuka tanpa kata sandi yang diperlukan.

FortiSandbox dari Fortinet memberi penggunanya kemampuan untuk sepenuhnya mengintegrasikan teknologi sandbox ke dalam infrastruktur perangkat keamanan yang ada. FortiSandbox merupakan perangkat *multi-layer* sandbox dengan fitur-fitur *pre-filtering* seperti antivirus yang sangat komprehensif, proses CPRL, dan akses *cloud* terhadap FortiGuard Labs, lembaga riset global untuk ancaman keamanan jaringan. CPRL (*Compact Pattern Recognition Language*) merupakan paten yang dimiliki oleh Fortinet dimana teknologi ini bekerja secara proaktif mendeteksi *signature threat* melalui metode *deep inspection*, yang caranya jauh melebihi pendeteksian secara konvensional. Hasil dari proses CPRL ini dapat mendeteksi lebih dari 50000 varian, baik *known* maupun *unknown*. CPRL yang ada pada FortiSandbox secara proaktif mendeteksi *signature*, baik APT (*Advanced Persistent Threat*) maupun teknik-teknik AET (*Advanced Evasion Techniques*) yang sudah kita bahas sebelumya, memfungsikan FortiSandbox untuk lebih fokus menganalisa *threat* yang jauh lebih kompleks. Dengan konfigurasi minimal, Fortisandbox dapat sepenuhnya berintegrasi dengan perangkat FortiGate, FortiMail, FortiWeb dan FortiClient Anda. Anda dapat mengkonfigurasi perangkat-perangkat ini untuk mengirim file (atau sekumpulan file) ke FortiSandbox untuk dianalisa dan jika FortiSandbox menemukan file yang dianggap berbahaya atau berisiko, penilaian tersebut akan dikembalikan ke perangkat pengirim untuk dilakukan tindakan sesuai dengan kebijakan yang telah ditentukan.

- **Aspek *Network Analyzer* dan *Monitoring via* FortiAnalyzer**

FortiAnalyzer adalah salah satu solusi produk dari Fortinet yang dapat melakukan penarikan data *log* (*Network Security Logging*) dan *report* (*Reporting Appliances*) yang terintegrasi dengan semua produk Fortinet. Dengan adanya FortiAnalyzer kita dapat mengelola *log* dan *report* antar perangkat jaringan dengan begitu mudah, serta melakukan analisa dari apa yang sedang terjadi dalam suatu jaringan. Selain dalam bentuk *appliance*, FortiAnalyzer juga tersedia dalam bentuk *virtual machine*. Untuk versi virtualnya, FortiAnalyzer dapat berjalan pada *platform* VMware vSphere, Xen, KVM maupun Hyper-V. Dengan tidak adanya perbedaan dan kemampuan antara versi *appliance* maupun versi *virtual*, FortiAnalyzer memberikan pengawasan *monitoring* yang lengkap dengan hasil *report* yang dapat disesuaikan dengan kebutuhan.



Gambar 8. Komponen Kunci dari FortiSandbox

FortiAnalyzer dengan sistem *log* dan *report* terpusat atau tersentralisasi, memberikan *alert* secara *realtime* serta investigasi dan respon terhadap *event* dari apa yang sedang terjadi. Kemudahan dalam me-*review log* yang sudah dapat dikonversi dalam bentuk dokumen HTML/CSV/XML/PDF.

Dengan sistem *log* yang terpusat, FortiAnalyzer mampu memberikan *log* dan analisa *report* dari masing-masing perangkat jaringan terhadap ancaman yang terjadi secara global, tentunya hal ini akan memberikan kemudahan bagi seorang IT administrator dalam melakukan pemeliharaan perangkat jaringan, terlebih perusahaannya memiliki banyak cabang.

Beberapa fitur yang dimiliki oleh FortiAnalyzer yaitu Sentralisasi *Log* & *Report* Perangkat, Otomasi *Indicators of Compromise* (IOC), Tampilan Aktivitas Jaringan Secara *Realtime* Maupun Historis, Integrasi Dengan *Fortinet Security Fabric*, *Custom Report*, Pencarian *Log* Untuk Analisa Forensik, dan *Realtime Monitoring* & *Alert*.

Berinteraksi satu sama lain di dalam jaringan, keenam aspek produk di atas membentuk *platform Fortinet Advanced Threat Protection*, yang secara cerdas dan kolaboratif bertugas untuk menangani 3 poin penting dalam menghadapi *advanced persistent threat* yang sudah diulas sebelumnya, yaitu:

1. Mencegah ancaman yang sudah diketahui/*known* masuk ke dalam jaringan.
2. Mendeteksi ancaman yang belum diketahui/ *unknown*, seandainya ancaman tersebut berhasil masuk ke dalam jaringan.
3. Mengurangi dampak dari setiap pelanggaran keamanan (*known/unknown*) yang terjadi dan memastikan bahwa hal serupa dapat dicegah dikemudian hari.

Pencegahan (*Prevent*)

Langkah pertama dalam pencegahan *advanced persistent threat* adalah *identity control*, dimana harus dipastikan bahwa pengguna maupun perangkat yang tervalidasi dengan benar yang dapat masuk dan mengakses sumber daya jaringan yang ada.

Selanjutnya adalah teknologi pencegahan terpadu dari Fortinet, yang terdiri atas antivirus, *anti-phishing*, URL *filtering*, *intrusion prevention*, *application control* dan *endpoint control*. Komponen-komponen tersebut menjadi bagian dari solusi *Advanced Threat Protection* dari Fortinet, dengan *engine* dari antivirus sebagai bagian yang paling *critical*.

Gambar 9. Kerangka Advanced Threat Protection Fortinet

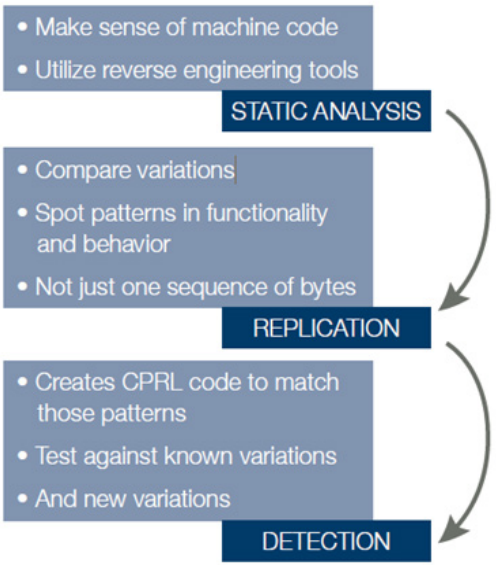
Sebelumnya, mendeteksi *signature* dari sebuah *threat* pada dasarnya dilakukan dengan membandingkan ke *fingerprint database* dari sebuah *known malware*, dan sifatnya reaktif. Ini artinya, ancaman tersebut akan bisa dideteksi dan dicegah ketika menemukan *signature* yang sama persis dengan *fingerprint database* yang dimaksud, tapi ketika ancaman itu merupakan suatu *coding* yang benar-benar baru (*unknown*), otomatis ancaman itu akan lewat proses pendeteksian secara konvensional tersebut.

Fortinet mempunyai paten yang dinamakan *Compact Pattern Recognition Language* (CPRL), dimana teknologi ini bekerja secara proaktif mendeteksi *signature threat* melalui metode *deep inspection*, yang caranya jauh melebihi pendeteksian secara konvensional. Hasil dari proses CPRL ini dapat mendeteksi 50000 lebih varian baik *known* maupun *unknown*.

Dengan diterapkannya teknologi CPRL di semua lini produk dari Fortinet, indikasi ancaman *known* maupun *unknown* mayoritas dapat segera dihentikan, terlepas dari sisi sektor mana serangan itu datang, apakah *via email*, *web browsing*, *transfer file*, atau bahkan USB *drive* yang sudah terinfeksi, semuanya dapat dikenali dan dicegah masuk ke dalam jaringan.

Deteksi (*Detect*)

Untuk membatasi kerusakan dari sebuah ancaman yang belum dikenal sebelumnya, dimana tidak ada *signature* antivirus ataupun *intrusion prevention* yang efektif saat ini, sistem pada jaringan kita haruslah waspada terhadap perilaku jaringan yang tidak biasa maupun *code* berbahaya setiap saat, kondisi ini dapat diatasi dengan sistem keamanan berlapis dari FortiGate dan FortiSandbox.



Gambar 10. Compact Pattern Recognition Language (CPRL)

FortiSandbox merupakan perangkat *multi-layer* sandbox dengan fitur-fitur *pre-filtering* seperti antivirus yang sangat komprehensif, proses CPRL, dan akses *cloud* terhadap FortiGuard Labs, serta lembaga riset global untuk ancaman keamanan jaringan. Apabila permasalahan tidak dapat diatasi oleh proses *pre-filtering* di atas, sampel-nya akan dilewatkan ke *virtual code emulation environment* di FortiSandbox untuk dieksekusi, sehingga dapat ditentukan apakah sampel file tersebut benar-benar berbahaya atau tidak.

Apabila sampel itu memang merupakan *code* berbahaya, FortiSandbox akan membuat *signature* sementara terhadap sampel file tersebut dan meneruskannya ke semua komponen di dalam kerangka Fortinet *Advanced Threat Protection* (FortiGate / FortiMail / FortiWeb / FortiClient), dan paralel meng-*upload signature* tersebut secara detail ke FortiGuard Labs untuk dianalisis lebih lanjut dan juga pendistribusian global produk Fortinet di seluruh dunia.

Mitigasi (*Mitigate*)

Ada beberapa proses yang akan dilakukan oleh FortiSandbox ketika ada indikasi keberadaan *malware* di dalam jaringan.

- ***Containment***

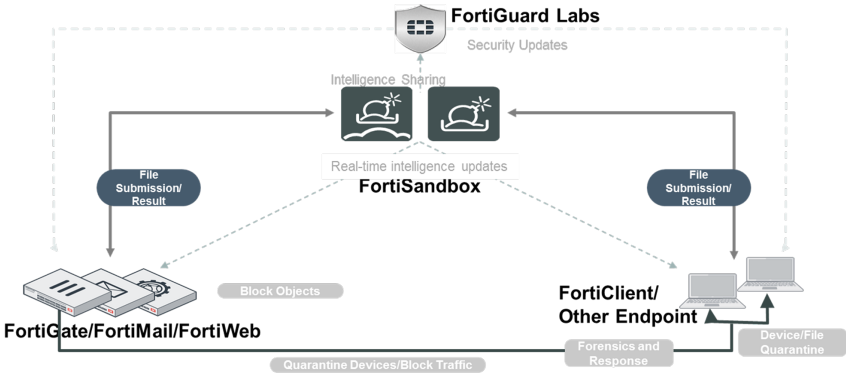
  Pada proses ini erat kaitannya dengan segmentasi jaringan. FortiGate dengan NGFW serta FortiGuard *services*-nya menyediakan segmentasi fisik maupun fungsional di setiap perangkatnya, melalui beragam pilihan *interface* berkecepatan tinggi dan akselerasi *hardware* melalui desain kustomisasi ASIC-nya. Dengan FortiOS sebagai perangkat lunaknya, segmentasi dapat dilakukan pada FortiGate berdasarkan beberapa kriteria seperti identitas pengguna, aplikasi yang digunakan, lokasi maupun jenis perangkatnya. Dengan cara ini, indikasi keberadaan *unknown malware* oleh FortiSandbox diteruskan ke FortiGate untuk disegmentasi di titik awal indikasi itu berada. Dalam hal *known*, FortiGate akan langsung melakukan segmentasi jaringan maupun karantina terhadap *host* yang dicurigai terinfeksi dan menginformasikannya kepada IT *Security Manager* agar dapat ditindaklanjuti lebih lanjut.

- ***Analysis* dan *Memory***

  Di saat yang sama, analisa dilakukan secara menyeluruh terhadap sehingga yang tadinya *unknown* menjadi *known threats*. FortiSandbox lalu memperbaharui *knowledge* dari insiden ini ke FortiGuard dimana nantinya akan didistribusikan ke jaringan produk-produk Fortinet diseluruh dunia dalam bentuk *signature update*. Proses ini untuk mencegah terjadinya insiden yang sama di kemudian hari.

Kesimpulan

Pandemi COVID-19 telah menciptakan lingkungan yang ideal bagi para penjahat dunia maya untuk meluncurkan kampanye *phishing* yang dimaksudkan untuk memungkinkan kegiatan-kegiatan kriminal mulai dari pencurian kredensial sederhana hingga



Gambar 11. Kerangka Kerja ATP Fortinet

penipuan langsung. Saat ini, salah satu istilah dalam industri keamanan jaringan yang sedang populer adalah *Advanced Persistent Threat* (APT). Secara umum APT adalah ancaman akses tidak sah terhadap suatu jaringan secara terus menerus, yang tujuan utamanya untuk mencuri informasi berharga. Dalam menanggulangi APT, dibutuhkan ketelitian maupun kejelian kita saat mengamankan perangkat dan aset jaringan perusahaan. Sifat APT yang dalam satu waktu dapat menggabungkan serangan terhadap sektor-sektor tertentu hingga eksploitasi bermacam vulnerabilities pada sisi teknis maupun manusianya dalam suatu organisasi. Hal ini mengakibatkan kesulitan dalam proses deteksi maupun pencegahannya. Diperlukan suatu sistem keamanan jaringan yang terintegrasi.

Masalah selanjutnya yang muncul akibat pandemi ini adalah penurunan drastis pada pemasukan yang diterima oleh perusahaan sehingga memaksa *management* untuk memangkas biaya operasional, terlebih apabila badan usaha mereka terpaksa ditutup dalam rentang waktu yang tidak pasti. Hal ini akan berdampak pada konsentrasi perusahaan untuk melakukan perawatan terlebih pembaharuan pada infrastruktur jaringan dan sistem informasi perusahaan.

Fortinet sebagai salah satu vendor keamanan jaringan yang ternama, menghadirkan solusi yang komprehensif untuk dua masalah utama tersebut. Terkait kebutuhan akan suatu sistem keamanan yang terintegrasi, Fortinet dengan *Security Fabric*-nya mempunyai 2 kelebihan unik dibanding kompetitor di segmen *market* yang sama. Yang pertama adalah keunikan dari perangkat lunaknya yang menjadi inti dari semua segmen produk dari Fortinet, dan kesatuan inilah yang mampu memberikan respons keamanan berlapis, integrasi, kolaborasi serta otomasi di setiap lini keamanan di dalam jaringan dalam menghadapi gangguan ancaman keamanan yang terus berkembang dan semakin kompleks setiap harinya.

Kelebihan Fortinet dibanding kompetitor yang kedua adalah FortiGuard, yang merupakan sebuah jaringan riset global untuk ancaman keamanan jaringan, menyediakan "vaksin" bagi *known* maupun *unknown zero-day threat* diseluruh dunia selama 24 jam, 365 hari secara *realtime*. Sebagai member dari *Cyber Threat Alliance* dan lembaga-lembaga riset *threat* lain, Fortinet dengan FortiGuard-nya bertukar informasi akan segala ancaman keamanan jaringan baik yang *known* ataupun *unknown* yang sedang maupun akan terjadi di jaringan global dunia. Hal ini dimaksudkan untuk dapat melakukan penanganan terhadap ancaman keamanan yang ada menjadi lebih cepat, efektif, dan terotomasi secara pintar.

Solusi dari tantangan selanjutnya mengenai masalah berkurangnya pemasukan perusahaan sehingga fokus untuk investasi dibidang infrastruktur jaringan atau IT menjadi berkurang, Fortinet dengan Fortigate-nya melalui NSS Labs ditetapkan sebagai NGFW dengan TCO (*Total Cost of Ownership*) yang sangat murah, hanya sekitar 2 USD per Mbps untuk tiap data yg diproteksi.[3]

Atas ancaman *Advanced Persistent Threat* yang menjadi lebih kompleks terlebih di masa pandemi COVID-19 ini, Fortinet mempunyai solusi *Advanced Threat Protection System*, yang terbagi ke dalam beberapa aspek yaitu *Aspek Network Firewalls via* FortiGate, Aspek *Email Server via* FortiMail, Aspek *Web Server via* FortiWeb, Aspek *End Points via* FortiClient, Aspek *Network* Sandbox *via* FortiSandbox, dan Aspek *Network Analyzer* & *Monitoring via* FortiAnalyzer.

[3] *https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/brochure-nss-lab-independent-validation.pdf*

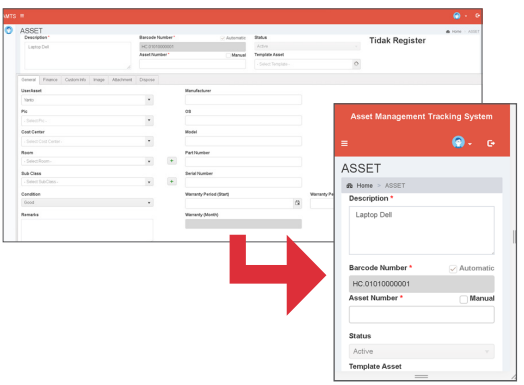
#AssetOnTrack
AMTS ENTERPRISE EDITION V.6

Manage your General Affairs' assets more effectively, faster, with better precision.

Asset Management & Tracking System
BY ACS GROUP

Kepentingan manajemen aset meningkat seiring dengan jumlah aset yang bertambah dalam sebuah perusahaan. Banyaknya variasi barang juga mempersulit pendataan barang-barang tersebut jika dilakukan secara manual, dan dapat mengakibatkan investasi waktu yang tidak produktif. Solusi asset *tracking online* yang juga dapat diakses dengan *mobile device* menjadi sangat penting.

Solusi *Asset Tracking Management System* atau AMTS dari ACS Group dapat mempermudah pendataan dan pelacakan lokasi aset. Fungsi utama dari AMTS adalah pelacakan dan *monitoring* dari asset-asset yang biasanya digolongkan asset divisi *General Affairs*, misalnya meja kursi, proyektor, APAR, AC, komputer perusahaan dengan suatu sistem yang *centralized* dan secara *mobile* mudah dioperasikan. AMTS *Enterprise Edition* v.6 menggunakan teknologi *web* responsif HTML5 yang memungkinkan akses *via browser* komputer dan juga pada *mobile device* dengan tampilan yang otomatis menyesuaikan.



Gambar 1. Responsive web application automatic adjustment screen

Software AMTS dibuat pada infrastruktur Microsoft *web base solution* dengan menggunakan Microsoft SQL *server* sebagai database sentral, dimana *deployment* dari AMTS membutuhkan *staging data* dengan *server* dengan 2 opsi pilihan, *On-Premise* atau *On-Cloud*. AMTS dilengkapi dengan aplikasi *mobile* dan sudah terintegrasi dengan barcode label printer.

AMTS ON-PREMISE

Pada paket *On-Premise License*, infrastruktur *customer* masih perlu dilengkapi dengan fisik Server, Windows Operating System server, dan Database SQL Server. Minimum *requirement* untuk OS server: Windows 2012, SQL server 2012, *processor* Quad Core Intel Xeon, dengan RAM 16GB; sedangkan untuk *client*-nya dapat diakses minimum dengan Windows 7 OS dan *browser* yang fleksibel.

AMTS ON-CLOUD

Cloud configuration ke *Private Cloud* akan dilakukan ACS Group, dan *client* tidak memerlukan pengadaan infrastruktur server (tidak perlu biaya tambahan untuk *man*-power perawatan *server* & jaringan serta listrik).

Sistem kerja AMTS

Baik *On-Premise* atau *On-Cloud*, secara garis besar dapat dijelaskan sebagai berikut:

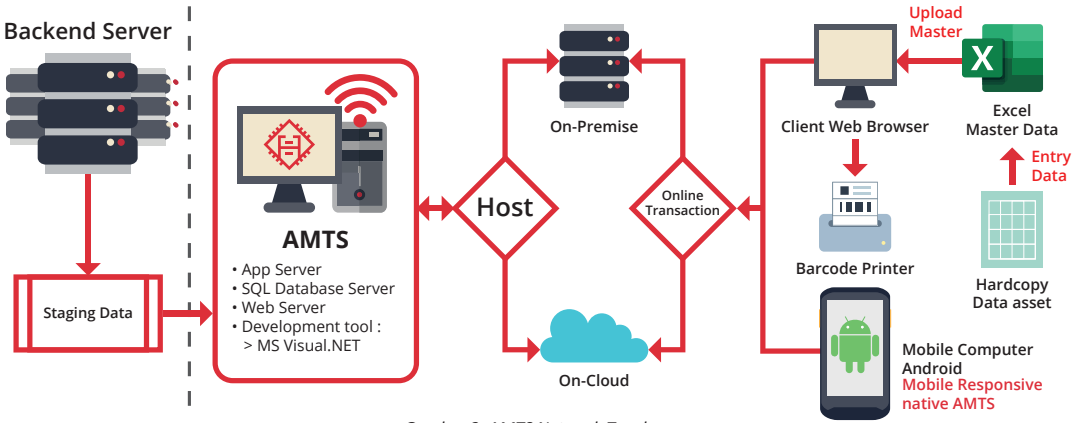
a. Selama ada koneksi jaringan via Wi-Fi atau internet, data akan *synchronize* langsung ke *web application* dan *mobile computer*.

b. *Upload* data master dari *spreadsheet* dilakukan *via web application*.

c. Untuk memastikan validitas data, maka setiap aset harus ada alokasi ruangannya agar status pada AMTS dapat menjadi '*registered*' atau terdaftar di system AMTS.

d. Label *barcode* / QR *code* sebagai identitas Aset kemudian dapat dicetak dan ditempelkan pada setiap aset.

e. Setiap ruangan juga memiliki *barcode*/QR *code* unik untuk memudahkan proses *stock opname*/ pencarian asset.



Gambar 2. AMTS Network Topology

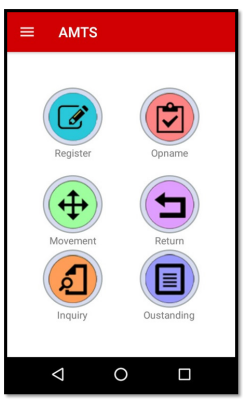
FITUR-FITUR AMTS

- ***ROLE MANAGEMENT***

  Setiap user dapat diatur autorisasinya untuk mengakses fitur-fitur tertentu, dan memberikan hak *approval* dari transaksi yang sudah diatur (seperti transaksi *opname*, *maintenance*, *upload* master aset).

- **LEVEL PELACAKAN**

  Filter kepemilikan / pertanggungjawaban sebuah aset dapat ditentukan berdasarkan *Holding Company*, Perusahaan, *branch*, *sub-branch*, divisi, dan *department*. *Level* informasi dari Lokasi Aset dapat didefinisikan secara area, gedung, lantai, dan ruangan.



Gambar 3. AMTS Android Mobile

- **REGISTRASI**

  Semua data asset yang masuk ke AMTS harus dipastikan terregistrasi dengan melakukan proses registrasi *via mobile* atau *automatic* register *via* proses *upload* data master aset. Aset yang sudah teregistrasi (‘*registered*’) akan mudah dilacak dan user dapat mengelolanya dengan mudah.

- ***COST CENTER***

  Setiap aset di AMTS dapat ditentukan *department* “pemilik”nya, sehingga alokasi pertanggung jawaban jelas.

- **LAMPIRAN ASET**

  Aset info dapat ditambahkan dengan lampiran file dokumen pdf, termasuk foto atau gambar aset yang dapat ditambahkan atau diperbarui saat asset opname dilakukan

- ***ASSET COMPONENT***

  Transaksi *Asset Component* digunakan untuk mendefinisikan aset-aset yang menjadi ‘*child*’/anak dari aset utama yang tidak dapat dipisahkan dari suatu aset utama. Contohnya kendaraan *ambulans* sebagai aset utama memiliki ‘*child*’ atau *sub-*aset tabung oksigen, *bed portable*, dongkrak, ban cadangan.

- **DUPLIKASI ASET**

  Transaksi Duplikasi Aset dapat mempercepat proses registrasi aset dengan jenis dan info yang sama, sebagai contohnya: 25 unit PC dengan spesifikasi teknis yang sama dengan satu kali transaksi dan

kemudian dapat menambahkan informasi tambahan lainnya.

- ***ASSET MOVEMENT* & MUTASI ASET**

  Dengan adanya aplikasi transaksi *movement* di aplikasi *mobile*, maka perpindahan aset anda ke lokasi lain akan terus terlacak dan tidak akan kehilangan informasi keberadaannya.

- ***BORROW-RETURN***

  Seringkali aset perusahaan yang dipinjamkan kepada karyawannya seperti laptop atau alat peraga perlu juga dilacak agar pertanggungjawabannya jelas ketika terjadi sesuatu pada aset tersebut. Transaksi *Borrow-Return* akan mengingatkan peminjam aset dan yang menyetujui peminjaman tersebut dengan mengirimkan notifikasi *via email* ketika tanggal sudah mendekati/melewati *overdue*.

- ***SERVICE MONITORING***

  Berbagai aset biasanya memerlukan perawatan berkala, contohnya penggantian *accu* pada mobil operasional, *service* kendaraan, *service* AC. Dengan fitur Notifikasi/*Reminder*, *user* yang sudah ditentukan akan mendapatkan email pengingat agar menjaga ketepatan waktu pengembalian aset.

- ***OPNAME REPORT***

  Permudah *stock opname* dan identifikasi pertanggungjawaban aset di lokasi dengan *handheld* aplikasi Android, atau akses *web-version* AMTS dengan *browser* apapun. Laporan dapat diekspor ke excel atau pdf, dengan *template standard* yang dapat disesuaikan keperluan *user*.

- ***INQUIRY***

  Dalam *menu Inquiry*, setiap *user* dapat memilih data *report/inquiry* data yang ingin ditampilkan berdasarkan *sub-branch*, lokasi, *asset class*, penanggungjawab, tanggal pembelian, dan lain-lain; dan setiap *user* dapat membuat *template* sendiri.

- ***ASSET DISPOSAL***

  Jika suatu aset sudah tidak digunakan atau masa pemanfaatannya sudah habis atau tidak perlu dilacak lagi, maka dapat dieksekusi dengan transaksi *Asset Disposal*.

*/ Penulis : Kenneth Looho (ken.looho@acsgroup.co.id)

Event Virtual ACS Group

Pandemi Covid-19 banyak membatasi aktivitas kegiatan perusahaan, namun ACS Group terus berinovasi dengan mengadakan kegiatan *webinar* yang sudah dilakukan dua bulan belakangan ini dengan tujuan yang sama yaitu memberikan pengetahuan/*update product* tentang solusi tepat guna bagi para pelanggan setia. Karena kegiatan operasional bisnis terus berjalan untuk memenuhi kebutuhan para pelanggan mereka, disamping kebutuhan tersebut tentu perlunya peningkatan faktor keamanan, efektivitas dan efisiensi lewat solusi tepat guna yang diberikan pada acara webinar ini.

Update product yang dipaparkan pada *webinar* ini bukan hanya produk dari ACS Group saja namun bekerjasama antara lain dengan HIKVISION, ARUBA HPE dan FORTINET.

Webinar "Thermal Camera Solution" (HIKVISION Product)

Pemerintah menerbitkan protokol-protokol baru untuk menyambut Era "*New Normal*", selain untuk memutus penyebaran covid-19, Pemerintah juga ingin meningkatkan kembali sektor bisnis yang sempat menurun akibat pandemi covid-19. Protokol baru seperti pemindaian suhu tubuh, selalu memakai masker dan pembatasan interaksi, wajib diterapkan di segala lini publik dan bisnis.

Secara tidak sadar peran teknologi dapat diandalkan agar protokol tersebut dapat dijalankan dengan lebih aman, efisien dan dapat dipertanggungjawabkan.

Hikivision sebagai perusahaan penyedia produk dan solusi keamanan inovatif terkemuka di dunia, menyediakan solusi inovatif terkait protokol menyambut era "*New Normal*" yang cocok digunakan di berbagai area dan industri.

Solusinya adalah "*Back to business solution*", dimana di dalamnya terdapat solusi *contactless* seperti: perangkat pemindaian suhu dan masker menggunakan *fever thermal camera* yang dapat memindai 30 orang sekaligus, kemudian ada juga terminal pemindaian suhu ditambah kontrol akses dan mesin absensi (*minmoe*), serta *people counting camera* sebagai upaya membatasi jumlah orang dalam suatu ruangan dan dapat juga mendeteksi jarak sebagai upaya *social distancing*. Semua itu dapat divisualisasi dalam 1 layar dan semua data pemindaian tersebut juga bisa di-*export* sebagai data laporan yang dapat dipertanggungjawabkan.

Webinar #SwitchPerfect (ARUBA HPE Product)

ArubaOS-CX adalah produk switch *modern* dari Aruba yang memiliki *analytics* dan juga *automation*, berbeda dengan switch tradisional pada umumnya. ArubaOS-CX switch memiliki portfolio untuk *positioning* di segala posisi, baik *branch*, *access*, *aggregation*, bahkan *core* pada *data center*. ArubaOS-CX memiliki berbagai macam fitur, mulai dari *Virtual Switching Extension* (VSX) sebagai solusi *high availibility*, dimana bisa dilakukan *upgrade* tanpa adanya *downtime*, NetEdit sebagai solusi untuk *deployment*, *configuration*, dan *automation* pada switch, *Network Analytics Engine* (NAE) sebagai solusi *automated monitoring* & *troubleshooting* dan juga *real-time visibility*, dan *Dynamic Segmentation* untuk solusi *automated* IoT dan *User Security*.

Solusi lainnya dari Aruba yaitu banyaknya solusi *remote access* yang dapat disesuaikan dengan berbagai kebutuhan seperti remote AP (*Access Point*) dimana AP dapat membuka akses ke kantor sehingga kita dapat mengakses *resource* kantor seperti layaknya sedang berada di kantor, VPN (*Virtual Private Network*) perorangan dengan Aruba VIA, atau bahkan membuat jaringan secara SD-WAN dengan menggunakan perangkat Aruba. Di sisi lain dari pembuatan akses yang handal dari luar kantor, keamanan jaringan juga sangat perlu diperhatikan dimana dalam hal ini Aruba melakukan proteksi akses terhadap semua orang yang ingin melakukan akses ke jaringan kantor dari segala sumber baik itu menggunakan kabel, nirkabel, ataupun akses remote seperti VPN. Aruba dengan Clearpass Policy Manager

melakukan pengaturan akses tersebut agar admin jaringan dapat memiliki *visibility* terhadap semua perangkat sehingga jelas mana yang perangkat kerja, pribadi, smartphone, laptop, dan sebagainya dan selanjutnya dapat melakukan pengaturan yang sangat fleksibel dan tepat secara otomatisasi.

Webinar #AssetOnTrack (AMTS Product by ACS Group)

Melalui *webinar* dengan tema #AssetOnTrack di sini ACS Group merilis versi terbaru dari *software Asset Management & Tracking System* (AMTS): AMTS *Enterprise Edition* V.6; dengan *web version* menggunakan basis HTML5 (*web responsive*) dan Android OS sebagai basis aplikasi *mobile*. Terdapat 2 opsi *deployment* pada versi ini: *On-Premise* atau *On-Cloud*. Untuk detailnya dapat Anda lihat di halaman 16 tentang topik AMTS *ENTERPRISE EDITION* V.6.

Webinar #ClubForti (FORTINET Product)

Transformasi Digital sudah terjadi di semua sektor Industri, momen ini dipercepat dengan adanya pandemi covid-19 dan beberapa perusahaan menerapkan "*work from home*" untuk menunjang produktivitas perusahaan. Hal ini tentu akan membuat *attack surfaces* semakin melebar.

Fortinet sebagai perusahaan yang bergerak di bidang *Security* menawarkan solusi keamanan untuk menunjang kinerja perusahaan seperti:

Fortigate + FortiClient untuk *Teleworker solution*, FortiToken yang memberikan solusi 2-*Factor Authentication*.

Fortiweb sebagai proteksi aplikasi berbasis web dimana sudah menggunakan teknologi *Machine Learning* untuk mengurangi *False* Positif dan memudahkan dalam *Management* perangkat.

Serta FortiMail sebagai *Email Security Solution* untuk memberikan kenyamanan *user* dalam berkomunikasi *via email* yang sudah didukung *Threat Inteligence* berbasis AI dan *Machine Learning*.

Zebra Technologies

ZEBRA

TC21/TC26 TOUCH COMPUTER

Solusi untuk sektor industri : Retail, Field Mobility, Transportation, Manufacturing, Warehouse Management, & Hospitality.

Komputer sentuh TC21 dan TC26 adalah perangkat dengan harga yang terjangkau yang dirancang khusus untuk kebutuhan di area bisnis kecil dan menengah. Produk ini memiliki Layar HD 5" yang mudah dibaca sekalipun di area luar di bawah sinar matahari cerah, produk yang rugged, tahan terhadap cipratan air, debu(IP67) dan mampu beroperasi selama 10 jam bahkan lebih(14 jam dengan optional baterai). TC21 dan TC26 hadir dengan kamera belakang 13 MP yang beresolusi tinggi; opsional 5 MP pada kamera depan serta memiliki kualitas suara yang superior dan fungsionalitas melalui seluler dengan VoLTE; Teknologi VoWiFi Zebra yang canggih, yang disertakan dengan Lisensi Mobility DNA Enterprise, mampu memberikan kualitas suara yang superior pula pada semua aplikasi suara WiFi Anda - misalnya, Push-to-Talk Express.

Zebra Technologies

MC3300X MOBILE COMPUTER

Solusi untuk sektor industri : Manufacturing, Retail, & Warehouse Management

Evolusi berikutnya dari Zebra menghadirkan mobile komputer keypad/sentuh MC3000 yang rugged, dikemas dengan fitur-fitur baru untuk menangani kebutuhan yang semakin meningkat dari ekonomi berbasis permintaan dan e-commerce saat ini. Didukung oleh Android 10 serta processor ultra powerful octa-core 2,2 GHz dan RAM 4 GB / Flash 32 GB bahkan dikemas pula dengan baterai 7000 mAh yang mampu digunakan untuk operasional selama tiga shift membuat produk ini menjadi terdepan di kelasnya. Fitur tambahan antara lain:

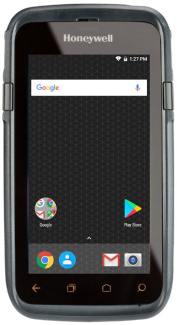
1. 2x2 Multiple-User Multiple Input Multiple Output (MU-MIMO) technology dan WorryFree WiFi
2. 4-inci (800 x 480) WVGA dengan Corning Gorilla Glass
3. Class 2, Bluetooth v5.0 with BR/EDR and Bluetooth Low Energy (BLE) Support
4. Integrated dengan scan engine SE4850, mampu memindai barcode 1D dan 2D pada jaarak 7,6 cm sampai 21,4 M
5. All Touch Terminal Emulation (ATTE) yang didukung oleh Wavelink

Zebra Technologies

ZQ511/ZQ521 MOBILE PRINTERS

Solusi untuk sektor industri : Transportation, Manufacturing, Retail, & Hospitality

ZQ511 ™ dan ZQ521 ™ - adalah Mobile Printer yang tangguh dan terbaik di kelasnya dengan desain kelas militer sehingga dapat digunakan untuk aplikasi di industri apa pun. Memiliki peringkat IP54 tahan terhadap debu dan zat padat lainnya serta zat cair karena sudah terlindungi oleh kemasannya tanpa perlu casing pelindung lagi. ZQ511 ™ dan ZQ521 sudah dilengkapi dengan batterai 3250 mAh mampu mencetak dengan kecepatan cetak (5+ inch per menit) dengan fitur "mode draf" untuk pencetakan hanya teks saja. ™ dan kedua printer ini tersedia dalam model RFID, mampu mencetak label tag UHF RFID untuk semua kebutuhan pelacakan Anda. Didukung pula oleh Wi-Fi 802.11ac dan protokol keamanan terbaru, ditambah Bluetooth 4.1 Klasik.



Honeywell

Dolphin CT60 Handheld Computer

Solusi untuk sektor industri : Warehouse, Retail, Field Mobility, & Manufacturing

Dolphin ™ CT60 merupakan Mobile computer yang dibangun di atas platform Mobility Edge ™, yang menawarkan pendekatan secara terintegrasi, dapat diulang, dan dapat diskalakan berdasarkan platform perangkat keras dan perangkat lunak secara umum - membebaskan pelanggan dari kendala yang dihadapi saat ini seputar integrasi dan teknologi yang tidak fleksibel tanpa mengorbankan fitur keamanan, keandalan, kinerja, atau manajemen perusahaan. Produk ini juga ditenagai oleh Prosesor 2 GHz Qualcomm Snapdragon ™ 660 octa-core yang mampu menghasilkan pemrosesan transaksi 1,8 x lebih cepat, serta memiliki tampilan layar 4,7" Corning® Gorilla® Glass yang jelas dan mudah dibaca baik di dalam maupun di luar ruangan, dan dapat digunakan dengan sentuhan jari, sarung tangan, atau stylus. Mampu memindai barcode linear dan 2D pada jarak 10 cm sampai 9 meter.

Honeywell

Dolphin CN80 Mobile Computer

Solusi untuk sektor industri : Warehouse, Field Mobility, & Logistics

Dolphin CN80 merupakan perangkat Android Enterprise yang dibuat untuk kebutuhan dan kemudahan di lapangan, agar tetap up-to-date untuk penggunaan jangka panjang. Memiliki opsi dalam pemindaian barcode 1D/2D pada jarak 0,15 m hingga 15,2 m (6 inci hingga 50 kaki) yang biasanya diperlukan untuk operasional di gudang. Dolphin CN80 adalah produk yang rugged tahan terhadap benturan/jatuh pada ketinggian 3 m di atas beton. Produk ini juga memiliki peringkat IP65/ IP67 yang tahan terhadap semprotan debu maupun cipratan air, bahkan jika terendam sekalipun. Tersedia opsi unit untuk operasional di area cold storage dan non-incendive.

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

FOTO DI DOMPET

Ada seorang suami, sebut saja Paijo yang di dalam dompetnya terdapat foto istrinya. Saat teman-temannya melihat, ia dipuji sebagai suami yang sangat baik.

Lalu, satu di antara temannya bertanya apa fungsinya membawa foto sang istri.

Paijo menjawab: "Kalau aku punya permasalahan di kantor, aku selalu memandang foto itu, dan permasalahan yang dihadapi hilang begitu saja".

"Wah alangkah berbahagianya kamu mempunyai istri seperti itu, bagaimana bisa begitu?" tanya teman-temannya.

Paijo menjawab kembali: "Ya, kalau saya melihat foto istri saya, semua permasalahan apa pun di kantor, menjadi tidak ada apa-apanya dibandingkan dengan permasalahan dengan dia!"

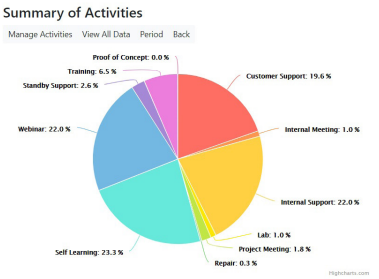
KOLOM KETAWA

Aktivitas Team Engineer Selama WFH

Bekerja dari rumah atau work from home yang dilaksanakan sejak bulan Maret 2020 yang lalu merupakan himbauan Pemerintah agar dapat meminimalisasi penyebaran virus Covid-19. Para pelaku usaha tentunya menindaklanjuti himbauan dari Pemerintah dengan memberlakukan para karyawannya untuk bekerja dari rumah (Work From Home atau WFH). ACS Group sebagai perusahaan penyedia solusi bagi banyak perusahaan yang bergerak di berbagai bidang industri turut memberlakukan kegiatan ini namun dalam melaksanakan kegiatan WFH ini para staff khususnya engineer ACS baik di Jakarta dan yang ada di seluruh cabang tetap melakukan hal terbaik untuk mendukung layanan bagi para pelanggan ACS dengan cara remote support bagi pelanggan yang mengalami kendala teknis dan jika diperlukan melakukan kunjungan ke lokasi pelanggan untuk menindaklanjuti gangguan yang terjadi tentunya dengan mentaati protokol kesehatan yang diharuskan seperti penggunaan masker, menjaga jarak, dan selalu mencuci tangan sebelum dan sesudah aktivitas dengan tujuan agar operasional pelanggan dan perusahaannya tetap dapat berjalan dengan baik dan lancar.

Selain daripada hal diatas, para engineer juga terus meningkatkan kemampuannya dan keahliannya dengan mengikuti serangkaian pelatihan dan pembelajaran secara daring/online baik seperti webinar, online training, ujian sertifikasi dan virtual meeting. Pembelajaran daring tersebut antara lain diberikan dari vendor/principle, distributor dan lembaga pendidikan termasuk pelatihan mengenai Keselamatan dan Kesehatan Kerja (K3) yang merupakan upaya untuk menjamin keselamatan dan kesehatan jasmani maupun rohani tenaga kerja.

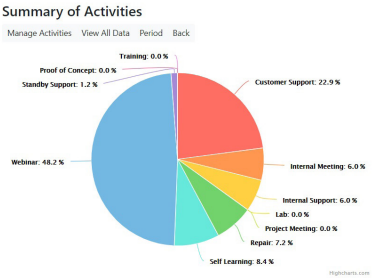
Kegiatan yang mereka lakukan dapat anda lihat dari bagan yang kami tampilkan di bawah ini.



Team ENS JKT

Period - All Time

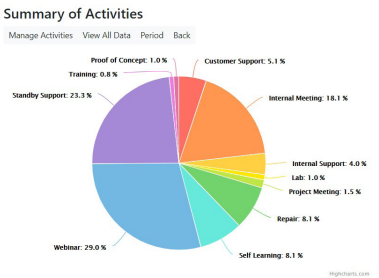
Category	Total
Customer Support	76
Internal Meeting	4
Internal Support	85
Lab	4
Project Meeting	7
Repair	1
Self Learning	90
Webinar	85
Standby Support	10
Training	25
Proof of Concept	0



Team Cabang Surabaya

Period - All Time

Category	Total
Customer Support	19
Internal Meeting	5
Internal Support	5
Lab	0
Project Meeting	0
Repair	6
Self Learning	7
Webinar	40
Standby Support	1
Training	0
Proof of Concept	0



Team Cabang Bali

Period - All Time

Category	Total
Customer Support	37
Internal Meeting	131
Internal Support	29
Lab	7
Project Meeting	11
Repair	59
Self Learning	59
Webinar	210
Standby Support	169
Training	6
Proof of Concept	7

Fortinet Mengakuisisi OPAQ

Fortinet® sebagai pemimpin global dalam solusi keamanan siber yang luas, terintegrasi, dan otomatis, pada tanggal 20 Juli 2020 mengumumkan telah mengakuisisi OPAQ Networks, penyedia cloud Secure Access Service Edge (SASE) yang berbasis di Herndon, Virginia. Solusi cloud Zero Trust Network Access (ZTNA) OPAQ melindungi organisasi yang terdistribsi jaringannya - dari pusat data, ke kantor cabang, ke pengguna jarak jauh, dan perangkat Internet of Things (IoT).

Dengan mengakuisisi OPAQ, tidak seperti penyedia keamanan cloud lainnya, Fortinet akan memberikan:

- Skalabilitas, Kinerja, dan Keamanan yang terbaik dibandingkan cloud security vendor lainnya.
- Solusi keamanan cloud security yang terintegrasi dengan true Zero Trust security, tidak seperti ZTNA provider lainnya yang meninggalkan banyak unprotected gaps terhadap attack surface.
- Satu jenis ZTNA solution dengan inovasi keamanan yang berkelanjutan dalam skalabilitas, dengan memanfaatkan bakat tim R&D terbaik Fortinet untuk menghadirkan security substance “under the hood”.
- Security dan networking yang terintegrasi sepenuhnya, Termasuk Fortinet SD-WAN, dan melanjutkan pendekatan Security-driven Networking.
- The most partner-friendly ZTNA offering in the market that remains true to Fortinet’s ongoing commitment to its valued partners.

Zebra Technologies Mengakuisisi Reflexis Systems

Zebra Technologies Corporation mengumumkan untuk mengakuisisi Reflexis Systems, 28 Juli 2020.

Reflexis adalah provider terkemuka untuk solusi intelligent workforce management bagi industri ritel, food service, perhotelan dan perbankan.

Reflexis sebagai pemimpin pasar global dalam retail task management and workforce management, tentunya akan menambah portofolio produk untuk perangkat lunak dari Zebra Technologies. Reflexis ONE™ intelligent work platform saat ini sudah digunakan oleh ratusan pelanggan di seluruh dunia, dengan Reflexis ONE para manager/user yang terkait dapat menyederhanakan pelaksanaan, meningkatkan komunikasi, dan mengoptimalkan keputusan tenaga kerja.

Extreme Networks Mengakuisisi Aerohive Networks Seharga $272 Juta

Extreme Networks mengumumkan telah mengakuisisi perusahaan Aerohive Networks senilai $ 272 juta. Kesepakatan ini tentunya akan memperluas portofolio Extreme Networks dalam hal cloud-managed WiFi dan network access control (NAC) sehingga melengkapi solusi on-prem WIFI dan NAC dari Extreme Networks sebelumnya.

Aerohive sendiri didirikan pada tahun 2006, perusahaan ini memiliki kurang lebih 30.000 pelanggan cloud wireless LAN di area vertikal seperti pendidikan, kesehatan, pemerintahan serta ritel. Aerohive merupakan salah satu perusahaan pertama yang menawarkan controller-less wi-fi dan cloud network management. Aerohive sekarang ini juga telah meluncurkan tiga jenis produk access points WIFI-6.

Hewlett Packard Enterprise Mengakuisi Silver Peak

Hewlett Packard Enterprise + silver peak

Hewlett Packard Enterprise mengumumkan bahwa mereka telah menandatangani perjanjian definitif untuk mengakuisisi Silver Peak, vendor pemimpin dalam teknologi SD-WAN (Software-Defined Wide Area Network), dengan nilai transaksi akuisisi senilai $ 925 juta. Silver Peak akan digabungkan dengan unit bisnis HPE Aruba sehingga akan memperluas kepemimpinan teknologi Aruba khususnya pada sektor SD-WAN yang sangat besar pasarnya dan terus berkembang pesat.

Kombinasi Aruba dan Silver Peak ini akan mempercepat transformasi cloud untuk perusahaan-perusahaan dengan solusi jaringan edge-to-cloud yang komprehensif yang mencakup semua aspek baik untuk jaringan kabel (LAN), jaringan nirkabel (WLAN), dan jaringan area luas (WAN).

Teknologi SD-WAN dari Silver Peak yang canggih dapat melengkapi dan memperkuat Edge Service Platform (ESP) Aruba. Dengan menggabungkan solusi SD-WAN dari Silver Peak dengan solusi SD-Branch dari Aruba, maka pelanggan dapat menyederhanakan penyebaran konfigurasi dan perangkat pada kantor cabang, memudahkan dengan konektivitas WAN untuk cloud-connected distributed enterprises, serta mentransformasi operasi bisnis tanpa harus mengorbankan kualitas maupun keandalannya.

Nutanix Telah Mengangkat Fetra Syahbana Sebagai Country Manager

NUTANIX
YOUR ENTERPRISE CLOUD

Nutanix Inc telah mengangkat Fetra Syahbana sebagai Country Manager yang baru untuk Indonesia. Fetra Syahbana sendiri memiliki pengalaman lebih dari 25 tahun di industri IT untuk enterprise. Sebelum bergabung dengan Nutanix, beliau berkarier sebagai Country Manager F5 Networks untuk Indonesia dan hampir dua dekade Fetra berkarir sebagai General Business Country Manager di IBM Indonesia.

Di tempat yang baru sekarang ini beliau bertanggung jawab dalam mengarahkan strategi bisnis, akuisisi pelanggan, dan memperluas pasar Nutanix di Indonesia.

Zebra Technologies SEA Partner eSummit 2020

ZEBRA **2020 & Beyond**
Winning in the New Room

Zebra Technologies mengadakan event Zebra Technologies SEA Partner eSummit 2020 yang berlangsung secara live dan diikuti lebih dari 240 peserta dari 7 negara di South East Asia pada tanggal 15 Juli 2020 yang lalu. ACS Group tergabung dalam acara secara live ini.

Topik bahasan yang dibawakan pada acara Zebra eSummit 2020 ini:

1. Zebra Android Enterprise Devices
2. Zebra Mobility DNA

Zebra DNA adalah portfolio software, application dan utilities yang memungkinkan transformasi perangkat Zebra mobile computers, scanners dan printers untuk solusi bagi enterprise. Zebra DNA meliputi Mobility DNA, Print DNA and DataCapture DNA guna memastikan semua perangkat Zebra dilengkapi dengan kapabilitas yang dibutuhkan dalam mengoptimalkan operasional pengunaan sehari-harinya.

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.

Professional Level :

- 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)

Associate Level :

- Aruba Certified Mobility Associate (ACMA)
- Aruba Certified Switching Associate (ACSA)

- Cambium Networks ePMP Certified
- Honeywell Certified
- 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 (PMP)® Certified
- Samsung Knox Certified
- Zebra Technologies Certified, etc.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Make cyber risk a priority for yout Board → **Produce Supporting risk management policies**

← **Determine your risk appetite** ←

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

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

- ABB Enterprise Business Solutions
- Roambee - IOT Real-time Shipment Tracking for Supply Chain
- AMTS - Asset Management and Tracking System
- LTS - Laundry Tracking System
- GAS-V - Gate Access System - Vehicle
- ABS - Agriculture Plantation and Mill Management

BUSINESS PARTNERS

ABB · 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(H), 4205187(H)
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(H); 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