Solution Use Case

Healthcare

majentai

Securing the EHR

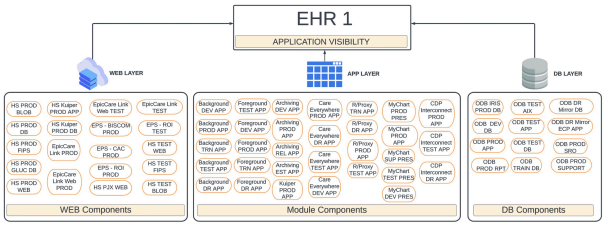
Secure the EHR by establishing application visibility and context across data center and cloud environments before introducing layered segmentation and automated policy enforcement. This reduces breach risk, improves control consistency, and removes the uncertainty that keeps critical healthcare applications overexposed or dependent on perimeter-only protection.

Use Case Approaches

1: Visibiltiy

EHR environments are complex, interconnected, and often difficult to fully understand. Without clear application context, teams struggle to know what they are protecting and where risk is concentrated.

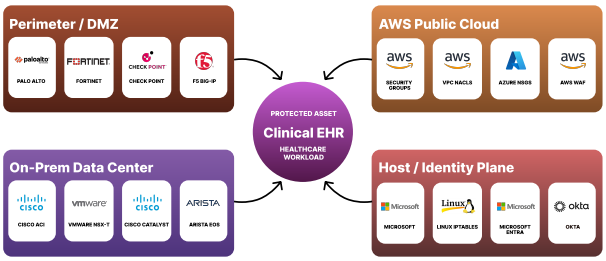
- Limited visibility into EHR components across data center and cloud
- Unclear dependencies between applications, infrastructure, and users
- Difficulty prioritizing controls based on exposure and criticality



2: Not Hybrid-Cloud Ready

Security policies often do not translate cleanly across data center and cloud environments. This creates inconsistent protection and makes change management slower and riskier.

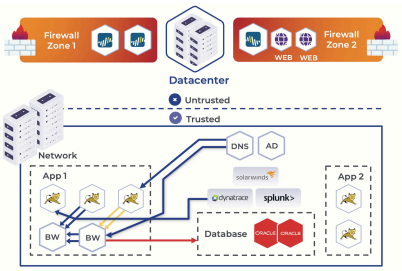
- Separate policies for data center and cloud platforms
- Inconsistent enforcement across hybrid infrastructure
- Manual policy changes that are complex, time-consuming, and high-risk



3: One Layer of Security

Relying on a single layer of defense leaves critical EHR systems exposed if that layer fails. EHR protection needs coordinated controls across multiple enforcement points.

- Breach or misconfiguration of one layer can expose critical systems
- Firewall-centric policy limits application flexibility and scalability
- Lack of layered segmentation from perimeter to workload/node



Solution

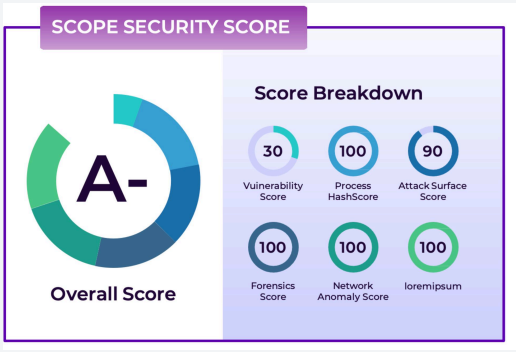
Majentai helps healthcare organizations secure EHR environments by combining visibility, risk scoring, layered segmentation, and automation.

Our approach is designed to help teams understand the full application landscape, define consistent controls, and apply policy across both data center and cloud environments with greater speed and confidence.

Enable Visibility and Provide Context
Majentai begins by mapping the EHR application environment across infrastructure, applications, dependencies, and external connections.

Key activities

- Map application components across data center and cloud environments
- Identify internal and external dependencies tied to the EHR ecosystem
- Assess exposure points across infrastructure, users, and systems
- Develop a scorecard based on exposure, criticality, and operational impact



Application	Criticality	Elements	Score
Epic	High	DC Dallas Azure East-VA	C -
PACS GE	High	DC Dallas	B -

Securing the EHR

majentai

Approach

Majentai defines and operationalizes a unified segmentation model that protects the EHR across data center and cloud environments. The approach combines layered controls with automation so policy can be applied consistently, adapted quickly, and managed with less operational risk.

Define a Unified and Layered Segmentation Model

Majentai designs segmentation around how the EHR actually operates, including its applications, dependencies, users, and infrastructure. This creates coordinated protection across multiple enforcement points instead of relying on a single control layer.

- Develop segmentation controls across firewalls, SDN, cloud-native tools, and host-based controls
- Align policy to application behavior, criticality, and dependency maps
- Reduce unnecessary communication between systems and workloads
- Centralize control from the perimeter down to the node

Automate Unified Policy Across Data Center and Cloud

Majentai helps move policy management from manual, fragmented changes to a consistent automated model. This allows security teams to update controls more quickly and reliably as the EHR environment changes, scales, or moves.

- Define policy standards that apply across data center and cloud platforms
- Use automation and orchestration to make security changes consistently
- Improve speed and reliability of policy updates
- Help controls evolve as the EHR application changes, scales, or moves

Success Story

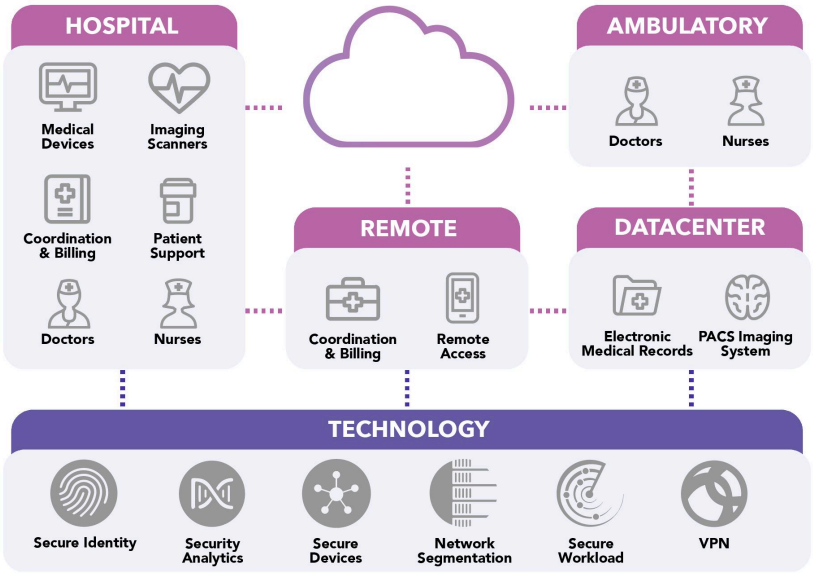
Large Healthcare Provider Required to Pass Regulatory Pen Test

A large healthcare provider faced an aggressive timeline after a security audit identified critical gaps around flagship applications, including Epic, GE PACS, and other healthcare systems. Majentai helped accelerate the organization's zero-trust journey by applying proven protection models aligned to the customer's business and compliance needs.

Secure Applications & Records
Reduced exposed records from 7M to fewer than 100

Device Automation & Lockdown
Profiled users and devices for secure access

Proactive Anomaly Detection
Identified threats before business impact



Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit https://majentai.com