DATA BREACH DEFENDER™
FOR U.S. HOSPITALS

Purpose-Built for Early-Stage Detection, Notification, and Containment

Celerium's® **Data Breach Defender** helps hospitals detect and contain early-stage breach activities–often the precursors to ransomware or double-extortion attacks.

Originally engineered for the **Department of Defense** to protect critical defense suppliers (DIB), Data Breach Defender now delivers that same speed, automation, and more to healthcare.

TRUSTED IN HEALTHCARE

American Hospital Association™
Preferred Cybersecurity & Risk Service

PREFERRED CYBERSECURITY AND RISK SERVICE PROVIDER

Celerium has been selected by the AHA as an excellent solution provider for their Automated data breach prevention, detection and defense solutions. We can confidently recommend Celerium as a reliable source of support for our nation's hospitals and health systems in their efforts to defend against sophisticated cyberthreats and ransomware attacks.

John Riggi
National Advisor for Cybersecurity and Risk
American Hospital Association

Health-ISAC COMMUNITY SERVICES

COMMUNITY SERVICES PROVIDER MEMBER

CHIME®

CORPORATE MEMBER

HIMSS®

CORPORATE SPONSOR

We were quickly sold on Celerium's Data Breach Defender and absolutely love what we've seen! We started seeing the benefits almost immediately. In today's increasingly threatening environment, having this kind of protection and visibility is paramount. Any healthcare facility looking to stay ahead of emerging threats should join the program today and experience the benefits for themselves.

Robert Greenhoe
Technology Director | Munising Memorial Hospital

WHO DATA BREACH DEFENDER HELPS

Hospital IT Executives

Gain early-stage visibility into potential theft of **ePHI** and other patient data from critical systems identifying suspicious data movements before mass exfiltration or ransomware encryption occurs.

Hospital Compliance & Privacy Officers (CCOs, CPOs)

Reduce exposure from third-party data breaches now among the fastest-growing risks in healthcare. Additionally, improve your supplier's conformance with your hospital's Business Associate Agreements (BAA).

Hospital CEOs & Boards

Strengthen your hospital's enterprise risk posture with a cost-efficient, fast-track solution. Protect patient data across your organization and throughout your third-party ecosystem. Minimize reputational, financial, and regulatory exposure while enhancing overall resilience and board confidence.

KEY VALUES

Speed and Automation

- Detect and contain early-stage theft of patient data
- Stop breach activity before large volumes of ePHI are stolen and potentially before ransomware attacks
- Minimize regulatory exposure, operational disruption, and reputational damage

Financial Impact Reduction

- **Fewer stolen records can mean less financial impact**
- **Less disruption to hospital service delivery:** fewer hospital diversions
- **Reduced reputational risk:** stronger trust with patients and payors
- **Improved IT Operational Efficiency**

At Reeves Regional Health, we deployed Celerium's solution in just minutes, and the results were immediate and dramatic. The platform quickly delivered visibility into threats we hadn't previously detected, providing enterprise-grade protection without disrupting operations. Celerium has become a cornerstone of our cybersecurity strategy.

John Gresham
CIO | Reeves Regional Hospital

Within the first hour, this has prevented unauthorized access within our systems and saved [network admin] hours of work dealing with employee lockouts and manual blocks.

Justin Mumm
Network Admin
Crawford County Memorial

FAST-TRACK IMPLEMENTATION FOR OVERLOADED IT TEAMS

Celerium understands that hospital IT organizations are stretched thin.

That's why we engineered **Data Breach Defender to be implemented in under 30 minutes** with **no hardware or software installation** required.

I was amazed by the results immediately after completing the 30-minute implementation of Data Breach Defender. I could instantly see detailed threat activity targeting our organization. The visibility into potential threats prompted me to enable automated blocking of the highest-risk activity, powered by Celerium. The solution is simple, actionable, and effective.

Michelle Miller
Director of IT | Creative Care

THIRD-PARTY DATA BREACH DEFENSE

- Extend breach detection to your **high-risk suppliers (Business Associates)**
- Identify transmissions to **organizations impersonating legitimate suppliers**
- Strengthen third-party risk programs and regulatory compliance

HOW DOES DATA BREACH DEFENDER RELATE TO MDR, XDR, AND SOC-AS-A-SERVICE PROVIDERS?

Outside security services play an important role—but they have limits.

Managed Detection and Response (MDR) and Extended Detection and Response (XDR) providers are valuable for managing the *dozens or even hundreds of security alerts* that can overwhelm a hospital's IT staff. Their focus is typically on *end-user systems*—workstations, desktops, and mobile devices rather than on critical clinical systems and servers.

SOC-as-a-Service providers are also used by many smaller hospitals to provide 24×7 coverage that internal teams can't maintain. These services help reduce alert fatigue and improve overall security visibility.

However, hospitals often face **two major challenges** with outside SOC, MDR, or XDR providers:

1. **Compliance Concerns:**

   Hospitals may be uncomfortable allowing third-party analysts to view or process data from systems that handle sensitive patient information (ePHI).

2. **Response Risk:**

   While hospitals often trust external providers to take action on user devices, they are understandably cautious about allowing outsiders to isolate or disconnect *critical clinical systems* like, EHR, PACS, or pharmacy servers where mistakes could disrupt patient care.

This is where Data Breach Defender fits in.

Data Breach Defender doesn't compete with MDR or XDR, it **complements** them.

Rather than chasing thousands of low-level alerts, Data Breach Defender focuses on a hospital's *core systems that store or process ePHI data.*

- **Internal by design:** Data Breach Defender keeps, by default, sensitive data and telemetry inside for the use by your IT staff. Nothing is shared with external service providers unless you choose to.
- **Autonomous coverage:** When your SOC or IT staff are offline, overnight, on weekends, or over holidays, Data Breach Defender continues monitoring and will automatically alert your team to suspicious data breach activity. Think of Data Breach Defender as an **automated in-house data breach SOC.**
- **Integrated containment:** Data Breach Defender can work alongside your existing EDR tools, enabling your internal team, not an outside provider, to take isolation or containment actions when appropriate.

Finally, Data Breach Defender can also be used to reduce risk from third-party breaches through a number of different solutions. Outside providers do not normally focus on data breach risks relating to a hospitals business associates.

Together, your outside providers handle broad detection and response across user devices, while **Data Breach Defender safeguards your hospital's most critical systems and ePHI**.

TECHNICAL HIGHLIGHTS

AI/Machine Learning Powered Detection

- Identifies **suspicious, possible, probable, and highly probable** breach activity
- Monitors traffic patterns for early signs of data theft and exfiltration

Blind Spot Coverage

Agentless implementation means hospitals can have visibility of:

- **Legacy sensitive, and unmanaged systems:** ICU, NICU, physician-owned systems, PCI payment terminals
- **Departmental systems:** EHR (Epic, Cerner), Pharmacy, Imaging, Radiology
- **Pivot and staging systems exploited by threat actor:** Domain Controllers, File Servers, Cloud Backups

> *If I had Celerium's Smash & Grab feature, I would have known there were several large data transfers during the MOVEit breach.*
>
> **CISO**
> Large Houston Healthcare System

Notifications

Alerts can be sent to internal stakeholders (IT, Compliance, Privacy) or external partners under hospital-defined policies.

Containment Options

- **Surgical containment:** automated IP blocking
- **Isolation-based containment (2026):** via EDR integration (*e.g. SentinelOne®, CrowdStrike®*)
- Manual, semi-automatic, or fully automatic modes

DATA BREACH DEFENDER COMPLEMENTS — NOT REPLACES — YOUR EXISTING SECURITY SOLUTION

Solution	What It Does	How Data Breach Defender Adds Value
F5®	Access control to critical systems	Data Breach Defender provides continuous traffic monitoring and post-access breach detection
EDR (SentinelOne®, CrowdStrike®)	Endpoint protection	Data Breach Defender integrates with EDR to trigger automated containment
SecurityScorecard®	Third-party risk assessment	Data Breach Defender detects actual breach activity across third-party connections
MFA	Access prevention	Data Breach Defender operates post-prevention to detect and stop data theft after access has occurred
Hospital Firewalls	Manages Firewall Traffic	Data Breach Defender leverages your firewall to enable data breach detection and surgical based containment

JOIN OUR UPCOMING WEBINAR

In this executive-level webinar for healthcare leaders in IT, Compliance, Privacy, and the C-Suite, you will learn about emerging approaches to early-stage data breach detection and containment and how hospitals are strengthening patient safety, operational resilience, and cyber risk governance.

The session will cover new directions in data breach defense, practical considerations for hospital environments, and real-world insights from healthcare security leaders.

Speakers include: John Riggi (National Advisor for Cybersecurity and Risk, American Hospital Association), Vince Crisler (Celerium's Chief Strategy Officer and former White House CISO), and others.

REGISTER HERE →

ABOUT CELERIUM

Celerium® engineers turn-key rapid deployment data breach defense solutions for the healthcare industry. These solutions are powered by our cybersecurity technology which we have provided to defense suppliers via the DoD. We also provide cybersecurity and data-breach solutions for state and local government agencies and Managed Service Providers (MSPs).

Learn more at **www.Celerium.com** and follow us on X at **@CeleriumDefense**

CELERIUM.com