DNSSight
with **HYAS** inside

USE CASE

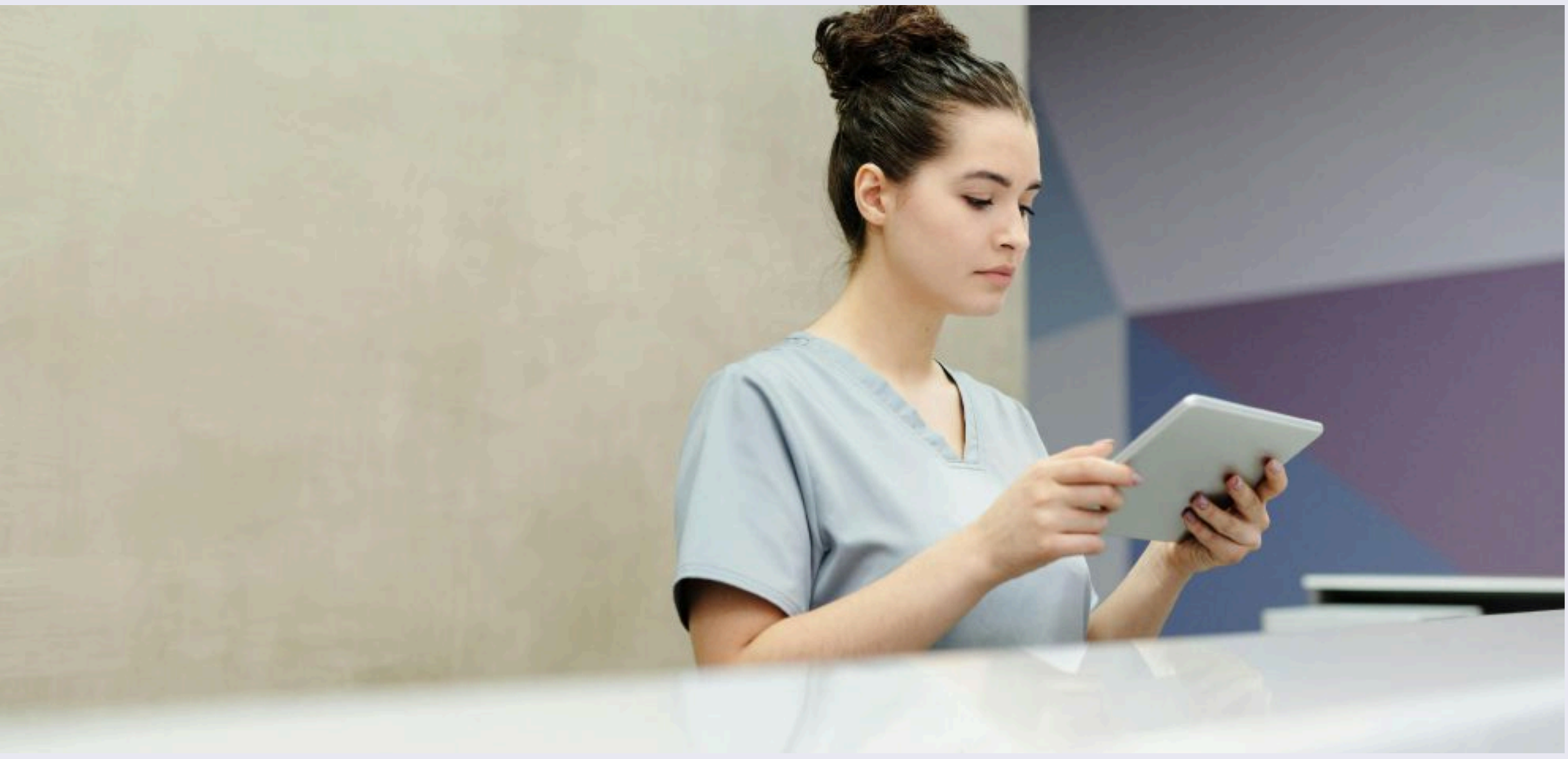
# Fortifying Healthcare Networks Through DNS Visibility

Empowering IoT and OT Security Without Overhauling Critical Operations

## BACKGROUND

A major healthcare provider operates a large network spanning hospitals, clinics, and specialised care facilities. Within this expansive environment, countless **IoT (Internet of Things) and OT (Operational Technology)** devices—infusion pumps, imaging systems, HVAC controls, and more—are all indispensable to patient care and facility management.

Yet these same devices often run on legacy systems that are challenging to patch or upgrade, leaving the organisation vulnerable to cyber threats.



The provider's existing security solutions—endpoint protection, firewalls, and network monitoring—work to block known malicious activity. However, pinpointing which device initiates a suspicious connection remains a painful task. The complexity intensifies when IoT or OT endpoints operate on older OS versions or proprietary protocols. Any disruption or downtime risks patient safety and operational continuity.

**DNSSight addresses these challenges by offering deep DNS visibility—identifying malicious requests and the devices behind them—without requiring disruptive infrastructure changes or agent installations.**

# CHALLENGE

## DISPARATE IOT & OT DEVICES

### Legacy Systems

Many medical devices run on outdated or specialised operating systems that can't accommodate additional security agents.

### Diverse Protocols

From lab equipment to climate control systems, each device communicates differently, making uniform oversight difficult.

## VISIBILITY GAPS

### Limited Log Correlation

Traditional security tools rarely map DNS queries to the specific device or user, leaving gaps in incident investigations.

### Critical Environment

Healthcare organisations must ensure minimal downtime; major network reconfigurations could disrupt life-saving services.

## THREAT LANDSCAPE

### Malware & Ransomware

Attackers recognise older, unpatched IoT/OT systems as a key vulnerability, using them to pivot deeper into the network.

### Zero-Day Attacks

Proprietary medical equipment often lags in patches, making any new exploit especially dangerous without real-time detection measures.

## COMPLIANCE & DATA PROTECTION

### Patient Privacy

Storing and transmitting sensitive health data, the organisation must align with regulations like HIPAA and GDPR (for global facilities) while safeguarding against cyberattacks.

### Audit Requirements

With multiple regulatory bodies auditing healthcare practices, robust logging and quick evidence retrieval are paramount.

# SOLUTION

## DNSSight for Healthcare IoT/OT Security

### AGENTLESS DNS VISIBILITY

#### Non-Invasive Monitoring

DNSSight monitors DNS traffic from every device without installing software on sensitive or legacy systems.

#### Real-Time Correlation

It automatically enriches DNS logs with user, device, and location data, revealing exactly which piece of equipment or system generated each request.

### EARLY THREAT DETECTION

#### Malicious Domain Alerts

Even if an IoT ventilator or lab machine attempts to connect to a known bad domain, DNSSight instantly flags and records it.

#### NX Domain & Short-Lived Domains

Many ransomware campaigns use fleeting or offline domains. DNSSight captures these queries, alerting security teams before an active compromise escalates.

### REDUCED OPERATIONAL IMPACT

#### Minimal Downtime

Deploying DNSSight does not require revamping network architecture or swapping out DNS servers—vital in a 24/7 healthcare setting.

#### No Agent Overload

Freeing staff from installing and managing software across hundreds or thousands of specialised devices reduces complexity and risk.

### COMPREHENSIVE SECURITY POSTURE

#### Integrated SIEM Workflows

DNSSight forwards critical DNS events to the organisation’s SIEM system, enriching broader threat intelligence.

#### Flexible Dashboards & Reporting

Security teams can rapidly investigate anomalies or produce compliance reports spanning entire hospital networks, clinics, and labs.

# RESULTS

## FASTER INCIDENT RESPONSE

### Pinpointing Specific Devices

When a suspicious DNS query appears, DNSSight's real-time correlation reveals the exact source device. The SOC can isolate or patch it before patients or services are impacted.

## IMPROVED SECURITY ROI

### No Major Overhaul

DNSSight leverages the existing DNS infrastructure, complementing firewalls, SIEMs, and other tools already in place.

### Less Administrative Overhead

With automated data enrichment and centralised dashboards, staff focus on action rather than manual log investigations.

## ENHANCED PATIENT SAFETY & COMPLIANCE

### Proactive Threat Management

Detecting threats earlier safeguards essential patient data, critical care equipment, and day-to-day operations.

### Clear Audit Trails

Every DNS query is stored and easily retrievable, ensuring compliance with stringent healthcare regulations and privacy mandates.

## FUTURE-READY DEFENCE

### Scalability Across Facilities

As the healthcare system expands—adding satellite clinics or acquiring new specialty centres—DNSSight can seamlessly integrate new endpoints.

### Broad Support for Legacy Devices

Even as older equipment remains in service, DNSSight continues to provide full DNS visibility, reducing potential blind spots.

# CONCLUSION

In an environment where patient safety is paramount and downtime can be life-threatening, DNSSight delivers the agentless, non-disruptive DNS visibility healthcare providers need. By shedding light on every DNS request, it allows security teams to swiftly detect compromised IoT and OT devices—without retooling networks or risking hospital operations.

For healthcare organisations aiming to protect critical data, maintain compliance, and secure a rapidly evolving fleet of medical and facility technology, **DNSSight stands out as a transformative yet practical solution.**