



# Cybersecurity Solutions

SMART helps organizations and businesses achieve the highest possible level of security for their technology assets and information by providing experienced cybersecurity professionals skilled in the latest security technologies and techniques.



# TABLE OF CONTENT

Assessment & Monitoring	3
Assessment & Monitoring Solutions	4
Network Security	5
Network Security Solutions	6
Application Security	7
Application Security Solutions	8
Endpoint Security	9
Email Security	10
Cloud Security	11
Cloud Security Solutions	12
Data Security	13

# Assessment & Monitoring



Identify potential security risks and vulnerabilities.



Review security policies and procedures



Provide recommendations for improving the organization's security posture



Conduct regular security assessments and audits.



Provide ongoing security awareness training for employees.



Conduct penetration testing, vulnerability scanning, and risk assessments



Conduct security awareness training for employees



Continuously monitor an organization's networks and systems for potential security incidents or breaches



Use advanced security tools and platforms, such as firewalls, intrusion detection and prevention systems, and security information and event management (SIEM) solutions



# Assessment & Monitoring Solutions

---

Security Design & Architecture

SOC Analysis L1, L2, L3

Threat detection and Incident response

SIEM security information & events management

MSSP Managed Security Services Provider

Vulnerability & Risk Management

# Network Security



**Network access control services:** Ensure only authorized users and devices can access organizational networks and systems.



**PAM systems:** Manage and monitor privileged accounts.



**Network segmentation:** Divide a network into smaller subnetworks to improve security and reduce the risk of unauthorized access.



**Virtual Private Network (VPN) services:** Provide secure remote access to organizational systems and data.



**Firewall services:** Block unauthorized access to networks



**Intrusion detection and prevention services:** Detect and prevent potential security threats.



**IAM systems:** Ensure only authorized users have access to sensitive information and systems.

# Network Security Solutions

---

NGFW next generation-firewall

IPS intrusion prevention system

VPN Virtual Private Network

NAC Network Access Control

IAM (Identity and Access Management)

CASB (Cloud Access Security Broker)

Load Balancing (LTM , GTM) local & Global traffic

ML Machine learning Firewalls

IDS intrusion detection system

ZTNA Zero-Trust Network Access

PAM (Privileged Access Management)

SASE (Secure Access Service Edge)

SD-WAN software-defined wide area network

# Application Security



Protect software applications from potential security threats and vulnerabilities.



Identify and mitigate security risks throughout the software development lifecycle, from design to deployment.

Typically include a range of security measures, such as:



Code review and analysis



Web application firewall (WAF) services



Penetration testing



Security testing and validation



Secure coding practices



# Application Security Solutions

---

WAF web application firewall

Penetration testing

Code, Configuration Review and Analysis

Web Proxy (Explicit – Reverse)



# Endpoint Security



Monitors endpoints for signs of cyber-attacks or malicious activity



Collects data on endpoint activity, network traffic, and system events.

## Key features include:



Forensic analysis



Reporting and alerts



Provides real-time threat detection and response capabilities.



Analyzes and correlates data to identify potential threats.



Endpoint monitoring



Threat detection



Incident response

## Solution:

● EDR Endpoint detection & response ●

● XDR Extended Detection and Response ●



# Email Security



Secure Email Gateways



Email Encryption Tools



Email Authentication



Secure Messaging Platforms



Spam Filters



Anti-Phishing Tools



Phishing Simulation and User Training

## Solutions:



Email security system



# Cloud Security



Secures cloud-based infrastructure, applications, and data.

## Key features:



Identity and access management (IAM):  
Manages user access to cloud-based resources and data and enforces security policies.



Data protection: Encrypts and protects data stored in the cloud to prevent unauthorized access.



Compliance management: Helps organizations comply with regulatory requirements and industry standards.



Protects against threats such as data breaches, cyber-attacks, and unauthorized access.



Network security: Protects cloud-based infrastructure from cyber-attacks with firewalls and intrusion detection and prevention systems.



Vulnerability management: Identifies and addresses security vulnerabilities in cloud-based infrastructure and applications.



# Network Security Solutions

---

● Cloud Firewall, FwaaS (Firewall as a services) ●

● Privacy management system ●

● MDM mobility device management ●

● Cloud SIEM & SOAR ●

● Cloud IPS/IDS ●

● IAM identity access management ●

● Cloud EDR ●

# Data Security



Protect sensitive data from unauthorized access, theft, or modification.



Use a combination of technologies and processes to ensure confidentiality, integrity, and availability of data.

## Key features include:



Data encryption: Protects sensitive data at rest and in transit.



Data loss prevention (DLP):  
Monitors data access and usage, prevents data leakage or theft.

## Solution:

DLP Data lose prevention.



# THEY'RE PART OF OUR SUCCESS

FORTINET



FORCEPOINT



LogRhythm

paloalto NETWORKS



SentinelOne



ManageEngine



SOPHOS



[www.smart.sa](http://www.smart.sa)



+966593440030



920024779



[info@smart.sa](mailto:info@smart.sa)

Saudi Arabia | GCC | Africa