

# Managed Network & Security Services

Mengelola jaringan yang kompleks dengan tetap mengutamakan *security* merupakan tantangan yang dihadapi perusahaan. Sering kali perusahaan harus bekerjasama dengan lebih dari satu *partner* dengan tingkat layanan yang berbeda. Ketika terjadi masalah, perusahaan harus mengidentifikasi dari mana sumber masalah tersebut, dan *partner* mana yang harus dihubungi.

*Managed Network & Security Services* merupakan layanan untuk mengelola jaringan perusahaan secara *end-to-end* mulai dari layanan network hingga perangkat perusahaan/CPE, dari *data center*, WAN hingga ke LAN, termasuk *data security* guna kelangsungan bisnis perusahaan. Solusi ini diantaranya **Managed Network Services MNS** (meliputi layanan MNS WAN dan MNS Cloud WLAN), **Managed Security Services** (meliputi layanan Security Operation Center dan Network & Web Application Security), serta **Security Consulting**.

Ruang lingkup layanan dapat disesuaikan berdasarkan kebutuhan dan skala bisnis perusahaan.

## Managed Network Services (MNS)

Mengelola *network* yang kompleks menjadi tantangan bagi bisnis perusahaan. Solusi *Managed Network Services* dapat memenuhi semua kebutuhan *network* perusahaan, yang meliputi *MNS Wide Area Network (WAN)* serta *MNS Cloud Wireless LAN (WLAN)*. Ruang lingkup layanan ini dapat disesuaikan berdasarkan kebutuhan perusahaan.

### MNS Wide Area Network (WAN)

*MNS Wide Area Network (WAN)* merupakan layanan pemantauan dan pengelolaan jaringan perusahaan secara *end-to-end* pada *network device* dan *carriage* secara proaktif dan cepat.

#### Fitur

- *CPE Services*, meliputi pemesanan, instalasi, pemeliharaan *hardware*.
- *Service Desk Support*, fasilitas *Single Point of Contact* untuk panggilan lokal maupun internasional.
- *Self-Service Customer Portal*, untuk *monitoring* status layanan.
- *Service Assurance*, jaminan layanan seperti *event monitoring*, notifikasi insiden, laporan gangguan secara *online*, dan *update* status layanan.
- *Reporting*, laporan performansi jaringan berbasis *web (availability & utilization)*.

#### Manfaat

- Meningkatkan produktivitas bisnis perusahaan.
- Mempercepat penyelesaian gangguan.

### MNS Cloud Wireless LAN (WLAN)

*MNS Cloud Wireless Local Area Network* merupakan layanan pengelolaan jaringan *wireless* berbasis *cloud*, sehingga dapat melakukan perubahan konfigurasi *Access Point* kapan & dimana saja walaupun tidak berada di lokasi *private network* perusahaan.

#### Fitur

- *High availability & disaster recovery*
- *Redundancy & service security*
- *Sign on mechanism*
- *Single management dashboard*

## Managed Security Services

Beragamnya teknologi IT saat ini telah memberikan tantangan kepada perusahaan, bagaimana menjaga *security* dan melakukan mitigasi resiko terhadap data dan informasi perusahaan. Solusi *Managed Security Services* memberikan kombinasi layanan *security* dan *data analytics*, lengkap dengan tim yang *expert* di bidang ini, yang meliputi *Security Operation Center* serta *Network & Web Application Security*. Ruang lingkup layanan ini dapat disesuaikan berdasarkan kebutuhan perusahaan.

### Security Operation Center

*Security Operation Center (SOC)* merupakan layanan pusat pengendalian pengamanan, *monitoring* dan analisa serangan *security* baik terhadap infrastruktur dan aplikasi secara *logical* maupun *physical*. SOC juga secara proaktif dan responsif melakukan penanganan insiden *security*.

#### Fitur

- *Monitoring logical attack & CCTV*
- *End to end monitoring dashboard*
- *Threat intelligence*
- *Correlation Engine/SIEM (Security Information & Event Management)*
- *Automated respond*

#### Manfaat

- Manajemen log dan *surveillance* selama 24x7.
- Meningkatkan keamanan IT perusahaan dengan mendeteksi dan merespon ancaman dan serangan sebelum berdampak terhadap bisnis.
- *Compliance* terhadap standar keamanan informasi internasional.
- Peringatan dini terhadap insiden *cyber security* sehingga mempercepat pemulihan ketika insiden terjadi.

### Network & Web Application Security

Jumlah *cyber attack* semakin meningkat, potensi kerugian yang bisa dialami adalah kehilangan *customer*, rusaknya *brand image*, *service outage* hingga pencurian data *confidential*. Solusi layanan *Network & Web Application Security* dengan berbagai macam opsi bisa dijadikan alternatif solusi berdasarkan kebutuhan bisnis Anda.

#### A. Global Internet Security

Melindungi infrastruktur IT perusahaan dari serangan *Distributed Denial of Service (DDoS)*, dimana arus lalu lintas internet dipantau untuk mendeteksi serangan dengan membandingkan lalu lintas normal dan memeriksa *header* paket.

### Fitur

- Perlindungan aplikasi, mitigasi serangan volumetrik terhadap layer 3 atau 4.
- Perlindungan jaringan, pemantauan lalu lintas internet untuk mendeteksi anomali.

### Manfaat

- Cakupan domestik dan global yang luas, lengkap dengan beberapa pusat *scrubbing* yang tersebar di seluruh dunia.
- *Portal monitoring*, kemudahan untuk mengawasi aktivitas pencegahan dan penganggulangan ancaman melalui *web portal* terintegrasi.
- Tersedianya bantuan *service desk* selama 24/7.
- *Low latency*, fitur *security* lengkap yang tidak menyebabkan *delay* untuk proses bisnis perusahaan.

## B. Web Application Protector

Melindungi aplikasi bisnis perusahaan dari ancaman serangan baik di tingkat jaringan maupun aplikasi yang terletak di *Data Center* atau *Cloud*.

### Fitur

- *Global Cloud Platform, platform cloud delivery* untuk memaksimalkan perlindungan.
- *DDoS Protection*, melindungi aplikasi dari serangan DDoS dengan menghentikan serangan diawal untuk minimalisasi *downtime*.
- *Application Firewall, firewall web* untuk melindungi aplikasi secara otomatis.
- *Automatic Updates*, sistem perlindungan *diupdate* secara berkala dan otomatis.
- *Virtual Vulnerability Patch*, melakukan penambalan *virtual* untuk celah keamanan di aplikasi.
- *HTTPS Protection*, dengan sertifikasi *Secure Sockets Layer (SSL)*.
- *High Uptime & Availability*, dengan ketahanan dan kemampuan perbaikan menunjang *uptime* dan *availability* sangat tinggi.
- *Best Route*, dilengkapi dengan fitur untuk menemukan rute terbaik di jaringan menuju aplikasi perusahaan.

### Manfaat

- *Easy to setup*, hanya dengan beberapa klik perlindungan sudah bisa diaplikasikan.
- *Easy to manage*, tidak memerlukan petugas khusus untuk melakukan pembaruan dan *setting* perlindungan.
- *Secure to operate*, melindungi aplikasi dari serangan keamanan sehingga mengurangi resiko *downtime* dan pencurian data.

### C. Next Gen Firewall

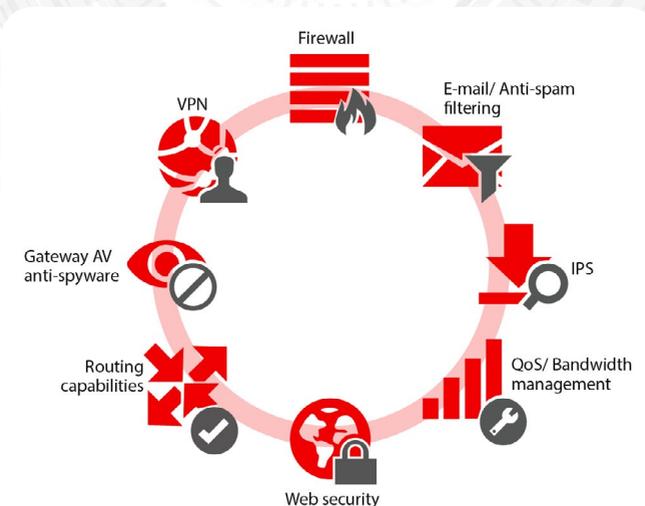
Layanan sistem keamanan *cyber* berupa *firewall* terintegrasi, *intrusion protection* untuk menjaga keamanan *network* melalui satu perangkat. Solusi ini meliputi *provisioning, distribution, design, installation, maintenance* dan *attack monitoring*. Disediakan juga laporan secara periodik yang memicu *alert* jika terjadi serangan.

#### Fitur

- *Firewall*, *blocking* trafik mencurigikan dan *malware* dengan cepat.
- *Intrusion Protection Service*, *blocking* trafik serangan yang berhasil menembus *firewall*.
- *Content Security Web Protection*, mencakup *anti virus* dan *web filtering*.
- *Advanced Threat Protection*, mencakup perlindungan lebih *secure* dan melindungi *mobile* akses juga.

#### Manfaat

- *Simplify Security*, sistem keamanan *up to date* sehingga mengurangi pekerjaan administrasi dan meningkatkan keamanan.
- *Cut Complexity*, layanan terkonsolidasi dengan fungsi lengkap yang memberikan kemudahan pengelolaan dan *monitoring* layanan.
- *Faster Problem Solution*, didukung oleh *service desk* untuk penyelesaian gangguan dan *proactive maintenance*.
- *Reduce Risk*, layanan yang sudah terbukti efektif menangani ancaman terhadap kegiatan bisnis sehari-hari.
- *Threats Protection*, perlindungan yang canggih terhadap ancaman untuk melindungi aset perusahaan.
- *Complete IT Control*, pengendalian dan visibilitas *end-to-end* pada semua layanan melalui *customer portal*.



### Layanan *Network & Web Application Security* sangat cocok bagi:

- Perusahaan yang memiliki kantor cabang dan *end-user* yang harus dilindungi.
- Perusahaan yang memiliki perhatian khusus pada kelangsungan dan keamanan bisnis dari ancaman serta serangan.
- Perusahaan yang ingin meningkatkan kendali pada sistem keamanan.
- Perusahaan yang ingin mengganti perangkat keamanan.
- Perusahaan yang cenderung ingin mengimplementasikan teknologi baru yang berdampak pada bisnis operasional di internal dan eksternal.

## Security Consulting

*Security Consulting* merupakan solusi layanan konsultasi untuk membantu perusahaan mendapatkan solusi terdepan pada sistem keamanan untuk melindungi bisnis perusahaan dari ancaman keamanan siber. Solusi ini meliputi *Cloud Network Design*, *Cloud Risk Assessment*, *Cyber Security Health Check*, *Network Architecture Assessment*, *Network Compliance Assessment*, *Penetration Testing*, dan *Vulnerability Assessment*.

### A. *Cloud Network Design*

*Cloud network design* membantu perusahaan melengkapi desain *cloud network* secara *high-level* sesuai kebutuhan, dengan menggunakan standar industri, praktek terbaik dan relevan.

### B. *Cloud Risk Assessment*

*Cloud risk assessment* membantu perusahaan mengidentifikasi dan menilai resiko terkait dengan infrastruktur *cloud*, selanjutnya menemukan tindakan korektif yang diperlukan untuk meningkatkan keamanan *cloud*.

### C. *Cyber Security Health Check*

*Cyber security health check* membantu perusahaan memahami potensi serangan dan kelemahan, cara kerja baru dan bagaimana mengidentifikasi serta memprioritaskan kegiatan untuk menurunkan resiko keamanan.

### D. *Network Architecture Assessment*

*Network architecture assessment* menilai dan mendokumentasikan desain arsitektur *network* perusahaan untuk defisiensi keamanan, kesenjangan terhadap *compliance*, serta kompleksitas yang tidak perlu.

### E. *Network Compliance Assessment*

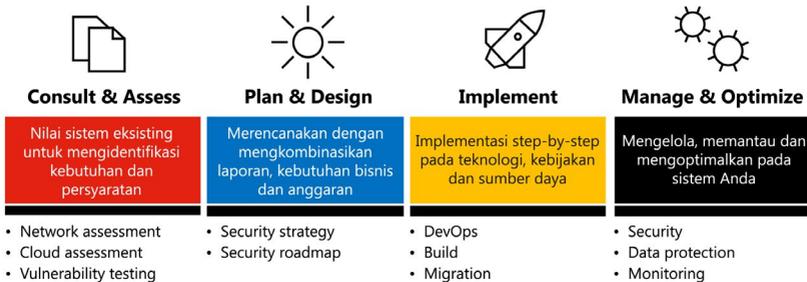
*Network compliance assessment* memberikan rekomendasi strategis pada *network compliance* dengan menganalisa jaringan untuk menentukan perbedaan terhadap kebutuhan *security compliance*, regulasi dan standar industri.

## F. Penetration Testing

*Penetration testing* (atau biasa disebut '*ethical hacking*') memberikan konsultasi keamanan untuk mengeksploitasi dan identifikasi tingkat keamanan pada infrastruktur dan aplikasi perusahaan untuk mengurangi resiko jika terjadi serangan di dunia maya serta untuk menjaga dari ancaman dan kerentanan baru.

## G. Vulnerability Assessment

*Vulnerability assessment* mengeksploitasi kelemahan, bagaimana mengurangi upaya, waktu dan biaya dalam menjaga jaringan dan memberikan rekomendasi pada kelemahan yang teridentifikasi pada infrastruktur perusahaan.



## Manfaat

- Perusahaan mendapatkan *insight* untuk memitigasi kelemahan infrastruktur dan aplikasi IT eksisting yang digunakan perusahaan.
- Meningkatkan sistem keamanan perusahaan dan memastikan sistem keamanan sesuai standar industri dan peraturan pemerintah.