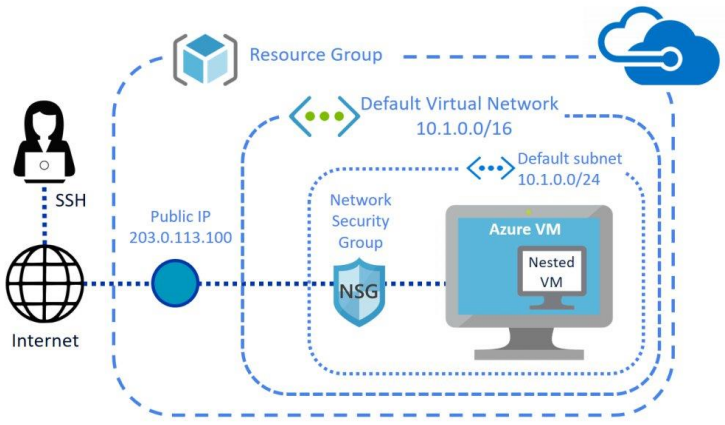
MODUL V

Kasus Kebocoran Data di Dunia Kesehatan dan Kemampuan Solusi Keamanannya

5.1. Kemampuan Keamanan di Microsoft

Dalam lingkungan kerja modern sekarang ini, para karyawan mulai bekerja dari jarak jauh bahkan mengelola akses ke sebuah aset dan sumber daya di organisasinya melalui jaringan virtual Azure (VNet) di rumah. Sebuah VNet dapat dibagi menjadi beberapa subnetwork (subnet) yang masing – masing saling berkaitan dengan sumber daya tertentu dan tugas yang berbeda. Saat mengamankan sumber dalam subnet kita dapat menggunakan grup keamanan jaringan. Apakah itu? Grup keamanan jaringan (NSG) membantu dalam proses izin dan tolak lalu lintas jaringan dari sumber daya Azure yang ada pada jaringan VNet yang kita gunakan seperti virtual mesin. Grup keamanan jaringan terdiri dari sebuah aturan yang menentukan bagaimana lalu lintas tersebut akan disaring saat proses addressing atau pengalamatan. Apabila mendapatkan grup keamanan jaringan yang sama maka dapat dikaitkan ke subnet dan antarmuka jaringan yang berbeda sebanyak yang dipilih. Aturan tersebut dievaluasi sesuai dengan prioritas menggunakan lima titik informasi yaitu sumber, port sumbernya, tujuan, port tujuannya dan protokol yang memproses dalam pengizinan dan penolakan dalam jalur lalu lintas. Tidak diperbolehkan untuk membuat dua aturan keamanan dengan prioritas dan arah yang sama.



Kemampuan Keamanan di Microsoft

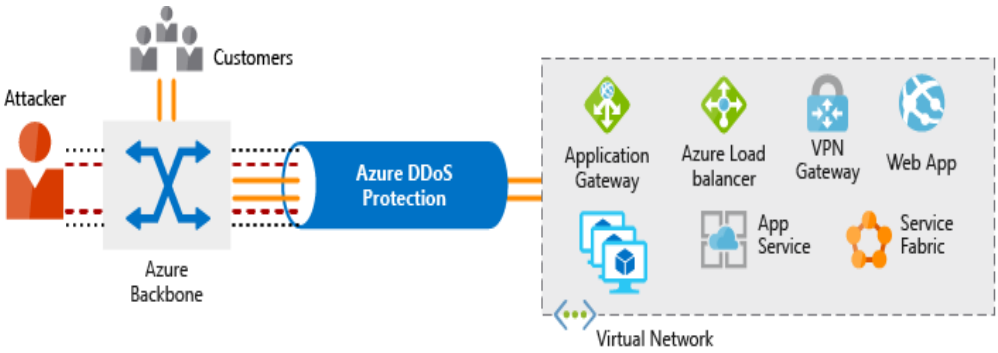
NSG mengontrol akses ke sumber daya di jaringan virtual dan subnet apapun yang terdiri dari aturan keamanan masuk dan keluar. Untuk setiap aturannya, dapat dilakukan penentuan sumber dan tujuan, port, protokol dan tindakan yang diperlukan. Aturan diproses berdasarkan prioritasnya dan Azure membuat serangkaian aturan yaitu tiga aturan masuk dan tiga aturan keluar agar memberikan tingkat keamanan dasar. Tidak dapat menghapus aturan default akan tetapi dapat menggantinya dengan membuat aturan baru dengan prioritas yang lebih tinggi dari sebelumnya.

5.1.1. Servis Terdistribusi Penolakan Serangan (DDoS)

Setiap perusahaan besar maupun kecil dapat menjadi sebuah target serangan jaringan yang sangat serius. Terdapat servis distribusi penolakan serangan atau Distributed Denial of Service (DDoS) yang bertujuan untuk meramaikan aplikasi dan server juga membuat tidak responsif atau lambat bagi pengguna. Serangan ini akan menargetkan titik akhir yang sedang menghadapi publik melalui internet. Ada tiga jenis serangan DDoS yang sering ditemui yaitu:

- Serangan volumetrik, serangan berbasis volume dalam membanjiri jaringan dengan lalu lintas yang terlihat terverifikasi serta membanjiri bandwidth yang tersedia. Jenis serangan ini diukur dalam bit per detik.
- Serangan protokol, membuat target yang tidak dapat diakses dengan menghabiskan sumber daya server dengan permintaan protokol palsu yang mengeksploitasi kelemahan pada protokol lapisan jaringan dan lapisan transportasi. Jenis serangan ini diukur dalam paket per detik.
- Serangan lapisan aplikasi, menargetkan paket aplikasi web untuk mengganggu transmisi data antarhost,

Layanan perlindungan DDoS Azure dirancang untuk membantu dalam melindungi aplikasi dan server dengan menganalisis lalu lintas jaringan serta membuang berkas yang terlihat seperti serangan DDoS.



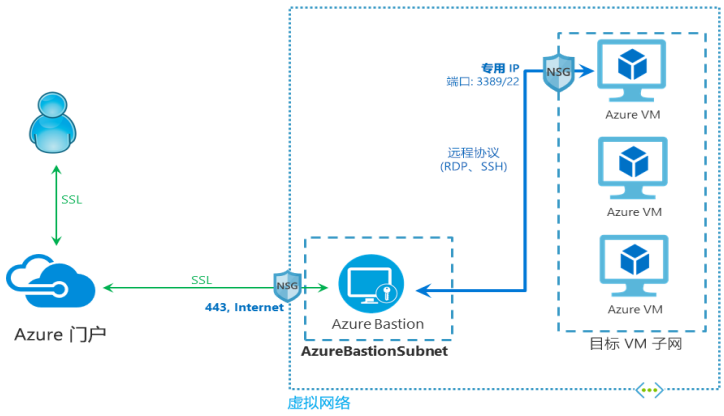
Servis Terdistribusi **Penolakan Serangan (DDoS)**

Azure DDoS Protection mengidentifikasi upaya penyerang, sehingga dilakukan proses pemblokiran lalu lintas dan memastikan bahwa hal tersebut tidak mencapai sumber daya Azure. Azure DDoS Protection menggunakan skala dan elastisitas jaringan global Microsoft untuk menghadirkan kapasitas mitigasi DDoS ke setiap wilayah Azure. Perlindungan yang diberikan yaitu mengelola data cloud dengan memastikan bahwa beban jaringan hanya mencerminkan penggunaan pelanggan yang sebenarnya. Perlindungan Azure DDoS ada dalam dua tingkatan yaitu dasar dan standar. Dasar berarti yang diaktifkan secara otomatis untuk setiap properti di Azure dan pemantauan lalu lintas yang selalu aktif dan mitigasinya secara real – time dari serangan tingkat jaringan umum. Memberikan pertahanan yang sama dengan layanan online Microsoft juga jaringan global Azure yang digunakan dalam mendistribusikan dan mengurangi

lalu lintas serangan di seluruh wilayahnya. Sedangkan tingkat standar memberikan kemampuan mitigasi ekstra yang disesuaikan secara khusus untuk sumber daya jaringan VNet. Kebijakan perlindungan dipantau melalui lalu lintas khusus dengan algoritma pembelajaran mesin. Kebijakan tersebut diterapkan ke alamat IP publik yang berkaitan dengan sumber daya yang disebarkan di jaringan virtual seperti Azure Load Balancer dan Application Gateway.

5.1.2. Azure Bastion

Azure Bastion menyediakan konektivitas protokol desktop jarak jauh (RDP) yang aman dan mulus dalam penggunaannya ke mesin virtual secara langsung dari portal Azure melalui Transport Layer Security. Ketika terhubung melalui Azure Bastion, maka mesin virtual tidak memerlukan alamat IP publik, agen, atau perangkat lunak klien khusus. Menggunakan Azure Bastion dapat melindungi mesin virtual dari mengekspos port RDP ke dunia luar bersamaan dengan tetap menyediakan akses aman.



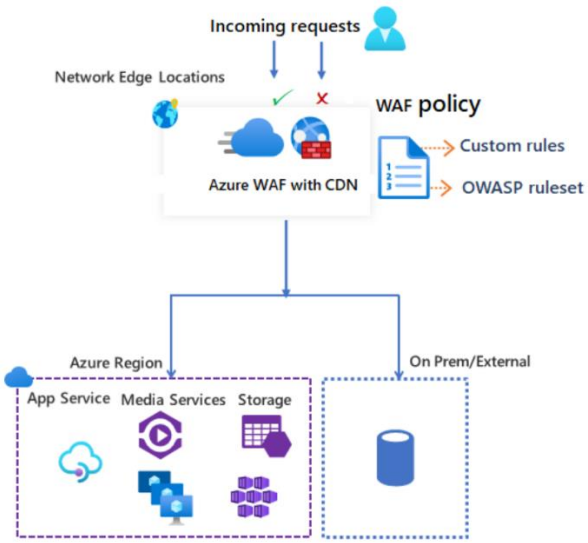
Azure Bastion

Fitur utama pada Azure Bastion yaitu:

- RDP di portal Azure, mendapatkan secara langsung di portal Azure dan menggunakan pengalaman sekali klik.
- Sesi jarak jauh melalui TLS dan traversal firewall untuk RDP, menggunakan web berbasis HTML yang secara otomatis mengalir ke perangkat lokal. Nantinya akan mendapatkan RDP dalam melintasi firewall perusahaan dengan aman.
- Tidak memerlukan IP publik di Azure VM, mendapat akses ke mesin virtual Azure menggunakan IP pribadi di VM masing – masing user.
- Tidak perlu mengelola NSG, terkelola sepenuhnya dari Azure yang diperkuat secara internal untuk menyediakan konektivitas yang aman.
- Perlindungan terhadap pemindaian port, VM melindungi dari pemindaian port oleh pengguna dan penyerang yang berada di luar jaringan virtual.
- Perlindungan terhadap eksploitasi zero – day, menjaga Azure Bastion tetap kokoh dan selalu terbarui.

5.1.3. Firewall Aplikasi Web (WAF)

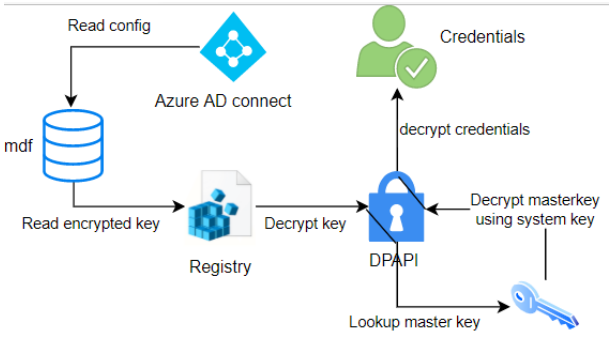
Aplikasi web semakin hari menjadi sasaran serangan yang mengeksploitasi kerentanan yang umum diketahui seperti injeksi data dan skrip lintas situs. Sehingga dibutuhkan patching untuk memperbaiki apabila terdapat kerusakan dan pemantauan secara ketat. WAF memberikan perlindungan terpusat pada sebuah aplikasi web dari eksploitasi dan kerentanan web yang terpusat untuk membantu membuat manajemen keamanan agar lebih sederhana. Sehingga meningkatkan waktu respons terhadap ancaman keamanan juga memungkinkan patching kerentanan yang diketahui pada tempat tertentu.



Firewall Aplikasi **Web (WAF)**

WAF memberikan jaminan perlindungan yang lebih baik kepada administrator aplikasi terhadap ancaman dan gangguan. WAF dapat digunakan dengan layanan Azure Application Gateway, Azure Front Door, dan Azure Content Delivery Network (CDN) dari Microsoft. WAF memiliki fitur yang disesuaikan untuk setiap layanan tertentu.

5.1.4. Enkripsi Data di Azure



Enkripsi Data **di Azure**

Sebagian besar organisasi menganggap bahwa data adalah aset yang berharga. Dibutuhkan strategi keamanan yang berlapis dan ketat agar dapat menjaga data yang dimiliki. Penggunaan enkripsi berfungsi sebagai garis pertahanan terakhir dan terkuat. Microsoft Azure menyediakan

cara berbeda – beda untuk mengamankan suatu data yang bergantung pada layanan atau penggunaan yang diperlukan. Enkripsi di Azure terbagi menjadi tiga seperti berikut:

- Enkripsi layanan penyimpanan Azure membantu melindungi data saat istirahat dengan mengenkripsi otomatis sebelum menyimpannya ke disk yang dikelola Azure serta mendekripsi data sebelum pengambilannya.
- Enkripsi disk Azure membantu mengenkripsi disk mesin virtual Windows dan Linux IaaS. Menggunakan fitur BitLocker standar industri untuk menyediakan enkripsi volume untuk OS dan disk data.
- Enkripsi data transparan (TDE) membantu melindungi Azure SQL Database dan Azure Data Warehouse dari ancaman aktivitas jahat dengan melakukan enkripsi dan dekripsi real – time dari database, terkait backup juga file log transaksi tanpa memerlukan perubahan di aplikasi.

Azure ke vault adalah layanan cloud terpusat untuk menyimpan rahasia aplikasi dan mengontrol rahasia aplikasi dengan menyimpannya di satu lokasi terpusat juga menyediakan akses yang aman seperti kontrol izin.

5.2. Cakupan Kemampuan Jaringan dan Platform Komputasi Awan Terhadap Manajemen Keamanan

Semakin banyak perusahaan yang memindahkan data ke komputasi awan maka hal pertama yang perlu dipertimbangkan adalah bagaimana agar data yang dimiliki tetap aman dalam penjagaannya. Kejahatan dunia maya sebagai bisnis multi – miliar dolar, karena kegagalan dalam melindungi data dapat terjadi kerugian dan reputasi. Manajemen postur keamanan komputasi awan (CSPM) adalah kelas alat yang baru dirancang untuk meningkatkan manajemen keamanan dengan menilai sistem sebuah perusahaan dan secara otomatis menginfokan staf keamanan di bidang IT apabila terdapat kerentanan. CSPM menggunakan alat dan layanan di lingkungan komputasi awan untuk memantau dan memprioritaskan peningkatan dan fitur keamanan. Alat dan layanan yang dimaksud yaitu:

- Kontrol akses berbasis zero trust, mempertimbangkan tingkat ancaman yang aktif selama keputusan kontrol akses.
- Penilaian risiko real time, memberikan visibilitas ke risiko teratas.
- Manajemen ancaman dan kerentanan (TVM), menetapkan pandangan holistik dari permukaan dan risiko serangan organisasi juga mengintegrasikannya ke dalam operasi pengambilan keputusan rekayasa.
- Kebijakan teknis, menerapkan pembatas dalam mengaudit dan menegakkan standar dan kebijakan organisasi untuk sistem teknis.
- Sistem dan arsitektur pemodelan ancaman.

Tujuan utama tim keamanan komputasi awan yang bekerja pada CSPM adalah untuk melaporkan dan meningkatkan postur keamanan organisasi setiap saat dengan berfokus dalam mengganggu

laba atas investasi penyerang potensi. Fungsi dari CSPM sendiri berguna bagi beberapa tim pada organisasi seperti tim intelijen ancaman, teknologi informasi, tim kepatuhan dan manajemen risiko, pemimpin bisnis dan UMKM, arsitektur dan operasi keamanan juga audit.

5.2.1. Microsoft Defender untuk Komputasi Awan

Azure Defender (Microsoft Defender for Cloud) adalah manajemen postur keamanan dan perlindungan ancaman. Microsoft Defender memenuhi tiga kebutuhan ketika mengelola keamanan sumber daya dan beban kerja di awan dan lokal:

- Mengkaji terus – menerus, mengetahui postur keamanan, identifikasi dan melacak kerentanan.
- Aman – memperkuat semua sumber daya dan layanan yang terhubung.
- Defend – mendeteksi dan mengatasi ancaman terhadap sumber daya, beban kerja dan layanan.

Fitur Microsoft Defender mencakup dua pilar keamanan cloud diantaranya yaitu manajemen postur keamanan (CSPM) dan perlindungan beban kerja cloud (CWP).

1. Fitur CSPM menyediakan visibilitas yang membantu dalam memahami situasi keamanan saat sekarang dan panduan pengerasan dalam membantu meningkatkan keamanan secara efisien dan efektif. Fitur utama yang memungkinkan untuk mencapai tujuan tersebut adalah keamanan skor. Microsoft Defender akan terus menilai langganan dan organisasi saat mengalami masalah keamanan yang nantinya akan digabungkan dengan semua temuan menjadi satu skor sehingga dapat diketahui secara sekilas bahwa semakin tinggi skor maka semakin rendah tingkat risiko yang teridentifikasi. Selain keamanan skor terdapat rekomendasi pengerasan berdasarkan kesalahan konfigurasi dan kelemahan keamanan yang teridentifikasi. Peta jaringan sebagai alat untuk melihat topologi beban kerja apakah setiap node dikonfigurasi dengan benar ataukah tidak.

Microsoft Defender **untuk Komputasi Awan**

2. Fitur CWP mendeteksi dan mengatasi ancaman terhadap sumber daya, beban kerja dan layanan. Perlindungan yang disediakan melalui paket – paket yang dapat dipilih di antaranya:

Paket Microsoft Devender	Fungsi
Microsoft Defender untuk server	Menambahkan deteksi ancaman dan pertahanan tingkat lanjut untuk Windows dan Linux
Microsoft Defender untuk app service	Mengidentifikasi serangan yang menargetkan aplikasi yang berjalan di atas App Service
Microsoft Defender untuk storage	Mendeteksi aktivitas yang berpotensi berbahaya di akun Azure storage
Microsoft Defender untuk SQL	Mengamankan database dan datanya di mana pun berada
Microsoft Defender untuk kubernetes	Menyediakan pengerasan lingkungan keamanan Kubernetes cloud – native, perlindungan beban kerja dan perlindungan run – time
Microsoft Defender untuk menampung pendaftar	Melindungi semua pendaftar berbasis Azure Resource Manager
Microsoft Defender untuk key vault	Melindungi ancaman tingkat lanjut
Microsoft Defender untuk manajer sumber daya	Memantau operasi manajemen sumber daya di organisasi
Microsoft Defender untuk DNS	Menyediakan lapisan perlindungan tambahan untuk sumber data yang menggunakan kemampuan resolusi yang disediakan
Microsoft Defender untuk perlindungan relasional terbuka	Menghadirkan perlindungan ancaman untuk basis data relasional sumber terbuka

Microsoft Defender **untuk Komputasi Awan**

Paket yang berbeda dapat diaktifkan secara terpisah dan akan berjalan secara bersamaan dalam memberikan pertahanan komprehensif untuk lapisan komputasi, data dan layanan.

5.2.2. Peningkatan Keamanan Microsoft Defender

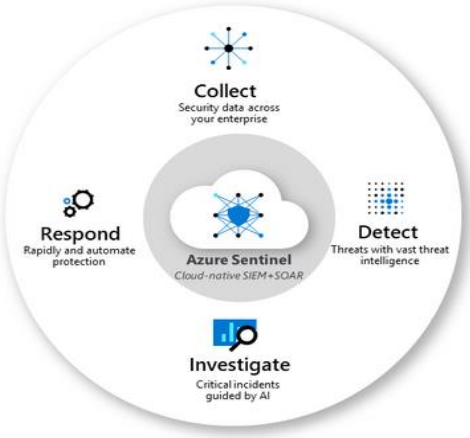
Microsoft Defender menawarkan dua mode yaitu tanpa fitur keamanan yang ditingkatkan (gratis) artinya diaktifkan secara gratis di semua langganan Azure. Penggunaannya memberikan skor aman dan fitur yang berkaitan yaitu kebijakan keamanan, penilaian keamanan berkelanjutan juga rekomendasi keamanan yang dapat ditindaklanjuti dalam membantu melindungi sumber daya Azure. Mode lainnya yaitu semua fitur keamanan yang ditingkatkan dengan memperluas kemampuan mode bebas ke beban kerja yang berjalan di awan pribadi dan publik lainnya. Selain itu dapat memberikan manajemen keamanan terpadu dan perlindungan ancaman di seluruh beban kerja cloud hybrid. Manfaat dari mode kedua ini yaitu dapat mendeteksi dan merespons titik akhir yang komprehensif, mudah menyebarkan pemindai ke semua mesin virtual,

melindungi sumber daya dan beban kerja pada platform, memastikan kepatuhan terhadap standar keamanan, melacak kepatuhan dengan berbagai standar, juga mengontrol akses aplikasi. Keamanan melalui Microsoft dan Center for Internet Security (CIS) telah mengembangkan praktik terbaik dalam membantu menetapkan dasar keamanan untuk platform Azure. Tolok ukur CIS digunakan dengan layanan dan alat keamanan Azure dalam membuat keamanan dan kepatuhan lebih mudah bagi aplikasi pengguna yang berjalan di layanan Azure. Setiap layanan dilengkapi dengan dasar yang sudah dirancang untuk membantu memberikan keamanan dan pengalaman yang konsisten saat mengamankan lingkungan.

5.3. Perlindungan Ancaman Microsoft 365 Defender

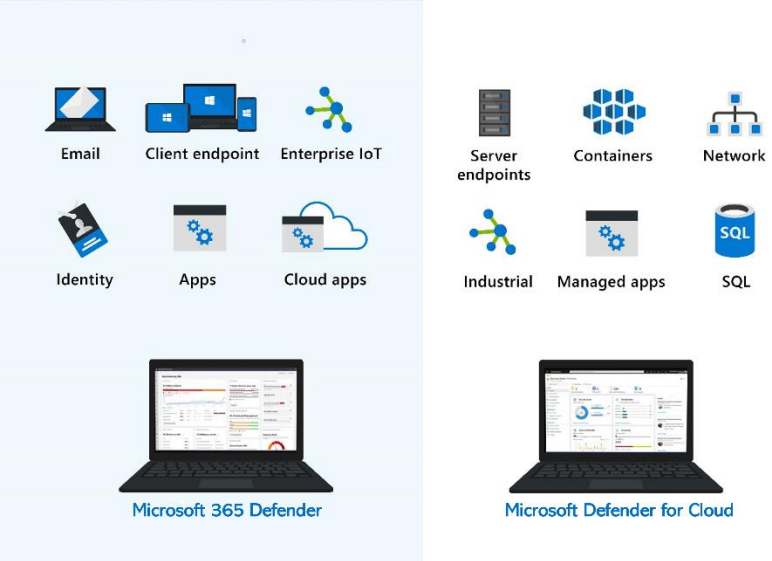
Melindungi sumber daya, aset, dan data organisasi dari pelanggaran dan serangan keamanan merupakan tantangan yang terus berlanjut dan semakin meningkat. Penjahat dunia maya akan sering meningkatkan aktivitas mereka di saat krisis nasional atau global dengan mencari atau mengeksploitasi situasi dan menemukan jalan ke dalam sebuah organisasi. Manajemen informasi keamanan (SIEM), respons otomatis orkestrasi keamanan (SOAR), dan deteksi respons yang diperluas (XDR) memberikan wawasan keamanan yang sangat baik dan otomatisasi keamanan yang dapat meningkatkan perimeter keamanan jaringan organisasi. SIEM adalah alat yang digunakan dalam mengumpulkan data dari seluruh area termasuk infrastruktur, perangkat lunak dan sumber daya. Di mana akan dilakukan analisis dengan mencari korelasi atau anomali dan menghasilkan peringatan. Sedangkan SOAR berperan dalam pengambilan peringatan dari banyak sumber yang akan memicu alur kerja dan proses secara otomatis yang dapat digerakkan oleh tindakan untuk menjalankan tugas keamanan yang mengurangi masalah. XDR hadir untuk keamanan yang cerdas, otomatis dan terintegrasi di seluruh domain organisasi. Ini membantu dalam mencegah, mendeteksi dan merespons ancaman di seluruh identitas, titik akhir, aplikasi, email, IoT, infrastruktur dan platform cloud.

5.3.1. Microsoft Sentinel Melindungi Ancaman Terintegrasi



Microsoft Sentinel Melindungi **Ancaman Terintegrasi**

Manajemen yang efektif dari perimeter keamanan jaringan organisasi memerlukan kombinasi alat dan sistem yang tepat. Microsoft sentinel adalah solusi SIEM/SOAR cloud – native skalabel yang memberikan analitik keamanan cerdas dan intelijen ancaman di seluruh perusahaan. Seperti diagram diatas yang menunjukkan fungsionalitas ujung ke ujung dari Microsoft sentinel yaitu dalam mengumpulkan data pada skala cloud di semua pengguna, perangkat, aplikasi dan infrastruktur baik di manapun. Adanya pendeteksi ancaman yang sebelumnya tidak ditemukan dan meminimalkan kesalahan positif menggunakan analitik dan intelijen ancaman juga menyelidiki ancaman dengan AI. Serta menanggapi insiden dengan cepat dan otomatisasi tugas keamanan umum. Microsoft sentinel hadir dengan banyak konektor yang tersedia secara langsung dan menyediakan integrasi real time. Perlindungan dari ancaman adalah medan pertempuran yang terus berkembang. Penjahat dunia maya semakin mencari kerentanan yang dapat di eksploitasi untuk mencuri, merusak atau memeras data, aset, dan sumber daya suatu organisasi atau perusahaan. Microsoft menyediakan rangkaian alat yang memberikan deteksi dan respons yang diperluas (XDR) melalui Microsoft 365 Defender dan Microsoft Defender untuk awan. Kedua alat tersebut terintegrasi dengan lancar dengan Microsoft sentinel dalam memberikan kemampuan perlindungan ancaman yang lengkap dan menyeluruh bagi organisasi.

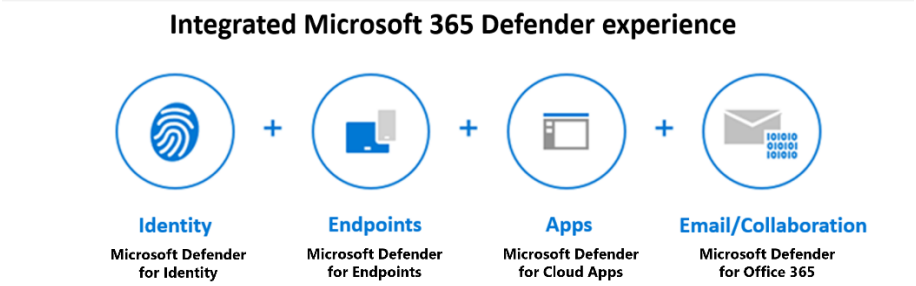


Microsoft Sentinel Melindungi **Ancaman Terintegrasi**

5.3.2. Microsoft 365 Defender

Microsoft 365 Defender adalah rangkaian pertahanan perusahaan yang melindungi dari serangan dunia maya yang semakin canggih. Dengan adanya Microsoft 365 Defender membantu dalam mengoordinasikan deteksi, pencegahan, penyelidikan, dan respons terhadap ancaman di seluruh email dan aplikasi secara native. Microsoft 365 Defender adalah solusi deteksi dan respons ancaman lintas domain yang terintegrasi juga memberikan pertahanan otomatis terkoordinasi di semua domain layanan untuk memblokir ancaman sebelum menjadi serangan. Microsoft 365 Defender dapat menghentikan serangan dan persistensi sebelum terjadi dan menghilangkan

kebingungan dan kekacauan yang terjadi pada portal keamanan yang tersembunyi. Salah satu solusi untuk menyatukan data ancaman untuk respons yang cepat dan lengkap misalnya Microsoft 365 Defender secara otomatis menghubungkan data sinyal tingkat domain ke dalam insiden untuk memberi tim keamanan garis waktu serangan penuh.



Microsoft 365 **Defender**

Paket Microsoft 365 Defender melindungi:

- Titik akhir dengan Microsoft Defender for Endpoint sebagai platform titik akhir terpadu untuk perlindungan pencegahan dalam mendeteksi pasca pelanggaran, penyelidikan otomatis dan respons.
- Email dan kolaborasi dengan Microsoft Defender untuk office 365, melindungi organisasi dari ancaman berbahaya yang ditimbulkan oleh pesan email, URL, dan lainnya.
- Identitas dengan Microsoft Defender untuk identitas dan Azure AD proteksi identitas, melakukan pengidentifikasian dan menyelidiki ancaman tingkat lanjut, identitas yang di susupi, dan tindakan orang dalam yang berbahaya dan diarahkan ke organisasi.
- Aplikasi dengan Microsoft Defender untuk aplikasi awan, solusi lintas SaaS komprehensif yang menghadirkan visibilitas mendalam, kontrol data yang kuat dan perlindungan ancaman yang ditingkatkan ke aplikasi awan.

Microsoft Defender untuk identitas adalah solusi keamanan berbasis awan yang menggunakan data direktori aktif lokal atau yang disebut sinyal dalam mengidentifikasi, mendeteksi dan menyelidiki ancaman tingkat lanjut. Microsoft tersebut mencakup area utama seperti memantau dan membuat profil perilaku dan aktivitas pengguna, melindungi identitas pengguna dan mengurangi permukaan serangan serta mengidentifikasi aktivitas mencurigakan dan penyerangan lanjutan di seluruh rantai pembunuhan serangan dunia maya. Berbeda dengan cakupan area utama yang dikhususkan oleh Microsoft Defender untuk office 365. Microsoft Defender Office 365 mencakup area utama berikut:

- Kebijakan perlindungan ancaman, menetapkan kebijakan perlindungan ancaman untuk menetapkan tingkat perlindungan yang sesuai dengan organisasi.
- Laporan, melihat laporan real time untuk memantau kinerja Microsoft Defender 365 di organisasi.

- Investigasi ancaman dan kemampuan respons, menggunakan alat cangggih untuk menyelidiki, memahami, mensimulasikan, dan mencegah ancaman.
- Kemampuan investigasi dan respons otomatis, menghemat waktu dan upaya untuk menyelidiki dan mengurangi ancaman.

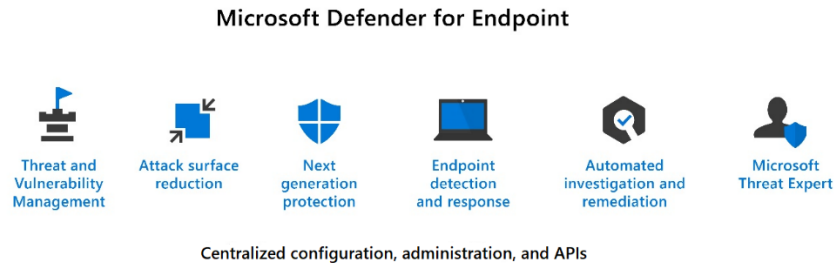
Microsoft Defender Office 365 tersedia dalam dua paket. Paket yang dipilih akan mempengaruhi alat yang akan digunakan.

1. Paket 1 menawarkan alat konfigurasi, perlindungan dan deteksi untuk rangkaian office 365
   a. Lampiran – memeriksa lampiran email untuk konten yang berbahaya.
   b. Tautan – memindai untuk setiap klik, tautan tersebut tetap dapat diakses tetapi tautan berbahaya yang akan diblokir.
   c. Lampiran SharePoint, OneDrive, dan Microsoft Teams – melindungi organisasi saat pengguna berkolaborasi dan berbagi file dengan mengidentifikasi dan memblokir file berbahaya di situs tim dan pustaka.
   d. Perlindungan anti phishing – mendeteksi upaya untuk meniru pengguna dan domain internal atau kustom.
   e. Deteksi real time – melaporkan real time yang memungkinkan untuk mengidentifikasi dan menganalisis ancaman terkini.
2. Paket 2 mencakup semua fitur inti di paket 1 dan menyediakan alat otomatisasi, investigasi, perbaikan dan simulasi untuk membantu dalam melindungi rangkaian office 365
   a. Pelacak ancaman – memberikan intelijen terbaru tentang masalah keamanan dunia maya yang berlaku dan memungkinkan organisasi untuk mengambil tindakan pencegahan sebelum ada ancaman yang sebenarnya.
   b. Penjelajah ancaman – melaporkan secara real time yang memungkinkan dalam mengidentifikasi dan menganalisis ancaman terkini.
   c. Investigasi dan respons otomatis (AIR) – mencakup serangkaian pedoman keamanan yang dapat digunakan secara otomatis seperti peringatan yang dipaksakan atau manual. Buku pedoman keamanan dapat memulai penyelidikan otomatis, memberikan hasil mendetail dan merekomendasikan tindakan yang dapat disetujui ataupun ditolak oleh tim keamanan.
   d. Simulator serangan – menjalankan skenario serangan realistis di organisasi untuk mengidentifikasi kerentanan.

5.3.3. Microsoft Defender Endpoint

Microsoft Defender Endpoint adalah platform yang dirancang untuk membantu jaringan perusahaan dalam melindungi titik akhir. Dilakukan dengan mencegah, mendeteksi, menyelidiki, dan menanggapi ancaman tingkat lanjut. Microsoft Defender Endpoint dapat menyematkan teknologi bawaan Windows 10. Teknologi ini mencakup sensor perilaku titik akhir yang

mengumpulkan dan memproses sinyal dari sistem operasi, analitik keamanan awan yang mengubah sinyal menjadi wawasan, deteksi dan rekomendasi, serta intelijen ancaman dalam mengindetifikasi alat penyerang, teknik, dan menghasilkan peringatan.



Microsoft Defender **Endpoint**

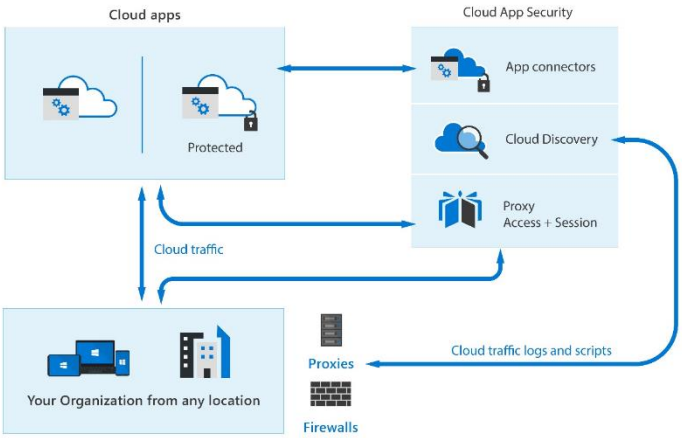
Microsoft Defender Endpoint meliputi beberapa hal berikut:

- Manajemen ancaman dan kerentanan, menggunakan sensor pada perangkat untuk menghindari perlunya pemindaian dan memprioritaskan kerentanan.
- Pengurangan permukaan serangan, melindungi jaringan dan web dengan mengatur akses ke alamat IP, domain, dan URL berbahaya serta membantu mencegah aplikasi mengakses lokasi berbahaya.
- Perlindungan generasi berikutnya, menggabungkan pembelajaran mesin, analisis data besar, penelitian ketahanan ancaman yang mendalam dan infrastruktur cloud Microsoft untuk melindungi perangkat di organisasi / perusahaan.
- Deteksi dan respons titik akhir, menyediakan deteksi serangan tingkat lanjut yang mendeteksi waktu nyata dan dapat ditindaklanjuti. Analisis keamanan dapat memprioritaskan peringatan, melihat cakupan penuh pelanggaran, dan mengambil tindakan respons untuk memulihkan ancaman.
- Invertigasi dan remediasi otomatis, fitur ini menggunakan algoritma inspeksi dan proses yang digunakan oleh analisis untuk memeriksa peringatan dan mengambil tindakan remediasi cepat menyelesaikan pelanggaran.
- Microsoft Threat Experts, layanan berburu ancaman yang terkelola menyediakan pusat operasi keamanan dengan alat pemantauan dan analisis untuk memastikan ancaman kritis tidak terlewatkan.
- Manajemen dan API, menyediakan API dalam mengintegrasikan dengan solusi lain.

5.3.4. Microsoft Defender Aplikasi Awan

Microsoft Defender Aplikasi Awan adalah Broker Keamanan Akses Cloud (CASB) yang sebagai solusi lintas SaaS komprehensif dan beroperasi sebagai perantara antara pengguna dan penyedia awan. Microsoft Defender ini memberikan visibilitas yang kaya ke layanan awan, kontrol atas

perjalanan data, dan analitik yang canggih untuk mengidentifikasi dan memerangi ancaman dunia maya di semua layanan awan Microsoft dan pihak ketiga. CASB bertindak sebagai penjaga gerbang untuk menengahi akses waktu nyata antara pengguna perusahaan dan sumber daya awan yang digunakan juga keberadaannya. CASB dapat mengatasi kesenjangan keamanan dalam penggunaan layanan awan oleh organisasi. Perlindungan tersebut disediakan oleh banyak kemampuan di seluruh area visibilitas, keamanan data, perlindungan ancaman dan kepatuhan.



Microsoft Defender **Aplikasi Awan**

Microsoft Defender untuk aplikasi awan dibangun di atas kerangka kerja yang menyediakan kemampuan berikut:

- Menemukan dan mengendalikan penggunaan Shadow IT, identifikasi aplikasi awan serta layanan IaaS dan PaaS yang digunakan oleh organisasi.
- Melindungi informasi sensitif, memahami, mengklasifikasikan paparan informasi sensitif apabila tidak digunakan.
- Melindungi dari ancaman dan anomali dunia maya, mendeteksi perilaku tidak biasa di seluruh aplikasi awan untuk mengidentifikasi ransomware, penyusupan pengguna atau aplikasi jahat yang berisiko tinggi dan memulihkan.
- Menilai kepatuhan aplikasi awan, menilai apakah memenuhi persyaratan kepatuhan yang relevan ataukah tidak.

Aplikasi office 365 untuk keamanan awan adalah subset dari Microsoft Defender yang memberikan peningkatan visibilitas dan kontrol untuk office 365. Cakupannya berupa mendeteksi ancaman berdasarkan log aktivitas pengguna, penemuan shadow IT aplikasi, mengontrol izin aplikasi, serta menerapkan kontrol akses. Portal Microsoft 365 Defender adalah ruang kerja khusus yang dirancang untuk memenuhi kebutuhan tim keamanan dan memberikan wawasan yang dapat ditindaklanjuti untuk membantu mengurangi risiko dan melindungi real digital. Portal Microsoft 365 Defender memungkinkan admin menyesuaikan panel navigasi untuk

memenuhi kebutuhan operasional harian. Admin dapat menyesuaikannya untuk menampilkan atau menyembunyikan fungsi dan layanan berdasarkan preferensi khusus pengguna.

5.3.5. Perbedaan Microsoft 365 Defender dan Microsoft Defender for Cloud

Terdapat skor aman untuk Microsoft 365 Defender dan Microsoft Defender for cloud, tetapi memiliki peran yang berbeda. Keamanan skor di Microsoft Defender untuk awan adalah ukuran postur keamanan langganan Azure pengguna. Sedangkan di Microsoft 365 Defender ukuran postur keamanannya berada di organisasi tepatnya di seluruh aplikasi, perangkat dan identitas pengguna. Skor aman menyediakan daftar langkah yang dapat diperoleh untuk meningkatkan skor pengguna. Langkah – langkah tersebut disebut sebagai tindakan peningkatan di Microsoft 365 Defender. Pada Microsoft Defender for Cloud, skor dinilai untuk setiap langganan. Sehingga langkah – langkah yang dapat diambil untuk meningkatkan skor disebut rekomendasi keamanan dan dikelompokkan ke dalam kontrol keamanan.

5.4. Studi Kasus Bidang Kesehatan Menggunakan Platform Komputasi Awan

Sebagian besar penerapan komputasi awan untuk bidang kesehatan di Indonesia masih tergolong baru, namun teknologi tersebut sudah digunakan di negara – negara maju. Indonesia perlu adanya edukasi serta pelatihan – pelatihan ke pengguna lokal untuk mengantisipasi adanya kekhawatiran tentang masalah keamanan dan privasi. *CT – Scan* salah satu contoh di bidang kesehatan yang mendapat dukungan dari perkembangan teknologi informasi, karena dapat menggambarkan struktur bagian dalam tubuh manusia yang hasilnya dapat disimpan sebagai data elektronik dan dilihat di layar komputer.

5.4.1. CCG NHS

CCG NHS

Pada tahun 2019, Grup Komisi Klinis (CCG) NHS terlibat dengan Intelogi untuk menyiapkan sistem manajemen tempat tidur dalam memperkirakan kebutuhan sumber daya secara akurat. Intelogi adalah mitra Microsoft yang berada di Inggris dan mengkhususkan diri dalam Microsoft 365 dan SharePoint dengan praktik yang didedikasikan untuk membangun solusi kustom menggunakan SharePoint, PowerApps, Flow, Power BI & Azure. Dengan keahlian yang dimiliki dapat memberikan solusi yang membantu setiap organisasi untuk menghindari jebakan yang umum terjadi pada proyek otomatisasi alur kerja. CCG NHS adalah organisasi yang dibentuk oleh Health and Social Care Act of 2012 untuk mengatur pemberian layanan NHS di Inggris. Dengan layanan teknologi informasi dan komunikasi (ICT) Hertfordshire, Bedfordshire dan Luton (HBL)

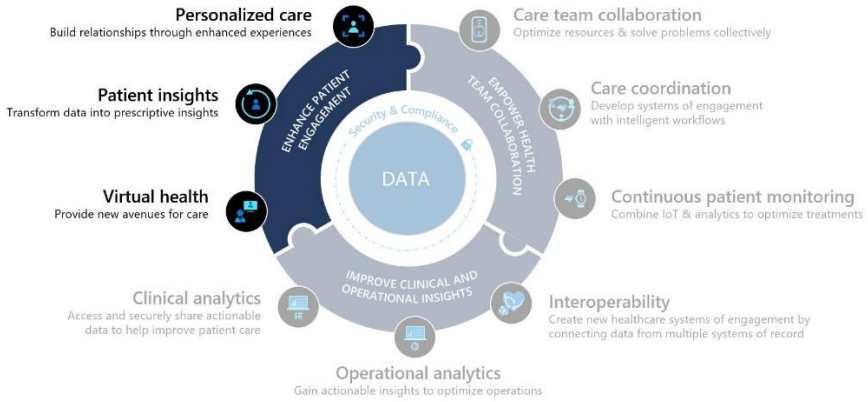
memungkinkan NHS dengan cara kerja yang aman, inovatif dan terjamin menggunakan layanan dan solusi TIK berbasis awan terbaru. Dalam memperkirakan staf, layanan, dan ketersediaan sumber daya secara aman dan akurat di antara klinik dan rumah sakit lokal, CCG NHS melibatkan Intelogi untuk membangun dan mengimplementasikan aplikasi yang dibangun melalui Microsoft SharePoint. Contohnya, seorang dokter NHS memutuskan lokasi mana yang harus ditempati oleh pasien tersebut dengan keinginan dari pasien seperti kelas VIP dan staf NHS pastinya harus segera mengidentifikasi dengan layanan yang dibutuhkan pasien. Sehingga perlu adanya pemantauan tempat tidur yang tersedia, pemulangan potensial, akses perawatan darurat, ketersediaan layanan dan juga jadwal. Secara historis, masing – masing CCG yang relevan memiliki satu titik kontak yang akan menelpon setiap klinik tertentu untuk mengetahui ketersediaan tempat tidur dan layanannya. Tugas manual tersebut memakan waktu sehari – hari petugas kesehatan dan membutuhkan waktu berjam – jam bagi staf dengan penerimaan telepon yang harus secara lisan menjelaskan keadaan klinik. Masalahnya akan lebih rumit apabila adanya staf yang terbatas untuk menjawab panggilan untuk memberikan pembaruan secara akurat terutama selama waktu sibuk ketika pengauditan belum dilakukan sebelum panggilan. Sehingga, HBL ICT memanfaatkan platform online di mana antara klinik tertentu dan rumah sakit dapat dengan mudah dan aman dalam memperbarui status layanan, ketersediaan ruangan (tempat tidur pasien), dan kemungkinan pemulangan (bagi pasien telah pulih). Solusi yang lainnya yaitu bagaimana pemberian akses ke data historis dalam memberikan fasilitas tren dan perkiraan sehingga dapat mengakses dasbor yang menarik dan mudah digunakan namun membutuhkan pelatihan yang minimal agar tidak kesulitan dalam penggunaannya. Dengan memanfaatkan SharePoint, Intelogi mampu membuat masukan konten menjadi tugas yang cepat dan sederhana bagi administrator klinik. Semua data dengan mudah dimasukkan ke dalam satu formulir dengan nama bidang dan pertanyaan yang jelas, langsung dari beranda organisasi, dan hanya membutuhkan waktu kurang dari satu menit untuk menyelesaikannya. Staf NHS dalam CCG dapat memberi mereka gambaran yang akurat tentang tempat tidur dan layanan yang tersedia untuk membantu mereka memutuskan dengan cepat dan tepat sehingga memberikan perawatan yang terbaik kepada pasien. Kemampuan untuk memperkirakan kebutuhan akan sumber daya dan staf tambahan sangat penting untuk kelancaran operasi yang tidak sebatas terhadap pasien tetapi juga untuk staf yang mungkin akan terbebani jika tidak memiliki sumber daya memadai. CCG telah memperluas jumlah pengguna dan mengembangkan solusi menjadi sistem bisnis yang dapat diandalkan. Lebih banyak organisasi mitra dalam kelompok yang lebih besar dan mengadopsi aplikasi karena mereka melihat organisasi lain mendapatkan manfaat dari penggunaan sistem tersebut.

5.4.2. Penjangkauan Pasien di Microsoft Cloud Kesehatan

Aplikasi penjangkauan pasien berfokus pada manajemen banyaknya pasien yang membantu mengatur dan mengotomatiskan pemasaran dan komunikasi dengan pasien. Hal ini sangat membantu penyedia layanan kesehatan dalam menjangkau pasien dengan pemberian target yang efisien. Penyedia dapat memilih layanan melalui email, teks, surat biasa atau kombinasi dan memberikan informasi kesehatan kepada sekelompok pasien dan anggota masyarakat tertentu. Kemampuan utama dari penjangkauan pasien meliputi beberapa hal berikut:

- Segmentasi pasien dibuat berdasarkan kumpulan data dan informasi efektivitas perawatan kesehatan (Healthcare Effectiveness Data and Information Set - HEDIS) standar industri untuk menyediakan kelompok pasien dasar.
- Kampanye keterlibatan pasien dengan membuat email khusus perawatan kesehatan yang menggunakan segmen pasien berdasarkan standar industri HEDIS.
- Manajemen acara, menggunakan templat manajemen penyedia, administrasi dan pendaftaran.

Penjangkauan pasien berfokus pada skenario prioritas tingkatkan keterlibatan pasien dengan menciptakan komunikasi yang dipersonalisasi berdasarkan wawasan pasien.

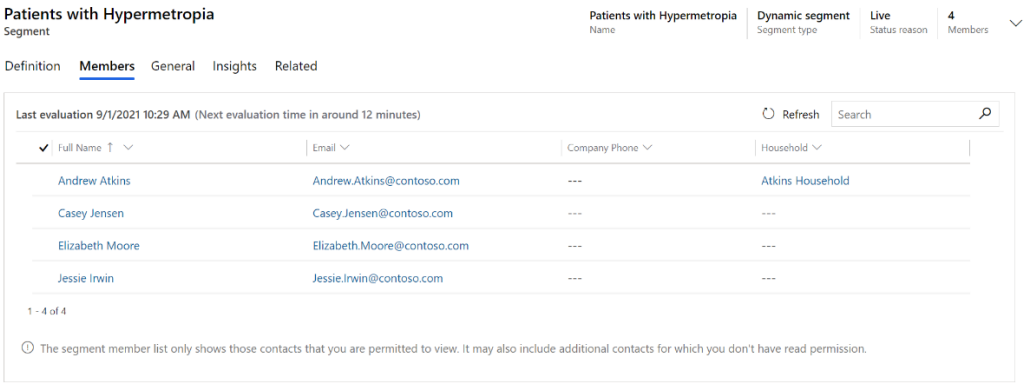


Penjangkauan Pasien di **Microsoft Cloud Kesehatan**

Ada sebuah studi kasus tentang kesehatan Elizabeth Moore, dimana Ia melakukan pemeriksaan tahunan tepatnya di awal tahun. Elizabeth mengetahui bahwa dia menderita hipermetropia yang menyebabkan kondisi mata yang umum pada orang dewasa di mana objek di dekatnya buram. Sebuah perusahaan kesehatan sejenis rumah sakit telah melihat masuknya pasien yang menderita hipermetropia dan memutuskan untuk meningkatkan upaya penjangkauan pasien dengan menyelenggarakan virtual pemasaran. Seperti yang diketahui bahwa perlu dilakukan sebuah aktivitas yang membutuhkan peran Microsoft Cloud.

1. Membuat segmen pasien, dalam proses membuatnya digunakan aplikasi Patient Outreach di Microsoft Cloud for Healthcare untuk mengelompokkan pasien ke dalam kelompok berdasarkan karakteristik yang serupa sehingga mereka dapat lebih tepat sasaran dengan

pengkomunikasian. Sasarannya yaitu penderita hipermetropia (kondisi penglihatan di mana objek di dekatnya terlihat tidak jelas). Langkah awalnya harus membuat sebuah aplikasi pemasaran melalui PowerApps dan apabila telah terbuat segmentnya. Maka pasien atau perawat kesehatan perlu melakukan pengisian data berupa pemilihan status di mana harus disetel ke status aktif. Selanjutnya menambahkan entitas terkait seperti kondisi dari pasien tersebut lalu di simpan. Nantinya dapat memilih sebuah tab anggota yang nantinya akan memperlihatkan nama pasien yang telah ditambahkan ke segmen dinamis.



Penjangkauan Pasien di **Microsoft Cloud Kesehatan**

2. Membuat pemasaran email, penggunaanya diperuntukkan menjangkau segmen pasien yang menderita hipermetropia. Email pemasaran membantu untuk berkomunikasi langsung dengan pasien yang berada di segmen tertentu. Di aplikasi penjangkauan pasien tersebut nantinya akan ada sebuah fitur email pemasaran dan memilih undangan via email dengan segmen yang sesuai dengan seminar yang akan diadakan. Nantinya dapat mengedit teks email seperti tanggal, judul seminar, deskripsi untuk mengundang pasien yang menderita penyakit yang dialami tersebut. Selain teksnya dapat dilakukan penambahan gambaran agar membuat ketertarikan kepada pasien penderita untuk mengikutinya. Setelah selesai melakukan pengeditan haruslah disimpan dan ditayangkan agar langsung sampai kepada email pasien penderita hipermetropi tersebut.
3. Membuat perjalanan pasien seperti proses pengobatan atau memperluas wawasan pasien penderita hipermetropia. Dapat membantu organisasi layanan kesehatan dalam memandu anggota segmen yang dipilih melalui proses komunikasi. Penyelesaiannya dengan menggunakan pesan otomatis, pembuatan aktivitas, poin keputusan interaktif dan banyak lainnya. Di aplikasi penjangkauan pasien tersebut ada sebuah fitur eksekusi pemasaran. Bisa ditambahkan untuk membuat perjalanan baru bagi pasien dan dapat melakukan penyetelan agar dapat dilihat oleh siapa saja. Setelah dibuat bisa di kirim ke email kepada pasien yang telah di beri akses melalui menu kontekstual dan disimpan. Marketing dinamis 365 akan menyalin perjalanan ke layanan pemasaran emailnya yang akan memulai perjalanan dengan memproses kontak, melakukan tindakan dan mengumpulkan hasil selama waktu yang diatur

untuk dijalankan. Setelah itu dapat dilakukan pengumpulan metrik dan wawasan utama dari sebuah catatan. Informasi ini akan tersedia pada waktu yang didasarkan pada tanggal dan waktu yang dipilih untuk memulai perjalanan pasien. Dapat dilakukan pengembalian untuk melihat hasil jika belum tersedia.

4. Membuat pemasaran acara virtual yang berfokus pada perawatan kesehatan yang sesuai dengan pasien penderita. Mengirim undangan acara seminar seperti mata sehat kepada semua orang di segmen pasien. Fitur manajemen pemasaran membantu mulai dari perencanaan dan penganggaran awal hingga promosi dan publikasi, pendaftaran peserta, siaran webinar (link meet), analisis akhir, perolehan prospek dan evalusasi. Di aplikasi penjangkauan pasien terdapat fitur acara dan tambahkan acara baru dengan memasukkan detail acaranya. Harus dipastikan juga bahwa pemasaran acara virtual di sesuaikan dengan bidang yang akan dilaksanakan acaranya. Setelah itu disimpan dan URL meetnya akan terlihat oleh pasien yang menderita sakit sesuai dengan topik acaranya dan dapat mengaksesnya melalui fitur yang disediakan atau yang terlihat oleh pasien atau pengguna.

Dengan demikian, Elizabeth Moore dapat melakukan konsultasi juga mengikuti acara virtual yang diadakan agar dapat menambah wawasan dalam proses perjalanan penyembuhan penyakit yang dialami olehnya. Sehingga dengan mudahnya tanpa harus bepergian untuk melakukan konsultasi dan untuk mengikuti acara, dia bisa mendapatkan fasilitas yang memadai melalui platform yang disediakan baik bagi tim kesehatan maupun pasien penderita. Macam – macam penyakit pun sudah di spesifikasikan dengan pasien penderitanya sehingga tidak tergabung dengan pasien penderita lain. Serta mudah bagi tim kesehatan untuk melakukan pemasaran atau broadcast terkait dengan penyakit tertentu.

DAFTAR PUSTAKA

Microsoft Security, Compliance, and Identity Fundamentals: Describe the capabilities of Microsoft security solutions - Learn | Microsoft Docs

Azure security baseline for Microsoft Defender for Cloud | Microsoft Docs

Azure Sentinel Pricing | Microsoft Azure

Microsoft 365 Defender | Microsoft Docs

Microsoft Cloud for Healthcare | Microsoft

Azure for Healthcare – Use Case | Microsoft Azure

NHS Clinical Commissioning Group engages with Intelogy to set up a bed management system to accurately forecast resource needs using Microsoft 365 - Microsoft Tech Community Resource Center (resources-techcommunity-microsoft-com.translate.goog)

Patient outreach in Microsoft Cloud for Healthcare - Learn | Microsoft Docs