EMTEL
business

Empowering your business with Next-Gen Security

Managed Security Solution

Value driven Secure Reliable

THE CYBER SECURITY LANDSCAPE

In today's digital age, cyber threats are becoming increasingly sophisticated and frequent, posing a significant risk to businesses and individuals alike. These threats come in many different forms and can cause a wide range of harm, from stealing personal data to disrupting critical infrastructure, with more and more of our personal and business activities taking place online. Therefore it is crucial to implement a robust cyber security framework that covers all aspects of your digital infrastructure.

Why Cyber Security is Important

The need for cyber security cannot be overstated. Here are some reasons why cyber security is crucial for businesses.

Protect Your Data: Cyber security protects your data from unauthorised access, theft, and other cyber threats.

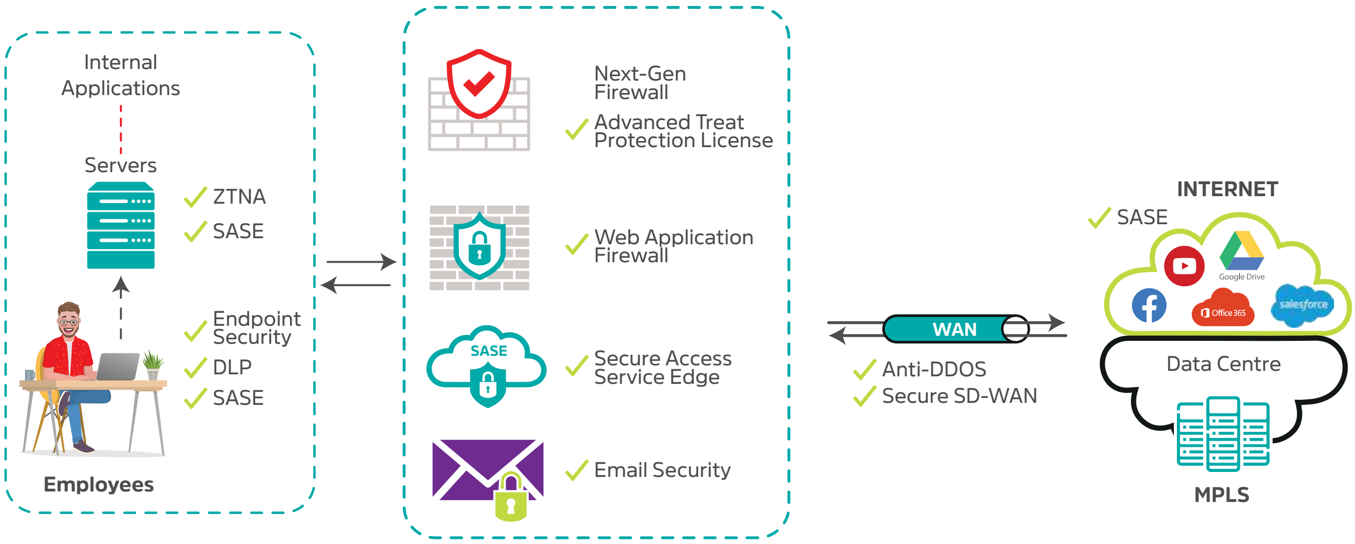
Avoid Financial Loss: Cyber-attacks can cause financial loss through data breaches, ransomware, and other cybercrimes.

Maintain Reputation: A cyber-attack can damage your brand reputation, making it difficult to win back customers' and other stakeholders' trust.

Meet Compliance Requirements: Many industries have compliance requirements for cyber security. Compliance ensures that you are following best practices to protect your data.

At Emtel Business , we provide cyber security solutions that cover multiple layers in order to meet your specific needs. It is not uncommon for enterprises to concentrate their security efforts on a single entry point, which can leave vulnerabilities that hackers can exploit with ease. It is therefore fundamental to secure your entire infrastructure to minimise risk and prevent potentially disastrous outcomes.

Security Architecture and Solution Portfolio



ANTI-DISTRIBUTED DENIAL OF SERVICE (ANTI-DDOS)

STAY ONLINE, STAY PROTECTED

Challenge

DDoS (Distributed Denial of Service) is a type of cyber-attack where a large number of compromised devices, often called a botnet, are used to flood a target website or online service with traffic, making it inaccessible to legitimate users.

DDOS attacks are increasing

Disrupting access to Business's websites, servers, or cloud-based services

Significant efforts & time

Companies need to spend significant time and resources to bring their digital assets online

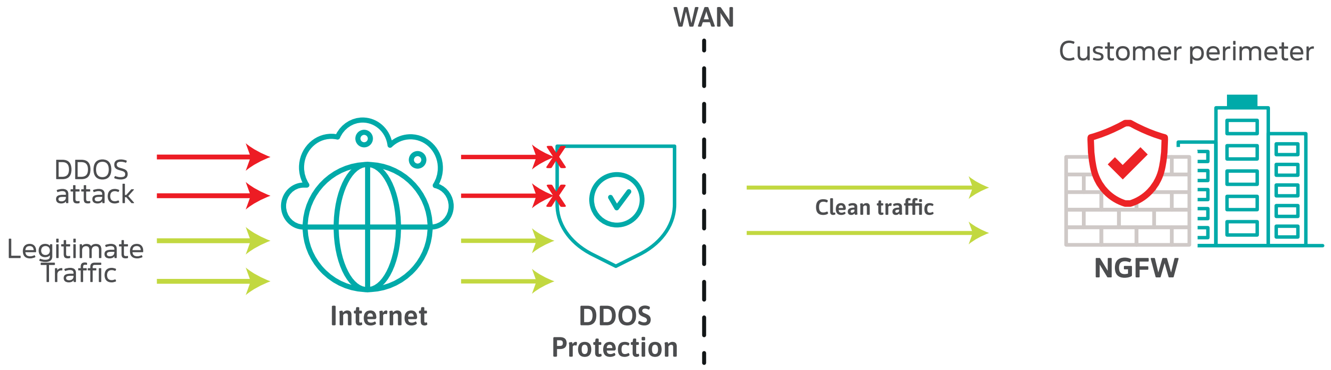
Short term & Long term implications

This includes downtime, loss of revenue, customer churn, legal issues, and more

DDoS - Protection Traffic Flow

All traffic coming from the internet for the tenant who subscribed for the DDoS solution will go through Emtel's detection devices. In case of any attack pattern detected, the malicious traffic is immediately dropped while the rest of the traffic will flow to the customer's network untouched.

The DDoS protection solution prevents saturation of customer internet link and service, by protecting against DDoS attacks only.



Always-On DDoS Protection Solution

- No human intervention required
- Unwanted Traffic are scrubbed immediately
- 100% of subscribed internet capacity will be protected with no additional equipment installed
- Customer portal available to view attacks via dashboard and reports
- Intelligent detection based on attacks patterns

MANAGED NEXT-GENERATION FIREWALL

PREVENT CYBER THREATS AND HAVE GRANULAR CONTROL OVER YOUR NETWORK TRAFFIC

Challenge

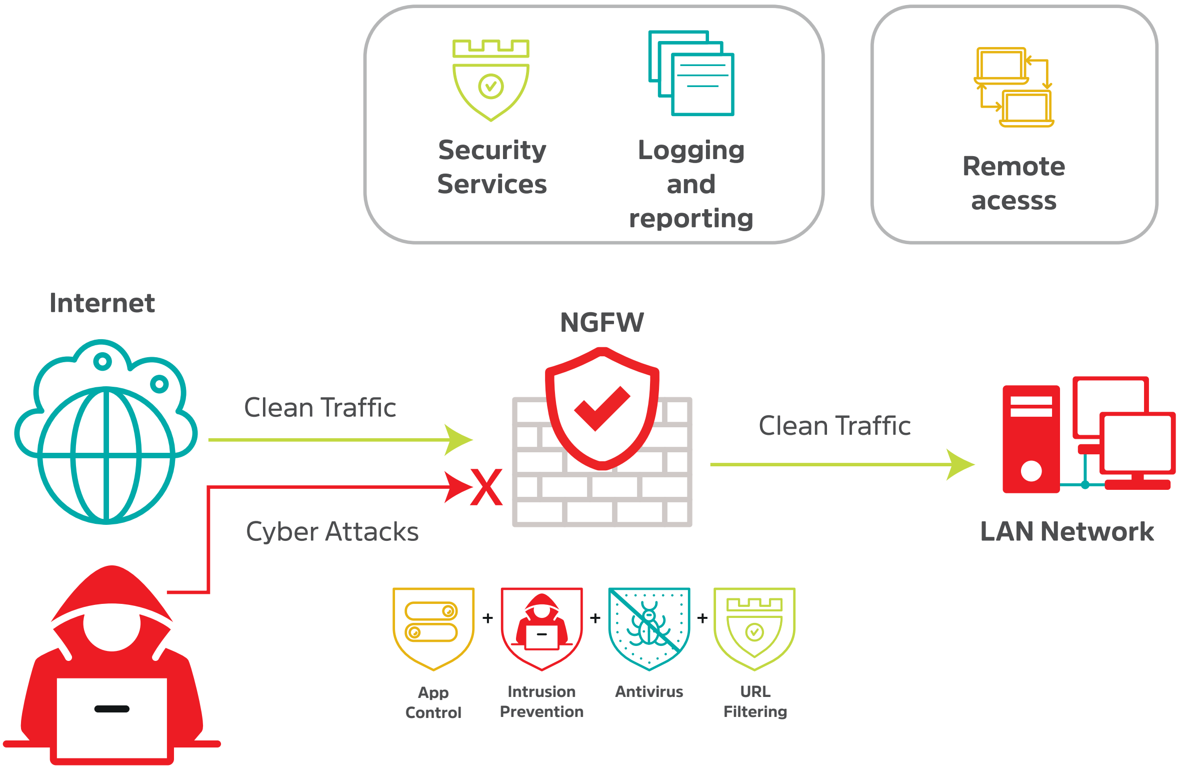
Traditional firewalls which perform packet filtering in terms of source, destination IPs and port blocking basically are vulnerable to higher level attacks since they do not perform a deep packet inspection of the network traffic.

Hence, they cannot be used to fight against the evolving tactics and techniques of hackers and cyber-attacks.

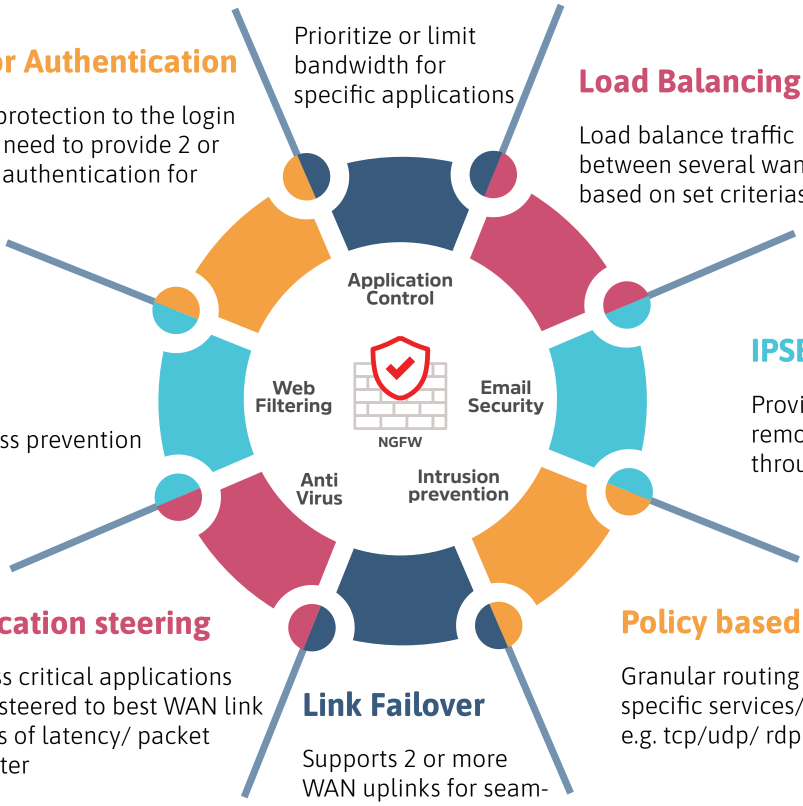
Solutions

Next generation firewalls (NGFWs) offer several benefits, including: Enhanced protection against cyber threats. They can inspect and analyse traffic more comprehensively and deeply than traditional firewalls, which helps them detect and prevent a greater variety of cyber-attacks than a traditional firewall.

NGFWs offer advanced threat detection and prevention capabilities, such as intrusion prevention, malware protection, and behavioural analysis, to help organisations stay ahead of emerging threats and also zero day attacks which was previously not feasible.



NGFW FEATURES AND CAPABILITIES



Traffic Shaping

Prioritize or limit bandwidth for specific applications

Multi-factor Authentication

Extra layer of protection to the login process. Users need to provide 2 or more forms of authentication for identify proof

Load Balancing

Load balance traffic between several wan links based on set criterias

IPSEC

Provide access to other remote sites or WFH through VPN.

DLP

Data loss prevention

Application steering

Business critical applications can be steered to best WAN link in terms of latency/ packet loss/ jitter

Link Failover

Supports 2 or more WAN uplinks for seamless failover in case of a WAN link degradation

Policy based routing

Granular routing in terms of specific services/ port numbers e.g. tcp/udp/ rdp

WHY EMTEL MANAGED FIREWALL?

- Fully managed Design & Installation
- Configuration & Maintenance
- Effective change Management
- Local availability of Stock
- Lower Total cost of ownership
- Single point of contact
- Regular Audit
- Firmware & Patch update

SECURE SD-WAN

SIMPLE, SECURE AND SCALABLE

Challenge

The rise of digital innovation and remote work has led to the emergence of increasingly sophisticated cyber-attacks and risks that traditional WAN solutions are not equipped to handle. Listed below are a few of the primary obstacles that are currently being encountered.

Limited Bandwidth: Traditional WAN networks often have limited bandwidth, which can result in slow application performance and decreased productivity

High Costs: WAN networks can be expensive to operate and maintain, especially when using dedicated MPLS circuits

Lack of Security: Traditional WAN networks may lack the level of security required to protect against today's sophisticated cyber threats

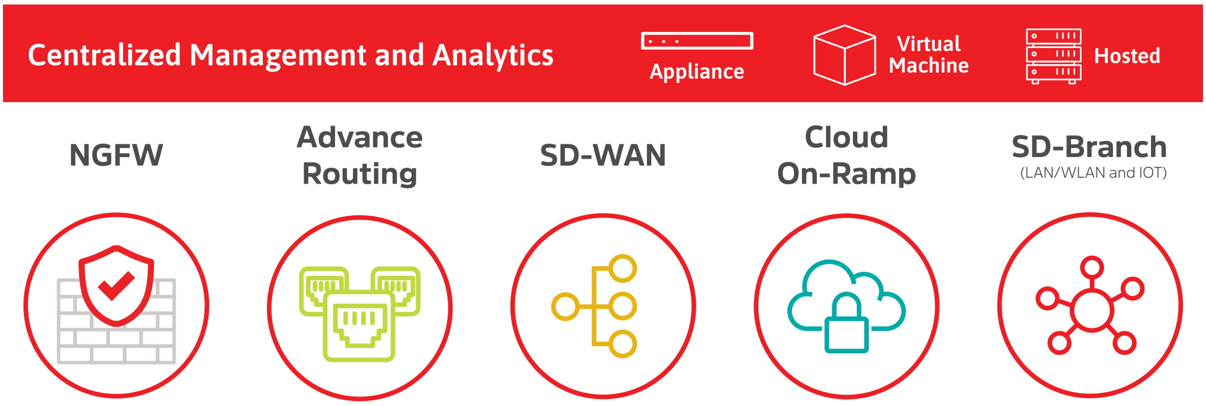
Complex Network Management: Managing a complex WAN network can be a challenge, especially when it involves multiple locations and different service providers

Limited Application Visibility: Traditional WAN networks often lack the visibility needed to identify and resolve application performance issues

Solution

Secure SD-WAN is a software-based solution that provides agile and secure management of enterprise networks. It connects branch offices, data centres, and cloud resources over various network types, ensuring advanced security, application optimisation, and centralised management.

The NGFW is a built-in feature in SD-WAN providing comprehensive security measures and simplifying network management. With Secure SD-WAN, you can optimise network performance and protect data from potential threats.



Centralized Management and Analytics

Appliance

Virtual Machine

Hosted

NGFW

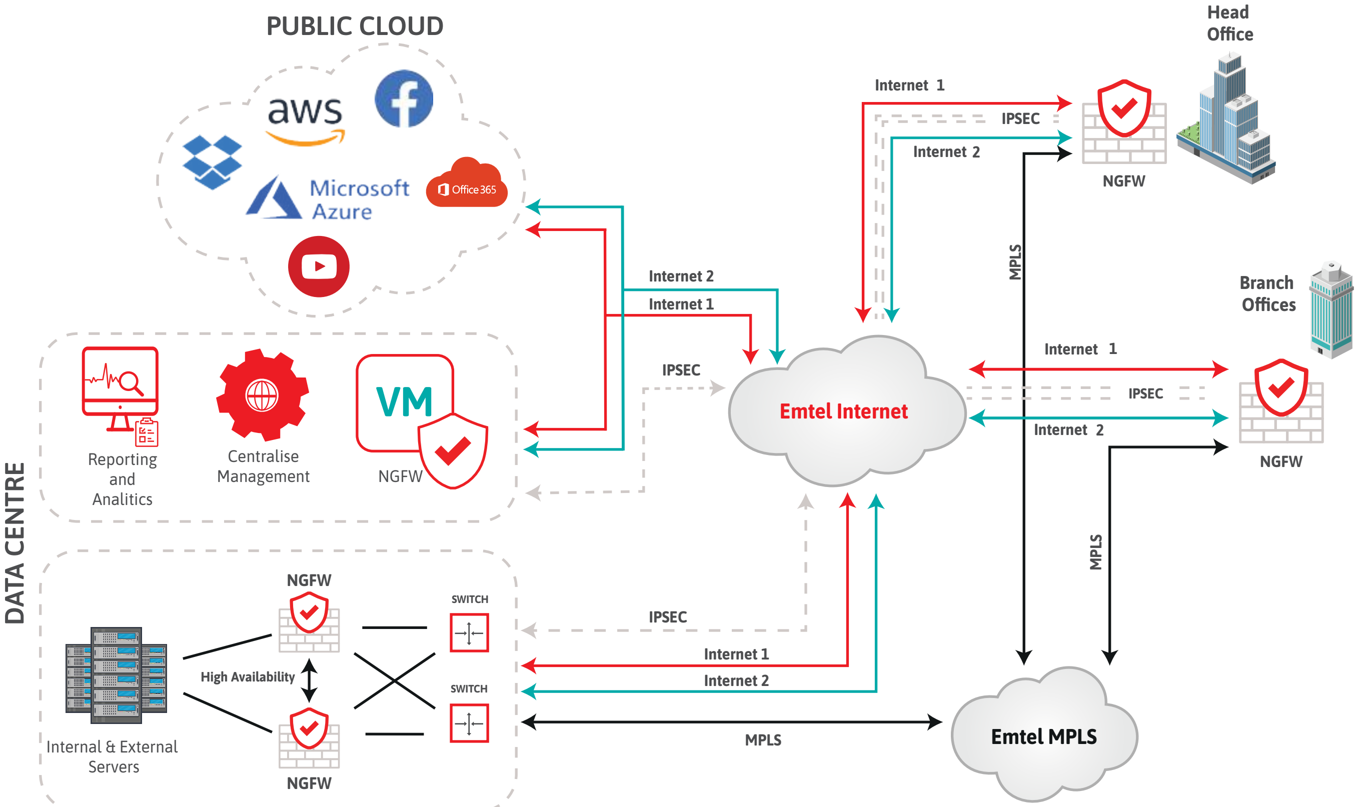
Advance Routing

SD-WAN

Cloud On-Ramp

SD-Branch (LAN/WLAN and IOT)

SD-WAN : USE CASE



Solution brief:

Enhanced security: Enables secure access to applications and services via all available WAN links

Application-aware WAN path control: Automatically direct network traffic along the most suitable paths based on the particular demands of each application

Flexible WAN selection: Achieve maximum business value through intelligent load balancing across multiple WAN links

Direct Internet breakout: Achieve greater agility, security, and cost savings while improving application performance and user experience, through local internet access at branch offices

Redundancy: Provides high availability for redundancy in terms of hardware and connectivity to hub and branch offices

Centralized Management: Single pane-of-glass management for all SD-WAN devices and provides configuration management

Reporting and Analytics: Provides reporting and analytics for all events and threats

Scalable: Solution that can grow and adapt to meet the changing needs of your organisation

WEB APPLICATION FIREWALL

ENHANCE YOUR WEB APPLICATION AND API SECURITY

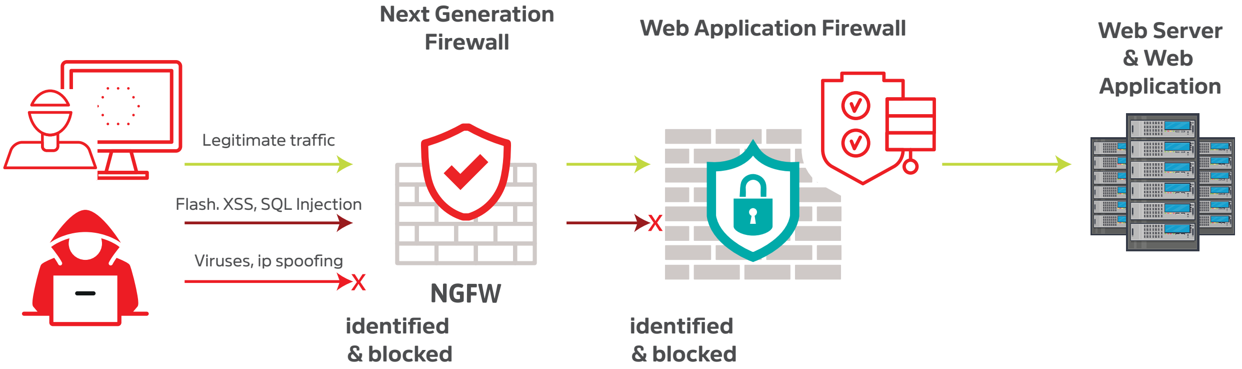
Challenge

Web applications are a primary target for cyber criminals looking to disrupt business operations. Enterprises often host their applications on web servers, which can pose security risks such as SQL injection, XML attacks, and Flash. Next Generation Firewalls may not be enough to protect against these risks.

Solution

A Web Application Firewall (WAF) is specifically designed to protect web applications by analyzing HTTP and HTTPS communication and blocking malicious requests. WAF operates at layer 7 as a reverse-proxy solution, providing an additional layer of security for web servers against known and zero day attacks.

WEB APPLICATIONS FIREWALL: HOW IT WORKS



EMTEL WAF Solution –Benefits in a nutshell

- Machine learning that detects and blocks threats while minimizing false positives.
- Multi-layer protection against the OWASP Top 10 application attacks embedded with machine learning to fight against known and unknown attacks.
- Advanced Bot Mitigation effectively protect web assets without imposing friction on legitimate users.
- Protection for APIs, including those used to support mobile applications.
- Visual analytics tools for advanced threat insights.
- Third-party integration and virtual patching.

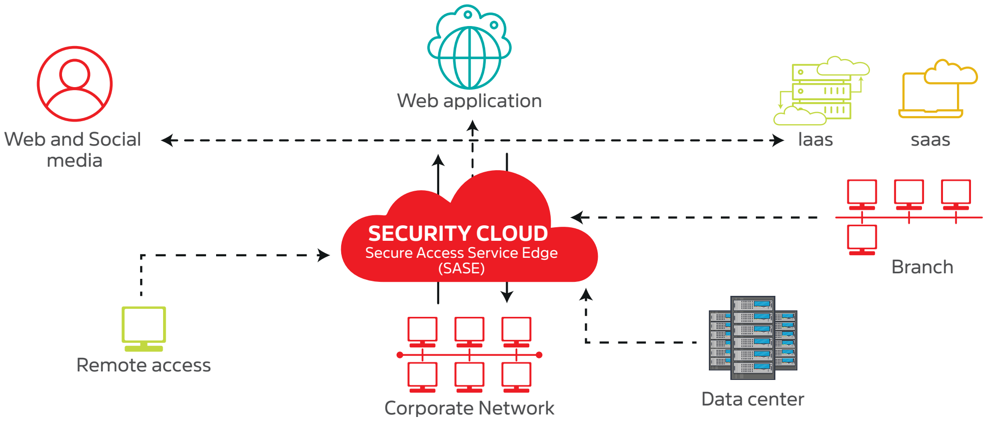
PROTECT DATA AND USERS EVERYWHERE

Challenge

Today's enterprise networks have evolved dramatically since traditional web security tools were first designed and built. Assets are now moving away from a centralised location (Office, Data Centre) to all places in the cloud where applications are hosted and effectively managed.

Solution

Secure Access Service Edge (SASE) is a cloud-native platform that integrates various security capabilities such as secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), and zero trust network access (ZTNA).



Single Platform: Consolidated, cloud-based solution reducing complexity of operations and eliminating need for multiple vendors and consoles.

Protect data and users everywhere: Extend data security and threat protection to users and data, regardless of their location.

No Trade-offs between performance and security: solution provides real-time, cloud-native security without compromising network performance or increasing the risk of security bypass by users.

Scalability: Designed for growth and adapting to your growth in users and traffic volumes.

Use cases

Cloud Security: A financial company uses SASE to secure their cloud apps, prevent data exfiltration, and protect against cloud-based threats.

Remote Workforce Security: A healthcare org uses SASE to ensure secure remote access, enforce strong authentication, and protect against cyber threats while complying with data protection regulations.

Application Access: A tech company uses SASE to provide secure access to cloud and on-premises apps, enforce policies against data leakage and malware attacks, and monitor application usage.

Compliance: An e-commerce company uses SASE to ensure regulatory compliance with GDPR and CCPA, with comprehensive visibility into data flows, detection of policy violations, and enforcement of compliance.

EMAIL SECURITY

DEFEND AGAINST EMAIL-BASED ATTACKS AND KEEP YOUR SENSITIVE DATA SECURE

Challenge

Email is a frequent target of cyber-attacks due to its use in communicating with external parties. Cyber criminals use email as a means to gain control over an organisation, gain access to confidential information, or disrupt IT access to resources.

Malware in email attacks is rising, giving attackers control over an organisation's workstations and servers, and the ability to change privileges, access sensitive information, monitor users' activities, and cause harm.

Solution

Our email security solution protects against various email-based threats. It utilises advanced security technology, to prevent, detect, and respond to email-based threats in real-time.

This solution leverages threat intelligence and behavioral analysis techniques to identify and block emerging and unknown malware threats. It analyses email patterns, sender reputation, and attachment behavior to detect suspicious activity and potential malware.

SECURE INBOUND EMAILS

Phishing/Spear/Whale Phishing
Impersonating
Business Email Compromise
Advanced/Targeted Attacks
Email-based Ransomware Threats
Illicit/Adult Content
Spam

SECURE OUTBOUND EMAILS

Responses to malicious emails
Intentional data exfiltration
Data leak prevention
Email encyption
Man-in-the-middle attacks

DETECT BUILDING BLOCKS

Malicious Content
Malicious Files
Malicious URLs

Deployment Types

Appliance
VM
Cloud

Operation Modes

Gateway
Transparent
Server
API 0365 API

Features and Benefits

Ai-Powered Protection
Protection Against Zero Days
Microsoft 365 Protection
Proven Efficacy
Protection Against Ransomware
Impersonation Detection

ENDPOINT PROTECTION

SAFEGUARD YOUR DEVICES AND DATA

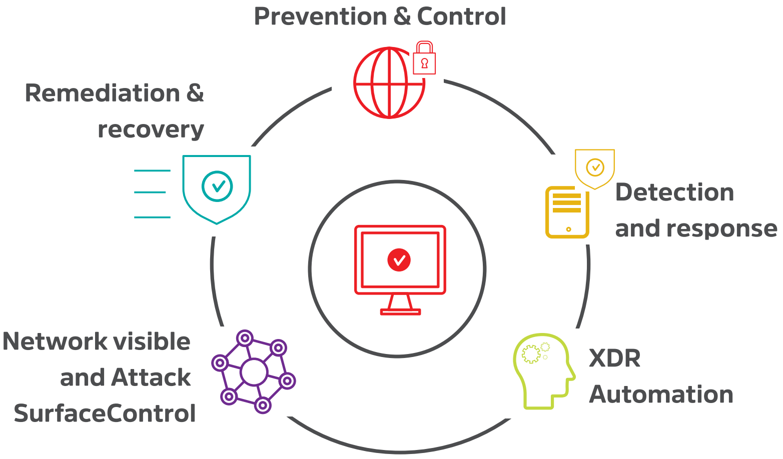
Challenge

Without endpoint protection, organisations face several challenges, including the risk of malware infections, unauthorised access, and data breaches. Malware infections can cause significant damage to endpoints, resulting in data loss, theft, and system failures. Cybercriminals can also gain unauthorised access to endpoints, steal sensitive data, and compromise the organization's overall security.

Solution

Our endpoint protection technology operates autonomously, without requiring human intervention, and can quickly detect and respond to attacks.

The platform can also automatically remediate threats, meaning that it can isolate and contain malicious software or files to prevent further damage to an organisation's systems.



FEATURES

- Autonomous endpoint protection that dentifies, blocks and reacts to attacks on all major vectors
- Uses Artificial Intelligence to eliminate threats in real time automatically for on premise and cloud environments
- Blocks and rollback unknown zero-day attacks/ threats
- Provides visibility into encrypted traffic with no impact on business operation
- Data Reporting of endpoint detection and response

INTEGRATION WITH EMTEL'S MANAGED FIREWALL SOLUTION

- Visibility into network flows, packets and events
- Network Access control, block callback and command-and-control
- Gain Visibility into and block lateral movement of cyber attackers through your network
- Consolidated protection across all types of devices
- Extended network to endpoint visibility and segmentation

Stay focused on your business.
We’ll take care of your cyber security needs.

Our solutions include:

Solution Design and Consultancy
Solutions Configuration and Management
Threat Protection
Security Policy Management
Reporting and Compliance
Vulnerability Assessments
24/7 Monitoring and helpdesk
Remote and Onsite support

Contact us:
emtel.business@emtel.com
www.emtel.com/business