KFTECH
SOFTWARE SOLUTIONS

Healthcare
IT Solutions

FinTech and
ERP Solutions

Cyber Security
Forensic Solutions

IP Surveillance
Software Solutions

IP Based
Public Address

www.kftechsols.com

+923216583228   mrakftech@yahoo.com   Linkedin.com/company/kftechsols

Table of Contents.

CONTENTS :	PAGES

KFTECH :

Introduction.

We are pleased to introduce ourselves as Leading software solutions provider with over 15+ years of unwavering commitment to excellence, KFTECH stands as a premier provider of cutting-edge solutions in Healthcare IT, FinTech, CyberSecurity, IoMT, IP surveillance and monitoring, and IP Network Public Address Systems. Our extensive portfolio of successful projects speaks volumes about our expertise and dedication to delivering unparalleled technology and software solutions across diverse sectors.

From serving clients in KSA, USA, Canada, UK, Ireland, and Japan to catering to healthcare, educational, government, corporate, and entertainment industries. KFTECH continues to lead the way in driving innovation and digital transforming businesses in worldwide.

Our Team.

Our strength lies in our dynamic team of over 40 seasoned professionals, each an expert in their respective fields. From Microsoft DotNet Core 8 (C#, ASP) and PHP (Laravel) to Node.JS and JavaScript, Python, iOS, Android, UI/UX design, MSSQL, MySQL, PostgreSQL, MongoDB etc. We boast a diverse array of talent capable of tackling any project with precision and skill. Moreover, our proficiency extends to cloud computing and deployment, ensuring seamless integration and optimal performance for our clients' solutions.

Why KFTECH ?

- *20+ years of professional experience and knowledge in Multi Domains.*
- *Multiple Software solutions and IT services provision under one Roof.*
- *KFTECH brings International IT Project Management expertise to the table.*
- *Offer more than just software dev -- our services include consultancy & training.*
- *Already working Internationally for KSA, USA, Canada, UK, Ireland & Japan.*
- *Unmatched expertise, comprehensive solutions, and unparalleled support.*
- *KFTECH Design, Develop, Integrate, Deploy, Support, and Provide Training.*
- *KFTECH understands Compliance and Regulations for client's Countries globally.*

KFTECH Projects.

- *E-Wallet App (LOOP) successfully delivered to KSA - Marina Marahaba group.*
- *Cab Dispatching App (RIDE) successfully delivered to KSA - Marina Marahaba group.*
- *Advance LMS delivered to Australian University (Agents, Teachers, Students) Portal.*
- *DICOM iPACS Server implementations for KSA - Saudi German Hospitals group.*
- *Advance Patient Mgmt Software (Dexterity) delivered to Ireland - Dexterity Clinics.*
- *Advance Patient Mgmt App (Dooctor) delivered to Ireland - Dexterity Clinics.*
- *Coordination Transformation Web App successfully delivered to KSA Geodesy Ministry.*
- *IT Infrastructure Consultancy provided to Saudi German Hospital in Dammam and Aseer.*
- *Doctor / Patient Appointment Booking Web Application for UK based Therapist Clinics.*
- *50+ EMR / EHR Portals deployments and Implementations for Mental Health, ENT, Optometry, Cardiology, Therapist, Dermatology, Oncology, OBGyn, Pathalogy, Orthpedic etc.*

IT Solutions and Services

IT Infrastructure Consulting :

KFTECH is IT Infrastructure Consulting and Digital Transformation Company. Since our inception in 2008, we've been pioneers in IT Consultancy and Software Solutions. With over 100+ successfully completed IT Projects and 500+ satisfied clients from Kingdom of Saudi Arabia, Middle East, Ireland, UK, USA, Canada and Japan we've earned our stripes.

Our Consulting services are designed to drive down costs while empowering organizations to craft, implement, and manage scalable, flexible, and dependable IT infrastructures.

KFTECH

IT Infrastructure Solutions :

- Servers Mgmt.
- Network Mgmt.
- IT Security Mgmt.
- Database Mgmt.
- Virtualization Mgmt.
- Domain DNS Mgmt.
- Cloud Hosting Mgmt.
- Dedicated VPS Mgmt.
- Virtualization Solutions.
- Docker Solutions.
- Amazon Web Services.
- Google Cloud Platform.
- Technical Auditing (QA/QC).
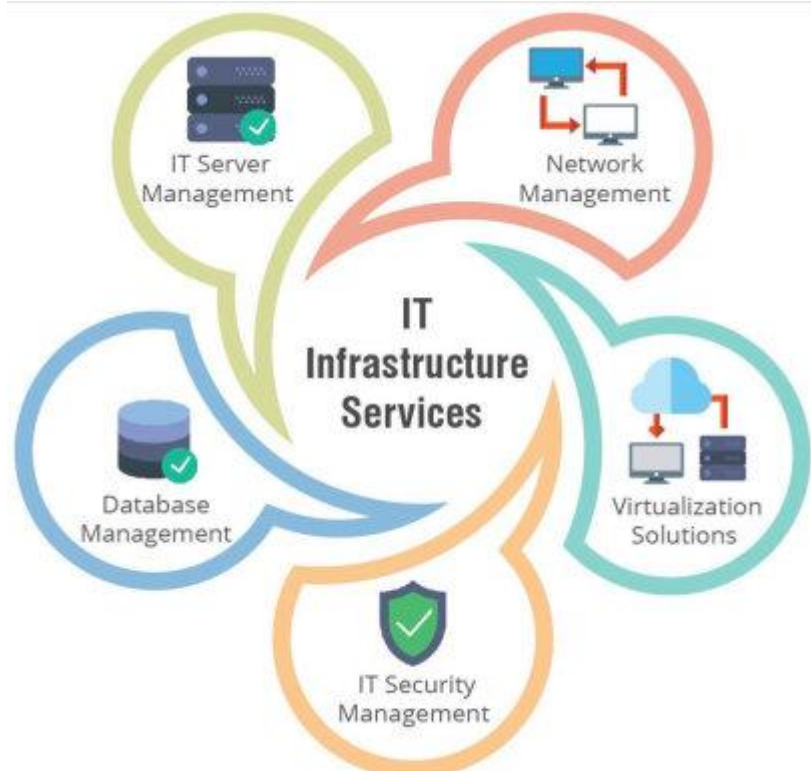
Cloud Computing Solutions :

We empower enterprises for the future with a tailored suite of cloud solutions and integrated deployment models, driving seamless enterprise transformation. Our expertise caters to businesses of all sizes, from small startups to large corporations, guiding them through a customized cloud journey. We prioritize agility and cost-effectiveness, ensuring businesses can swiftly address challenges and adapt to evolving market demands.

| Cloud Deployment Solutions | Cloud Migration Services | Cloud Managed Services | Cloud Integration | Cloud Computing |
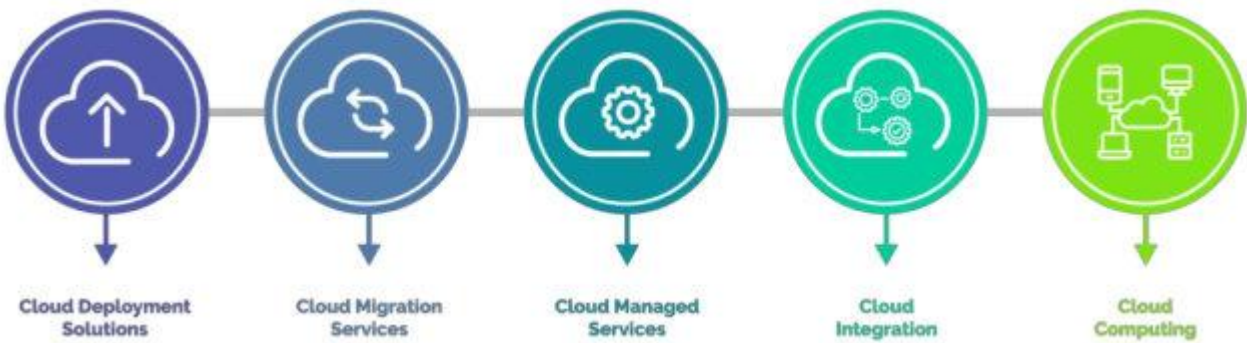
Amazon Web Services   Microsoft Azure   Google Cloud

KFTECH - Cloud Computing Services

- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).
- Software as a Service (SaaS).
- Containers as a Service (CaaS).
- Database as a Service (DaaS).

- Storage as a Service (STaaS).
- Backup as a Service (BaaS).
- Network as a Service (NaaS).
- Security as a Service (SEaaS).
- Monitoring as a Service (MaaS).

IT Monitoring Solutions :

KFTECH provides Monitoring of all mission-critical infrastructure components including Applications, Services, Operating Systems, Network Protocols, Systems Metrics, and Network Infrastructure.

Networks	Servers	Clouds	Applications	Services
Web Monitoring	Storage Devices	Virtual Machines	Java Applications	Databases

Nagios®

solarwinds
The Power to Manage IT

MONITORING SOLUTION
THAT CONTINUES TO SURPRISE
ZABBIX

KFTECH

IT Monitoring Solutions :

- Network Monitoring.
- Server Monitoring.
- Cloud Monitoring.
- Application Monitoring.
- Web Services Monitoring.
- Storage Devices Monitoring.
- Virtual Machine Monitoring.
- Databases Monitoring.
- End Point Monitoring.
- Dashboarding & Reporting.
- **Log & Event Management.**
- **Performance Monitoring.**

Security Operations Center (SOC), is a centralized facility where CyberSecurity analysts and professionals Monitor, detect, analyze, and respond to security incidents and threats in real-time. SOC typically contains monitoring tools, such as SIEM systems, IDS/IPS, EDR solutions, and other security technologies.

Software Development Services :

KFTECH custom software development services and solutions encompass a comprehensive approach, ranging from design and engineering to integration and upgrading of software systems tailored to meet our customers' specific goals. Our solutions are strategically crafted to address challenges such as enhancing operational efficiency, elevating customer experience, and ensuring compliance with industry standards.

With a focus on innovation and collaboration, we work closely with our clients to deliver robust, scalable solutions that not only meet their immediate needs but also anticipate future requirements. Whether you're looking to streamline your operations, enhance customer satisfaction, or achieve regulatory compliance, then Partner with us to unlock the full potential of your software environment and propel your business to new heights.

Our Technology Stack

Websites and Web Apps Development :

We specialize in crafting impactful web presences tailored for small to medium-sized businesses. Our expertise lies in designing compelling branding and developing fully responsive and stunning websites and Web applications compliant with W3C standards. With our bold design approach and meticulous use of clean, standards-based markup code, we ensure that our websites not only achieve exceptional search engine rankings but also drive increased conversions for your business.

We are specialized in the development of dynamic web applications, versatile admin dashboards, and powerful admin LTE platforms. With a keen understanding of modern web technologies and user-centric design principles.

These platforms offer advanced features such as real-time data synchronization, multi-user collaboration, and Customizable reporting, empowering businesses to stay ahead of the competition in today's fast-paced digital world. At every step of the development process, we prioritize quality, performance, and security. With our commitment to excellence and innovation, we stand ready to partner with businesses of all sizes to transform their digital vision into reality.

iOS and Android Apps Development :

As a iOS and Android apps development company, we specialize in transforming ideas into exceptional mobile experiences. With a team of seasoned developers and designers, we are committed to delivering cutting-edge solutions that captivate users and drive business growth. From concept to deployment, we leverage the latest technologies and industry best practices to create custom mobile apps tailored to meet your specific needs and objectives.

Whether you're a startup looking to disrupt the market or an established enterprise seeking to enhance your mobile presence, we're here to turn your vision into reality. Partner with us to unlock the full potential of mobile technology and stay ahead of the competition in today's digital world.

Mobile Apps Ready to Use

Healthcare IT Solutions

We are pleased to introduce ourselves as Leading software solutions provider with over 15+ years of unwavering commitment to excellence, KFTECH stands as a premier provider of cutting-edge solutions in Healthcare IT, FinTech, CyberSecurity, IoMT, IP surveillance and monitoring, and IP Network Public Address Systems. From serving clients in Kingdom of Saudi Arabia, USA, Canada, UK, Ireland, and Japan to catering to healthcare, educational, government, corporate sectors.

EMR / EHR Services :

- EMR / EHR Setup & Hosting
- Customization / Development
- Data Migration (ETL)
- 3rd party Integration
- Security and Compliance
- Training and Technical support
- Upgrades / Maintenance
- Performance Optimization
- Generate CDA / C-CDA Doc.

EMR / EHR Cloud Solutions :

- Dashboards Modernization
- Advanced Tele-Health
- Advanced Patient Portal
- Chronic Care Management
- Remote Therapy Management
- Remote Patient Monitoring
- Advanced Practice Management
- Medical Billing Services
- FHIR based Health Info Exchange.

KFTECH - Health IT Expertise :

- Health IT Applications - EMR / EHR, Practice Mgmt, Tele-Health, Remote Patient Monitoring
- Health Information Exchange & Interoperability (HL7 V2, V3, X12, HAPI FHIR, FHIR, SMART, Mirth)
- Robotic Process Automation (RPA) to automate Healthcare Business Tasks.
- AI implementation for Medical Imaging Detection and Classification (Annotation).
- CyberSecurity solutions for the Healthcare Information Exchanges.
- Data Mapping Sheets Preparation, Database Migrations, Backups and Restoration.
- Cloud Platforms AWS, AZURE and GCP utilization in deployment of Healthcare Web applications.
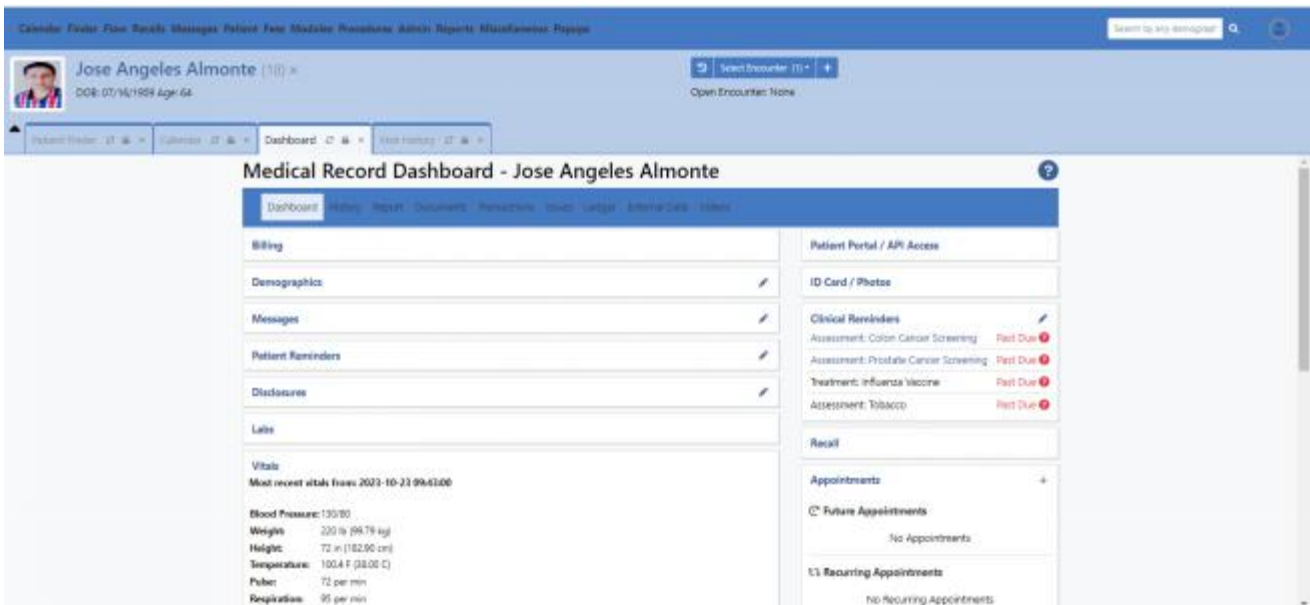
EMR / EHR (Local, Cloud) :

EMR (Electronic Medical Records) and EHR (Electronic Health Records) Softwares are digital solution that enables healthcare providers to manage patient health information electronically within a single healthcare organization, such as a hospital or clinic. These systems digitize and organize patient medical records, including information such as medical history, diagnoses, medications, treatment plans, lab results, and radiology images.

The benefits of EMR/EHR software are manifold. Firstly, it streamlines administrative tasks by automating processes such as appointment scheduling, billing, and prescription management, thereby increasing efficiency and reducing errors.

Secondly, EMR software improves the accuracy and legibility of medical records, enhancing communication and coordination among healthcare providers within the same organization.

Thirdly, it facilitates better clinical decision-making by providing quick access to comprehensive patient data, enabling healthcare professionals to make informed decisions about patient care.

Additionally, EMR systems contribute to improved patient outcomes by supporting preventive care, tracking patient progress over time, and identifying trends and patterns in health data.

Finally, EMR software enhances regulatory compliance by ensuring that patient records are complete, secure, and compliant with legal requirements and industry standards. Overall, EMR software plays a crucial role in modernizing healthcare delivery, improving patient care quality, and optimizing operational efficiency within healthcare organizations.

Scheduling

Advanced scheduling allows clinics to create repeating events, automated-workflows triggered by check-in, and patient reminds.

e-Prescribing

Enter a prescription into an encounter and have it electronically sent to the patient's pharmacy.

Medical Billing

Integrated billing supporting HIPAA ASC X12 Version 5010 Transaction and Code Set Standards.

CMS Reporting

Generate reports with just a few clicks

Lab Integration

Have lab orders automatically sent to a lab and integrate the results into a patient's chart automatically

Clinical Decision Rules

Navigate complex patient algorithms using the clinical decision rules engine to ensure the highest quality of care for patients.

Advanced Security

HIPAA-friendly, fine-grained access control objects, and industry-standard password hashing helps to protect your practice from intrusion

Multilingual Support

Available in over 30 languages, and customizable to add more.

openEMR/EHR is electronic health records and medical practice management application. It is ONC Certified and it features fully integrated electronic health records, practice management, scheduling, electronic billing, internationalization, and a whole lot more. It can run on Windows, Linux, Mac OS X, and many other platforms.

Features supported are listed below :

Patient Demographics :

- Track patient demographics.
- Primary info (name, dob, sex, id)
- Marital status
- Contact information of patient
- Contact Info of patient's employer
- Primary provider information
- HIPAA information
- Language and ethnicity
- Insurance coverage
- Deceased Tracking
- Fully Customizable
- Address verification with USPS API

Patient Scheduling :

- Patient Flow Board, Tracking, and Reporting
- Supports multiple facilities
- Appointment notify via email and sms
- Recall (reminders) Board
- Flexible appointment calendar
- Calendar features include:
  - Find open appointment slots
  - Categories for appointment types
  - Colors associated with appointment types and facility
  - Repeating appointments
  - Restricting appointments

Electronic Medical Records :

- Interoperability
  - CCDA
  - FHIR support for ONC US Core IG 4.0.0 (SMART on FHIR is included)
- Encounters
- Medical Issues
- Medications
- Immunizations
- Forms and clinical notes:
  - Vitals (growth charts included)
  - SOAP note
  - Review of systems
  - Eye (Ophthalmology/Optometry) Module
  - Template Driven Forms
    - CAMOS (Computer Aided Medical Ordering System)
    - Nation Notes (WYSIWYG editor)
  - Ability to create and customize forms
- Group Therapy
- Graphical Charting
- Labs
- Procedures
- Patient Reports
- Referrals
- Patient Notes
- Disclosures
- Electronic digital document mgmt
- Voice recognition ready (MS Windows Operating Systems)
- Paper Chart Tracking
- Electronic Syndrome Surveillance reporting
- Clinic Messaging
- Send and Receive Medical Records via Direct Messaging
- Dated Reminders
- Medical Image Viewer (DICOM)

Prescriptions :

- Online drug search
- Track patient prescriptions and medications
- Create and send prescriptions
- E-Prescribe
- Print, Fax, Email
- Customizable layout including options for DEA, NPI and state license numbers.
- In-house pharmacy dispensary support

Medical Billing :

- Flexible system of coding including CPT, HCPCS, ICD9, ICD10 and SNOMED codes, and the ability to add others
- Support for 5010 standards
- Support for Institutional Billing Standards (UB-04)
- Support for electronic billing to clearing houses such as Office Ally, ZierMED and ClaimRev using ANSI X12
- Support for paper claims
- Medical claim management interface
- Insurance Eligibility Queries
- Insurance Tracking Interface
- Accounts Receivable Interface
- EOB Entry Interface
- Customizable to work with a clearing house for automated 835 or ERA entry

Clinical Decision Rules :

- Physician Reminders
- Patient Reminders
- Clinical Quality Measure Calculations
- Automated Meaningful Use Measurement Calculations
- Fully Customizable and Flexible

Patient Portal :

- Modern User Interface
- Scheduling and Appointments
- Secure Messaging and Chat
- Online Payments
- Send Records via Direct Messaging
- Customized Forms
- New Patient Registration
- CCDA Support
- Reports
- Labs
- Medical Problems
- Medications
- Allergies
- Appointments

Reports :

- Appointments
- Encounters
- Patient Lists
- Prescriptions and Drug Dispensing
- Referrals
- Immunizations
- Clinical Measure Calculations
- Clinical Quality Measures (CQM) Calculations
- Automated Measure Calculations (AMC) and Tracking
- Syndromic Surveillance
- Pending Procedure Orders
- Ordered Procedure Statistics
- Paper Chart Tracking
- Sales
- Collections
- Insurance Distributions
- Insurance Eligibility

Multilanguage Support :

- Supports use of multiple languages within the same clinic
- Currently Supported Languages:
  - English (American)
  - Albanian, Armenian
  - Arabic
  - Chinese (Simplified)
  - Chinese (Traditional)
  - Danish
  - Dutch
  - French (Canadian)
  - French (Standard)
  - German
  - Urdu / Hindi
  - Italian
  - Japanese
  - Persian
  - Polish
  - Portuguese (European)
  - Romanian
  - Russian
  - Spanish (Latin American)
  - Spanish (Spain)
  - Swedish
  - Turkish
  - Vietnamese
- Fully supports UTF-8 encoding
- Supports RTL

Security :

- Support fRole Based & Custom Menus
- Ability to Encrypt Patient Documents
- Active Directory Support
- DB Connection Encryption Support
- Remotely accessible from any modern web browser with a suitable security certificate installed.

OpenEMR solutions for every specialty

Mental Health	Dermatology	ENT	Physiotherapy
Neurology	OBGyn	Oncology	Optometry
Orthopedic	Pathology	Podiatry	Surgery
Family Practice	Ophthalmology	Ambulatory	Wound care
Gastroenterology	Psychiatry	Urgent care	Pain management

openEMR Installation on Local or Cloud Hosting : $550 only. Monthly Support $100 (12 month contract).
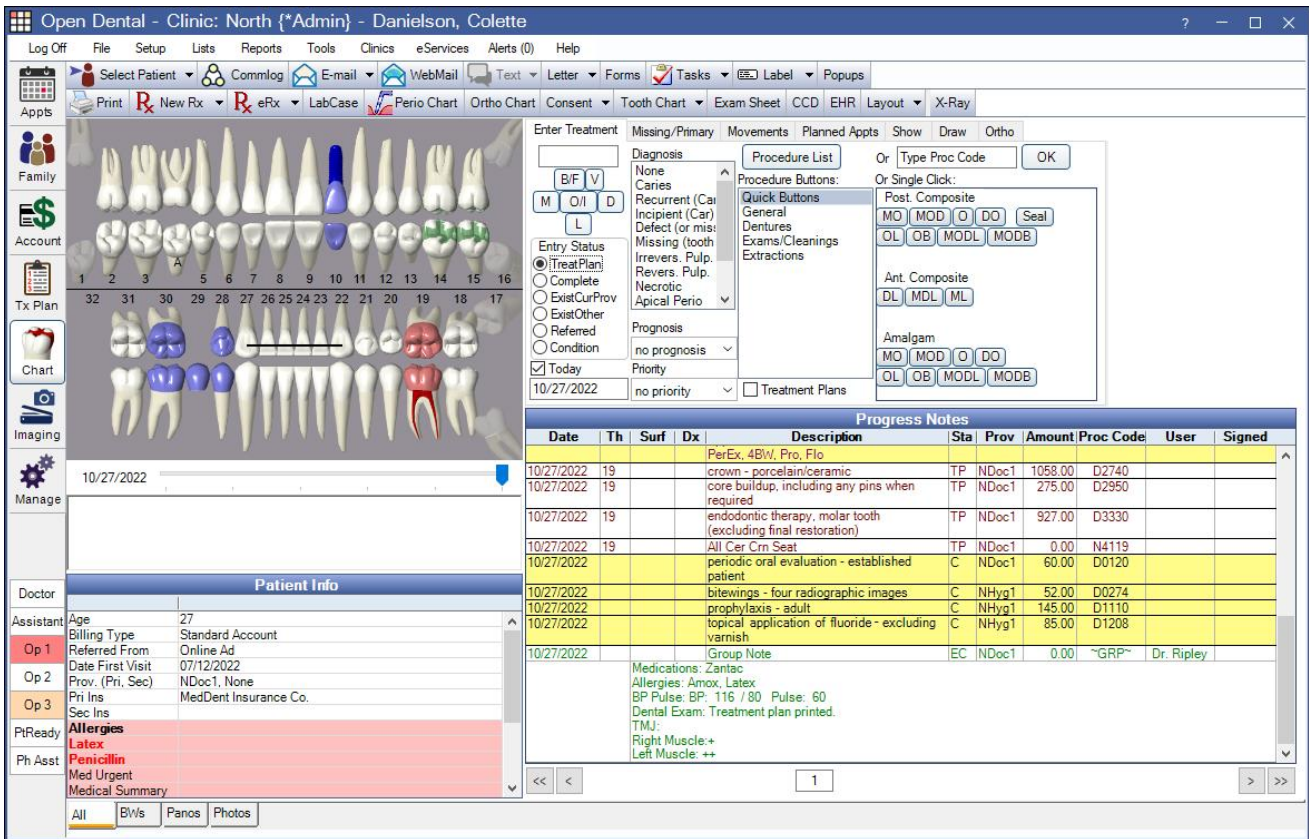openEMR installation on Linux (Ubuntu) : $700 only.

DEMO LINK :   https://www.kftechsols.com/bestemr
Username :   EMR-Provider16
Password :   emrProvider1@786

Dental Practice Management (Local, Cloud) :

Quality Software for Dental Offices :

Comprehensive, highly Customizable Dental Practice Mgmt software for practices of any size.

OpenDental is a comprehensive dental practice management software designed to streamline administrative tasks and enhance patient care in dental practices.

1. Appointment Scheduling :
OpenDental offers robust scheduling capabilities, allowing receptionists to efficiently manage appointments, reschedule, and track patient visits.

2. Patient Management :
It provides tools for managing patient demographics, treatment history, insurance information, and communication preferences.

3. Clinical Charting :
The software enables dentists to create and maintain detailed electronic dental charts, including diagnoses, treatment plans, progress notes, and imaging.

4. Billing and Invoicing : OpenDental facilitates accurate billing and invoicing processes, including insurance claims submission, payment tracking, and financial reporting.

5. **Treatment Planning :** Dentists can develop and present treatment plans to patients, including estimated costs, timelines, and alternatives, helping to improve case acceptance rates.

6. **Electronic Health Records (EHR) :** It offers a centralized repository for storing and accessing patient health records securely, ensuring compliance with healthcare regulations.

7. **Image Management :** OpenDental supports the integration of digital imaging devices, such as intra-Oral cameras and X-ray machines, allowing for efficient capture, storage, and retrieval of patient images.

8. **Reporting and Analytics :** The software generates various reports and analytics to help practices track key performance indicators, monitor productivity, and identify areas for improvement.

9. **Communication Tools :** It includes features for sending appointment reminders, treatment notifications, and other communications to patients via email, SMS, or automated phone calls.

10. **Customization and Integration :** OpenDental offers customization options to tailor the software to the specific needs of each dental practice. It also supports integration with third-party software and services for expanded functionality.

11. **HIPAA Compliance :** The software is designed with security and compliance in mind, helping practices adhere to HIPAA regulations and protect patient privacy.

12. **Support and Training :** OpenDental provides customer support and training resources to help practices optimize their use of the software and troubleshoot any issues that arise.

Overall, OpenDental aims to streamline dental practice operations, improve patient care, and enhance practice profitability through its comprehensive features and user-friendly interface.

OpenDental Installation :
Trial Version Installation charges for openDental on Local = $2000 only (once).

Monthly Support Fee :
$249 per month per location or office (12 month contract)
- Includes the software, Whats App support, and update software releases.
- Includes access to the Acquire and Video Capture Imaging Module features.
- Includes access to Web Forms, Patient Portal, eReminders, Automated eThanks Messages, and emailed General Messages.
- After 12 months, the monthly fee goes down to $219 only.

Open Eyes™ (Linux Based).

Posterior chamber IOL (In-the-bag fixation)
Medium pupil (diameter: 4mm), corneal size : normal
Peripheral iridectomy at 12 o'clock
Trabeculectomy bleb at 12 o'clock

Posterior chamber IOL (In-the-bag fixation)
Small pupil (diameter: 3mm), corneal size : normal
Trabeculectomy bleb at 11 o'clock
Peripheral iridectomy at 11 o'clock
Corneal thinning: dellen
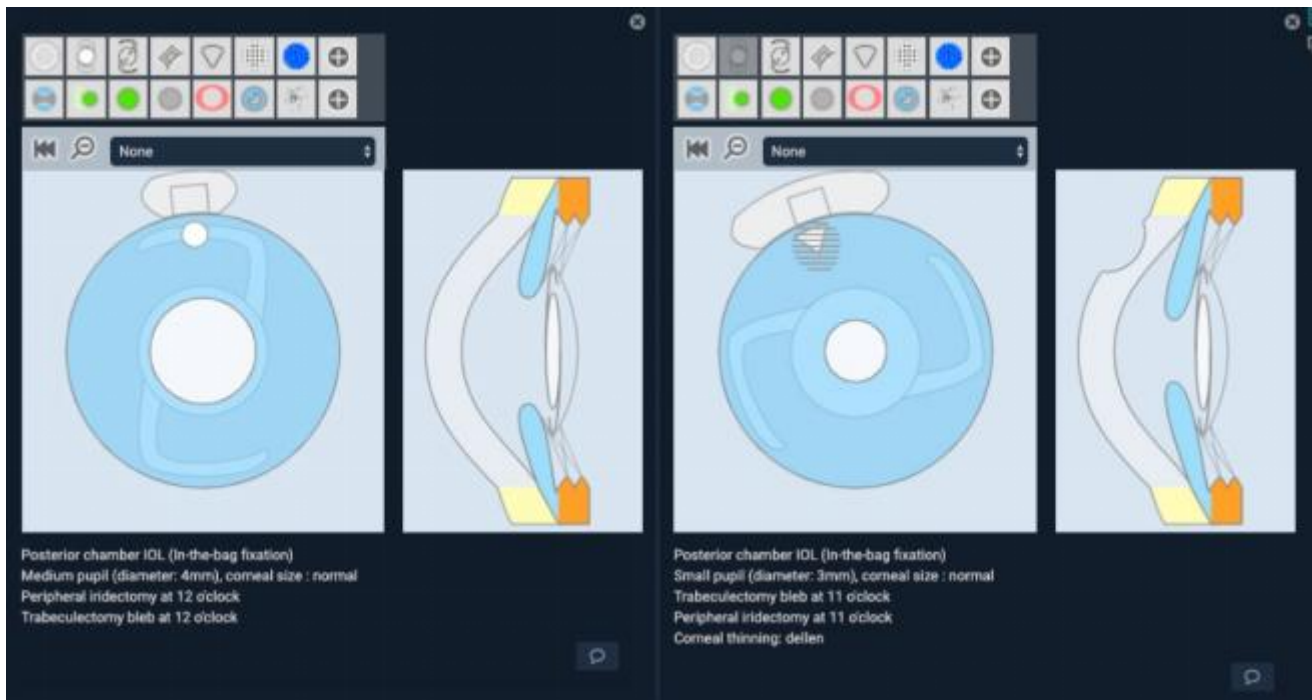
OpenEyes™ is the leading open source electronic patient record (EPR) for ophthalmology. It is fast in delivering content, fast to navigate and easy (and fun) to use. OpenEyes™ the EPR that will help you deliver data-driven patient care in the best way possible. OpenEyes™ is owned by the community and not by any individual or corporate entity. It can be customized to suit local needs and will scale to connect, seamlessly, primary and secondary eye care.   https://openeyes.apperta.org/oedetail
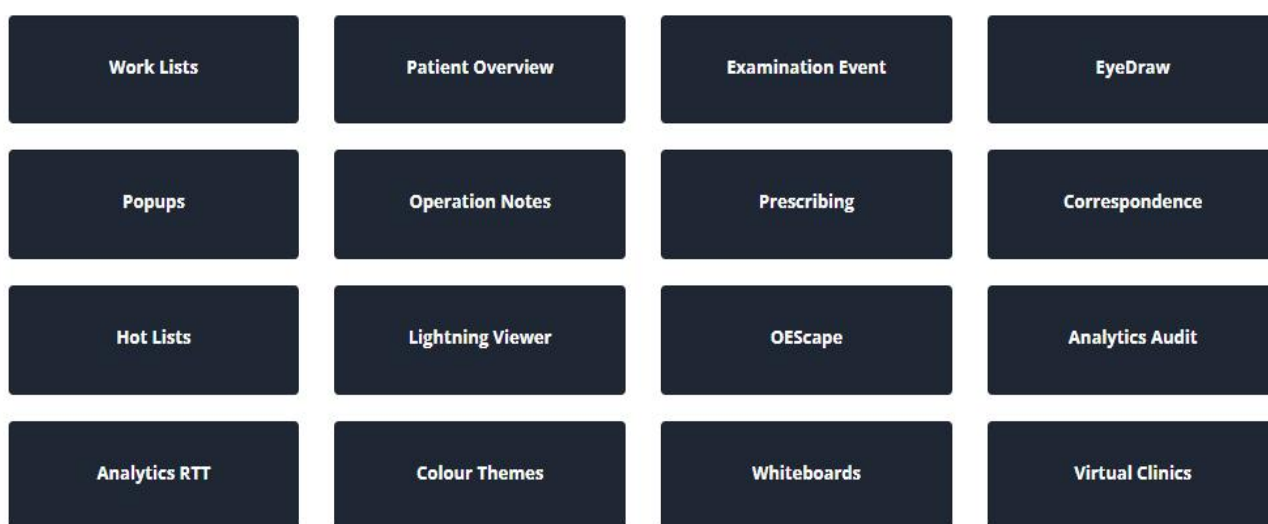
Some of our OpenEyes™ Enterprise Implementations

OpenEyes™ is an electronic patient record application for ophthalmology, developed with contributions from a range of hospitals, institutions, academic departments, companies and individuals. Intuitive to use and fast, it runs in a web browser to ensure that it can be accessed from just about any device in any location. OpenEyes™ will always be available free-of-charge under an open source license, making it a cost-effective option for eye care.

We will ensure that your clinical data integrates with hospital workflows and PACS system and that the connections to devices such as OCT machines or visual field devices are robust.

OpenEyes V3 is fast and fun to use. Some highlighted and more important features.

Work Lists	Patient Overview	Examination Event	EyeDraw
Popups	Operation Notes	Prescribing	Correspondence
Hot Lists	Lightning Viewer	OEScape	Analytics Audit
Analytics RTT	Colour Themes	Whiteboards	Virtual Clinics

OpenEyes Installation :
Full version Installation charges for openEyes on Local = $2000 only (once).

Monthly Support Fee :
$249 per month per location or office (12 month contract)
- Includes the software, Whats App support, and update software releases.
- After 12 months, the monthly fee goes down to $219 only.

TeleHealth (Web & Mobile Apps).

TeleHealth has changed the healthcare landscape by enabling clinicians to provide timely and effective care for improved patient outcomes. **DEMO** https://kftech.daily.co/healthtracker
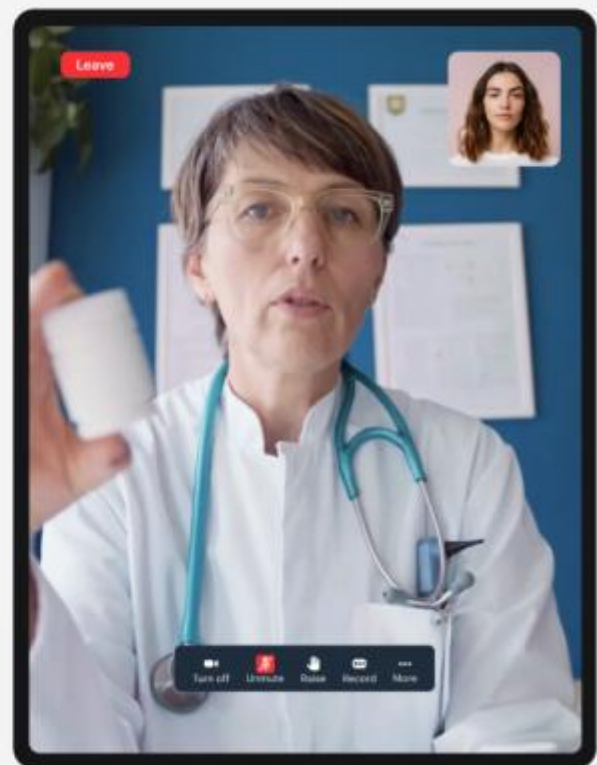
Cut call failure rates in half

Daily outperforms competitors in objective testing:

- lower video freeze rates and latency

- better performance on cellular data and other challenging networks

Daily also offers the industry's best engineering support, WebRTC dashboard, component libraries, and pre-call test logic.

Request our benchmarking white papers >

1 / 2

call failure rates
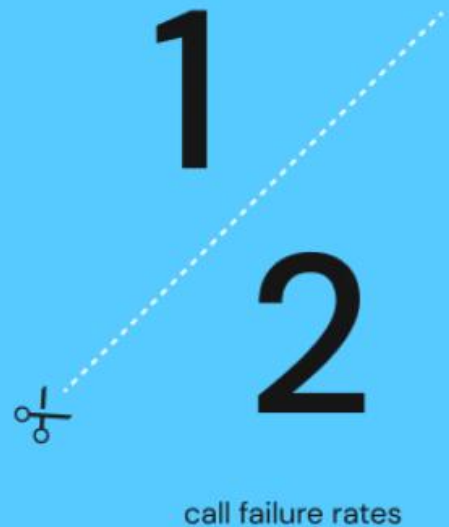
Ready for AI

Work with Daily and our partners to build AI-powered workflows:

- HIPAA-compliant transcription, recording, and AI-powered Clinical Notes API

- LLM-powered data pipelines

- Background blur and background replacement

- Noise cancellation

Advanced analytics

Daily gives you the industry's best tools:

- understand your users, usage, and app performance
- provide real-time customer support
- integrate with data platforms and cloud monitoring

Our dashboards are designed by engineers who wrote the WebRTC specification and pioneered WebRTC telehealth.

Rooms ⑦
354,892

Total sessions ⑦
1,242,018

400kb/s

200kb/s

Bitrate sent   16:11:02
Avg   386k
Max   400k
Min   205k

Trusted security and compliance

Daily is the industry leader in security-focused video architecture.

- ⊘ HIPAA compliance including an affordable HIPAA package that includes a signed BAA
- ⊘ SOC 2 Type 2
- ⊘ GDPR and EU-U.S. Data Privacy Framework
- ⊘ Regional data geo-fencing
- ⊘ True end-to-end encryption
- ⊘ High-touch engineering support

SOC-2

TLS/SSL

BAA

GDPR

HIPAA

TeleHealth Salient Features :

==========

- Ready-to-use video chat interface
- Built-in bandwidth management
- Cross-browser compatibility
- Screen sharing
- Active speaker and grid layout modes
- Text chat
- Emoji reactions
- Hand raising
- Participant list
- Network Analytics display
- Localized interfaces
- Electron compatible
- Recording (paid add-on).
- HIPAA compliance (paid add-on).
- Set Participants Numbers.

>> PRICING :

==========

- TeleHealth Web App Development = $10K (without any 3rd Party API)
- TeleHealth Mobile App (Android) Development = $12K (without any 3rd Party API)
- TeleHealth Mobile App (iOS) Development = $15K (without any 3rd Party API)

- Telehealth Web App with 3rd Party API = $6000 only
- Telehealth Mobile App (Android) with 3rd Party API = $8K
- Telehealth Mobile App (iOS) with 3rd Party API = $11K
(Video and Audio Chat 10000 minutes are Free every month).
(Video and Audio Chat API subscription= $0.0060 / participant / min).

- TeleHealth 3rd API integration in OpenEMR software = $1500 only.

- HIPAA Healthcare Add-On Enablement = $300 / month (12 month Contract).
- Cloud Recording Add-On Enablement = $0.05 / minute. (12 month Contract).

Note : 50% Advance Payment by Bank Transfer and remaining 50% will be received in two installments during milestones. Delivery Time minimum for Tele-Health Web or Mobile Application 3 - 4 months. Depends on Clients requirements.

DICOM + PACS Server Software.

DICOM (Digital Imaging and Communications in Medicine) is a standard for handling, storing, printing, and transmitting medical imaging information. PACS (Picture Archiving and Communication System) is a system used for storing, retrieving, presenting, and distributing medical images. A DICOM PACS server software, therefore, is a software solution that combines DICOM standards with PACS functionality to manage medical imaging data.

Key components and functionalities of a DICOM PACS server software:

1. Image Acquisition : DICOM PACS server software interfaces with various medical imaging modalities such as X-ray, MRI, CT scan, ultrasound, etc., to acquire digital medical images in DICOM format.

2. Storage : It provides storage capabilities to securely store DICOM images and associated metadata in a centralized repository. This storage may be on-premises or cloud-based, depending on the implementation.

3. Image Viewing: DICOM PACS server software allows authorized users, such as radiologists, clinicians, and specialists, to view medical images from any workstation within the healthcare facility. It typically includes tools for image manipulation, annotation, and measurement.

4. Image Distribution : It facilitates the distribution of medical images to authorized users, departments, or external entities such as referring physicians or consulting specialists. This can be done securely over a network or through other means of transmission.

5. Security and Compliance : It ensures the security and privacy of patient data in accordance with healthcare regulations such as HIPAA (Health Insurance Portability and Accountability Act) by implementing access controls, encryption, and audit trails.

6. Archiving and Retrieval : DICOM PACS server software supports long-term archiving of medical images and provides efficient retrieval mechanisms for accessing historical patient data as needed for diagnosis, treatment planning, and follow-up.

7. Workflow Optimization : It optimizes the radiology workflow by automating tasks such as image routing, prioritization, and reporting, thereby improving efficiency and productivity within the radiology department.
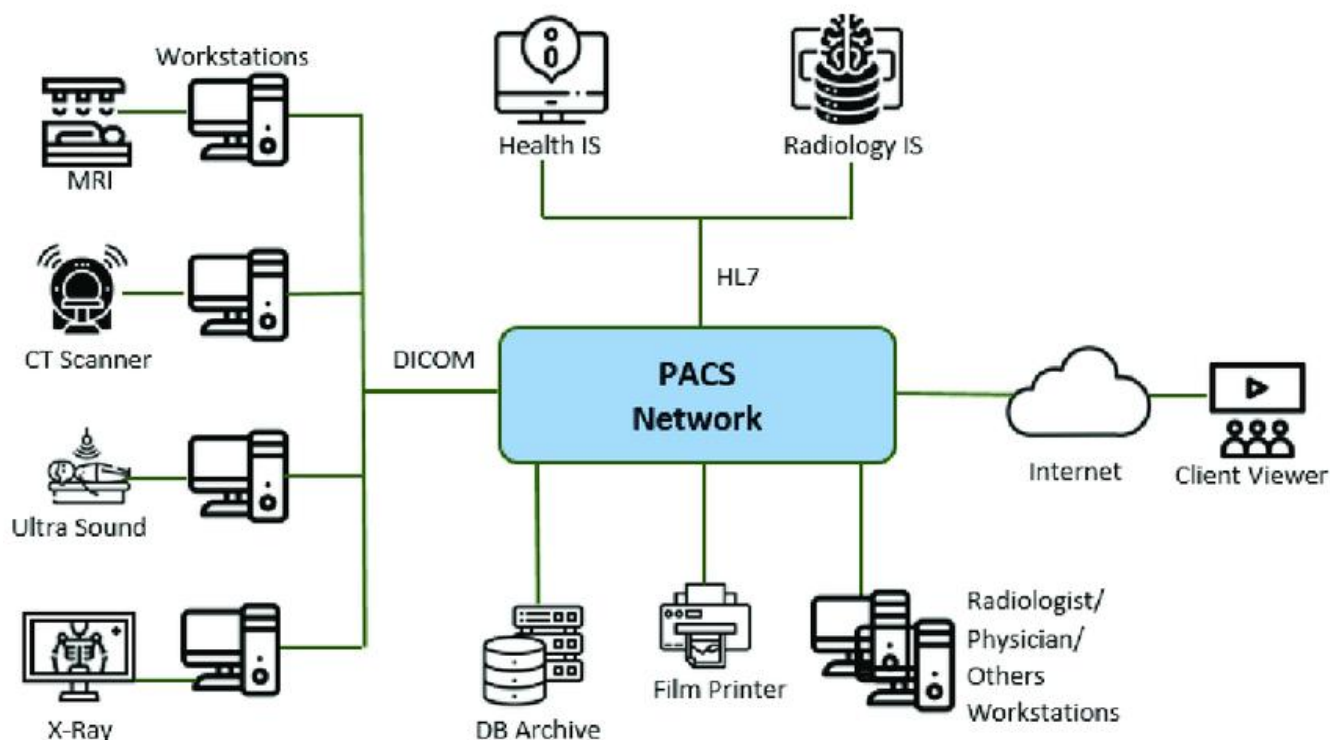

DIOOM + PACS Installation :
- PACS Server Installation Local or VPS = $4000 only.
- DICOM + PACS server will be connected with 2 Medical Modality.

Monthly Support Fee :
$350 per month per location or office and 2 modalities (12 month contract)
- Includes the software, Whats App support, and update software releases.
- After 12 months, the monthly fee goes down to $225 only.

DICOM Images Viewer Software.
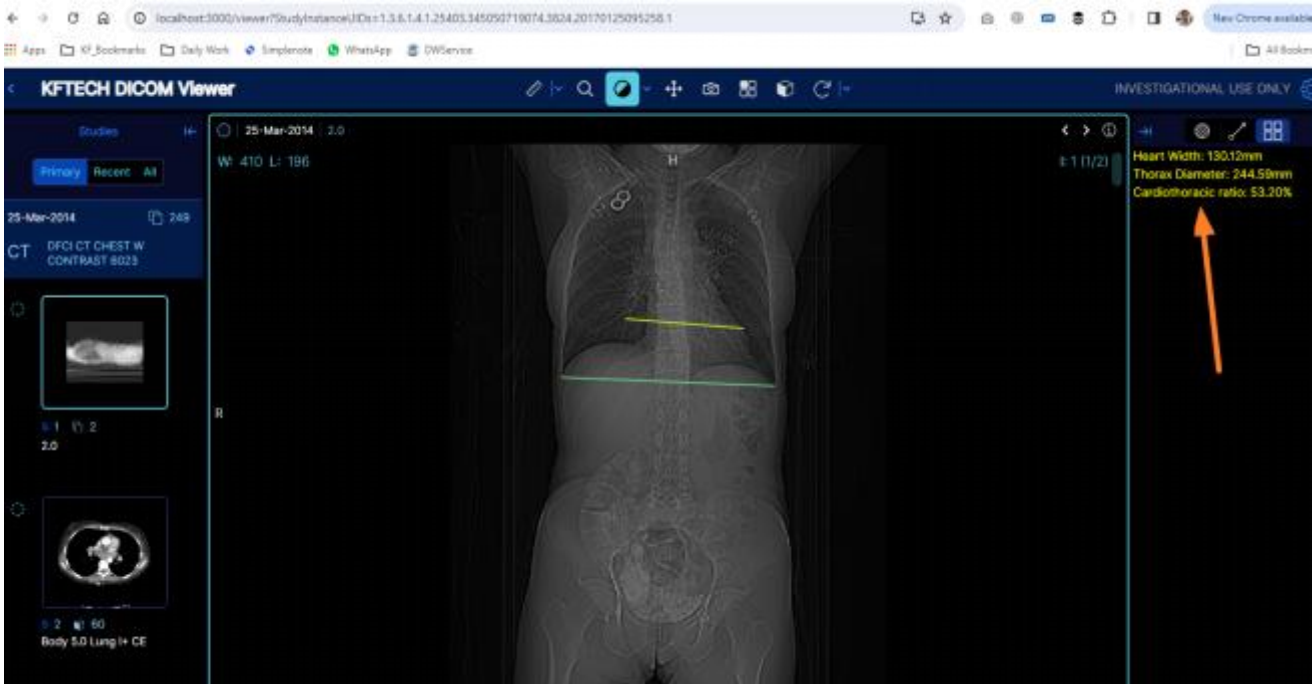
The OHIF Zero-footprint Viewer is an open-source, web-based medical imaging viewer designed to display and interpret DICOM (Digital Imaging and Communications in Medicine) images. It's a versatile tool used by healthcare providers, researchers, and developers for viewing medical images such as X-rays, MRI, CT scans etc. **DEMO** https://viewer.ohif.org

Some salient features of the OHIF Viewer :

1. Web-Based Interface : The OHIF Viewer is accessible through a web browser, allowing users to view medical images from any device with internet access, without the need for specialized software installations.

2. DICOM Support : It supports the DICOM standard, enabling users to load, view, and interact with DICOM images from various imaging modalities. This includes multi-frame DICOM series and associated metadata.

3. Multi-Modality Support : The viewer can handle a wide range of medical imaging modalities, including X-ray, MRI, CT, ultrasound, PET-CT, and more, making it suitable for use across different medical specialties.

4. Customizable Layout : Users can customize the layout and arrangement of image panels, toolbars, and other interface elements to suit their preferences and workflow requirements.

5. Annotation Tools : The viewer provides tools for annotating images, including measurement tools for distance, angle, and area measurements. Annotations can be added to images to highlight specific findings or structures.

6. Image Manipulation : Users can adjust various image parameters such as brightness, contrast, windowing, and zoom levels to optimize image visualization and interpretation.

7. Cross-Platform Compatibility : The OHIF Viewer is built using web technologies such as HTML, CSS, and JavaScript, making it compatible with multiple operating systems (Windows, mac-OS, Linux) and devices (desktops, laptops, tablets, mobile phones).

8. Integration Capabilities : It can be integrated with other healthcare IT systems such as PACS (Picture Archiving and Communication System), EMR (Electronic Medical Records), and RIS (Radiology Information System) for seamless access to patient data and imaging studies.

9. Performance and Scalability : The viewer is designed to deliver fast and responsive performance, even when loading large DICOM datasets or handling multiple users simultaneously. It can scale to accommodate the needs of small clinics to large hospitals.

10. Open-Source and Extensible : Being open-source, the OHIF Viewer allows developers to contribute to its development, customize its features, and integrate additional functionalities as needed. This fosters innovation and collaboration within the medical imaging community.

The OHIF Viewer is a powerful and flexible tool for visualizing and interpreting medical images, offering a user-friendly interface, extensive DICOM support, and Customizable features to meet the diverse needs of healthcare professionals and researchers.

OHIF Configuration with following :
1. AWS S3 Bucket.
2. Orthanc PACS.
3. DCM4Chee.
4. Firebase.
5. DICOM Web Servers.
6. Microsoft Azure.
7. Google Cloud Healthcare API.

OHIF Plugins Development :
1. Cobb Angle Tool.
2. CardioThoracic Ratio Tool.
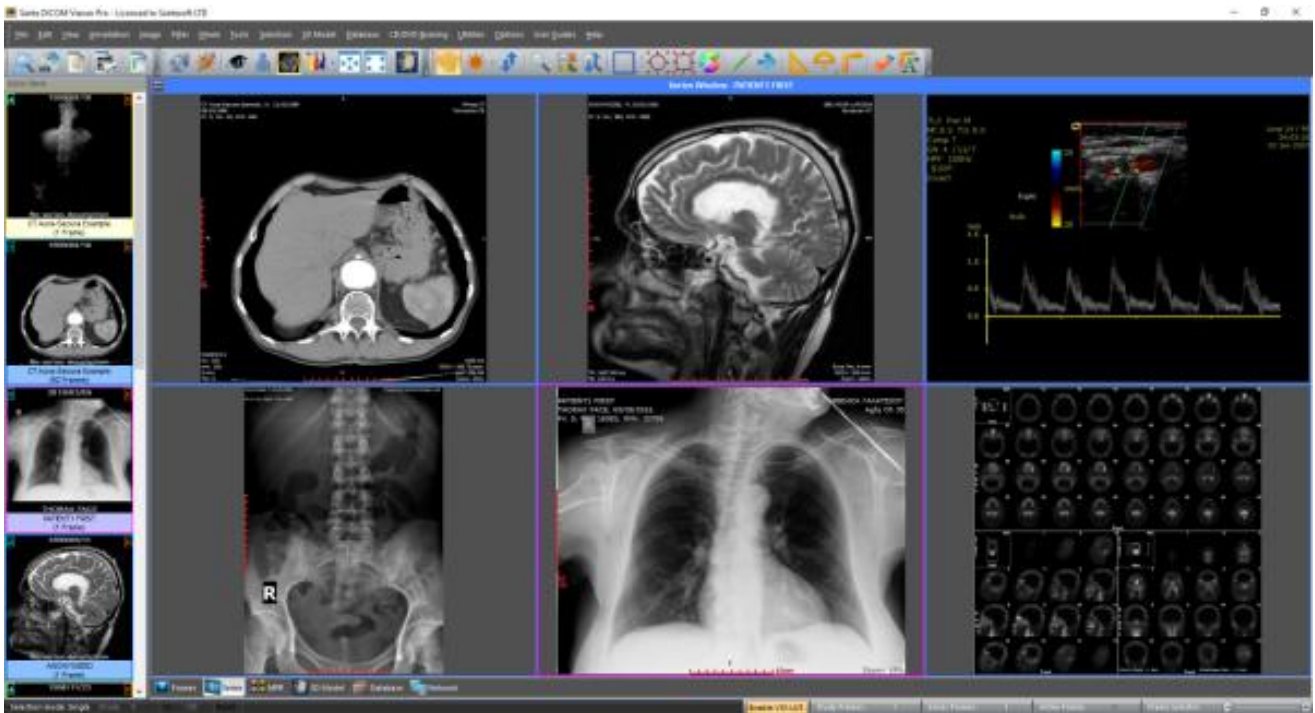3. Custom Tools development.

OHIF DIOOM Viewer Installation :
- Installation (Local or VPS) = $1500 only.
- DICOM Viewer will be connected with 1 PACS Server.

Monthly Technical Support Fee :
$100 per month per location or office / 1 PACS server (12 month contract)
- Includes the software, Whats App support, and update software releases.

DICOM Images Viewer Professional :

Retrieve, view, store, archive, manage and burn medical images.

DICOM Viewer Pro is a professional DICOM viewer, anonymizer, converter, PACS client, mini PACS server, patient CD/DVD burner (with viewer) and much more. Compatible WIN 11/10/8.1/8/7/Vista and Server 2022/2019/2016/2012/2008.   Price Single License $750 & Site License $3500 only.

- New, faster graphics engine (Direct2D instead of GDI+)
- TLS support for DICOM network connections
- **OHIF viewer** support (a study can be reviewed with OHIF viewer as well)
- Export network and database search results as CSV files
- Create new study, series and SOP instance UIDs during Anonymizing (user option)
- Memory and speed optimizations

Features and benefits :

- Powerful 2D / 3D DICOM workstation and viewer.
- Perpetual license that never expires.
- Free updates and free for lifetime
- PACS client that supports all the DICOM network services (C-FIND SCU/SCP, C-MOVE SCU/SCP, C-STORE SCU/SCP, C-GET SCU/SCP, C-ECHO SCU/SCP)
- It can be used as a mini PACS server as well (stored patients/studies depends on disk size).
- Migration tool for file transferring from other DICOM viewers
- Command line switches for integration with PACS servers (learn more...)

- Easy to use with native Windows "look and feel"
- Support of all charsets (latin, chinese, japanese, korean, cyrillic, arabic, greek, turkish, etc.)
- Creation of 3D model by the Iso-Surface technique
- Creation of 3D model by the Transfer Function (Volume rendering) technique
- Creation of 3D model by the Maximum Intensity Projection (MIP) technique
- Compatible with all modalities (CT, MR, NM, US, XA, MG, CR etc.), all manufacturers.
- Supports also jpeg, jpeg2000, tiff, png, and bitmap image formats
- Dual monitor support (new in version 10, learn more...)
- Structured Report support (new in version 10.3)
- Built-in DICOM File Editor.
- Support DICOMDIRs (view, open, create, edit, image/series selection for viewing transferring.
- Built-in Anonymizer (Patient data DE-identification, suitable as well for avoiding issues with the GDPR regulation 2016/679 of EU)
- Scout image / localizer support
- Support for Overlays.
- Study comparison side-by-side
- Attachment of PDF report files to studies
- Encapsulated PDF DICOM file support
- Printing to DICOM printers and Windows printers
- Creation of DICOM CD/DVD disks with free DICOM viewer for Windows and macOS
- Support of Epson and Primera CD/DVD Disk Publishers (robots)
- ROI selection tools (free hand, magic wand, eye-dropper, rectangle, circle, ellipse, polygon)
- ROI Statistical analysis (pixel count, min/max/mean value, standard deviation, area, volume)
- Synchronized frame view between the series
- Synchronized level-window between the series
- Synchronized field of view between the series
- Measurement tools (distance, angle, cobb angle, polyline, area, volume)
- Ultrasound region calibration module support (calibrated Ultrasound measurements)
- Annotation texts and arrows.
- Interpolated (smooth) zoom and advanced zoom tools (e.g. zoom dynamic, zoom window)
- Comparison of DICOM files tag by tag
- Built-in Hexadecimal File Editor
- Built-in Hexadecimal DICOM Viewer
- File searching with criteria (patient name, study ID etc.), within hard disk's or CD's folders
- File searching by tag's existence and/or tag's value, within hard disk's or CD's folders
- External DICOM dictionary support
- Image orientation (flip, rotate)
- Image processing filters (blur, sharpening, convolution masks, min/max/median mask etc.)
- Video (WMV) creation with or without annotations
- Batch convert to image formats (JPEG, TIFF, BMP, PNG, etc.)
- Batch Anonymizing, with ability of burned-in annotations removal
- Orthogonal Multi-planar Reconstruction (MPR)

Hospital Information Mgmt Software :

Hospital Information Management Software (HIMS), also known as Hospital Information System (HIS) or Hospital Management System (HMS), is a comprehensive software solution designed to manage various aspects of hospital operations and administration. It integrates multiple functionalities and modules to streamline workflows, improve efficiency, and enhance patient care within a hospital or healthcare facility.

DEMO Link : https://queuems.ctechmediasolutions.com
username : admin@admin.com
password : admin

Hospital Software Modules :

- In-Patient Department.
- Out-Patient Department.
- Emergency Department,
- Hospital Pharmacy.
- Hospital Cafeteria.
- Complaint Tickets.
- Miscellaneous.
- Cash Counter.
- Resource Scheduling.

- Admin Tools :
  - Staff Management.
  - Accommodation.
  - Transports.
  - Custom Invoice Items.
  - Departments.
  - Settings.
- Accounting.
- Blood Bank Management.
- Lab Management.

There is no fix price for HIS. Price depends on Client's requirements analysis and after discussing project complexity. We prepare proposal and present to Client.

Clinic Information Mgmt Software :
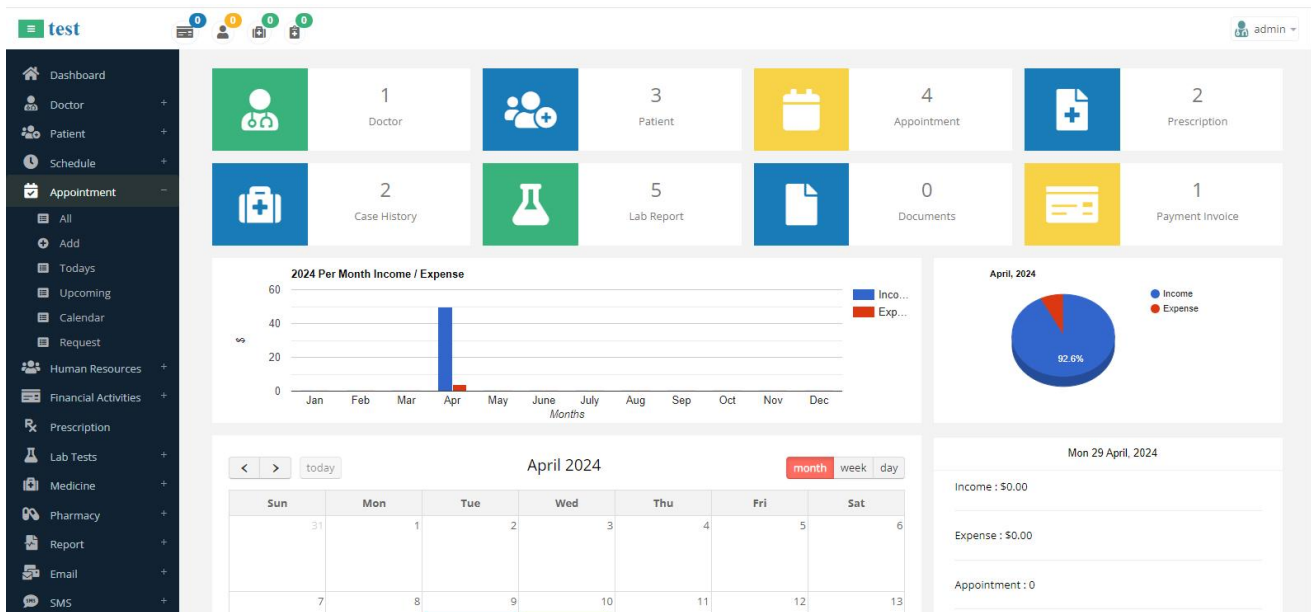
Clinic Information Management Software (also known as Clinic Management Software or Clinic Information System) is a type of software designed to streamline and automate administrative and clinical tasks in healthcare clinics, medical practices, and outpatient facilities. It serves as a central platform for managing various aspects of clinic operations, patient data, appointments, billing, and more. Here are some key features and functionalities of Clinic Information Management Software.

DEMO Link : https://clinic.iifatech-product.com/auth/login
username : admin@dms.com
password : 12345

Clinic Software Modules :

- Dashboard.
- Doctor Management.
- Patient Management.
- Scheduling.
- Appointment.
- Human Resources.
- Financial Activities.
- Prescription.
- Lab Tests.
- Medicine.
- Pharmacy.
- Reports.
- Email.
- SMS.
- Website.
- Settings.
- Profile.

There is no fix price for CIS. Price depends on Client's requirements analysis and after discussing project complexity. We prepare proposal and present to Client.

Pharmacy Shop Management Software :
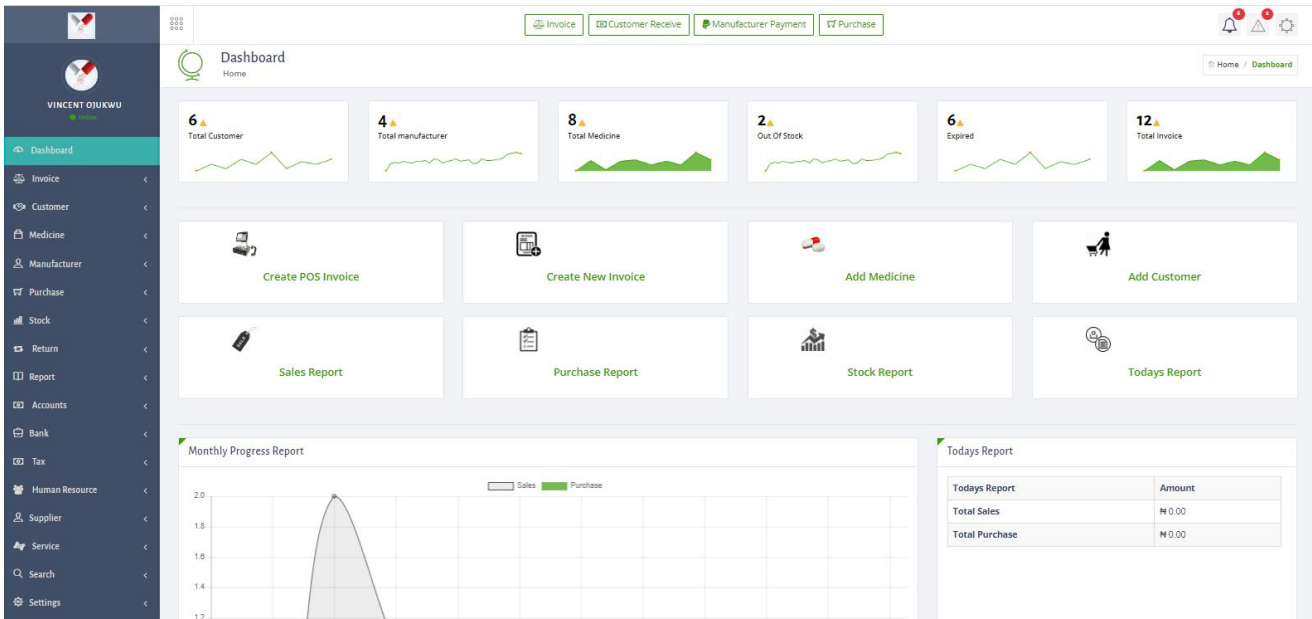
Pharmacy Shop Management Software (PMS), is a software designed for managing the operations of a pharmacy or a pharmacy shop. It helps pharmacists streamline various tasks related to inventory management, prescription processing and customer services.
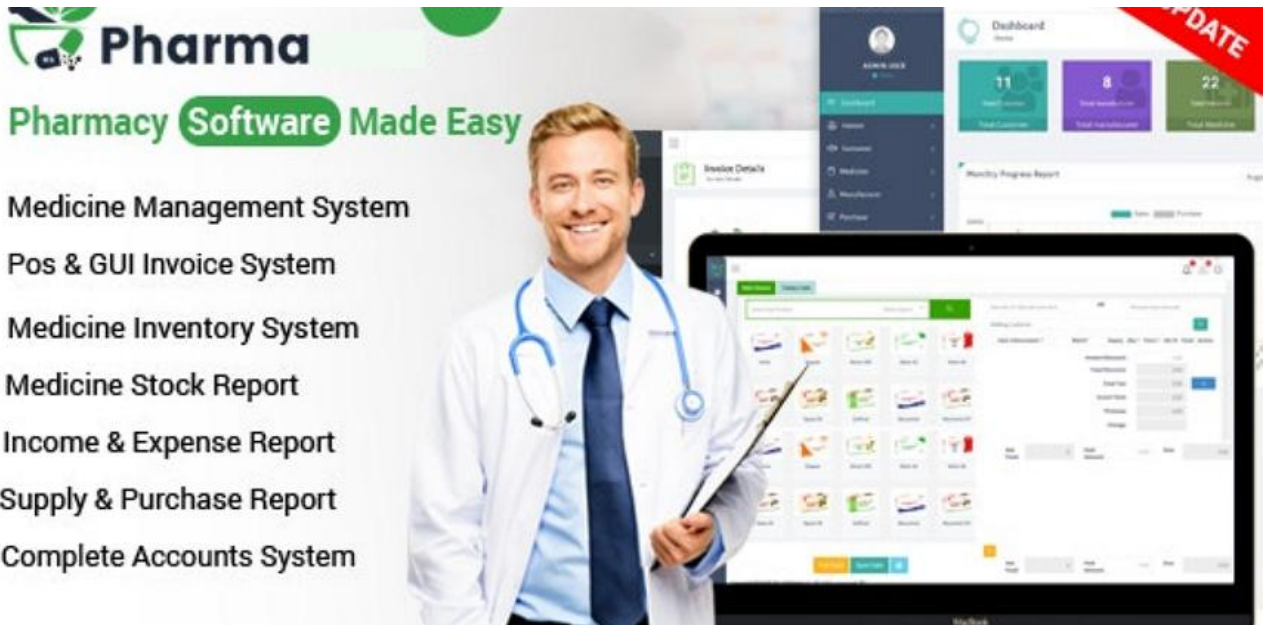
DEMO Link : https://limitlesscrm.net/pharmacy/Admin_dashboard/login
username : admin@gmail.com
password : admin123

Pharmacy Software Modules :

- Dashboard.
- Invoice.
- Customer.
- Medicine.
- Manufacturer.
- Purchase.
- Stock.
- Return.
- Reports.

- Accounts.
- Bank.
- Tax.
- Human Resource.
- Supplier.
- Service.
- Search.
- Settings.

- **Pharmacy Software Installation (Local PC) = $200 only.**
- Technical Support $10 / month (12 month contract).
- There are extra charges for the Customization requirements.
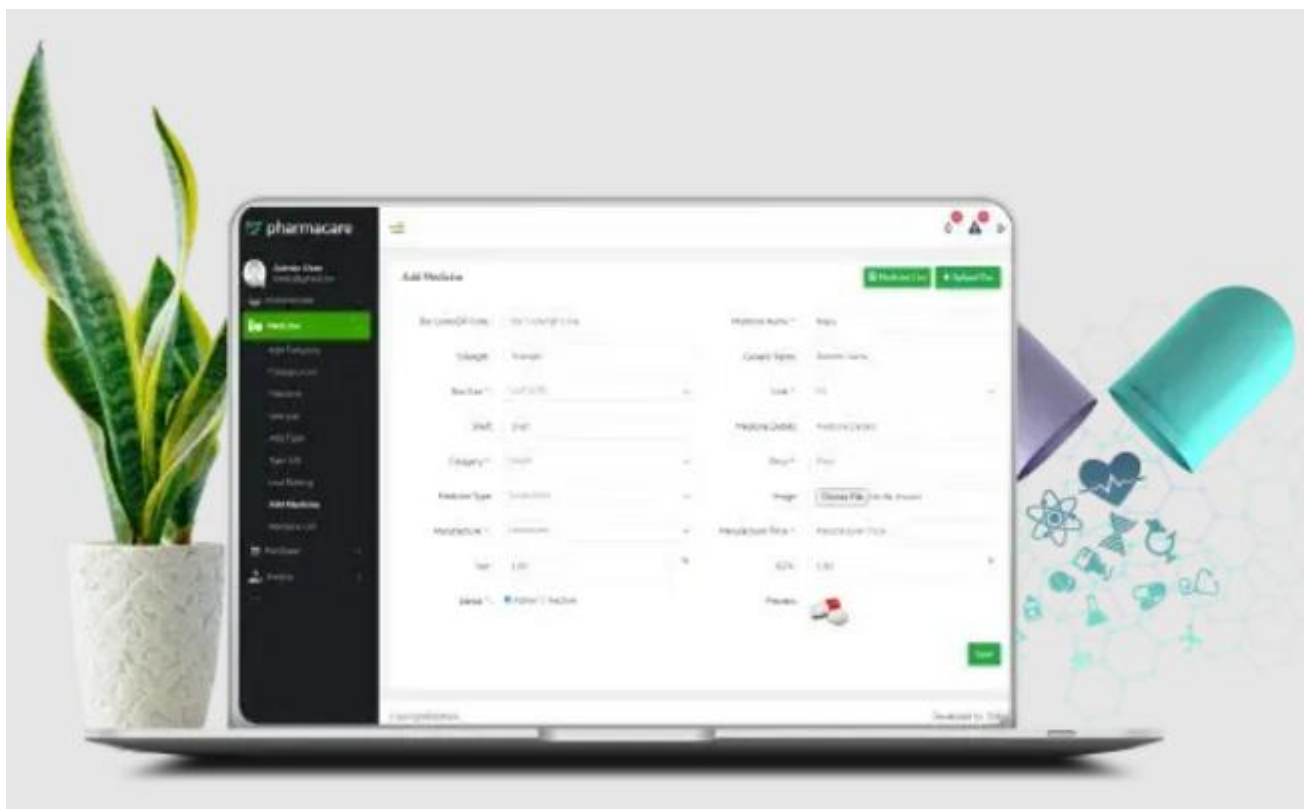
Doctor Patient Appointment System :

A doctor-patient appointment system built on WordPress using the Bookly plugin is a web-based solution designed to streamline the process of scheduling and managing appointments between doctors and their patients. Here's how it typically works:

1. WordPress Platform : WordPress serves as the foundation for the system. It provides the framework for building the website and managing its content.
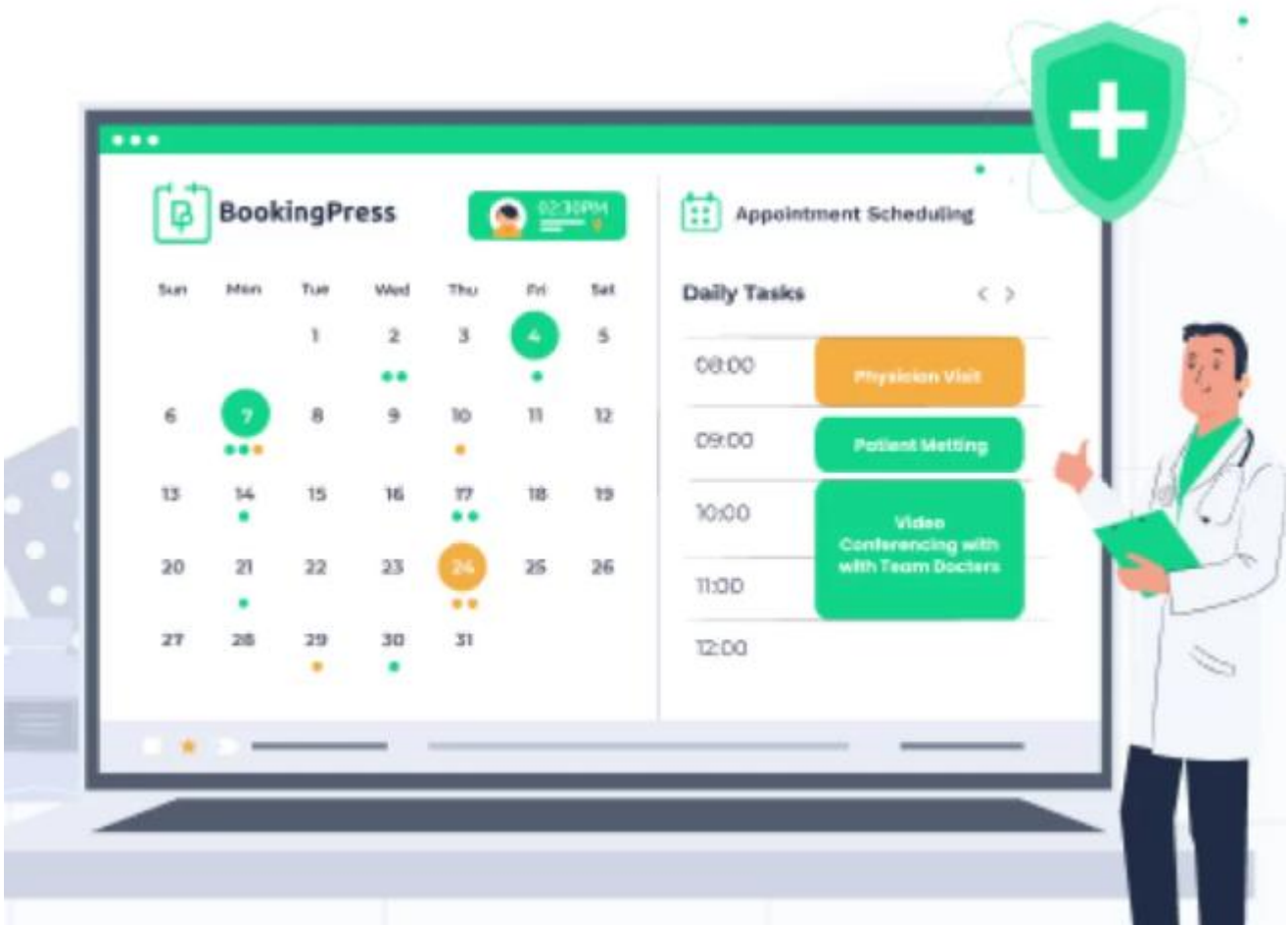
2. Bookly Plugin : Bookly is a popular appointment scheduling plugin for WordPress. It offers a range of features tailored for appointment-based businesses, including doctors' offices.

3. Frontend Interface : The system provides a user-friendly front-end interface where patients can view available appointment slots, select a suitable time, and book an appointment with doctor.

4. Customization : The system can be customized to match the branding and specific needs of the doctor's practice. This may include customizing colors, adding logos, and configuring appointment types and duration.

5. Appointment Management : Doctors and clinic staff have access to a back-end dashboard where they can manage appointments, view patient details, and make scheduling adjustments as needed. They can also set their availability, block off time slots for breaks or emergencies, and manage their overall calendar.

6. Automated Reminders : The system can send automated reminders to both doctors and patients to reduce no-shows and improve appointment attendance rates. These reminders can be sent via email or SMS, depending on the configuration.

7. Payment Integration (Optional) : Some implementations may include payment integration, allowing patients to pay for appointments online at the time of booking or upon arrival at the clinic.

8. Reporting and Analytics : The system may offer reporting and Analytics features, enabling doctors and clinic administrators to track appointment metrics, analyze booking patterns, and make data-driven decisions to optimize scheduling efficiency.

Doctor-Patient appointment system using WordPress and the Bookly plugin provides a convenient and efficient way for patients to book appointments with their healthcare providers while helping doctors and clinic staff manage their schedules effectively.
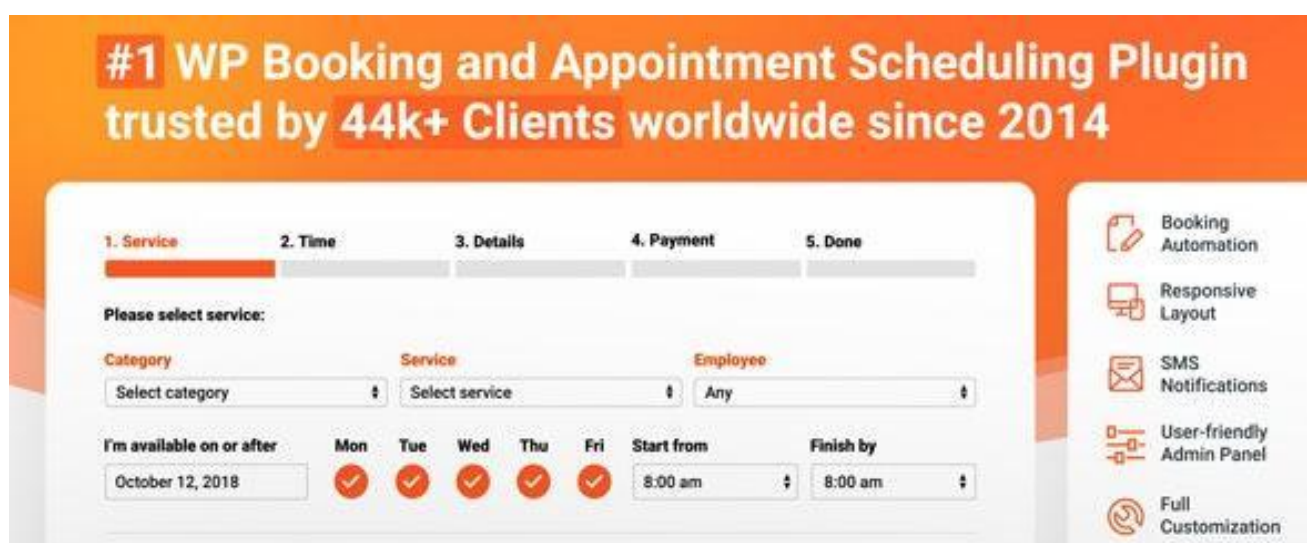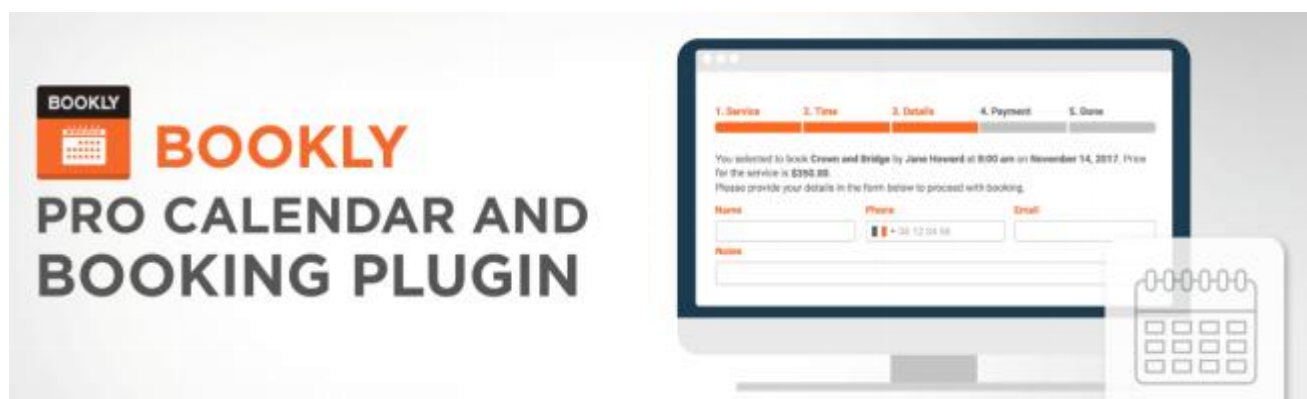
Note : There is no fix price for Appointment Booking System. Price depends on Client's requirements analysis and after discussing project complexity. We prepare proposal and present to Client.

Medical Lab Info Management System :

Enterprise Grade Lab Information Management Software (LIMS) is a specialized software solution designed to manage and streamline laboratory workflows and data management processes. It serves as a centralized system for handling a wide range of laboratory tasks, including sample tracking, data analysis, quality control, and compliance management.
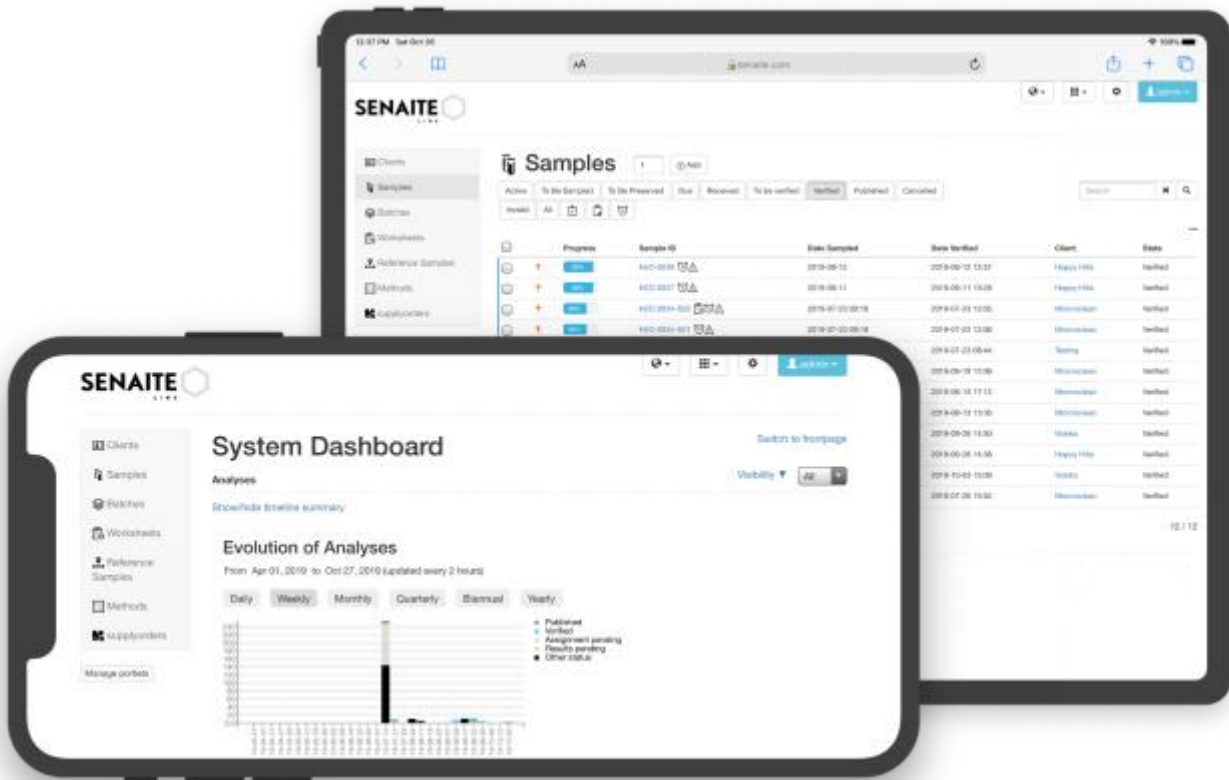
Some key features and functionalities in Senaite LIMS.

1. Sample Management : Software allows laboratories to efficiently manage sample information, including sample registration, tracking, and storage. It supports Barcode labeling, sample accessioning, and chain of custody tracking to ensure accurate sample identification and traceability.

2. Data Management : Software provides a centralized database for storing and managing laboratory data, including test results, experimental data, and associated metadata. It supports version control, audit trails, and data integrity checks to maintain data quality and compliance with regulatory standards.

3. Workflow Management : Software enables laboratories to automate and streamline their workflows, from sample receipt to result reporting. It offers configurable workflow templates, task management tools, and instrument integration capabilities to optimize laboratory processes and minimize turnaround times.

4. Instrument Integration : Software integrates with a wide range of laboratory instruments and equipment to automate data capture and analysis. It supports bidirectional communication with instruments, allowing for seamless transfer of data and results between the LIMS and analytical instruments.

5. Quality Control : Software includes features for managing quality control processes, such as calibration, proficiency testing, and quality assurance. It enables laboratories to monitor instrument performance, track quality control samples, and generate reports to ensure compliance with regulatory requirements.

6. Compliance Management : Software helps laboratories maintain compliance with regulatory standards and accreditation requirements, such as ISO 17025, GLP, CLIA, and FDA regulations. It provides features for documentation management, audit trails, electronic signatures, and compliance reporting to support regulatory inspections and audits.

7. Reporting and Analytics : Software offers robust reporting and Analytics capabilities for generating Customizable reports, graphical dashboards, and data visualizations. It enables laboratories to analyze trends, monitor key performance indicators, and make data-driven decisions to improve operations and research outcomes.

8. User Access Control : Software provides role-based access control to restrict access to sensitive data and functionality based on user roles and permissions. It ensures data security and confidentiality by controlling who can view, modify, or delete information.

Software LIMS offers a comprehensive solution for managing laboratory workflows, data, and compliance requirements effectively, making it a valuable tool for laboratory professionals.

Try SENAITE Lab Software :

NOTE: A **Docker Hub** account is needed. To create account Click Here

Click on Hyperlink below to get 4 hours to try SENAITE LIMS :
http://play-with-docker.com/?stack=https://raw.githubusercontent.com/senaite/senaite.docker/master/stack.yml

A sandbox environment will be created after click "Start" button on above hyperlink. This will take about 2-3 Minutes and the final screen will display a button with the port number 8080 displayed on it. This will open the SENAITE site in your web browser.

NOTE: If the link to port 8080 is not displayed on the site, you have to click the **OPEN PORT** button and enter 8080 in there.

It might be that this site will not load immediately, because the server is still in startup process. Please wait and reload until the SENAITE site appears.

Authentication:
User : admin
Password : admin

SENAITE LIMS Installation :
- Installation (Local or VPS) = $2500 only.

Monthly Support Fee :
$150 per month per location or office. (12 month contract)
- Includes the software, Whats App support, and update software releases.

Performance

Eliminate manual or repetitive tasks to increase the efficiency

Process Automation

Amongst other functionalities, SENAITE comes with highly-customizable workflows to drive users through the analytical process, easy-to-use UI for data registration, automatic import of results, data validation and transition constraints.

Equipment Integration

SENAITE can be easily integrated with instruments by using off-the-shell interfaces for data import and export. Custom interfacing is supported too. Import instrument results and avoid human errors in the carrying over process.

Turnaround Time

Reduce the turnaround time on results reports delivery. Assign priorities to samples and due dates for tests, plan and assign the daily work by using worksheets and keep track of delayed tests immediately.

Radiology Information Management System :

RIS is an acronym for Radiology Information System. As the name implies, a RIS is a software program that facilitates patient workflow throughout a radiology department. Before RIS systems were developed, everything was done by hand. Everything was paper-based, from scheduling books to daily logs to manually created productivity reports. Not only was this very time consuming, it also opened the door to human error.

There are several types of radiology information systems, such as –

1. **Standalone RIS**
2. **Integrated RIS**
3. **Web RIS**
4. **Mobile RIS**
5. **Cloud RIS**
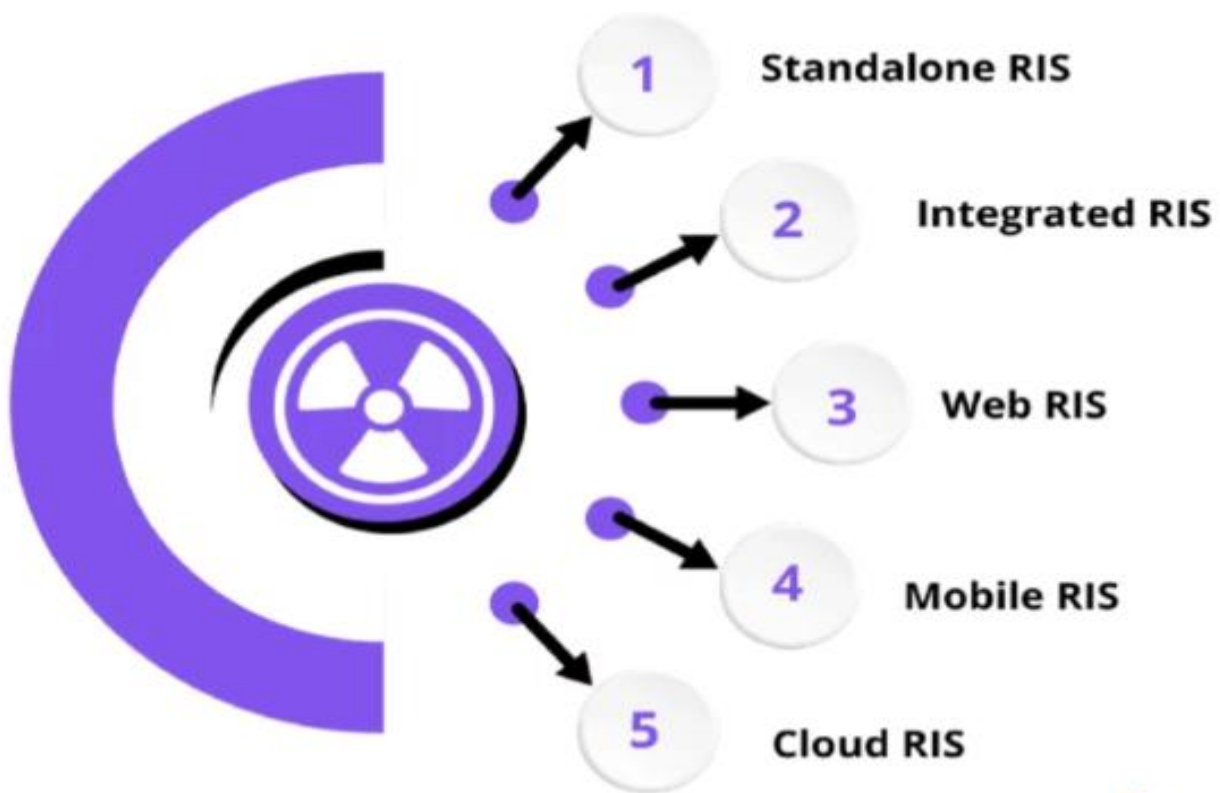
- **Standalone RIS :** A standalone system manages all the radiology tasks for one organization. It cannot connect with other healthcare systems.

- **Integrated RIS:** It integrates with other healthcare information systems (like EMR and PACS). Such RIS facilitates a better overview of a patient's medical history.

- **Web RIS:** Anyone with an active internet connection can log onto this RIS. It is accessible through a web browser.

- **Mobile RIS:** These RIS systems are responsive and run on mobile devices. Users can access these systems on the go.

- **Cloud RIS:** A cloud-based radiology information system is an RIS hosted on a cloud server. A third-party vendor often handles the maintenance of this system. They usually leverage cloud-computing technology in healthcare.

What are the Core Components of Radiology Information System ?

Implementing an RIS can help your workforce streamline processes accurately. You will also be able to reduce medical errors and transcription mistakes in charts. It helps to coordinate care across departments. Send updates from the imaging department to the patient's primary healthcare provider. Apart from this. there are a lot of other functionalities of RIS. It could include :

- Registration,
- Scheduling,
- Billing and reporting,
- Simplifying processes.

Top core components of the radiology information system :

- **Patient Management :**

RIS keeps patient history records and helps in booking, scheduling, and order tracking. It eliminates the need for manual paper-based documentation.

- **Reporting :**

With RIS, you can generate digital reports providing timely and valuable insights. It helps find any bottlenecks, trends, and other key markers. Perfect for optimizing the workflows and performance.

- **Image Storing and Tracking**

The system simplifies tracking images from medical imaging devices and related patient datasets. Store medical images from imaging devices and other patient details on the database.

- **Billing**

This component helps maintain patient billing information and issue electronic invoices. As a result, you can minimize the risks of declined or delayed payments.

- **Data Analytics and Sharing**

With RIS, you can :
- Generate reports on no-show patients.
- Track radiologist workload.
- Track the dollar volume of exams
- and other vital aspects of the radiology department life-cycle.

These reports provide invaluable insights to find gaps in healthcare processes. Sharing actionable insights with concerned stakeholders is much simpler now.

- **HIPAA Compliance Mechanisms**

The radiology software deals with sensitive patient information, like names and personal details. It must follow the Health Insurance Portability and Accountability Act (HIPAA) rules. The Act is in place to protect people's privacy.

Your RIS system should include security measures to avoid breaking HIPAA rules. There might even be severe penalties for negligence. Some basic steps to safeguard involve :

- automatic backups,
- logging off when not in use,
- and end-to-end data encryption.

RIS/PACs Workflow
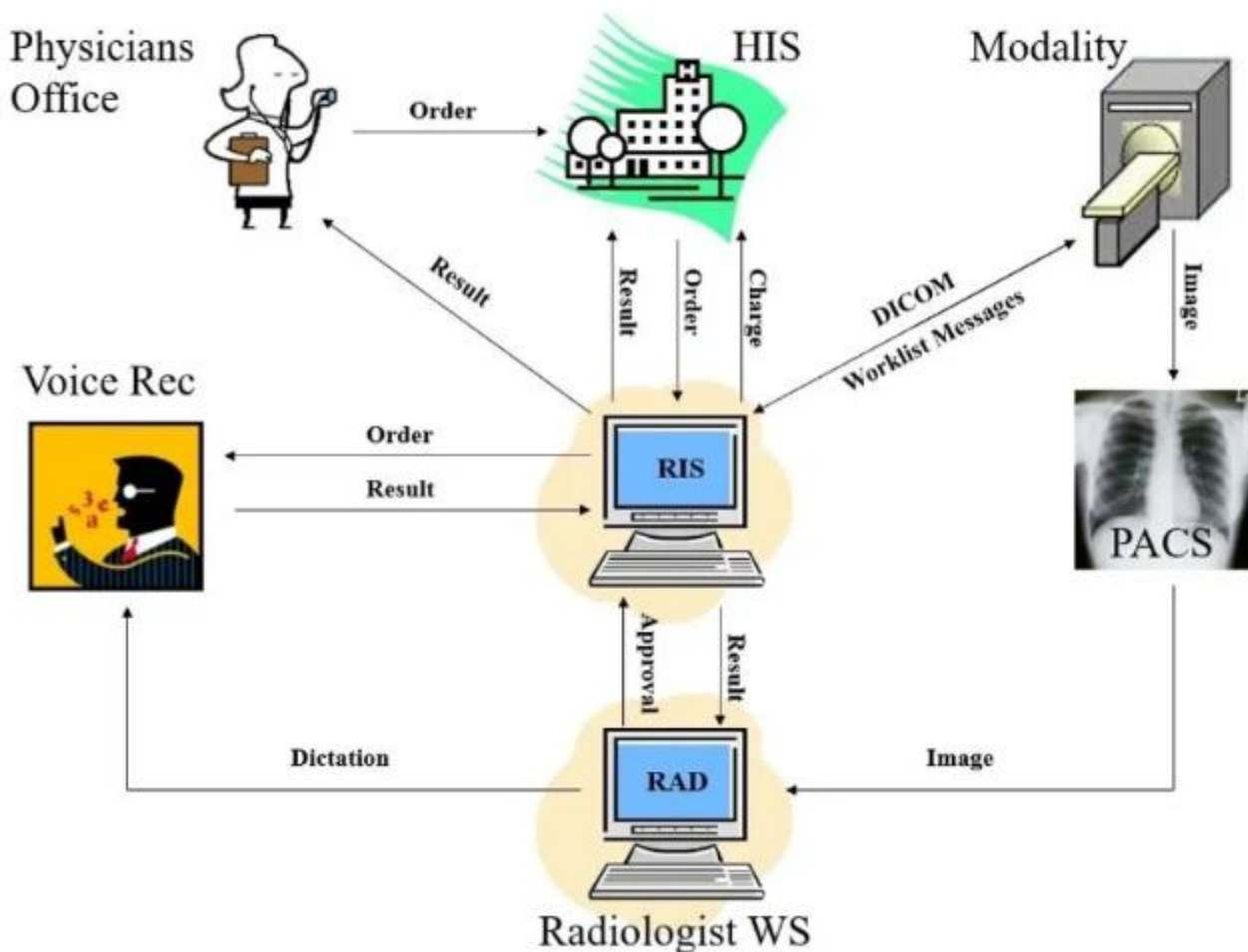
RIS Installation or DEMO:
- There is no ready-made software, We analyze and develop after getting Client's project requirements and delivery time will be normally 5-6 months.

RIS Development Cost (Estimated Not Fix) :
Dedicated Team will be hired for project and Cost will be almost US $25K.
- Includes the software development, User Manual and Technical Documentation.

Healthcare Information Exchange & Database Migration Services (ETL) :

Health Information Exchange (HIE) and Database Migrations are both crucial components in the realm of healthcare data management, albeit serving different purposes.

Health Information Exchange (HIE) :

Health Information Exchange (HIE) refers to the electronic sharing of healthcare-related information among different healthcare organizations, such as hospitals, clinics, laboratories, pharmacies, and other healthcare providers. The primary goal of HIE is to facilitate the secure and interoperable exchange of patient health information across disparate systems and organizations, thereby improving the quality, safety, and efficiency of healthcare delivery.

Key features and benefits of HIE include :

1. Interoperability : HIE enables different healthcare systems and applications to communicate and exchange data seamlessly, regardless of the underlying technology or vendor.

2. Patient Centric Care : HIE allows healthcare providers to access comprehensive and up-to-date patient health records from various sources, enabling more informed clinical decision-making and coordinated care delivery.

3. Reduced Duplication and Errors : HIE helps eliminate redundant tests, procedures, and paperwork by providing access to shared patient information, reducing the risk of medical errors and improving healthcare efficiency.

4. Continuity of Care : HIE promotes continuity of care by ensuring that relevant patient information is available to healthcare providers across different care settings, such as hospitals, primary care offices, and specialty clinics.

5. Public Health Surveillance : HIE supports public health initiatives by facilitating the timely exchange of health data for disease surveillance, outbreak detection, and population health management.

Database Migrations :

Database migration refers to the process of transferring data from one database system or schema to another, typically to upgrade to a new database platform, consolidate multiple databases, or restructure the existing database architecture. In the context of healthcare IT, database migrations are often performed to modernize legacy systems, implement new applications, or comply with regulatory requirements.

Key considerations and best practices for database migrations include:

1. Data Mapping and Transformation : Before migrating data, it's essential to analyze the existing data schema, map data fields between the source and target databases, and implement any necessary data transformations or conversions to ensure data compatibility and integrity.

2. Testing and Validation : Database migrations should be thoroughly tested in a controlled environment to verify data accuracy, completeness, and consistency before deploying changes to production systems. Testing should include both functional and performance testing to identify and address any issues or bottlenecks.

3. Backup and Rollback : It's crucial to create backups of the source data and maintain rollback procedures in case of migration failures or data corruption. This ensures that data can be restored to its original state in the event of unforeseen issues during the migration.

4. Data Governance and Compliance : Database migrations should adhere to data governance policies and regulatory requirements, such as HIPAA (Health Insurance Portability and Accountability Act) in the United States, to protect patient privacy and maintain data security throughout the migration process.

5. Documentation and Communication : Comprehensive documentation should be maintained throughout the migration project, including migration plans, data mapping specifications, testing results, and post-migration procedures. Effective communication with stakeholders is essential to ensure transparency and alignment with business objectives.

In summary, Health Information Exchange (HIE) facilitates the electronic sharing of healthcare data among different organizations, while database migrations involve transferring data between database systems or schemas to support system upgrades, modernization efforts, and regulatory compliance in healthcare IT environments.

HIE / Database Migration Project Initiation Process :

To initiate a Health Information Exchange (HIE) or database migration project for a client in the healthcare sector, We need to gather several key pieces of information to ensure a successful and smooth transition. Here's a list of essential information that we need from the client:

1. Current System Details :
- Information about the client's existing systems and infrastructure, including the types of databases (e.g., MySQL, SQL Server, Oracle) and applications in use.
- Details about the current data storage architecture, including data formats, schemas, and any data transformation processes currently in place.

2. Scope of Work :
- A clear understanding of the client's objectives and goals for the HIE or database migration.
- Specific requirements, such as the scope of data to be migrated, timelines, budget constraints, and any regulatory or compliance considerations.

3. Data Inventory :
- An inventory of the types of data stored in the client's systems, including patient health records, medical images, laboratory results, demographics, and other relevant information.
- Information about the volume and complexity of the data to be migrated, including any data quality issues or inconsistencies that may need to be addressed.

4. Data Mapping and Transformation :
- Detailed data mapping specifications that define how data elements in the source system correspond to those in the target system.
- Requirements for data transformation, cleansing, and normalization to ensure data integrity and compatibility between systems.

5. Integration Requirements :
- Any integration requirements with external systems, such as electronic health record (EHR) systems, laboratory information systems (LIS), radiology information systems (RIS), or third-party applications.
- Specifications for data exchange protocols, standards, and formats, such as HL7, DICOM, FHIR, or other interoperability standards.

6. Security and Privacy :
- Requirements for data security, access control, encryption, and compliance with privacy regulations, such as HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation).
- Any specific security measures or certifications required for handling sensitive healthcare data.

7. Testing and Validation :
- Plans for testing and validating the migration process, including test scenarios, data validation procedures, and acceptance criteria.
- Requirements for staging environments, testing environments, and production cutovers to minimize disruption to operations.

8. Training and Support :
- Training needs for end-users, administrators, and IT staff involved in managing the new system or using HIE functionalities.
- Support and maintenance requirements after the migration or implementation phase, including ongoing technical support, updates, and system monitoring.

9. Documentation and Communication :
- Documentation requirements, including migration plans, technical specifications, data dictionaries, and user manuals.
- Communication channels and protocols for regular updates, status reports, and project milestones throughout the engagement.

By gathering this comprehensive information upfront, We can ensure that the HIE or database migration project is well-defined, properly scoped, and aligned with the client's requirements and expectations.

There is no fix price for HIE or DB Migration. Price depends on Client's requirements analysis and after discussing project complexity. We prepare proposal and present to Client.

HL7 messaging and Interoperability Solutions.

HL7 (Health Level Seven) messages and interoperability play critical roles in facilitating the exchange of health information between different healthcare systems and applications.

HL7 Messages :

HL7 messages are a standardized format used for transmitting healthcare-related data between different systems, such as electronic health record (EHR) systems, laboratory information systems (LIS), radiology information systems (RIS), pharmacy systems, and other healthcare applications. HL7 is a set of international standards developed by the HL7 organization to promote interoperability and the seamless exchange of health information.

HL7 messages typically consist of structured data elements organized into segments, fields, and components, following specific message structures defined by HL7 standards. These messages can convey a wide range of information, including patient demographics, clinical observations, laboratory results, diagnostic images, medication orders, and administrative data.

There are several versions of the HL7 standard, including HL7 v2.x and HL7 v3. HL7 v2.x is the most widely used version and is based on text-based, pipe-delimited messages. HL7 v3

is based on XML and is designed to be more robust and semantically rich, but it has seen less adoption compared to HL7 v2.x.

Interoperability :

Interoperability refers to the ability of different healthcare systems, applications, and devices to seamlessly exchange and use health information effectively. It involves not only technical standards like HL7 but also organizational, semantic, and workflow considerations to ensure that data can be shared, understood, and used across disparate systems and settings.
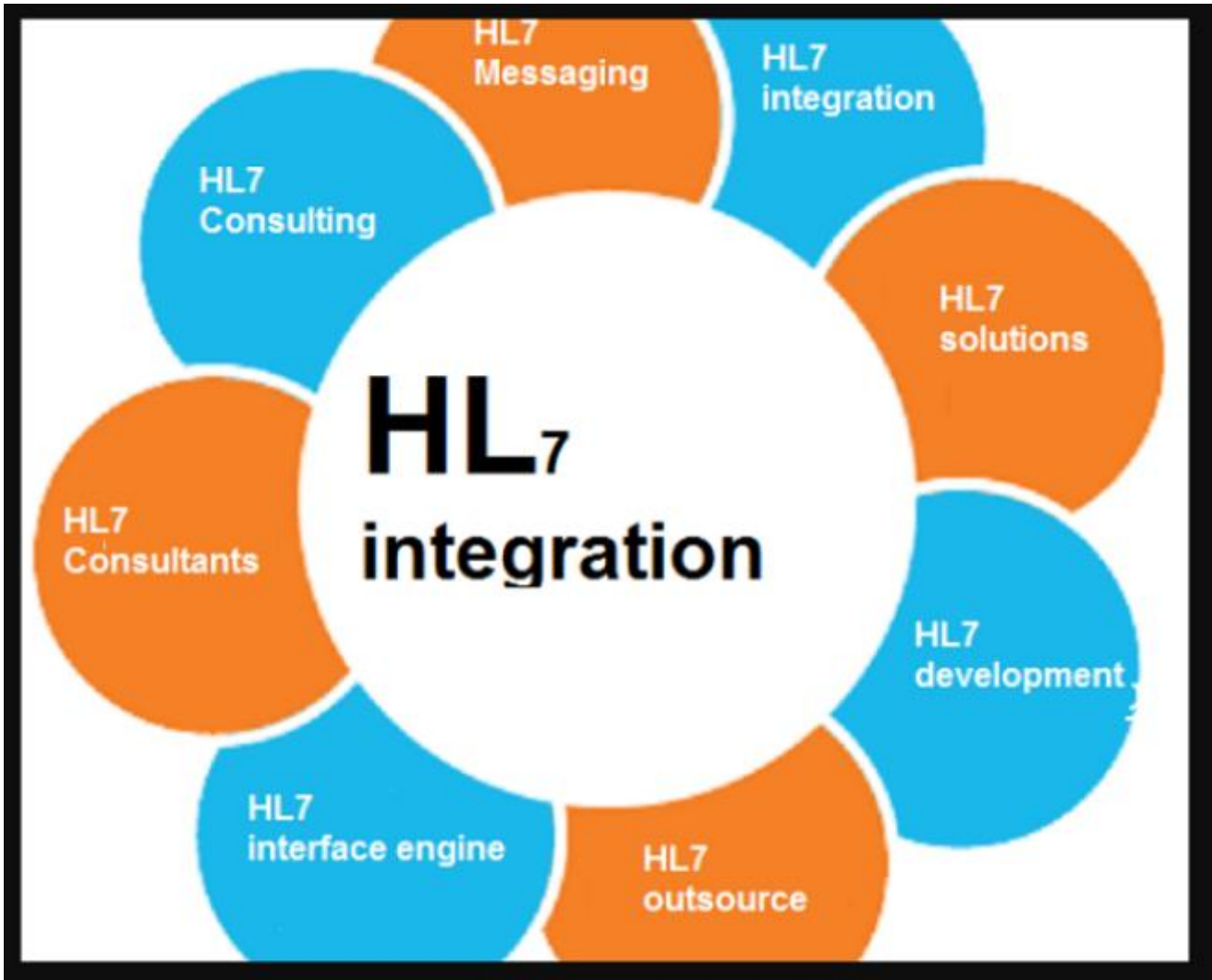
Interoperability enables healthcare providers to access comprehensive and up-to-date patient information from various sources, regardless of the vendor or technology used. It supports continuity of care, care coordination, and informed decision-making by ensuring that relevant health information is available when and where it's needed.

Interoperability can be achieved at different levels, including:

- **Foundational Interoperability :** Ensuring basic connectivity and data exchange capabilities between systems.

- **Structural Interoperability :** Ensuring that data exchanged between systems follows a common format or structure, such as HL7 messages or other standardized formats.

- **Semantic Interoperability :** Ensuring that exchanged data has shared meaning and can be understood and interpreted consistently across systems, regardless of the terminology or code systems used.

Achieving interoperability requires collaboration among healthcare stakeholders, including healthcare providers, technology vendors, standards organizations, policymakers, and regulatory agencies. It involves addressing technical, organizational, regulatory, and cultural barriers to data exchange and collaboration to realize the full potential of health information technology in improving patient care and outcomes.

In summary, HL7 messages and interoperability standards play essential roles in enabling the seamless exchange of health information and promoting interoperability across disparate healthcare systems and applications. They provide the foundation for connected, patient-centered care and support the delivery of high-quality, coordinated healthcare services.

HL7 Messages Format Conversion Services :

HL7 messages format conversion services are specialized tools or software solutions designed to facilitate the transformation of HL7 messages between different versions of the HL7 standard or between HL7 and other healthcare data exchange formats. These services play a crucial role in enabling interoperability and data exchange between disparate healthcare systems and applications that may use different versions of the HL7 standard or non-HL7 formats.

Key features and capabilities for HL7 format conversion services :

1. HL7 Version Conversion :
These services support the conversion of HL7 messages between different versions of the HL7 standard, such as HL7 v2.x and HL7 v3. This includes parsing HL7 messages in one version, interpreting their data elements, and generating equivalent HL7 messages in another version.

2. HL7 to Other Formats Conversion :
In addition to HL7 version conversion, these services may support the conversion of HL7 messages to other healthcare data exchange formats, such as XML, JSON, or CSV. This enables integration with systems and applications that may use non-HL7 formats for data exchange.

3. Other Formats to HL7 Conversion :
Conversely, these services may also support the conversion of non-HL7 formats to HL7 messages. This allows healthcare organizations to ingest data from external sources, such as medical devices, sensors, or third-party applications, and transform it into HL7 messages for integration with their internal systems.

4. Mapping and Transformation :
HL7 messages format conversion services often include tools or capabilities for mapping and transforming data elements between different message formats. This may involve defining mapping rules, data translations, and data validations to ensure that the converted messages adhere to the target format's requirements.

5. Validation and Error Handling :
HL7 messages format conversion services typically include validation and error handling features to ensure data integrity and quality throughout the conversion process. This may involve checking message syntax, semantics, and compliance with HL7 standards, as well as handling errors and exceptions gracefully.

6. Integration and Interoperability :
HL7 messages format conversion services are integrated into healthcare IT ecosystems and interoperable with other systems and applications through standard interfaces, protocols, and APIs. This enables seamless data exchange and interoperability across diverse healthcare environments.

NOTE :
There is no fix price for HL7 Integration, HL7 Interoperability and HL7 Format Conversion.
Price depends on Client's requirements analysis and after discussing project complexity.
We prepare proposal and present to Client.

LMS Radiology Learning Mgmt System :

An LMS (Learning Management System) for radiology, also known as a Radiology Learning Management System (Radiology LMS), is a specialized software platform designed to facilitate the management and delivery of radiology education and training programs. These systems are tailored to the unique needs of radiology departments, residency programs, medical schools, and continuing education providers, offering a comprehensive suite of features to support teaching, learning, and assessment in the field of radiology.

Some key features and functionalities typically offered by LMS platforms specifically designed for radiology education:

1. Course Management : Radiology LMS platforms allow administrators to create, manage, and deliver radiology courses and learning modules. They provide tools for organizing course content, scheduling classes, and setting prerequisites.

2. Content Authoring and Repository : These systems often include built-in authoring tools or support for integrating content from external sources. Radiology educators can create multimedia-rich learning materials, such as lectures, presentations, case studies, and interactive simulations, and store them in a centralized content repository.

3. Virtual Classroom : Radiology LMS platforms may offer virtual classroom capabilities, allowing instructors to conduct live or recorded online lectures, webinars, and interactive sessions. Students can participate in real-time discussions, ask questions, and collaborate with peers.

4. **Learning Resources and Libraries :** Radiology LMS platforms provide access to a wide range of learning resources, including textbooks, journals, articles, videos, images, and reference materials

relevant to radiology education. These resources are often curated and organized to support specific learning objectives and curriculum requirements.

5. Assessment and Evaluation : These systems enable instructors to create and administer assessments, quizzes, exams, and practical exercises to evaluate students' knowledge and skills in radiology. They support various question types, automated grading, and feedback mechanisms to provide learners with timely feedback on their performance.

6. Competency Tracking and Progress Monitoring : Radiology LMS platforms allow administrators and instructors to track learners' progress, monitor their competency development, and generate reports on learning outcomes. They may include competency frameworks, learning plans, and performance dashboards to support competency-based education and training.

7. Collaboration and Communication : Radiology LMS platforms facilitate communication and collaboration among learners, instructors, and administrators through discussion forums, messaging systems, and social learning features. They foster a sense of community and enable knowledge sharing and peer support among radiology learners.

8. Integration with PACS and Imaging Systems : Some advanced Radiology LMS platforms offer integration with Picture Archiving and Communication Systems (PACS) and imaging modalities, allowing learners to access real patient cases, medical images, and diagnostic studies for educational purposes. This integration enhances the realism and relevance of radiology education and training.

Radiology Learning Management Systems play a vital role in modernizing radiology education, providing learners with flexible, interactive, and engaging learning experiences while supporting the evolving needs of radiology educators and training programs.

KFTECH RAD LMS :
provides invaluable
education of radiologists
and trainees

Technology Stack :
Moodle │ OHIF │ PHP Laravel
DICOM + PACS Server Software

NOTE : There is no fix price for Radiology LMS System. Price depends on Client's requirements analysis and after discussing project complexity. We prepare proposal and present to Client.

Patient Tele Monitoring Solutions (IoMT).

Patient Tele-Monitoring Solutions, also known as IoMT (Internet of Medical Things) in the healthcare context, are technological systems designed to remotely monitor patients' health status, vital signs, and medical data outside of traditional healthcare settings, such as hospitals or clinics. These solutions leverage interconnected medical devices, sensors, and communication technologies to collect and transmit patient data in real-time, enabling healthcare providers to monitor patients remotely, make timely interventions, and provide personalized care.

Patient Tele-Monitoring - Key components and features :

1. Medical Devices and Sensors : Patient Tele-Monitoring solutions utilize a variety of medical devices and sensors to capture relevant health data from patients. These devices can include wearable fitness trackers, smartwatches, blood pressure monitors, glucometers, pulse oximeters, ECG monitors, and other remote monitoring devices.

2. Data Collection and Transmission : The collected health data, such as vital signs, activity levels, medication adherence, and symptom data, are transmitted securely to a central monitoring platform or healthcare provider's system using wireless communication technologies, such as Wi-Fi, Bluetooth, or cellular networks.

3. Central Monitoring Platform : Patient Tele-Monitoring solutions typically include a centralized platform or dashboard where healthcare providers can access and review patient data in

real-time. This platform may feature Customizable dashboards, alerts, and Analytics tools to facilitate data interpretation and decision-making.

4. Remote Patient Monitoring : Healthcare providers can remotely monitor patients' health status, trends, and adherence to treatment plans using patient Tele-Monitoring solutions. They can track changes in vital signs, symptoms, and medication adherence, identify potential health issues or deteriorations early, and intervene as needed to prevent complications or hospitalizations.

5. Alerts and Notifications : Patient Tele-Monitoring solutions can generate automated alerts and notifications to healthcare providers in response to predefined thresholds or abnormal patterns detected in patient data. These alerts enable timely interventions and clinical decision-making, reducing the risk of adverse events and improving patient outcomes.

6. Data Integration and Interoperability : Patient Tele-Monitoring solutions may integrate with electronic health record (EHR) systems, health information exchanges (HIE), and other healthcare IT systems to ensure seamless data exchange and interoperability. This integration enables healthcare providers to access patient data within their existing workflows and enhances care coordination.

7. Scalability and Flexibility : Patient Tele-Monitoring solutions are scalable and adaptable to various clinical settings, patient populations, and care pathways. They can be customized to meet the unique needs and requirements of different healthcare organizations, specialties, and use cases.
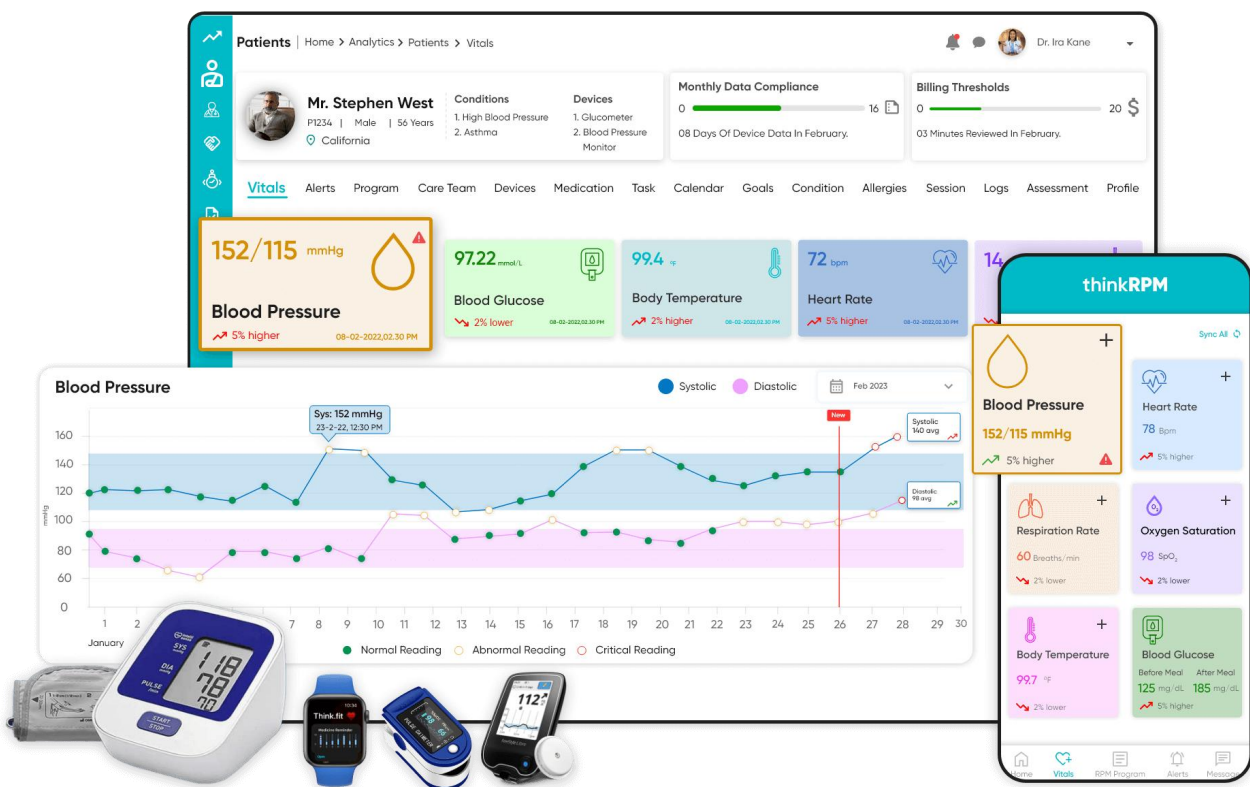
NOTE : There is no fix price for Patient Tele-Monitoring. Price depends on Client's requirements analysis and after discussing project complexity. We prepare proposal and present to Client.

What is Cyber Security ?

CyberSecurity refers to the practice of protecting computer systems, networks, devices, and data from unauthorized access, Cyber attacks, damage, or theft. It encompasses various technologies, processes, and practices designed to ensure the confidentiality, integrity, and availability of digital assets and services. Here are some key benefits of CyberSecurity :

1. Protection Against Data Breaches : CyberSecurity measures help safeguard sensitive data from unauthorized access, preventing breaches that could result in data theft, leakage, or manipulation.

2. Prevention of Financial Loss : Effective CyberSecurity measures mitigate the risk of financial exploitation by preventing unauthorized access to financial systems, transactions, and assets.

3. Maintaining Operational Continuity : Cyber attacks often disrupt business operations by causing system outages, data loss, or service downtime. By implementing robust CyberSecurity measures, organizations can minimize the impact of Cyber incidents and ensure continuity of operations.

4. Preservation of Reputation and Trust : A successful Cyber attack can damage an organization's reputation, erode customer trust, and undermine stakeholder confidence. CyberSecurity helps protect brand integrity by demonstrating a commitment to safeguarding sensitive information.

5. Compliance with Regulatory Requirements : Many industries are subject to regulatory standards and compliance mandates related to data protection and CyberSecurity. Implementing effective CyberSecurity controls helps organizations meet legal and regulatory obligations, avoiding penalties, fines, and legal liabilities associated with non-compliance.

6. Protection of Intellectual Property : Intellectual property (IP) assets such as patents, trademarks, and proprietary information are valuable assets for businesses. CyberSecurity measures safeguard against theft, espionage, or unauthorized access to IP assets, preserving innovation, competitiveness, and business continuity.

CyberSecurity is crucial for safeguarding digital assets, mitigating risks, ensuring business resilience, and fostering trust in the digital ecosystem.

End - Point Security Solutions :

Endpoint security, also known as endpoint protection, refers to the strategy and tools deployed to secure endpoints, such as desktops, laptops, servers, mobile devices, and other devices connected to a network. Endpoint security aims to detect, prevent, and respond to threats targeting these endpoints, ensuring the security and integrity of the network and the data stored on these devices.

Trojans | Ransomware | Malicious Websites | Adware | Spyware

Here are some key benefits of endpoint security:

1. Protection Against Malware : Endpoint security solutions include antivirus, anti-malware, and anti-spyware capabilities that detect and remove malicious software from endpoints. This helps prevent malware infections and protects against ransomware, Trojans, viruses, and other forms of malicious software that can compromise system integrity and steal sensitive data.

2. Data Loss Prevention (DLP) : Endpoint security solutions include data loss prevention features that monitor and control the movement of sensitive data across endpoints, preventing unauthorized access, leakage, or ex-filtration of confidential information. DLP capabilities help organizations maintain compliance with data protection regulations and safeguard intellectual property and customer data.

3. Endpoint Visibility and Control : Endpoint security solutions provide administrators with visibility into endpoint activities, configurations, and vulnerabilities across the network. Centralized management consoles enable administrators to enforce security policies, apply patches and updates, and monitor endpoint compliance to security standards.

4. Incident Response and Remediation : Endpoint security solutions facilitate rapid incident response and remediation by providing real-time alerts, threat intelligence, and forensic analysis capabilities. Automated response actions, such as isolating compromised endpoints, quarantining malicious files, and rolling back unauthorized changes, help contain incidents and minimize the impact of security breaches.

End-Point security plays a crucial role in defending against evolving Cyber threats, securing endpoints from malware attacks, protecting sensitive data, and maintaining compliance with regulatory requirements.

ClamAV is an open source (GPLv2) anti-virus toolkit, provides number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and advanced tool for automatic database updates. https://www.clamav.net Download for Windows, Linux, Mac.

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Intrusion Detection/Prevention System :

IDS and IPS are CyberSecurity solutions for network security by detecting/preventing malicious activities.
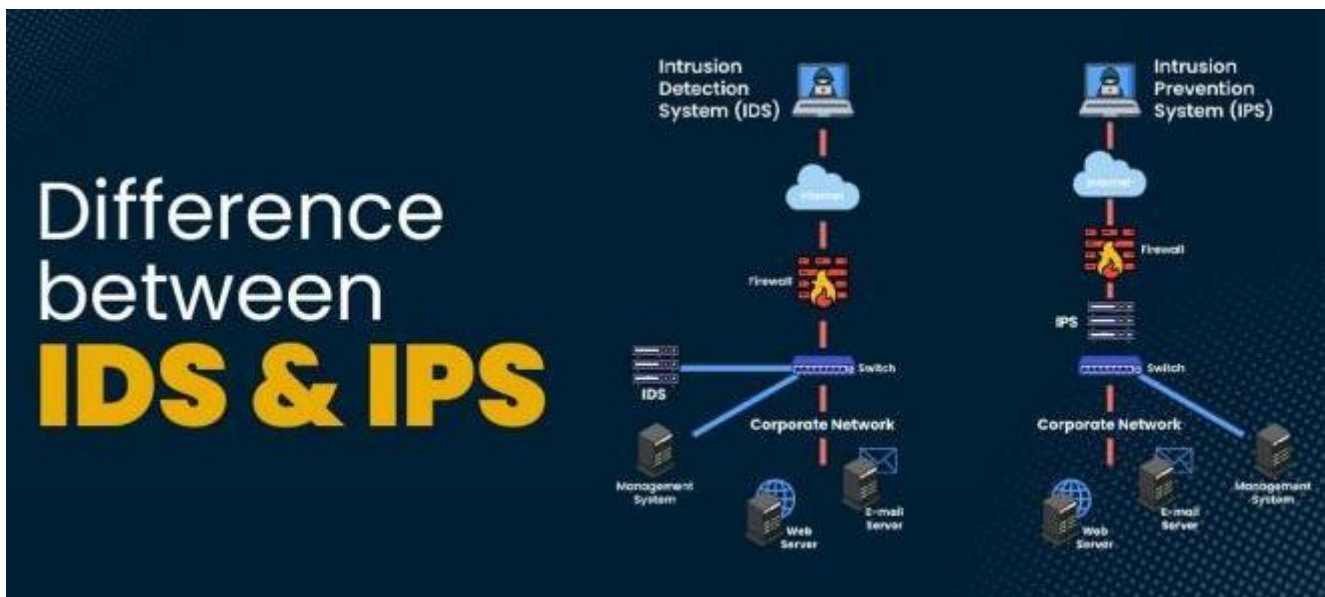
1. IDS (Intrusion Detection System) :

- An IDS is a security tool that monitors network traffic or system activities for suspicious patterns or signs of security threats.
- It analyzes incoming and outgoing network packets, logs, and system events in real-time to identify potential security incidents.
- IDS can detect various types of threats, including unauthorized access attempts, malware infections, denial-of-service (DoS) attacks, and policy violations.
- When an IDS detects suspicious activity, it generates alerts or notifications to notify security administrators, allowing them to investigate and respond to potential threats.
- IDS operates in a passive mode. it detects/alerts suspicious activity but does not prevent attacks.

2. IPS (Intrusion Prevention System) :

- An IPS is an advanced security tool that not only detects but also actively blocks or prevents security threats in real-time.
- Like an IDS, an IPS monitors network traffic or system activities for signs of malicious behavior, using similar detection techniques such as signature-based detection, anomaly detection, and behavioral analysis.
- However, unlike an IDS, an IPS has the capability to take automated action to block or mitigate identified threats, such as dropping malicious packets, terminating connections, or updating firewall rules to block malicious IP addresses.
- IPS is deployed inline within the network traffic flow, allowing it to inspect and filter traffic in real-time before it reaches its destination.
- By actively blocking threats at the network perimeter or within the internal network, IPS helps prevent security breaches, data ex-filtration, and service disruptions caused by cyberattacks.

IDS and IPS are both essential components of network security infrastructure, providing complementary capabilities for threat detection and prevention.

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Vulnerability Assessment & Pen Testing (VAPT) :

VAPT stands for Vulnerability Assessment and Penetration Testing. It's a comprehensive security testing approach used to identify and address vulnerabilities in an organization's information systems, applications, networks, and infrastructure.
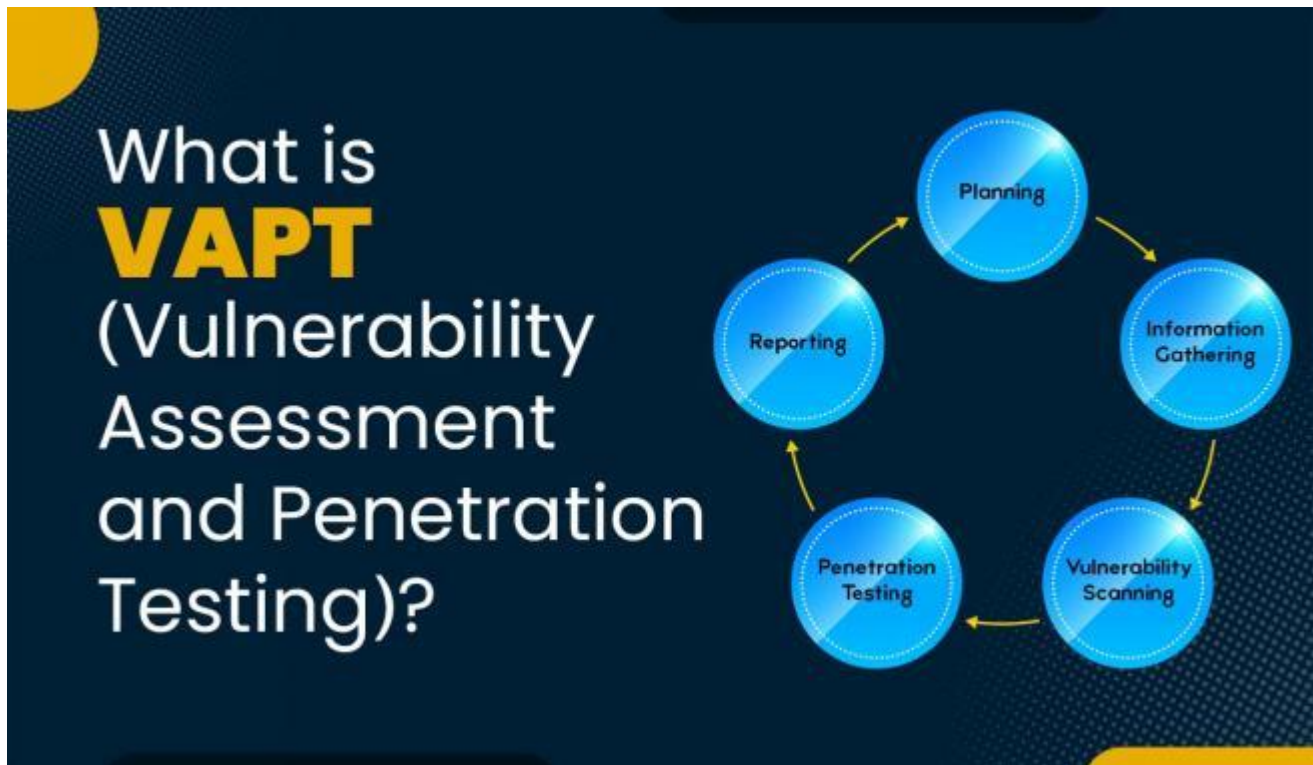
1. Vulnerability Assessment (VA) :
- Vulnerability assessment involves the systematic examination of IT systems, networks, and applications to identify security weaknesses or vulnerabilities.
- This process typically includes automated scanning tools and manual inspection techniques to discover known Vulnerabilities, Misconfigurations, and weaknesses in software, hardware, or system configurations.
- Vulnerability assessments provide organizations with a prioritized list of vulnerabilities, along with recommendations for remediation or mitigation to strengthen their security posture.

2. Penetration Testing (PT) :
- Penetration testing, also known as ethical hacking, involves simulating real-world cyberattacks to evaluate the security of an organization's systems and networks.
- Penetration testers, often referred to as ethical hackers, attempt to exploit identified vulnerabilities to gain unauthorized access, escalate privileges, or compromise sensitive data.
- Penetration testing methodologies may include reconnaissance, vulnerability exploitation, privilege escalation, lateral movement, and ex-filtration of data.
- The goal of penetration testing is to identify security weaknesses that could be exploited by malicious actors and provide recommendations to improve defensive measures and mitigate risks.

By combining vulnerability assessment and penetration testing, VAPT provides a comprehensive evaluation of an organization's security posture and helps identify and remediate vulnerabilities before they can be exploited by attackers. It helps organizations:

- Identify and prioritize security vulnerabilities based on their severity and potential impact on business operations.

- Evaluate the effectiveness of existing security controls and defenses in detecting and preventing Cyber threats.

- Identify gaps and weaknesses in security policies, procedures, and configurations.

- Improve incident response preparedness by simulating real-world cyberattacks and testing incident detection and response capabilities.

- Enhance overall security awareness and promote a proactive approach to CyberSecurity risk management.

VAPT is an essential component of a robust CyberSecurity program and is often conducted periodically or in response to significant changes in an organization's IT environment, such as new system deployments, software updates, or regulatory requirements.
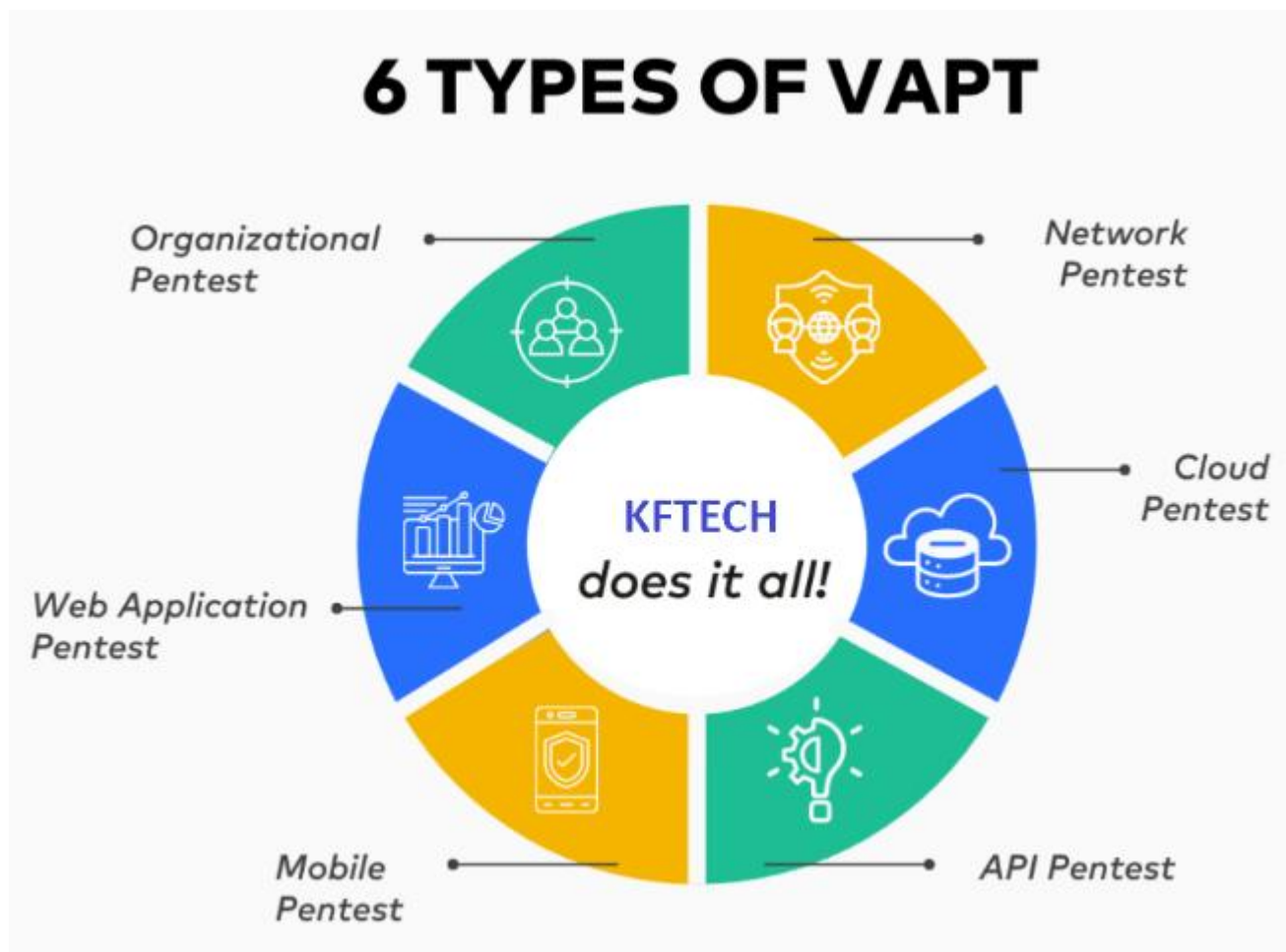
For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Web Application Firewall (WAF) :

A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.
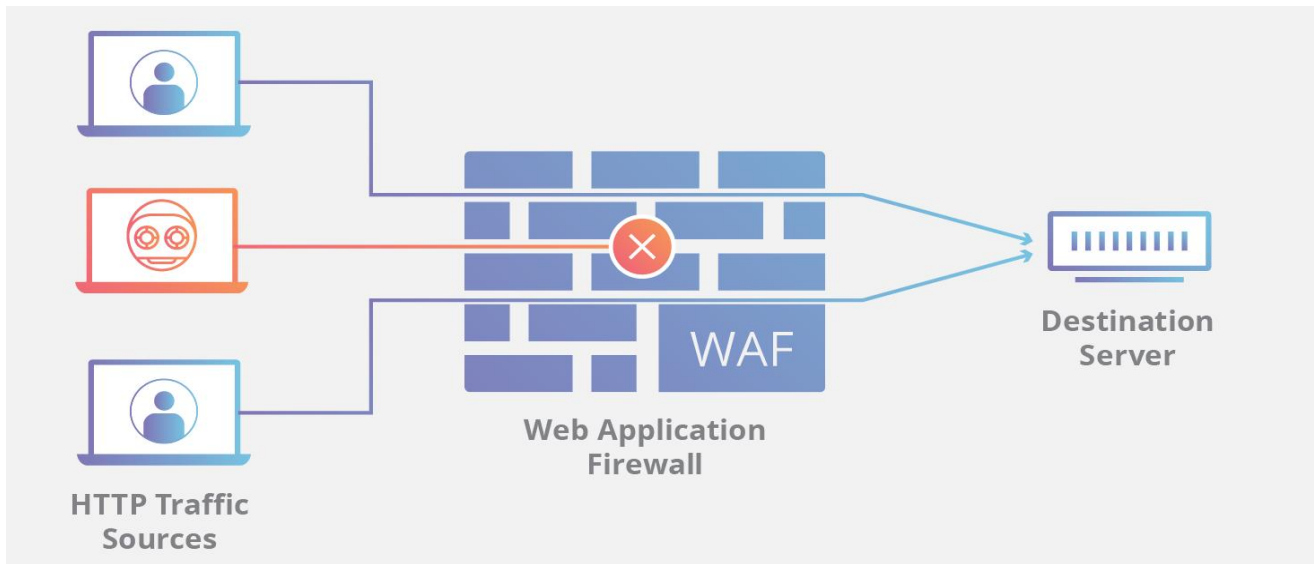
By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies. A WAF can be implemented in three different ways Network-based, Host-based, Cloud-based **:**

Network Based WAF

They have low latency as they are installed locally

Host Based WAF

It is easy to fully integrate it into the software of a web application

Cloud Based WAF

These are also regularly updated so that hackers can't use the vulnerabilities to access the user data

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Website and Network Monitoring Solutions :

Website and network monitoring are both essential components of a comprehensive IT infrastructure monitoring strategy, but they focus on different aspects of an organization's digital environment.
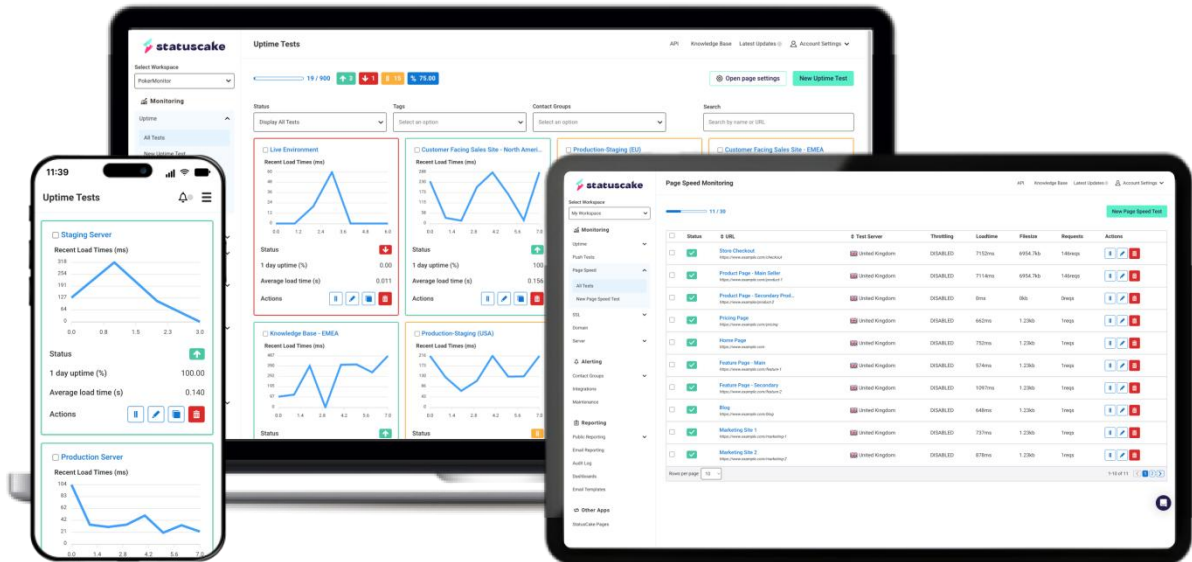
1. Website Monitoring :

- Website monitoring involves the continuous observation and measurement of a website's performance, availability, and functionality.
- It checks various aspects of a website, including uptime, response time, page load speed, and functionality of critical features such as login forms, checkout processes, and API endpoints.
- Website monitoring tools use synthetic transactions or real user monitoring (RUM) to simulate user interactions with the website and detect issues such as downtime, slow page loads, broken links, and errors.
- The goal of website monitoring is to ensure a positive user experience, minimize downtime, and identify and resolve issues that may impact website performance and availability.

2. Network Monitoring :

- Network monitoring involves the continuous surveillance of network infrastructure, devices, and traffic to detect and analyze performance issues, security threats, and anomalies.
- It monitors network devices such as routers, switches, firewalls, servers, and endpoints to collect data on network traffic, bandwidth usage, latency, packet loss, and device health.
- Network monitoring tools use SNMP (Simple Network Management Protocol), packet sniffing, flow monitoring, and other techniques to gather network performance metrics and identify abnormal behavior or security incidents.
- The goal of network monitoring is to ensure the optimal performance, availability, and security of the network infrastructure, detect and troubleshoot network issues, and prevent or mitigate network outages and security breaches.

While website monitoring focuses on the user-facing aspects of a website and ensures its availability and performance from the end user's perspective, network monitoring provides visibility into the underlying

infrastructure that supports the website's operation. Both types of monitoring are crucial for maintaining the reliability, performance, and security of an organization's digital assets and ensuring a positive user experience. Integrating website and network monitoring tools allows organizations to proactively identify and resolve issues affecting website availability, performance, and security, ultimately improving overall operational efficiency and customer satisfaction.

A comprehensive Monitoring Suite that includes Audit, Monitoring, Configuration Management, Remote Control, ITSM, Inventory and System Security.

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Incident Management and Response Solutions :

A website incident response system is a structured process and set of procedures implemented by an organization to effectively detect, analyze, mitigate, and recover from security incidents that affect their website or web applications. It involves a coordinated effort among various stakeholders, including IT teams, security personnel, developers, and management, to respond promptly and efficiently to incidents that threaten the security, availability, or integrity of the website.

Incident response system include :

1. Incident Detection : Monitoring tools and technologies are used to detect abnormal behavior, security breaches, or unauthorized activities on the website or web server. This may involve network monitoring, log analysis, intrusion detection systems (IDS), web application firewalls (WAF), and other security solutions.

2. Incident Triage : When a potential incident is detected, it is triaged to determine its severity, impact, and urgency. Incident triage involves assessing the nature of the incident, identifying affected systems or assets, and prioritizing response efforts based on predefined criteria and risk assessment.

3. Response Planning : A predefined set of response procedures, workflows, and escalation paths are established to guide the response to different types of incidents. Response plans outline roles and responsibilities, communication protocols, containment strategies, and steps for evidence preservation and forensic analysis.

4. Containment and Mitigation : Immediate actions are taken to contain the incident and prevent further damage or unauthorized access. This may involve isolating affected systems, blocking malicious traffic, applying patches or fixes, resetting compromised credentials, or temporarily taking the website offline if necessary.

5. Investigation and Analysis : A thorough investigation is conducted to determine the root cause of the incident, identify the attack vectors or vulnerabilities exploited, and gather evidence for forensic analysis. This may involve examining logs, analyzing network traffic, reviewing system configurations, and collaborating with internal or external security experts.

6. Communication and Notification : Transparent and timely communication with stakeholders, including customers, partners, regulators, and the public, is essential to manage the impact of the incident and maintain trust and credibility. Incident notifications may include details of the incident, its impact, and mitigation measures being taken.

7. Remediation and Recovery : Once the incident is contained and investigated, remediation measures are implemented to address the root cause of the incident and prevent similar incidents from occurring in the future. This may involve patching vulnerabilities, improving security controls, updating policies and procedures, and enhancing employee training and awareness.

8. Post-Incident Review : After the incident has been resolved, a post-incident review or "lessons learned" session is conducted to evaluate the effectiveness of the incident response process, identify areas for improvement, and update incident response plans and procedures accordingly.

Incident response system is crucial for organizations to effectively manage security incidents and minimize the impact on their website, reputation, and business operations.
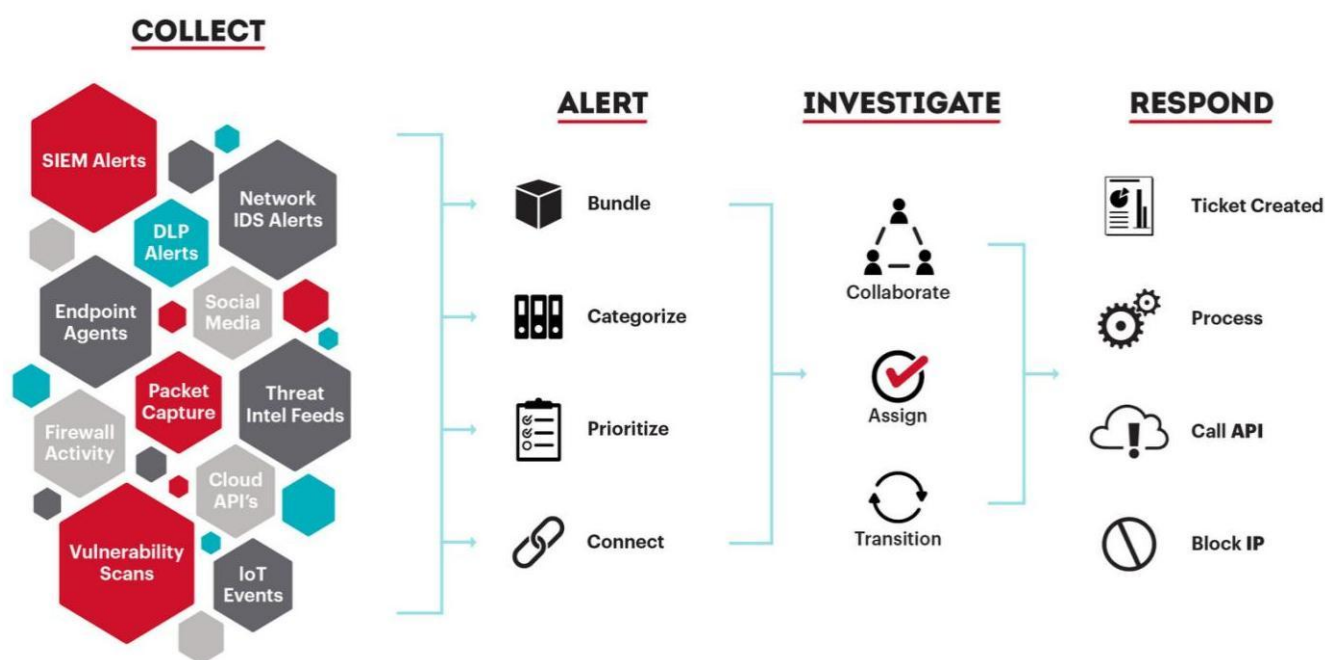
Website Secure Backup Solutions :

Website backup solutions are tools or services designed to create copies of a website's data, files, databases, and configurations, allowing users to restore the website to a previous state in the event of data loss, corruption, or security incidents. These solutions are crucial for safeguarding website content, ensuring business continuity, and mitigating the risks associated with website outages.
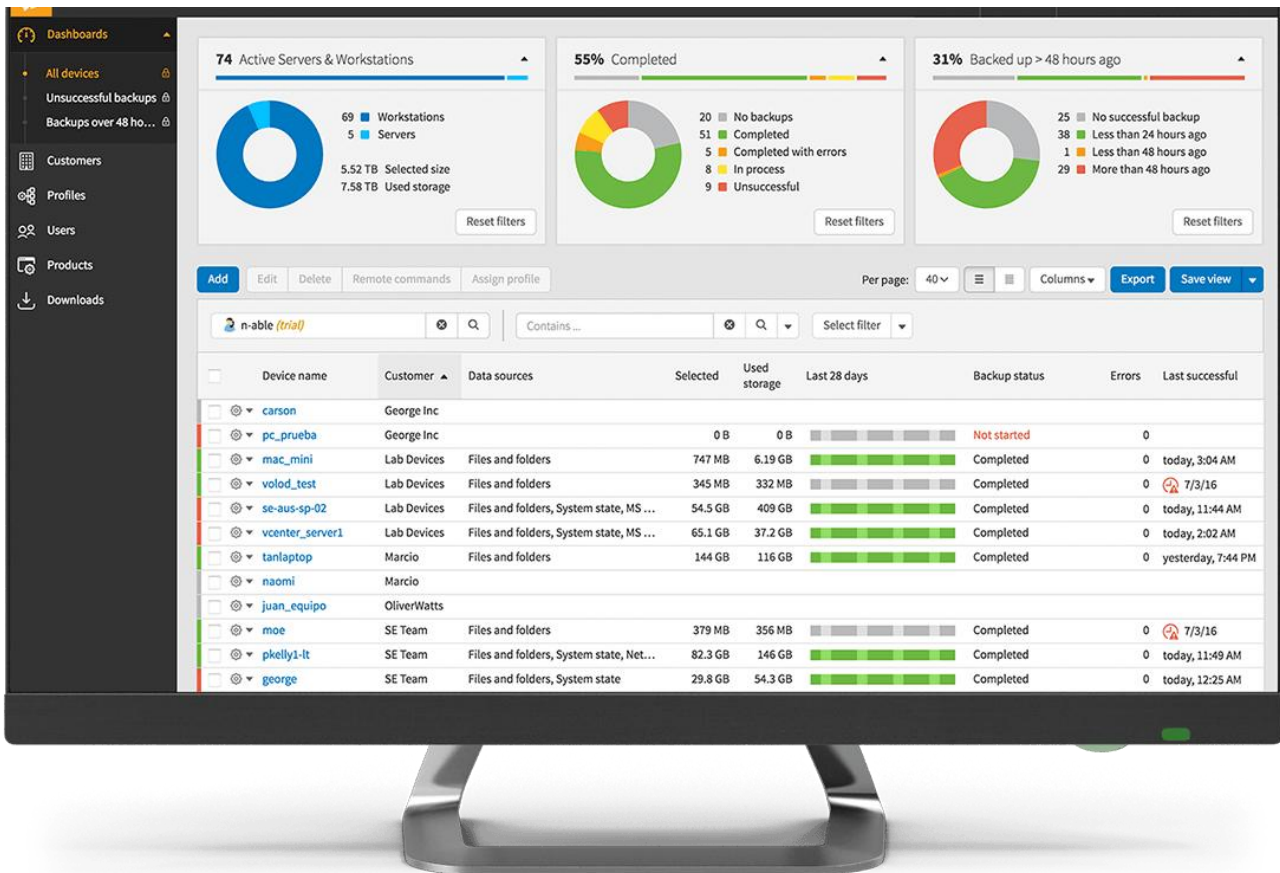
Website backup solutions include :

1. Automated Backup : Website backup solutions typically offer automated scheduling capabilities to perform regular backups of website data and files. This ensures that backups are created at predefined intervals without manual intervention, reducing the risk of data loss due to human error or oversight.

2. Full and Incremental Backups : Website backup solutions may support different backup types, including full backups and incremental backups. Full backups create copies of all website data and files, while incremental backups only capture changes made since the last backup, reducing storage requirements and backup times.

3. File and Database Backup : Website backup solutions often provide the ability to back up both website files (HTML, CSS, JavaScript, images, etc.) and databases (MySQL, PostgreSQL, MongoDB, etc.). This ensures that all components of the website, including content, settings, and user data, are included in the backup process.

4. Storage Options : Backup solutions may offer various storage options for storing backup files, including local storage, network-attached storage (NAS), cloud storage, and remote servers. Cloud storage options provide scalability, redundancy, and off-site storage, enhancing data protection and disaster recovery capabilities.

5. Versioning and Retention Policies : Website backup solutions may support versioning and retention policies to manage backup files effectively. Versioning allows users to store multiple versions of backups, enabling them to roll back to specific points in time if needed. Retention policies define how long backup files are retained before they are automatically deleted or archived.

6. Encryption and Security : To ensure the confidentiality and integrity of backup data, website backup solutions may offer encryption features to encrypt backup files both in transit and at rest. This helps protect sensitive information from unauthorized access, interception, or tampering during the backup process.

7. Restore and Recovery : Website backup solutions provide tools and interfaces for restoring website data and files from backup copies in the event of data loss or corruption. Users can initiate restore operations to recover the website to a previous state, minimizing downtime and restoring normal operations quickly.

Website backup solutions are essential for maintaining the availability, integrity, and security of websites by providing reliable data protection and recovery mechanisms. By implementing a robust backup strategy, organizations can mitigate the risks associated with website outages, cyberattacks, and data loss incidents, ensuring the continuity of their online presence and business operations.

WordPress Site Migration & Backup

Easy, Fast, Powerful

Scheduled Backups
Back up now or schedule it. Recover from failures within minutes.

Move WordPress With Ease
1. Bundle your site into a package.
2. Copy package to new host/domain.
3. Browse to the installer wizard.

Cloud Backups
Back up to Dropbox, FTP, Google Drive, OneDrive, or Amazon S3 for safe storage.

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Cloud Flare Zero Trust Solution :

Cloudflare Zero Trust is a security framework that shifts the focus from a traditional perimeter-based security model to a model where trust is established based on the identity of the user and the context of the access request. It ensures secure access to applications and data regardless of the user's location or device. **Zero Trust Network Access (ZTNA)** replaces traditional VPNs with a more secure, scalable, and user-friendly solution.

Why Use Cloudflare Zero Trust Solution?

1. Enhanced Security : Traditional security models rely on securing the perimeter, but with increasing remote work and cloud applications, the perimeter is no longer well-defined. Cloudflare Zero Trust protects resources by verifying every access attempt.

2. Reduced Risk : By applying the principle of least privilege, where users only get access to what they need, the risk of insider threats and data breaches is minimized.

3. Improved User Experience : Users get seamless access to applications without the need for cumbersome VPNs. This leads to better performance and productivity.

4. Scalability : Cloudflare's global network ensures that the solution can scale with the needs of businesses of all sizes, providing reliable performance regardless of user location.

5. Simplified Management : Centralized management of security policies across all applications and users reduces the complexity for IT teams.

Benefits of Using Cloudflare Zero Trust Solution :

1. Secure Access to Applications : Cloudflare provides secure, authenticated access to internal applications without exposing them to the internet.

2. DDoS Protection and Performance Optimization : Integrated DDoS protection and performance enhancements ensure that applications are not only secure but also performant.

3. Identity and Access Management Integration : Integration with major identity providers (IdPs) simplifies user authentication and access control.

4. Comprehensive Security Monitoring : Continuous monitoring and logging of user activity help in detecting and responding to threats swiftly.

5. Data Loss Prevention (DLP) : Policies can be set to prevent sensitive data from being accessed.

6. Device Posture Checks : Ensure that devices meet security standards before granting access, adding an additional layer of security.

7. Zero Trust Network Access (ZTNA) : Replaces traditional VPNs with a more secure, scalable, and user-friendly solution.

8. Simplified Security Posture : Unifies multiple security functions into a single platform, simplifying the overall security infrastructure.

9. Regulatory Compliance : Helps in achieving compliance with various regulations by ensuring robust access controls and monitoring.

Cloudflare Zero Trust is a modern security approach designed to secure access to applications and data in a world where traditional network perimeters no longer exist. By using this solution, organizations can enhance their security posture, reduce risk, improve user experience, and streamline their security management efforts.

The Power of Zero Trust

Cloudflare Zero Trust Security Platform

Set granular access controls for your networks and resources.

Advanced threat detection and response capabilities.

Segment your network and limit the access of devices and users to specific resources.

End-to-end encryption is provided to protect data in transit and at rest.

Multiple forms of authentication are supported, including biometrics, password-less, and multi-factor authentication.

Designed to help you meet compliance requirements for data security and privacy regulations such as GDPR, HIPAA and SOC 2.

Flexible and scalable architecture that can adapt to the changing needs of your organisation.

Integrates with a wide range of third-party tools and systems.

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Digital Forensic Solutions :

Digital forensics is a branch of forensic science focused on the recovery, investigation, and analysis of data found in digital devices. It is used to identify, preserve, recover, analyze, and present facts and opinions about digital information, often in relation to computer crimes. The goal of digital forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a digital device and who was responsible for it.

Key Areas of Digital Forensics

1. Computer Forensics : Deals with the investigation of computers, including desktop and laptop systems. It involves analyzing data stored on hard drives, solid-state drives, and other storage media to uncover evidence.

2. Network Forensics : Involves monitoring and analyzing computer network traffic to collect important information and evidence. It is often used to investigate CyberCrimes like hacking, unauthorized access, and data breaches.

3. Mobile Device Forensics : Focuses on the retrieval of data from mobile devices such as smartphones and tablets. This can include call logs, text messages, emails, photos, and GPS data.

4. Database Forensics : Involves the examination of databases and their metadata to uncover evidence. It is particularly useful in cases of database tampering, fraud, or unauthorized access.

5. Malware Forensics : Involves analyzing malicious software to understand its origin, functionality, and impact. This can include viruses, worms, Trojans, ransomware, and spyware.

6. Cloud Forensics : Deals with the investigation of data stored in cloud computing environments. It involves collecting and analyzing data that is distributed across multiple locations and often involves dealing with complex legal issues related to data ownership and jurisdiction.

Applications of Digital Forensics :

- ◆ **Criminal Investigations :** Helping law enforcement agencies to investigate and solve crimes involving digital devices.

- ◆ **Corporate Investigations :** Assisting companies in investigating internal fraud, intellectual property theft, and violations of company policies.

- ◆ **Incident Response :** Supporting CyberSecurity teams in responding to data breaches, hacking attempts, and other Cyber incidents.

- ◆ **Legal Proceedings :** Providing evidence and expert testimony in civil and criminal court cases.

Importance of Digital Forensics :

- ◆ **Crime Solving :** Essential in solving crimes involving digital technology, such as Cyber crimes, financial fraud, and identity theft.

- ◆ **Evidence Preservation :** Ensures that digital evidence is preserved in a manner that is admissible in court.

- ◆ **Data Recovery :** Helps in recovering lost or deleted data that may be critical to an investigation.

- ◆ **CyberSecurity :** Plays crucial role in understanding and mitigating threats and vulnerabilities.

- ◆ **Compliance :** Assists organizations in meeting legal and regulatory requirements related to data security and privacy.

Digital forensics is a critical field in today's digital age, providing the tools and techniques necessary to uncover and analyze digital evidence in a variety of contexts.

Data Loss Prevention Solution :

Data Loss Prevention (DLP) is a set of technologies, tools, and processes used to ensure that sensitive information does not get lost, misused, or accessed by unauthorized users. DLP systems monitor and control data flows across an organization's network to prevent unauthorized disclosure of sensitive information. This includes data at rest, in motion, and in use. DLP solutions are designed to detect and prevent data breaches by identifying, monitoring, and protecting data across various environments.
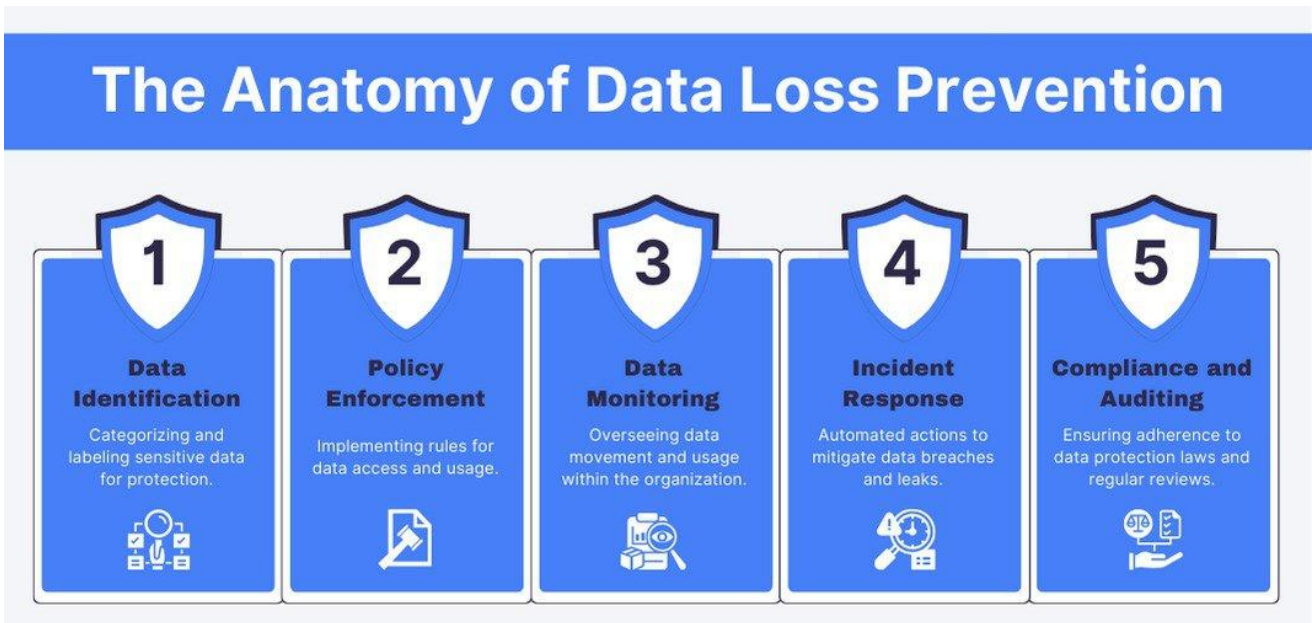

Key Functions of DLP :

1. Data Identification : Identifies sensitive data within an organization, such as Personally Identifiable Information (PII), financial data, intellectual property, and other critical business information.

2. Data Monitoring : Continuously monitors data as it moves through and out of the network to detect and prevent unauthorized access or transmission.

3. Data Protection : Implements policies and controls to prevent data loss, including encryption, access controls, and blocking unauthorized activities.

4. Policy Enforcement : Enforces organizational policies regarding data usage and transmission, ensuring compliance with regulations and standards.

5. Reporting and Alerts : Generates alerts and reports on data loss incidents, policy violations, and overall data security posture.

Benefits of Using Data Loss Prevention :

1. Protects Sensitive Information : DLP solutions help safeguard sensitive data, such as customer information, financial records, and intellectual property, from unauthorized access and breaches.

2. Regulatory Compliance : DLP helps organizations comply with data protection regulations and standards, such as GDPR, HIPAA, PCI DSS, and others, by enforcing policies and protecting sensitive data.

3. Prevents Data Breaches : By monitoring and controlling data flow, DLP systems can prevent data breaches caused by internal or external threats, reducing the risk of financial loss, reputational damage, and legal consequences.

4. Reduces Insider Threats : DLP helps detect and prevent data exfiltration by malicious or negligent insiders by monitoring user activities and enforcing strict data access controls.

5. Enhances Data Visibility : Provides comprehensive visibility into data movement and usage across the organization, helping identify vulnerabilities and areas of improvement in data security practices.

6. Protects Intellectual Property : DLP solutions prevent the unauthorized sharing or leaking of intellectual property and trade secrets, preserving the competitive edge of the organization.

7. Supports Endpoint Security : DLP extends protection to endpoints, ensuring that data on devices such as laptops, smartphones, and tablets is secure even when used outside the corporate network.

8. Improves Incident Response : By providing real-time alerts and detailed reports on data incidents, DLP systems enable faster detection and response to potential data loss events.

9. Reduces Human Error : DLP policies can prevent accidental data leakage by blocking unauthorized actions, such as sending sensitive information to the wrong recipient or uploading to unsecured platforms.

10. Supports Data Classification and Management : DLP solutions assist in classifying and managing data, ensuring that sensitive information is appropriately handled and protected throughout its lifecycle.

Data Loss Prevention is a critical component of an organization's overall data security strategy. By implementing DLP solutions, organizations can protect sensitive information, comply with regulatory requirements, prevent data breaches, and reduce the risk of insider threats. The visibility, control, and protection offered by DLP systems help safeguard an organization's most valuable asset: its data.
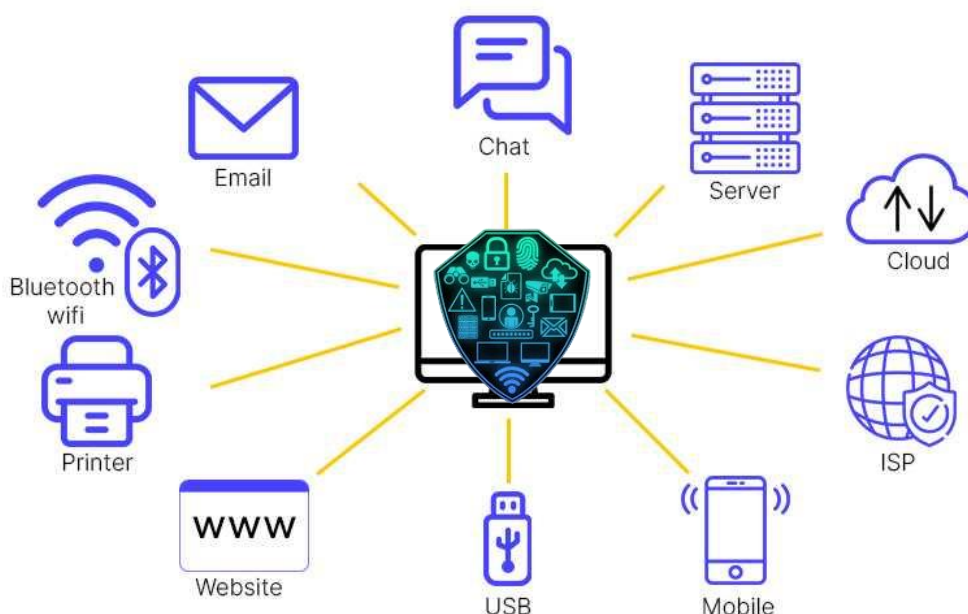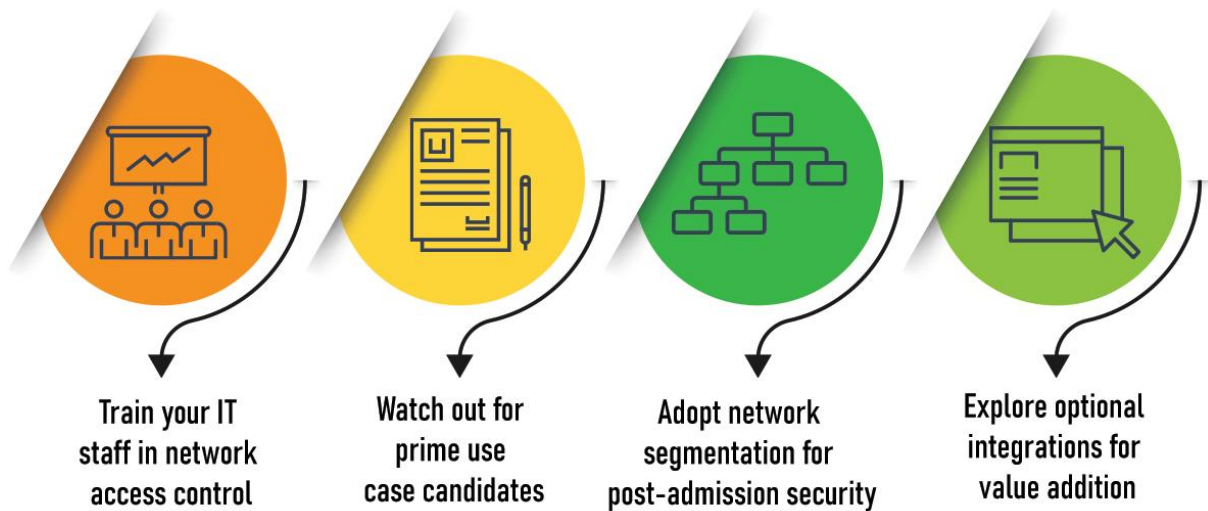
Network Access Control Solutions :

Network Access Control (NAC) is a security solution that manages and regulates the access of devices to a network. NAC solutions enforce security policies on devices as they attempt to access network resources, ensuring that only compliant and authorized devices can connect. This is achieved through a combination of authentication, authorization, and policy enforcement mechanisms. NAC solutions are designed to improve network security by controlling device and user access based on predefined security policies.

BEST PRACTICES OF NETWORK ACCESS CONTROL

Train your IT staff in network access control

Watch out for prime use case candidates

Adopt network segmentation for post-admission security

Explore optional integrations for value addition

Key Components of NAC Solutions :

1. Authentication : Verifies the identity of users and devices attempting to connect to the network. This can involve username/password pairs, certificates, or multi-factor authentication (MFA).

2. Authorization : Determines what level of access an authenticated user or device should have, based on roles and policies.

3. Compliance Checking : Ensures that devices meet specific security requirements (e.g., updated antivirus software, operating system patches) before granting access.

4. Policy Enforcement : Applies security policies that dictate what resources and services users and devices can access once connected.

5. Monitoring and Reporting : Continuously monitors network access and generates reports on compliance, access patterns, and potential security threats.

Benefits of Using Network Access Control Solutions :

1. Enhanced Security : NAC solutions help prevent unauthorized access to the network by ensuring that only authenticated and compliant devices can connect. This reduces risk of data breaches & unauthorized activities.

2. Improved Compliance : By enforcing security policies and ensuring that devices meet regulatory and organizational standards, NAC solutions help organizations maintain compliance with industry regulations such as GDPR, HIPAA, and PCI DSS.

3. Reduced Risk of Malware and Viruses : By checking devices for compliance with security policies (such as having up-to-date antivirus software and patches), NAC solutions help prevent infected devices from accessing the network and spreading malware.

4. Access Control Based on User Role : NAC solutions allow for granular access control, ensuring that users only have access to the resources necessary for their role. This minimizes the risk of insider threats and accidental data leakage.

5. Visibility and Monitoring : NAC solutions provide detailed insights into who and what is accessing the network, allowing for better monitoring and detection of suspicious activities. This helps in identifying and responding to potential threats more quickly.

6. Guest Network Management : NAC solutions can provide secure and controlled access for guests and visitors, ensuring they can connect to the network without compromising security. Features like guest self-registration and sponsor-based access are often included.

7. Support for BYOD and IoT : As organizations increasingly adopt Bring Your Own Device (BYOD) and Internet of Things (IoT) strategies, NAC solutions help manage and secure these diverse devices, ensuring they meet security requirements before accessing the network.

8. Automated Responses : NAC solutions can automatically respond to non-compliant devices by quarantining them or redirecting them to remediation portals. This reduces the burden on IT staff and ensures consistent enforcement of security policies.

9. Scalability : NAC solutions are designed to scale with the organization, supporting large and complex network environments with thousands of devices.

10. Integration with Other Security Solutions : NAC solutions often integrate with other security tools such as firewalls, SIEM (Security Information and Event Management) systems, and endpoint protection solutions, enhancing the overall security posture of the organization.

Network Access Control solutions are essential for modern network security, providing comprehensive control over who and what can access network resources. By enforcing security policies, ensuring device compliance, and providing detailed visibility and monitoring.
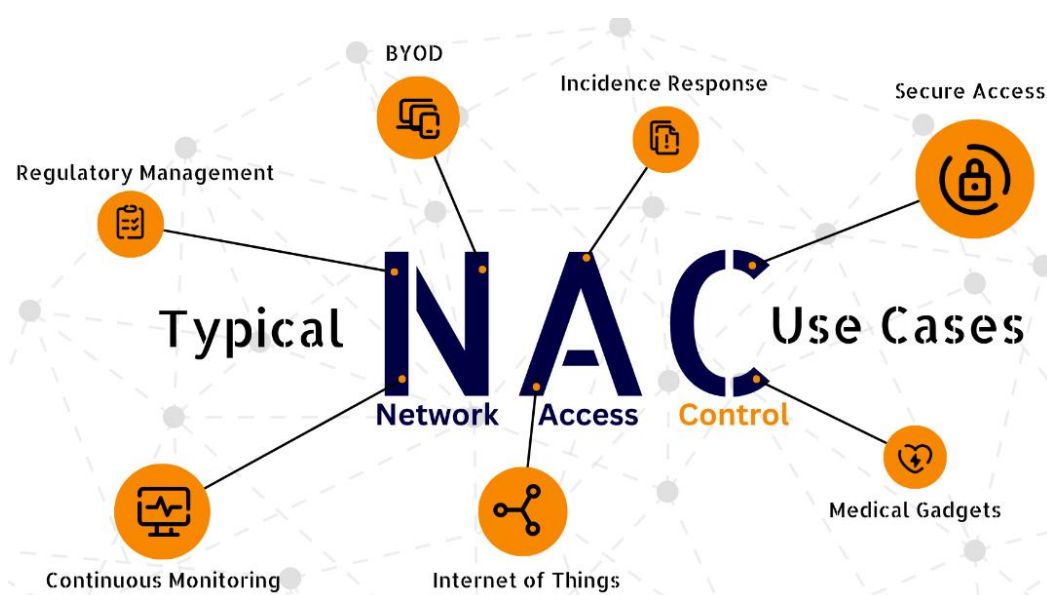
For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

IP Surveillance Solutions

Modular Video Surveillance with AI Analytics :

A complete video surveillance solution with unlimited flexibility owing to its innovative construction-set principle. Easy for non-tech savvies, powerful for professionals, it allows to build both small and enterprise-level systems with truly unlimited number of cameras (up to several thousand cameras on single computer). The program works on Windows, Linux, Mac OS and Android devices (full-featured version) with full remote access and view from any mobile devices and computers.

Xeoma offers auto-detection of and support for almost any cameras – IP, ONVIF, USB webcams, H.264, H.265, H.264+, H.265+, MJPEG, MPEG4, PTZ, WiFi (up to 99.9% of cameras on the market supported). With its help, in just a few seconds a computer and a camera will turn into a ready to work out-of-the-box surveillance system.

Intellectual motion detector with advanced false alarm avoiding logic, motion-triggered or scheduled notifications (SMS, email, sound alarm, etc.) and screen captures, work with sound are perfect for staff monitoring and parental control.

Shared access rights, encryption, password protection, network clustering, also on operating systems without graphical shell, make monitoring efficient and stable even for professional-scale surveillance systems. No installation and no admin privileges required. Professionals will certainly appreciate automatic backup to FTP server, powerful web server and remote view of all cameras with sound (flash video streaming), cyclic archive with export feature.

Key Features :

Camera/sources processing :
- ✓ Compatible with any webcams, analog cams, including WiFi wireless CCTV cameras
- ✓ Supports IP-cameras (including H.264, H.265, H.264+, H.265+, JPEG/MJPEG, MPEG-4, Fisheye, PTZ and ONVIF, wireless cams, i.e. perfect both for wired and wireless CCTV)
- ✓ Any resolution (Mega pixel)
- ✓ Screen captures from all monitors simultaneously
- ✓ Adjustable sound quality and sound volume
- ✓ Up to 2 000 cameras can be connected on 1 computer !

Professional surveillance made easy :
- ✓ Free rebranding and customization.
- ✓ Quick setup: group settings of modules.
- ✓ Quick navigation and control of cameras with Device list.
- ✓ Hardware acceleration QuickSync (Intel) and CUDA (NVidia graphics) Windows & Linux.
- ✓ Possibility to set decoding on the client side to lower CPU and network load.
- ✓ Backup and restore configuration.
- ✓ Failover and automatic switching to the backup server if the main one/ones is down.
- ✓ Redistribution of resources in case of camera's failure.
- ✓ Restoring configuration and making backup via interface (Main menu – Install – Restore).
- ✓ Setup of cameras, modules, and schemes in a configuration file.
- ✓ Creating a surveillance network of CCTV software servers by using web server.
- ✓ Multi-Server and Multi-Client connection architecture for video surveillance of any size.
- ✓ Flexible setup of access rights (user permissions).
- ✓ Password protection of settings.
- ✓ Work with multiple monitors (video-walls).
- ✓ Pop-up monitor mode with showing active cameras and detected motion/or other events on the necessary monitor (Pop-up window).
- ✓ Objects masking/blurring (for private territories).
- ✓ Sound detector that can react to screaming, shooting, breaking windows etc.
- ✓ TLS-encryption between server and clients.
- ✓ Support of IPv4 and IPv6 protocols.
- ✓ Heat map of the areas with most action in them.
- ✓ Digital zoom in real-time or archive.
- ✓ Support for PTZ control and 360° camera image rotation.
- ✓ Instant screenshots of camera image

Intellectual Modules and Features:
- ✓ Fisheye cameras image De-Warping
- ✓ eMap – map of your video surveillance site with interactive cameras on it
- ✓ Face detection
- ✓ Object detector to follow objects even if they're not moving
- ✓ Synchronization with camera's SD card
- ✓ Synchronization with cashier registers
- ✓ LDAP active directory synchronization
- ✓ Home automation system integration thanks to HTTP request sender & HTTP switcher modules

- ✓ Possibility to create your own cloud video surveillance service with Xeoma Pro
- ✓ Privacy masking to blur areas you're not supposed to record, or faces
- ✓ Automatic object tracking with zoom (PTZ tracking) and visualization of moving objects
- ✓ Sabotage detector to notify you when problems are detected
- ✓ PTZ control also in browsers
- ✓ Quick turning on/off of chains remotely (HTTP Switcher) and locally (Button Switcher)
- ✓ Search in archive for motion events by time or in selected areas
- ✓ RTSP and HTTP broadcasting: emulation of IP cameras streaming in MJPEG, JPEG, H264, etc.

Remote Access:
- ✓ Remote view via mobile devices (Android, iPhone, iPad supported)
- ✓ Online view of all cameras with sound
- ✓ Full remote access to settings, archive and cameras from a workstation
- ✓ Internet broadcasting
- ✓ Possibility to embed camera image to your site
- ✓ Remote access even with dynamic IP address
- ✓ View of archives and basic setup in web browsers

Motion Detector:
- ✓ Setting up of zone(s) of any size and shape to monitor for motion
- ✓ Visual motion detection, with time of the last detected movement shown on preview
- ✓ Setting up maximum object size to be ignored, and sensitivity level of sensor
- ✓ Pre-record option to store several seconds preceding motion detection
- ✓ Post-record to continue recording after the event has finished
- ✓ Enhanced algorithm to avoid false alarms caused by pets or weather changes

Archive :
- ✓ Loop recording.
- ✓ Adjustable maximum size of archive and compression rate of images stored to archive
- ✓ Possibility to store archive onto different HDDs, RAIDs
- ✓ Support for network attached storage (NAS), Google Cloud disc, etc.
- ✓ User-friendly built-in media player with multi-thread rapid playback mechanisms and search for motion event or specific time
- ✓ Export of a selected extract right from the viewer
- ✓ Deletion of unneeded extracts from the viewer
- ✓ Search for motion events by time and in selected areas
- ✓ Simultaneous synchronized view of several archives

Notifications and Reactions :
- ✓ Text message (SMS) sending
- ✓ E-mail notifications (with attached JPEG images and MJPEG videos)
- ✓ Event-triggered pop-up window
- ✓ Sound Alarming
- ✓ Running a specified external program
- ✓ FTP server upload of images and videos with sound
- ✓ Saving files to the specified path with cyclic recording

All High-demand Features :

- ✓ Hidden mode of work
- ✓ WEBM (VP8 and VP9), MPEG-4, MP4 and MJPEG video formats
- ✓ Marking (embedded time/date, custom text, GPS coordinates, or image stamp over camera's stream)
- ✓ Scheduler, setting up when system's components are to start/end work
- ✓ Adjustable volume of sound in preview mode
- ✓ Quick setup: duplicating of chains
- ✓ Adjustable preview mode (camera layouts, window transparency, font)
- ✓ Automatic slide show of real-time images
- ✓ 1-click-easy updates
- ✓ New versions notifications

Advantages :

- ✓ Full-featured work on Windows, Mac OS X, Linux and Android
- ✓ Full featured trial (demo) edition can be used multiple times
- ✓ Ready to work right after downloading with default settings
- ✓ No admin rights required
- ✓ Simple additional settings
- ✓ Flexible control like in a children's construction set
- ✓ Innovative intuitive graphical interface
- ✓ Dynamic development and addition of cutting-edge features

Available in Main languages :

English, Spanish, Italian, Brazilian Portuguese, Chinese, French, German, Japanese, Hungarian, Polish, Russian.

Additional languages :

Dutch, Danish, Romanian, Turkish, Croatian, Finnish, Greek, Czech, Bulgarian, Vietnamese, Swedish, Slovenian, Taiwanese, Korean, Ukrainian and Belorussian.

Typical applications :

- ➢ Object monitoring in non-working hours (office, store, warehouse)
- ➢ Security surveillance (perimeter security monitoring, car, etc.)
- ➢ Smart home systems integration
- ➢ Staff monitoring (industry workers, office employees, caregivers and home staff)
- ➢ Monitoring of activity of children and office workers on computer, control over visited sites
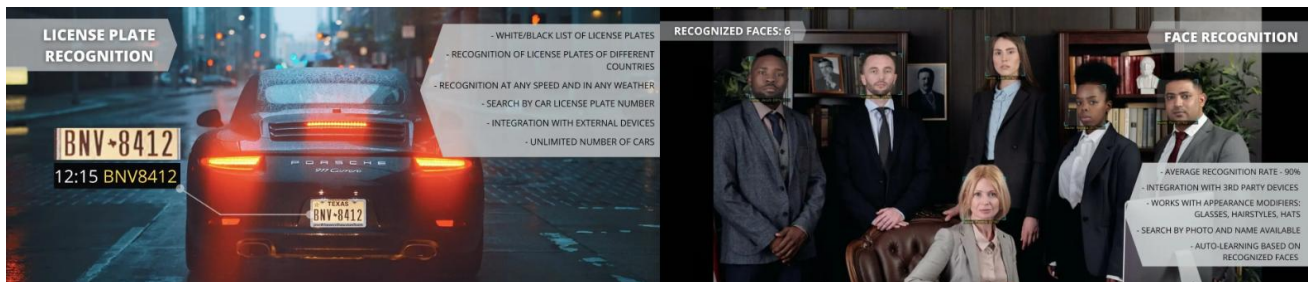- ➢ Pet surveillance
- ➢ Watching machinery in industries

Multiple Camera Views
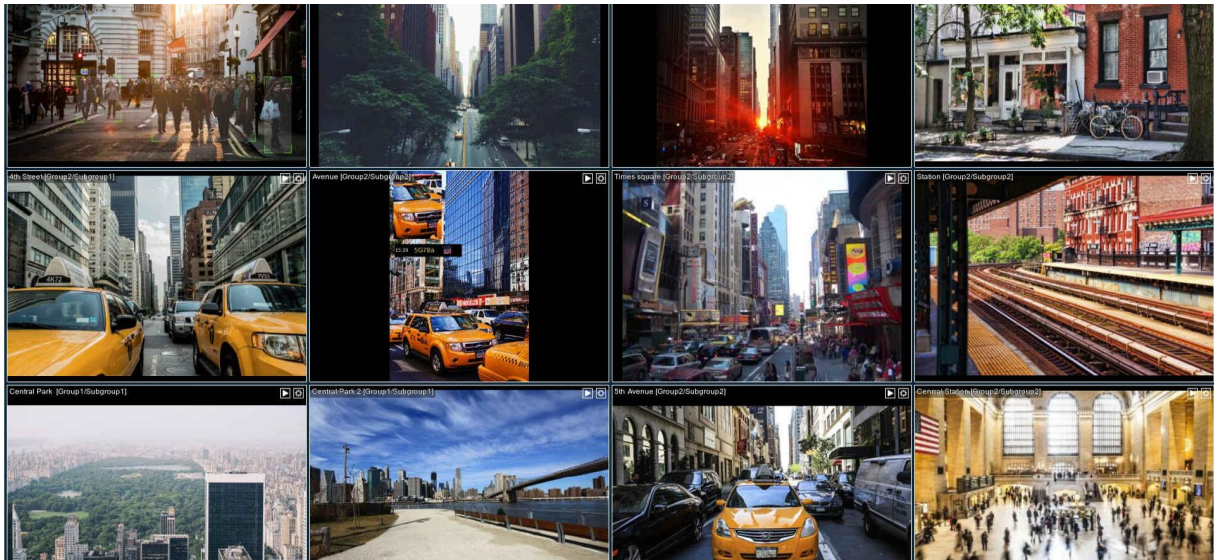
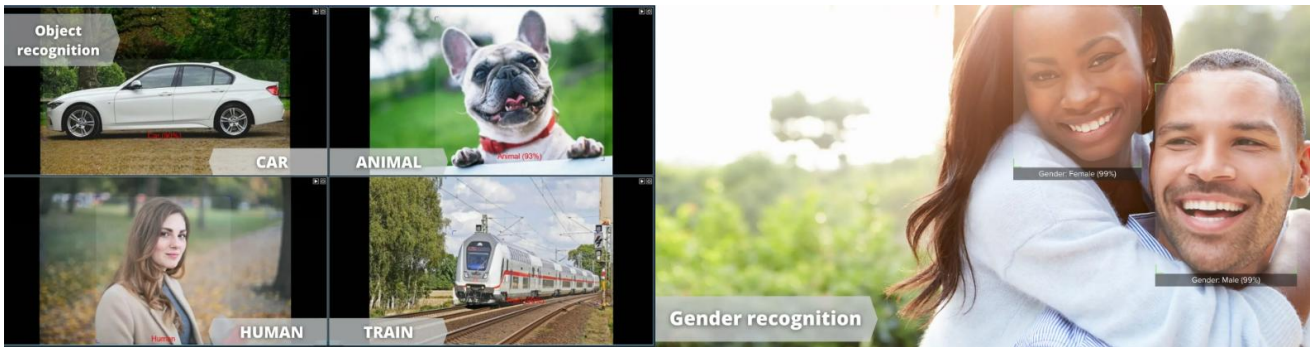# Emotions and Age Recognition
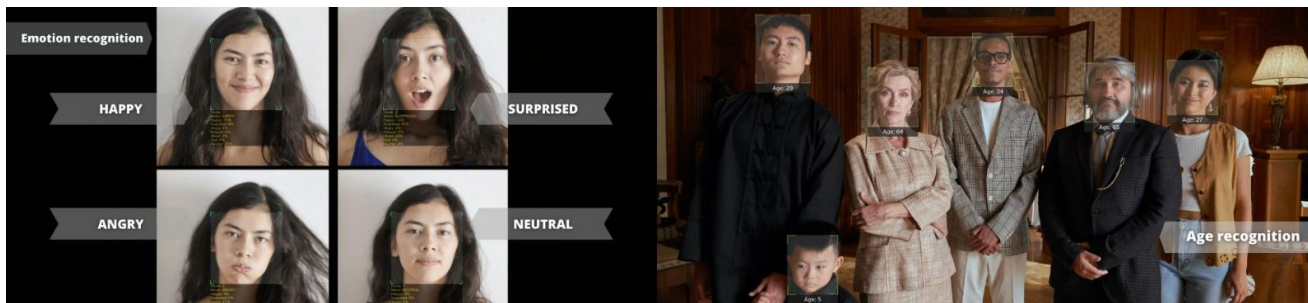
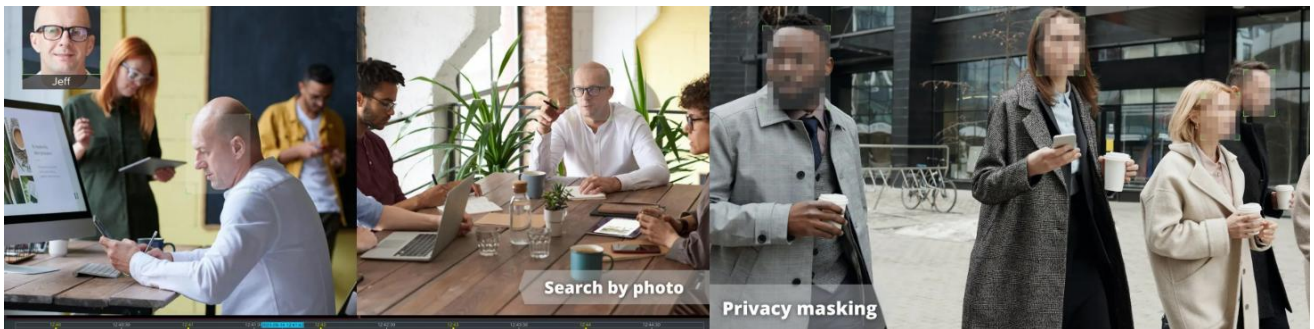# ANPR and Face Recognition

Text and Sound Event Detection

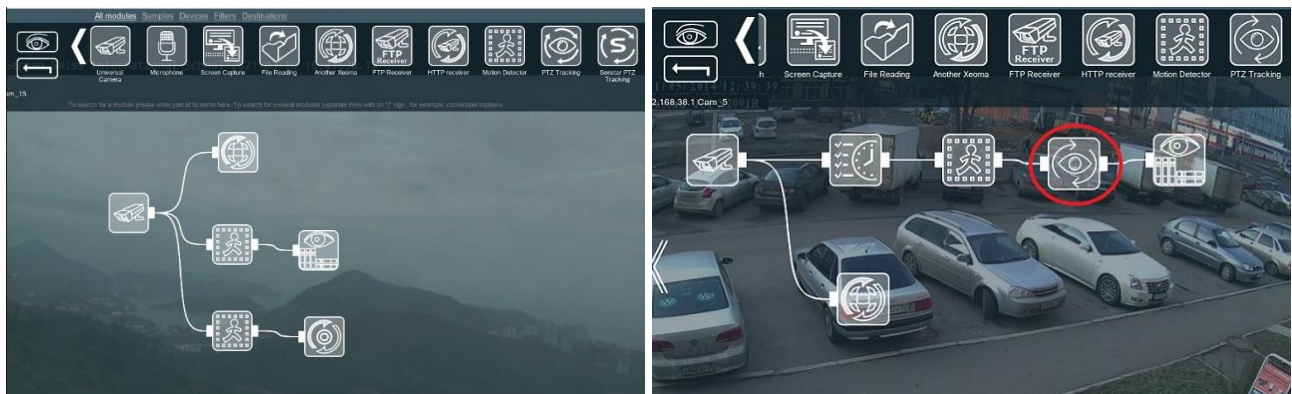# Object and Gender Recognition

Search by Photo and Privacy Masking

Sports Tracking and Slip/Fall Detection

Best #1 Modular Extendable Video Surveillance Software

For Order or more info, please contact WhatsApp +923216583228 or Email : mrakftech@yahoo.com

Thanks

More Exiting Solutions are Coming Soon.

Company Websites :
https://www.kftechsols.com
https://linkedin.com/company/kftechsols

Email : mrakftech@yahoo.com
Whats App : +923216583228
Skype : rashidLahore