Healthcare’s Cyber Briefing

March 5, 2026

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

Healthcare’s Cyber Briefing

- Critical Threat Brief
- Education Session: When the Cloud Becomes the Attack Surface: Hybrid Risk, Identity, and Governance in Healthcare
- Q+A

FEATURING:

Dave Bailey, VP Consulting Solutions & Strategy
Jackie Mattingly, Senior Director, Consulting Services, Regional and Critical Access Hospitals
Brian McManamon, General Manager, Managed Cloud and Managed Security Services

Threat Level Elevated

Iranian Cyber Threat Escalation Following U.S.–Israel Strikes

On February 28, 2026, coordinated U.S. and Israeli military strikes targeted Iranian assets. Within hours, Iranian-affiliated cyber groups initiated retaliatory operations.

Healthcare has historically been considered a high-impact civilian target during geopolitical escalation due to its operational sensitivity and patient safety implications.

Federal partners indicate there is currently no specific credible threat directed at U.S. healthcare organizations. However, historical patterns show that military escalation often coincides with increased cyber activity targeting civilian infrastructure.

This escalation materially increases risk to U.S. healthcare organizations through:

1. Heightened likelihood of disruptive cyber activity
2. Potential disruption of medical and pharmaceutical logistics tied to Middle East shipping routes

Executive leadership should treat this as a near-term resilience event — validate cyber readiness while confirming supply continuity for critical medications and devices.

Breach Portal Updates

Dave Bailey, VP Consulting Solutions & Strategy

Clearwater

Hacking/IT Incidents Dominate Feb Breach Reports

- All February incidents were Hacking/IT incidents reflecting a broader pattern of ransomware and threat actor targeting of the health sector
- Business Associate involvement present in more than a third of the cases underscoring the risk exposure through third-party service providers

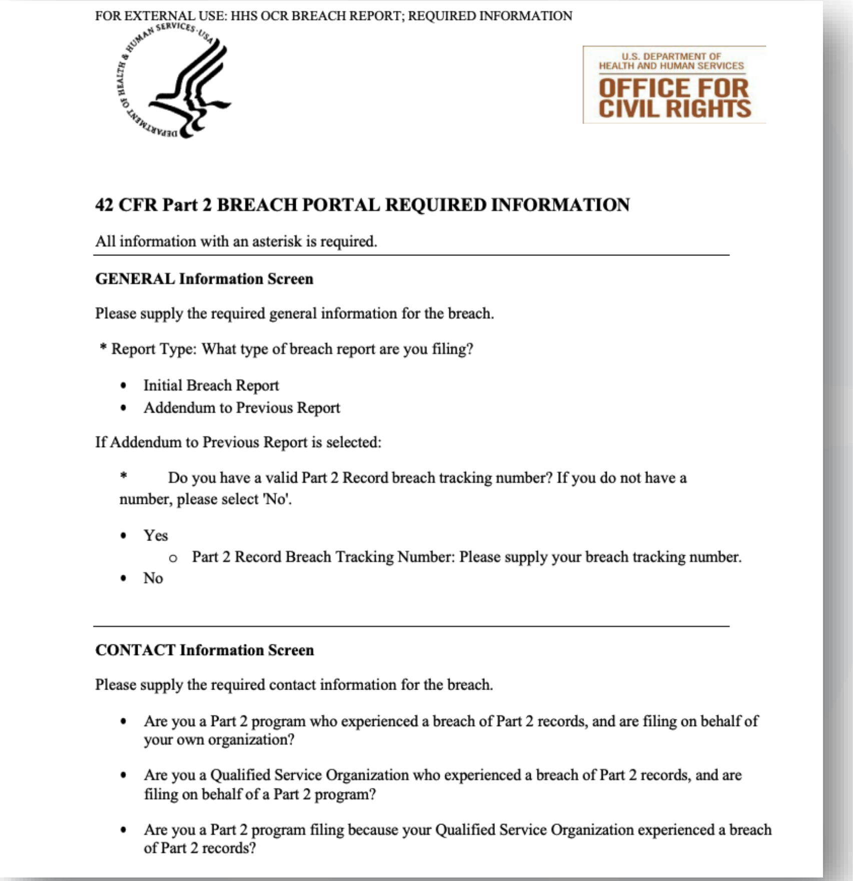
17 new breaches reported in February totaling **939,612** affected individuals

Source: U.S. Department of Health & Human Services - Office for Civil Rights

Clearwater

OCR Launches Part 2 Enforcement Program, New Breach Portal Features

- Effective **Feb. 16, 2026**, entities subject to 42 CFR Part 2 rules, commonly known as "Part 2," are required to comply with breach notification requirements or else face penalties aligned with those administered under HIPAA.



FOR EXTERNAL USE: HHS OCR BREACH REPORT; REQUIRED INFORMATION

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

42 CFR Part 2 BREACH PORTAL REQUIRED INFORMATION

All information with an asterisk is required.

GENERAL Information Screen

Please supply the required general information for the breach.

* Report Type: What type of breach report are you filing?

- Initial Breach Report
- Addendum to Previous Report

If Addendum to Previous Report is selected:

* Do you have a valid Part 2 Record breach tracking number? If you do not have a number, please select 'No'.

- Yes
  - Part 2 Record Breach Tracking Number: Please supply your breach tracking number.
- No

CONTACT Information Screen

Please supply the required contact information for the breach.

- Are you a Part 2 program who experienced a breach of Part 2 records, and are filing on behalf of your own organization?
- Are you a Qualified Service Organization who experienced a breach of Part 2 records, and are filing on behalf of a Part 2 program?
- Are you a Part 2 program filing because your Qualified Service Organization experienced a breach of Part 2 records?

Source: https://ocrportal.hhs.gov/ocr/breach/

Risk Analysis Enforcement Focus Continues

On February 19, OCR announced settlement with Top of the World Ranch Treatment Center (TWRTC), marking OCR's 11th enforcement action under its Risk Analysis Initiative

OCR's investigation found that **TWRTC failed to conduct an accurate and thorough risk analysis** of its ePHI as required by the HIPAA Security Rule

*"In a time where health care providers and other HIPAA regulated entities are facing unprecedented cybersecurity threats, **compliance with the HIPAA Risk Analysis provision is more essential than ever**," said OCR Director Paula M. Stannard. "Covered entities and business associates cannot protect electronic protected health information if they haven't identified potential risks and vulnerabilities to that health information."*

Source: https://www.hhs.gov/press-room/ocr-settles-hipaa-security-rule-investigation-twrtc.html

Healthcare Industry Threat Information

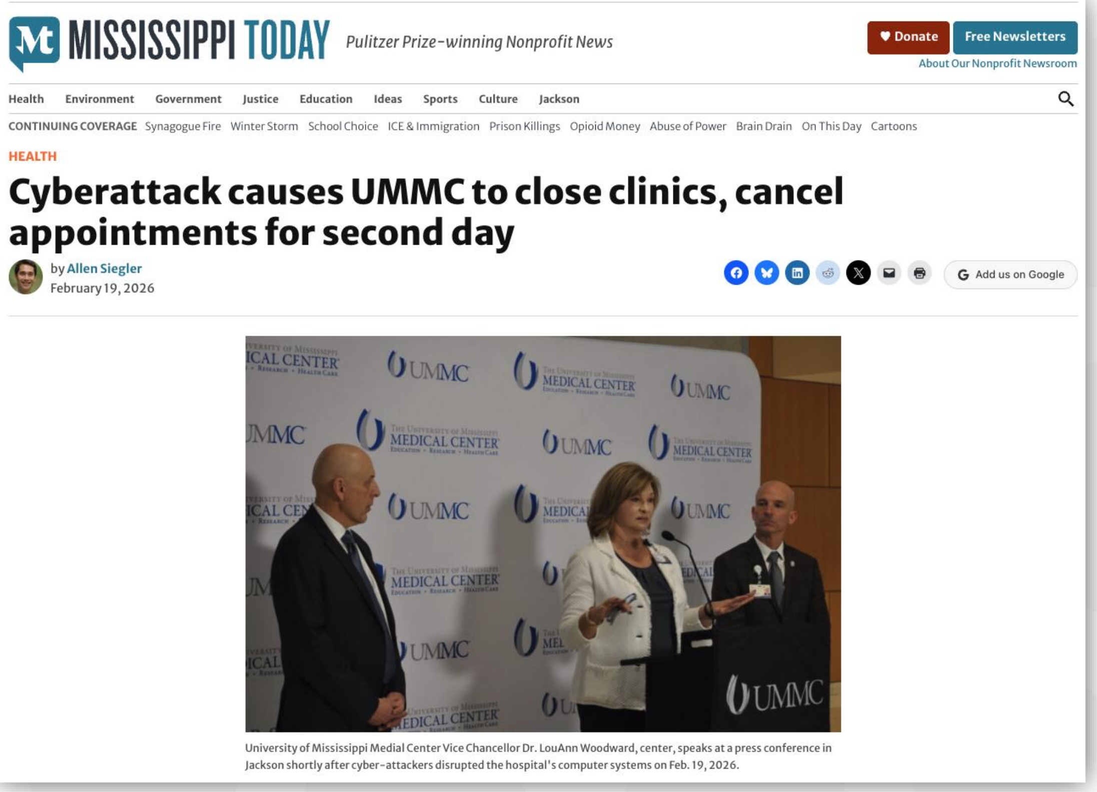
Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

Major ransomware attack on Feb. 19, 2026, paralyzed the University of Mississippi Medical Center’s IT systems

- The attack disrupted access to *Epic* and other core operational systems.
- UMMC expects *normal operations and access to electronic health records to resume gradually*, though full recovery, including a forensic investigation into scope and data exposure, could take *weeks to months*



HEALTH

Cyberattack causes UMMC to close clinics, cancel appointments for second day

by Allen Siegler
February 19, 2026

University of Mississippi Medial Center Vice Chancellor Dr. LouAnn Woodward, center, speaks at a press conference in Jackson shortly after cyber-attackers disrupted the hospital's computer systems on Feb. 19, 2026.

The healthcare sector faced an intense wave of financially motivated attacks throughout February

Lazarus Group Medusa Ransomware Attacks

- A North Korean-nexus threat actor has shifted tactics to deploy Medusa ransomware-as-a-service against US healthcare and non-profit organizations. These operations utilize custom backdoors such as Comebacker and Blindingcan for initial network compromise and data theft before encryption

Healthcare University REDCap Server Exploitation

- A China-nexus actor targeted a US medical research university by exploiting a REDCap server to deploy INFINITERED malware. The campaign focused on harvesting credentials and exfiltrating sensitive research and national security-related content from user emails and storage

Critical Zero-Day Exploitation Monitoring

- On Feb. 10, 2026, Microsoft released security updates addressing more than 50 vulnerabilities, including six zero-days actively exploited in the wild. The campaign leverages three security feature bypass flaws—CVE-2026-21510 in Windows Shell, CVE-2026-21513 in the MSHTML engine, and CVE-2026-21514 in Microsoft Word—allowing attackers to evade SmartScreen prompts and execute malicious code via crafted shortcut files or documents.

Emerging Threats: Dohdoor Backdoor Targeting US Healthcare

- A sophisticated campaign identified as UAT-10027 is targeting US healthcare and education sectors with the Dohdoor backdoor. The malware utilizes DNS-over-HTTPS for covert C2 communications and employs process hollowing and EDR unhooking to maintain stealth

Ransomware Update

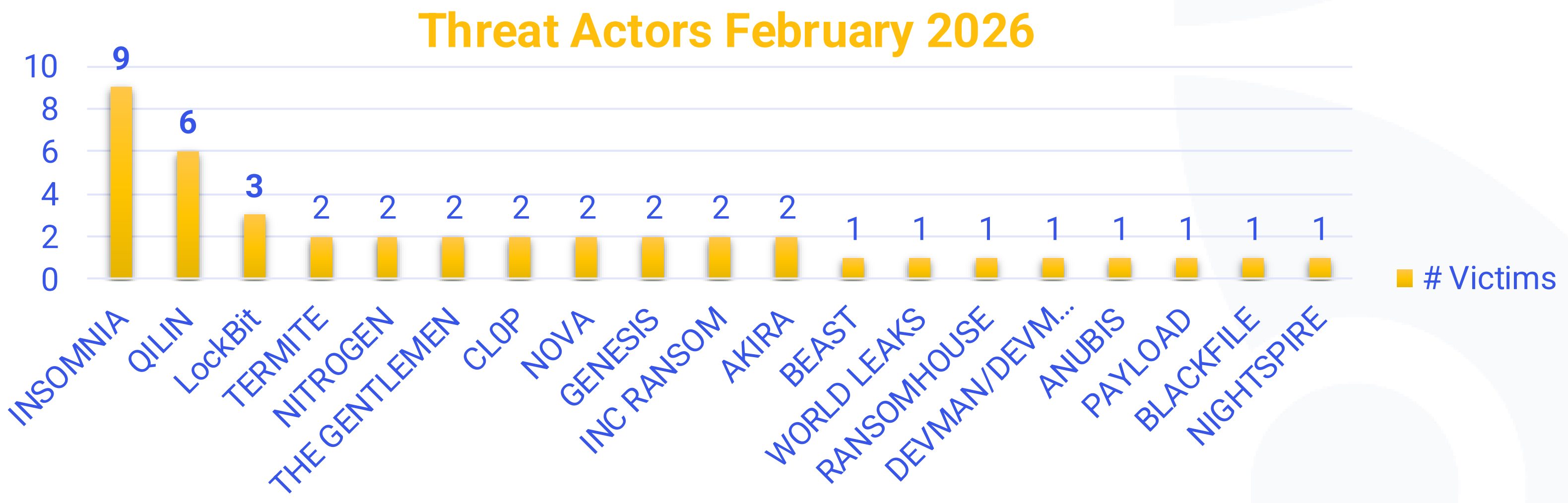
Impacts from Ransomware in February

Google Threat Intelligence

Clearwater

Number of reported victims climbs to 42 in the February up from 32 in Jan

INSOMNIA, QILIN and **LockBit** comprise of 42% of the reported data leaks



42
Victims

19
Threat Actors

Insights

- Healthcare remains a high-value, highly targeted sector
- Repeat victimization: at least one organization appeared under more than one ransomware group (Feb 3rd by DEVMAN & Feb 17th by LockBit)

Clearwater

Google Threat Intelligence

Sophisticated emerging groups

INSOMNIA

- INSOMNIA s an emerging extortion-focused entity that first appeared on data leak sites (DLS) in October
- Unlike traditional ransomware groups that prioritize disruptive system encryption, INSOMNIA appears optimized for stealthy data theft and "pure" extortion through the exposure of sensitive information
- leverages a hybrid operational model, acting both as a direct intruder and potentially as a broker for monetizing data stolen by other actors . Their technical approach emphasizes speed and low visibility:
- The group utilizes credential-based access, often sourcing credentials from infostealers or exploiting authentication bypass vulnerabilities They are known to abuse legitimate infrastructure, such as Windows Server updates, to move laterally within victim networks .
- Currently, the operation functions primarily as a data leak site rather than an encryption operation, as no specific ransomware variant or negotiation portal has yet been tied to the group

The Gentlemen

- Emerged as a highly sophisticated threat in mid-to-late 2025. Demonstrating advanced technical maturity, the group operates a Ransomware-as-a-Service (RaaS) model and quickly expanded its impact across Windows, Linux, and ESXi environments
- The Gentlemen utilize a double-extortion strategy, exfiltrating sensitive data before deploying a cross-platform locker written in Go and C
- Their operations are characterized by defensive evasion with the hallmark of the group weaponizing legitimate drivers to terminate protected security processes
- They leverage GPO’s to spread ransomware, use scheduled tasks to maintain persistence, and demonstrate technical sophistication with variants that include automatic restart features, 15% faster encryption, and support for multiple encryption modes

Ransomware Targeting Patterns

Impacts from Ransomware in February

Google Threat Intelligence

Clearwater

Specialty and outpatient providers represent the highest concentration of observed victims

Threat Actor	Hospitals	Specialty Practices	Dental	Senior Care	Diagnostic	Pharma/ Pharmacy	Research
INSOMNIA	⚪	🔴	⚪	🟡	🔴	⚪	⚪
QILIN	⚪	🔴	🟡	🟡	⚪	⚪	⚪
LockBit	⚪	🔴	🟡	⚪	⚪	⚪	⚪
CL0P	⚪	🟡	⚪	⚪	⚪	⚪	⚪
AKIRA	⚪	🟡	🟡	⚪	⚪	🔴	⚪
GENESIS	⚪	🔴	⚪	⚪	⚪	⚪	⚪

🔴 Multiple victims observed

🟡 Single victims observed

⚪ No victims observed

Threat Actor	Hospitals	Specialty Practices	Dental	Senior Care	Diagnostic	Pharma/ Pharmacy	Research
TERMITE	🔴	⚪	⚪	⚪	⚪	⚪	⚪
NOVA	⚪	⚪	⚪	⚪	🔴	⚪	⚪
RansomHouse	⚪	🟡	⚪	⚪	⚪	⚪	⚪
NITROGEN	⚪	🟡	🟡	⚪	⚪	🟡	⚪
BLACKFILE[1]	⚪	⚪	⚪	⚪	⚪	⚪	⚪
WORLD LEAKS	🟡	⚪	⚪	⚪	⚪	⚪	⚪
THE GENTLEMEN	🔴	⚪	⚪	⚪	⚪	⚪	⚪
BEAST	⚪	⚪	🟡	⚪	⚪	⚪	⚪
ANUBIS	⚪	🟡	⚪	⚪	⚪	⚪	⚪
INC RANSOM	⚪	🟡	⚪	⚪	⚪	🟡	⚪
NIGHTSPIRE	⚪	⚪	⚪	⚪	⚪	⚪	🟡
DEVMAN 2.0	⚪	🟡	⚪	⚪	⚪	⚪	⚪

Emerging & Secondary Actors

[1] Medical device adjacent victim

Key Takeaways

1. Secure identities first
2. Build recovery and breach resilience
3. Reduce lateral movement and vendor exposure through segmentation

Google Threat Intelligence Clearwater

Healthcare’s Cyber Briefing

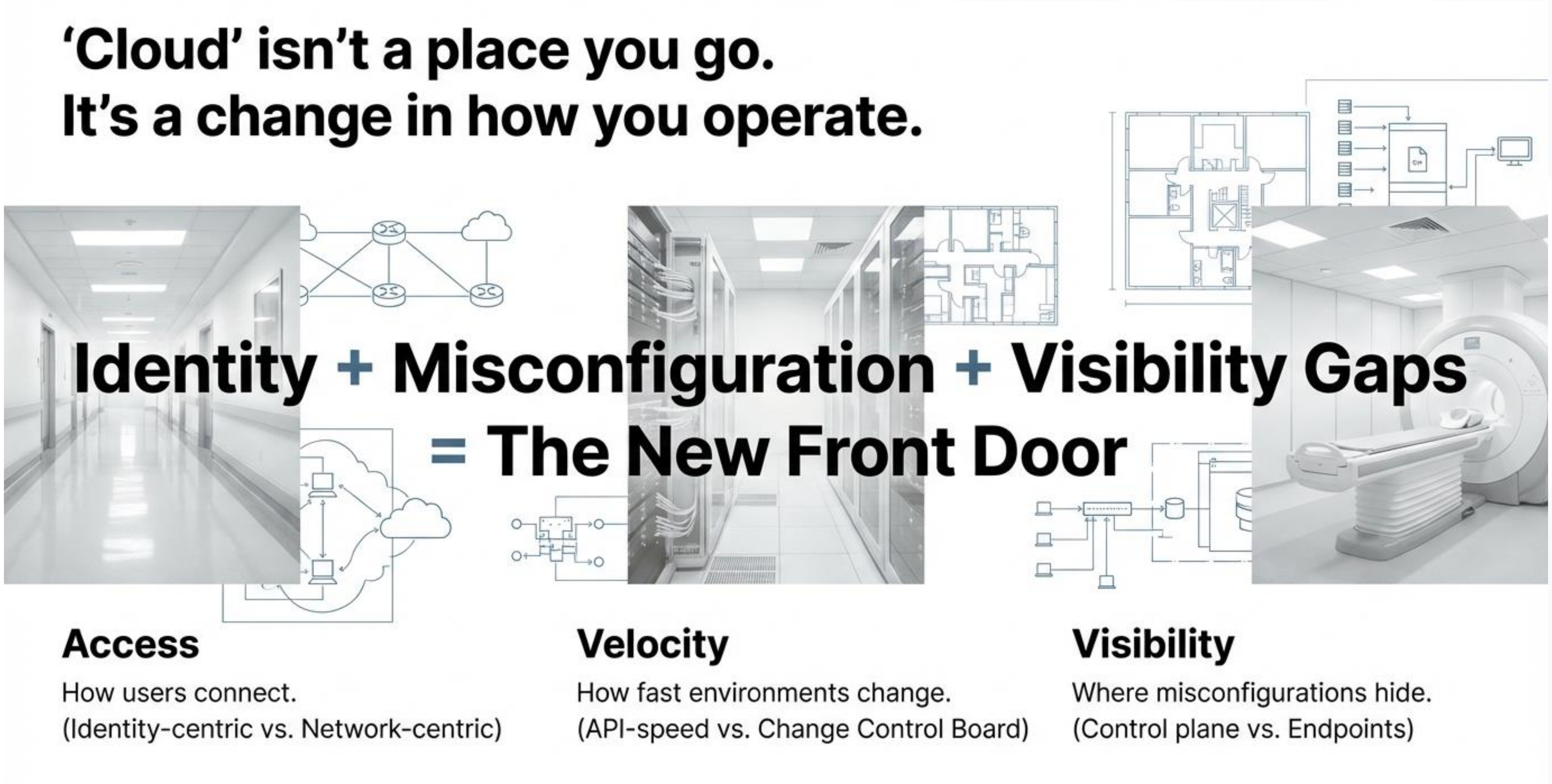
When the Cloud Becomes the Attack Surface: Hybrid Risk, Identity, and Governance in Healthcare

FEATURING:

Jackie Mattingly, Senior Director, Consulting Services, Regional and Critical Access Hospitals

Brian McManamon, General Manager, Managed Cloud and Managed Security Services

The New Reality of Hybrid Healthcare Security



‘Cloud’ isn’t a place you go.
It’s a change in how you operate.

Identity + Misconfiguration + Visibility Gaps
= The New Front Door

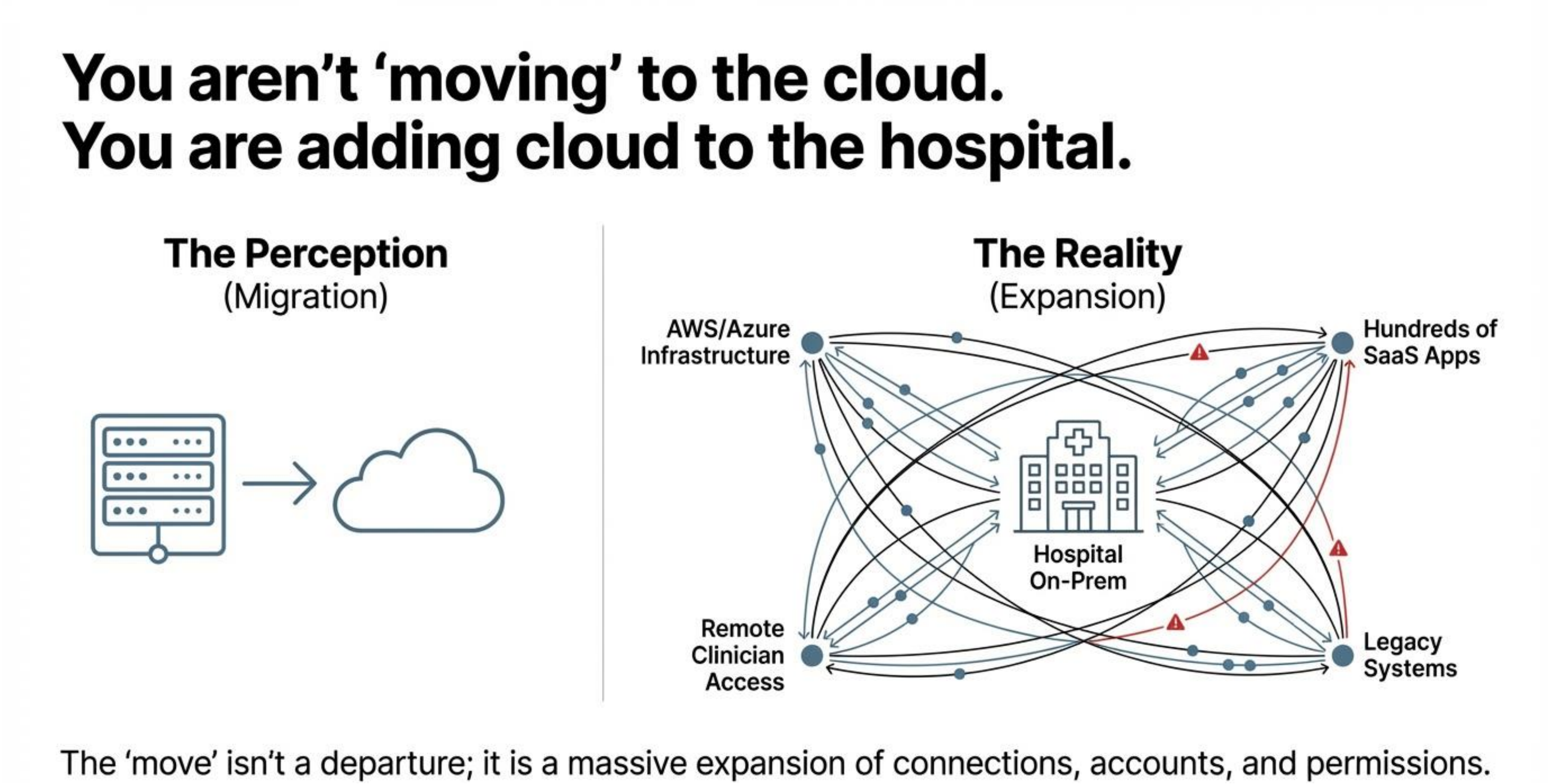
Access
How users connect.
(Identity-centric vs. Network-centric)

Velocity
How fast environments change.
(API-speed vs. Change Control Board)

Visibility
Where misconfigurations hide.
(Control plane vs. Endpoints)

Clearwater

The Great Misconception:
We Aren’t Moving, We’re Adding



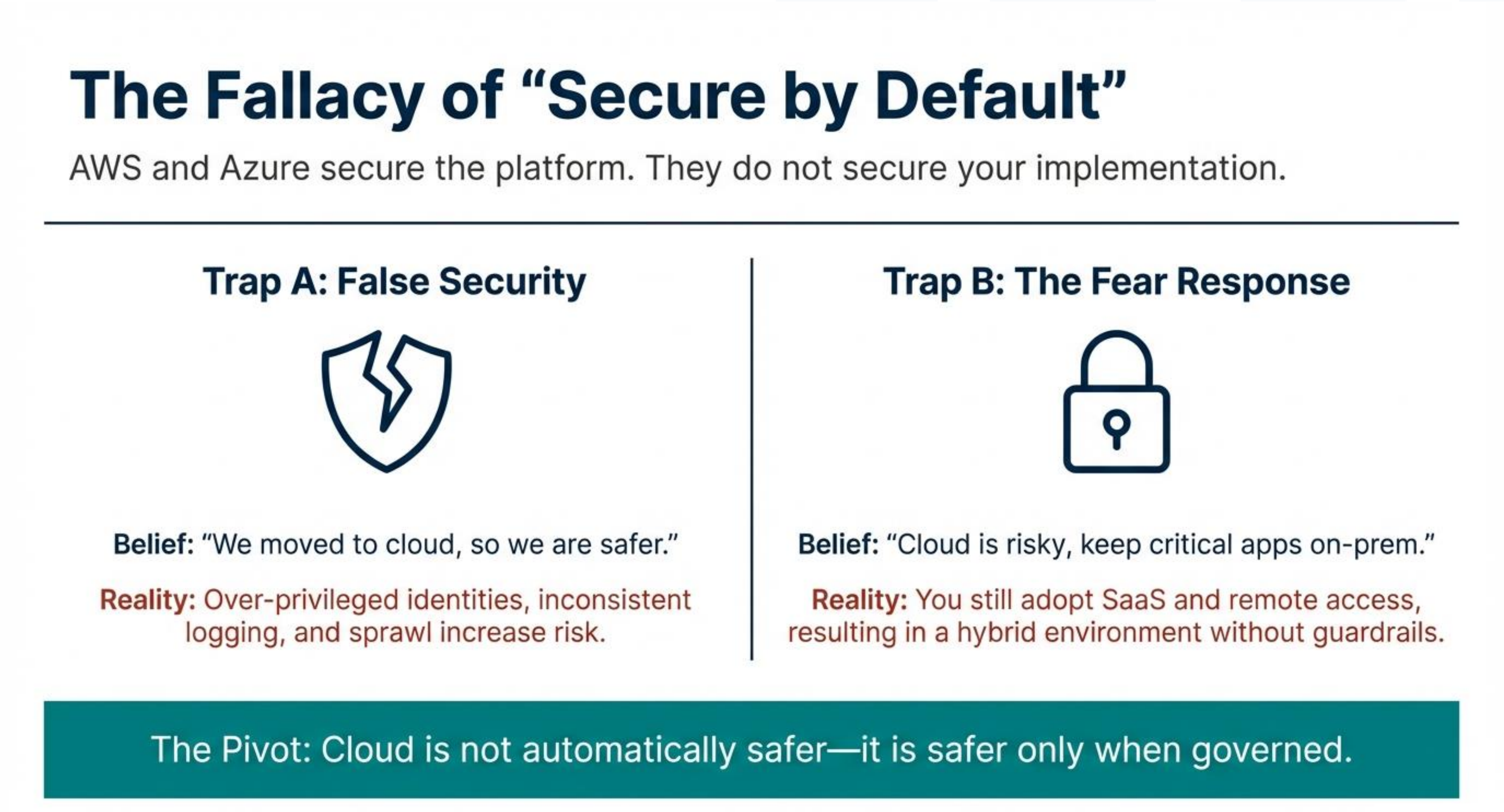
You aren’t ‘moving’ to the cloud.
You are adding cloud to the hospital.

The Perception
(Migration)

The Reality
(Expansion)

The ‘move’ isn’t a departure; it is a massive expansion of connections, accounts, and permissions.

Shared Responsibility



The Fallacy of "Secure by Default"

AWS and Azure secure the platform. They do not secure your implementation.

Trap A: False Security

Belief: "We moved to cloud, so we are safer."

Reality: Over-privileged identities, inconsistent logging, and sprawl increase risk.

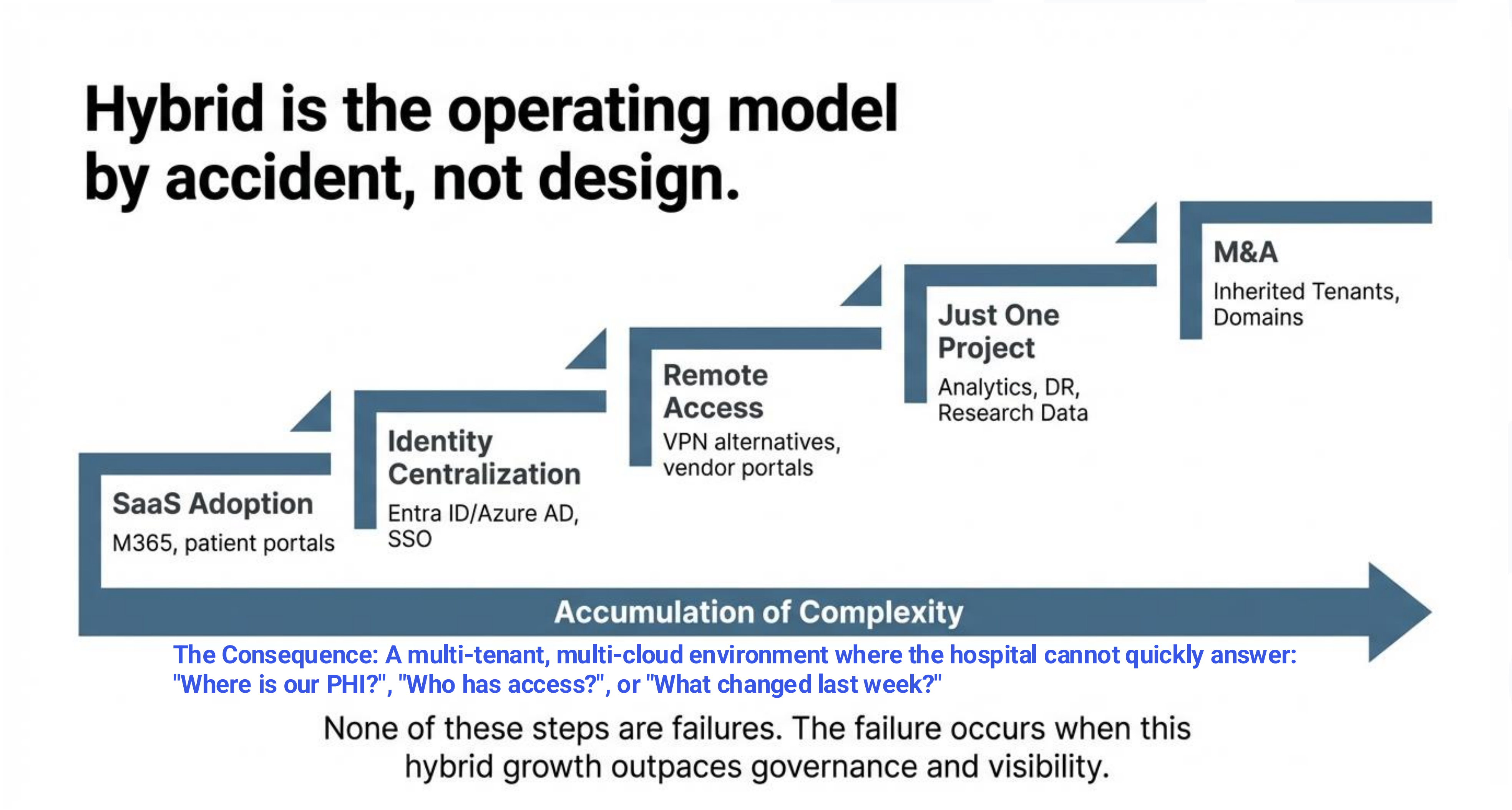
Trap B: The Fear Response

Belief: "Cloud is risky, keep critical apps on-prem."

Reality: You still adopt SaaS and remote access, resulting in a hybrid environment without guardrails.

The Pivot: Cloud is not automatically safer—it is safer only when governed.

Anatomy of the “Accidental Hybrid”



Hybrid is the operating model by accident, not design.

SaaS Adoption
M365, patient portals

Identity Centralization
Entra ID/Azure AD, SSO

Remote Access
VPN alternatives, vendor portals

Just One Project
Analytics, DR, Research Data

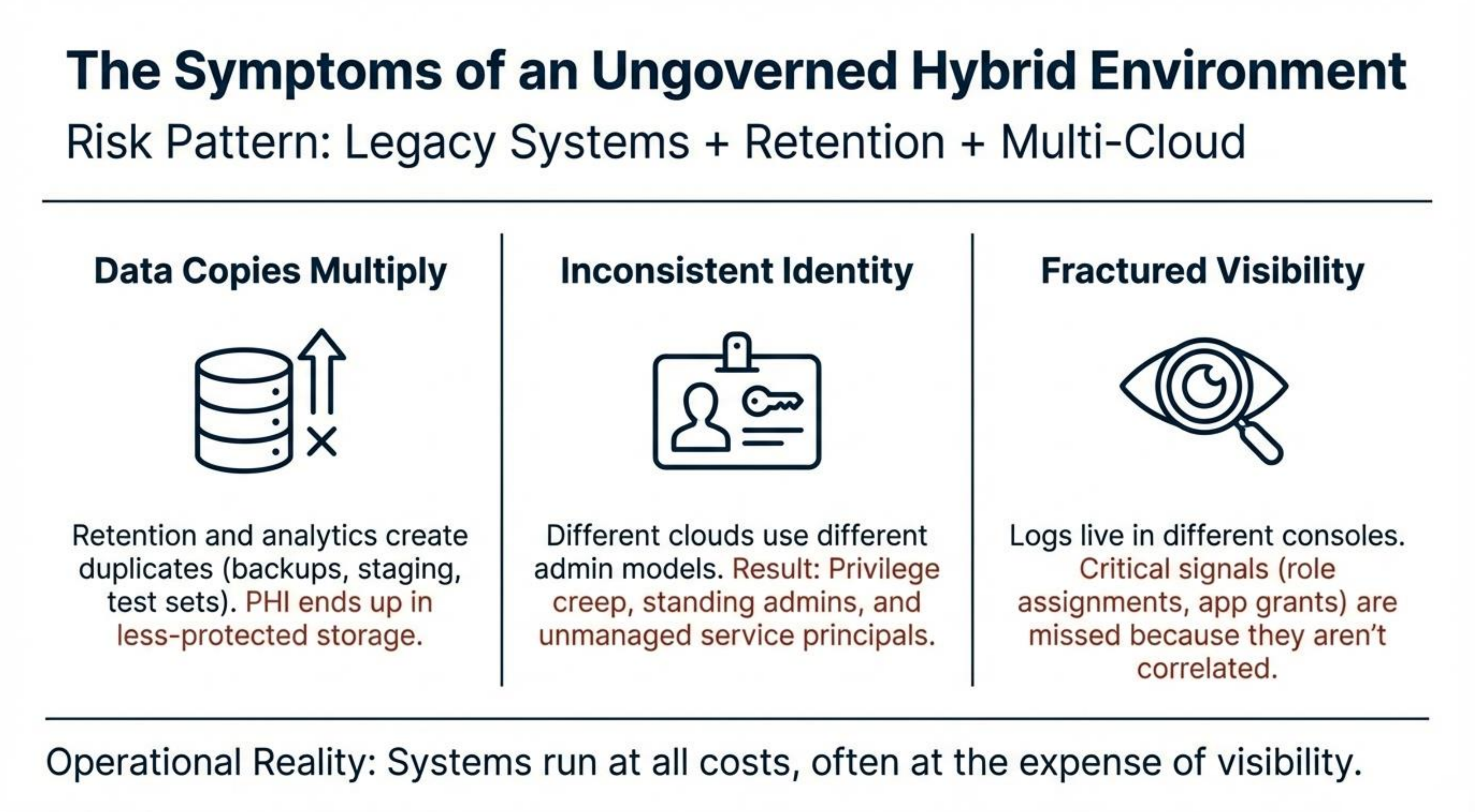
M&A
Inherited Tenants, Domains

Accumulation of Complexity

The Consequence: A multi-tenant, multi-cloud environment where the hospital cannot quickly answer: "Where is our PHI?", "Who has access?", or "What changed last week?"

None of these steps are failures. The failure occurs when this hybrid growth outpaces governance and visibility.

The Three Risks of Hybrid Sprawl



The Symptoms of an Ungoverned Hybrid Environment

Risk Pattern: Legacy Systems + Retention + Multi-Cloud

Data Copies Multiply

Retention and analytics create duplicates (backups, staging, test sets). PHI ends up in less-protected storage.

Inconsistent Identity

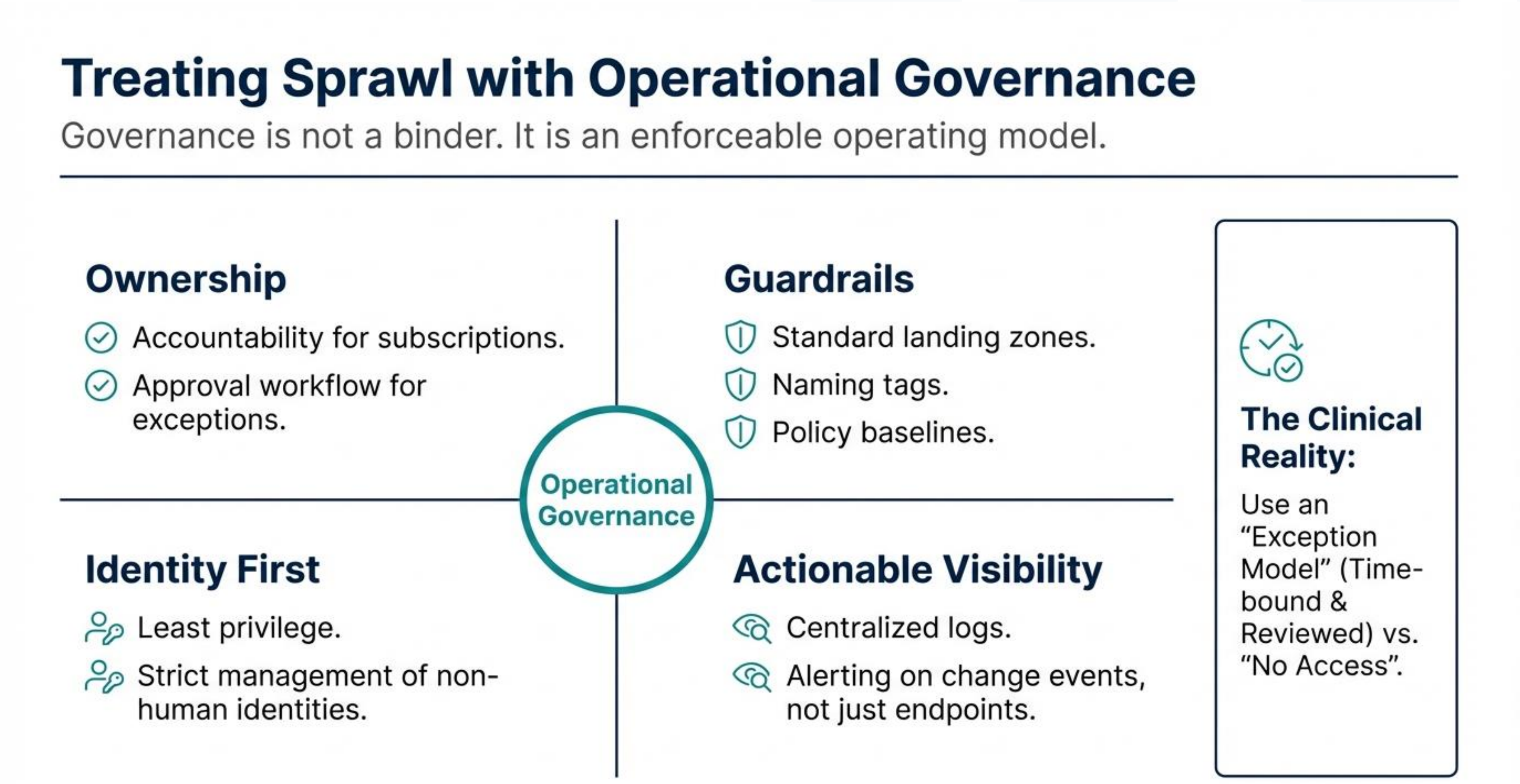
Different clouds use different admin models. Result: Privilege creep, standing admins, and unmanaged service principals.

Fractured Visibility

Logs live in different consoles. Critical signals (role assignments, app grants) are missed because they aren’t correlated.

Operational Reality: Systems run at all costs, often at the expense of visibility.

Governance is an Operating Model Not a Policy Binder



Treating Sprawl with Operational Governance

Governance is not a binder. It is an enforceable operating model.

Ownership

- ✓ Accountability for subscriptions.
- ✓ Approval workflow for exceptions.

Guardrails

- Standard landing zones.
- Naming tags.
- Policy baselines.

Identity First

- Least privilege.
- Strict management of non-human identities.

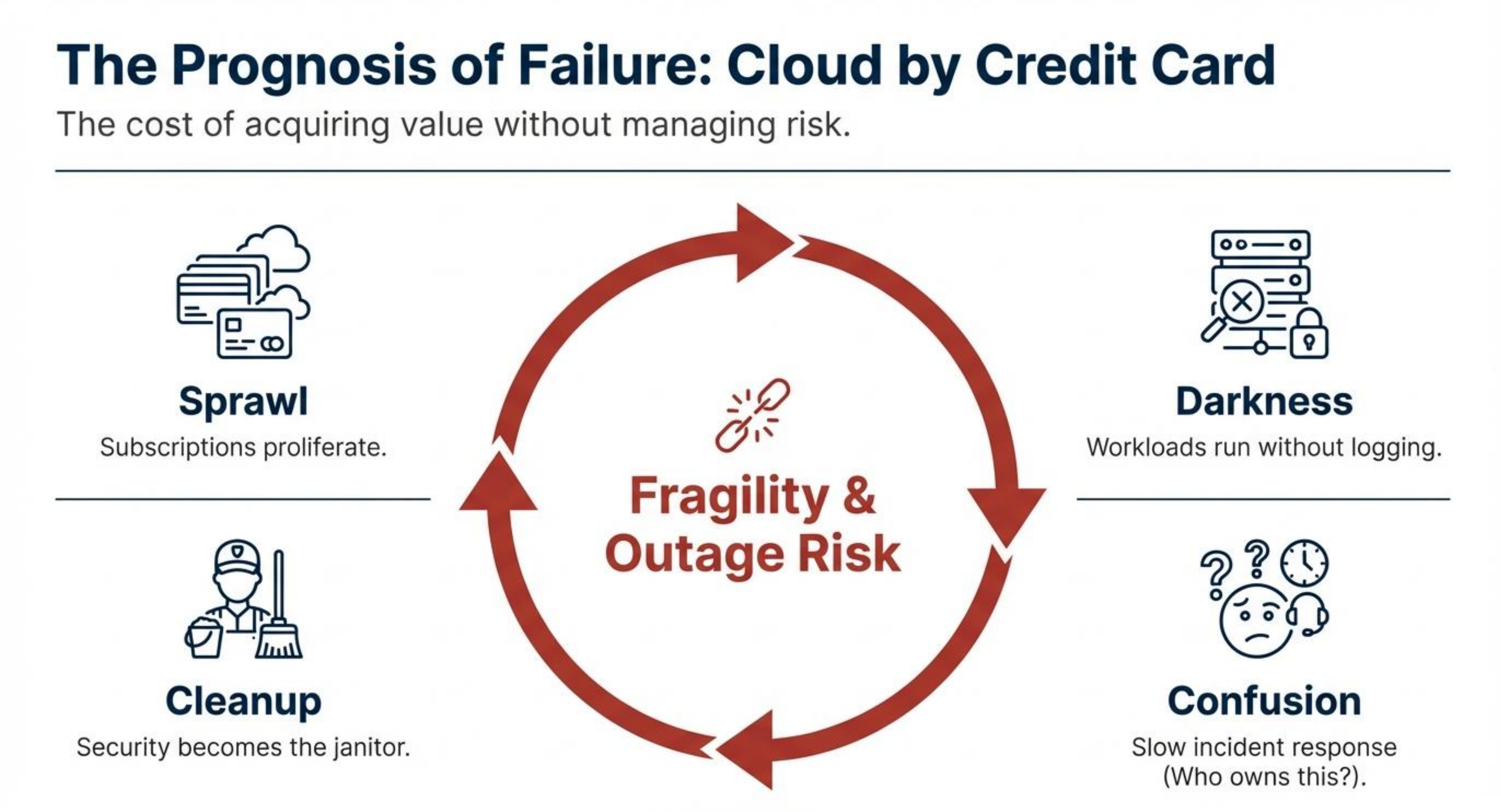
Actionable Visibility

- Centralized logs.
- Alerting on change events, not just endpoints.

The Clinical Reality:

Use an "Exception Model" (Time-bound & Reviewed) vs. "No Access".

Migration without Governance



The Prognosis of Failure: Cloud by Credit Card

The cost of acquiring value without managing risk.

Sprawl

Subscriptions proliferate.

Darkness

Workloads run without logging.

Fragility & Outage Risk

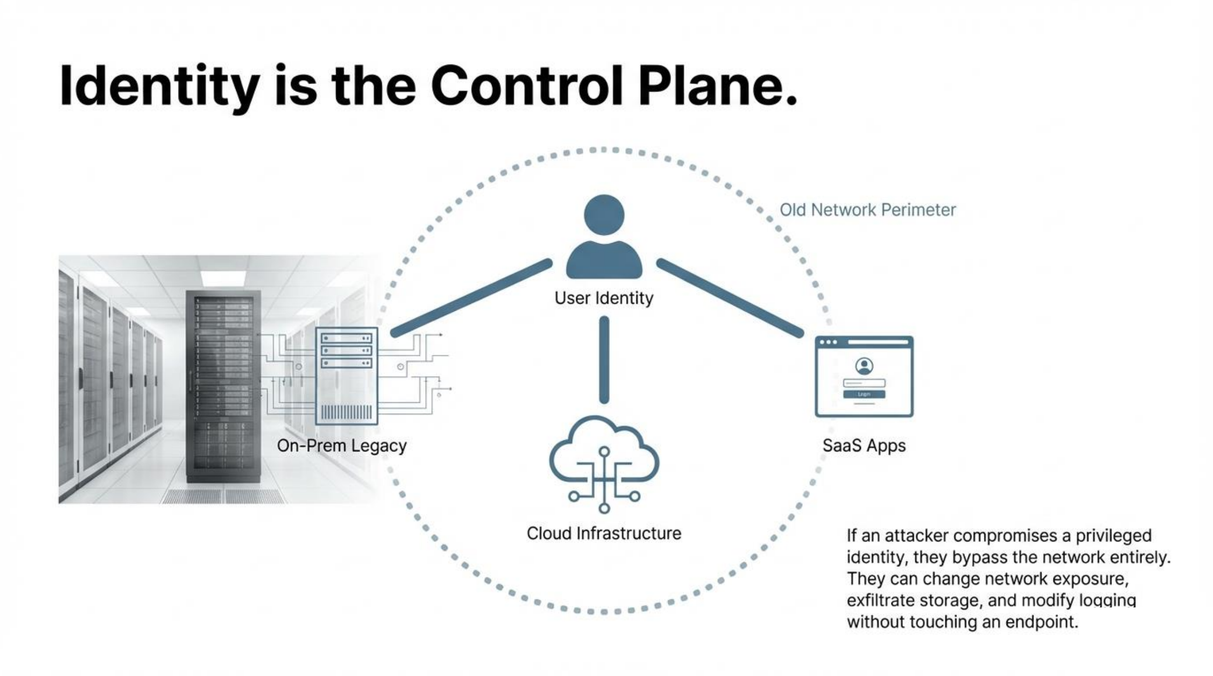
Cleanup

Security becomes the janitor.

Confusion

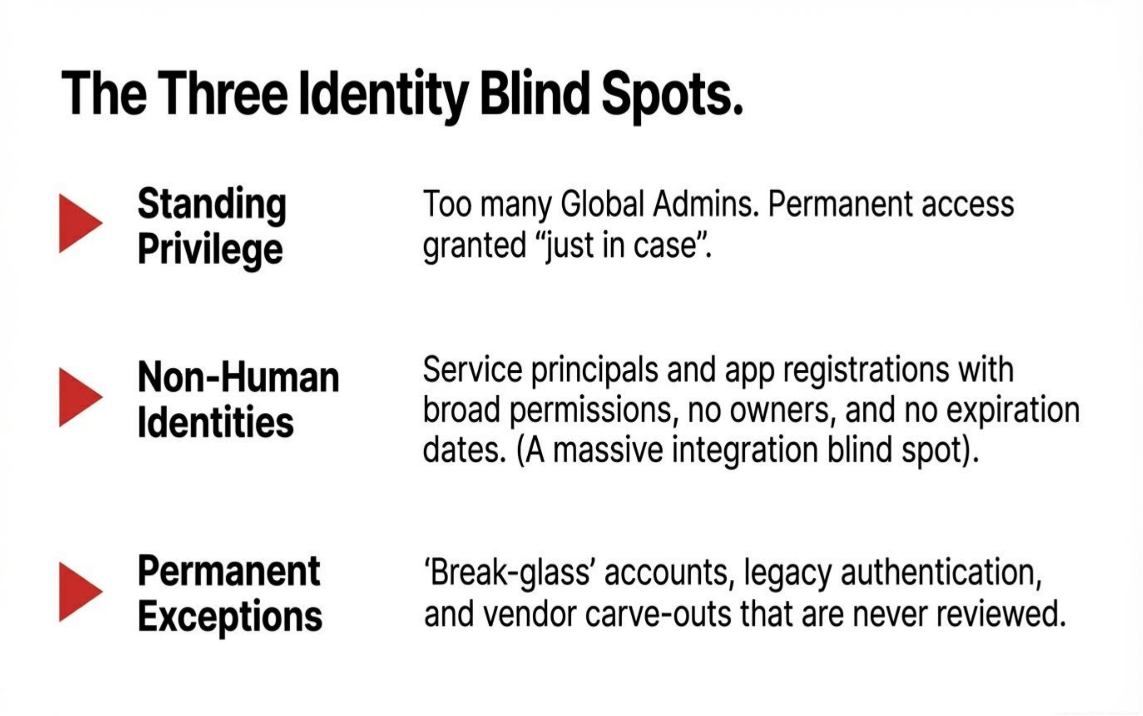
Slow incident response (Who owns this?).

Identity is the New Control Plane



Identity is the Control Plane.

If an attacker compromises a privileged identity, they bypass the network entirely. They can change network exposure, exfiltrate storage, and modify logging without touching an endpoint.



The Three Identity Blind Spots.

▶ **Standing Privilege** Too many Global Admins. Permanent access granted “just in case”.

▶ **Non-Human Identities** Service principals and app registrations with broad permissions, no owners, and no expiration dates. (A massive integration blind spot).

▶ **Permanent Exceptions** ‘Break-glass’ accounts, legacy authentication, and vendor carve-outs that are never reviewed.

Balancing Clinical Speed with Security Controls

Low Friction

Routine Clinical Access (SSO)

High Friction

1. Privileged admin functions
2. Bulk sensitive data access
3. New credential creation

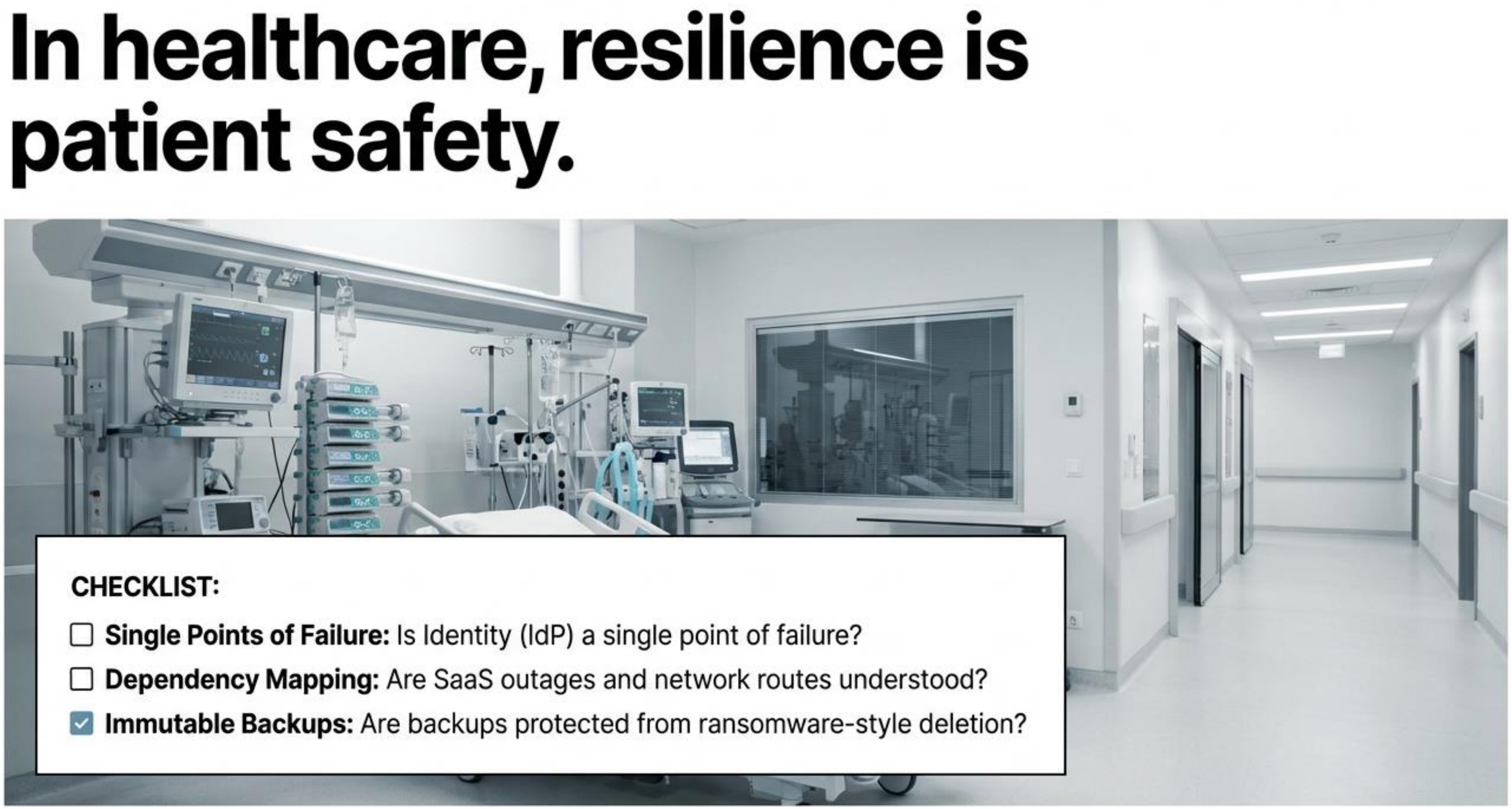
The Solution:
Risk-Based Friction

Clinicians need fast access;
Security needs tight control.

Tactic: Use 'Step-Up' controls for suspicious sign-ins or high-risk actions rather than slowing everyone down.

Key Strategy: The Exception Model
Exceptions are permitted to respect clinical urgency,
but they must be time-bound, owned, documented, and reviewed

Resilience is Patient Safety

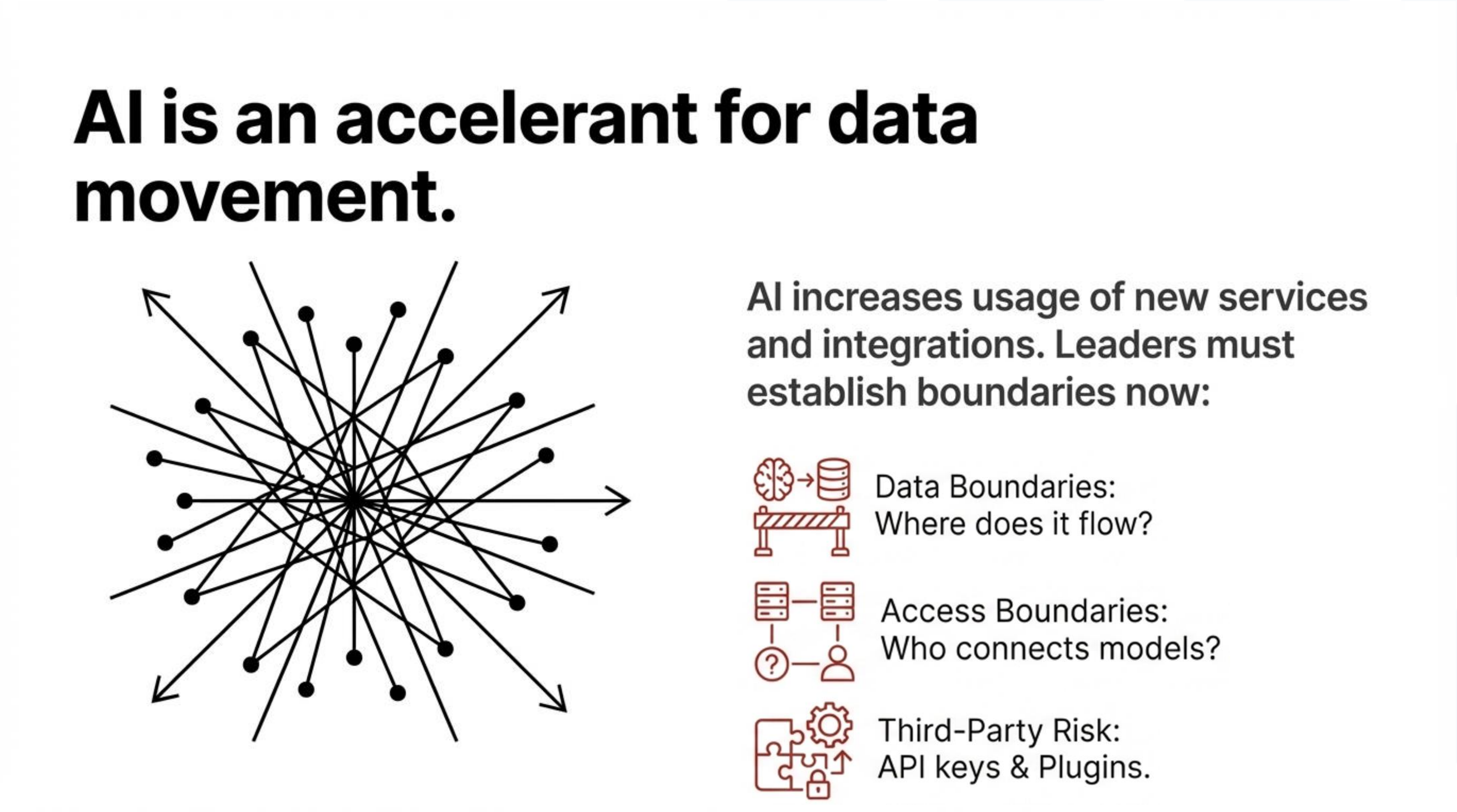


In healthcare, resilience is patient safety.

CHECKLIST:

- ☐ **Single Points of Failure:** Is Identity (IdP) a single point of failure?
- ☐ **Dependency Mapping:** Are SaaS outages and network routes understood?
- ☑ **Immutable Backups:** Are backups protected from ransomware-style deletion?

AI in the Cloud

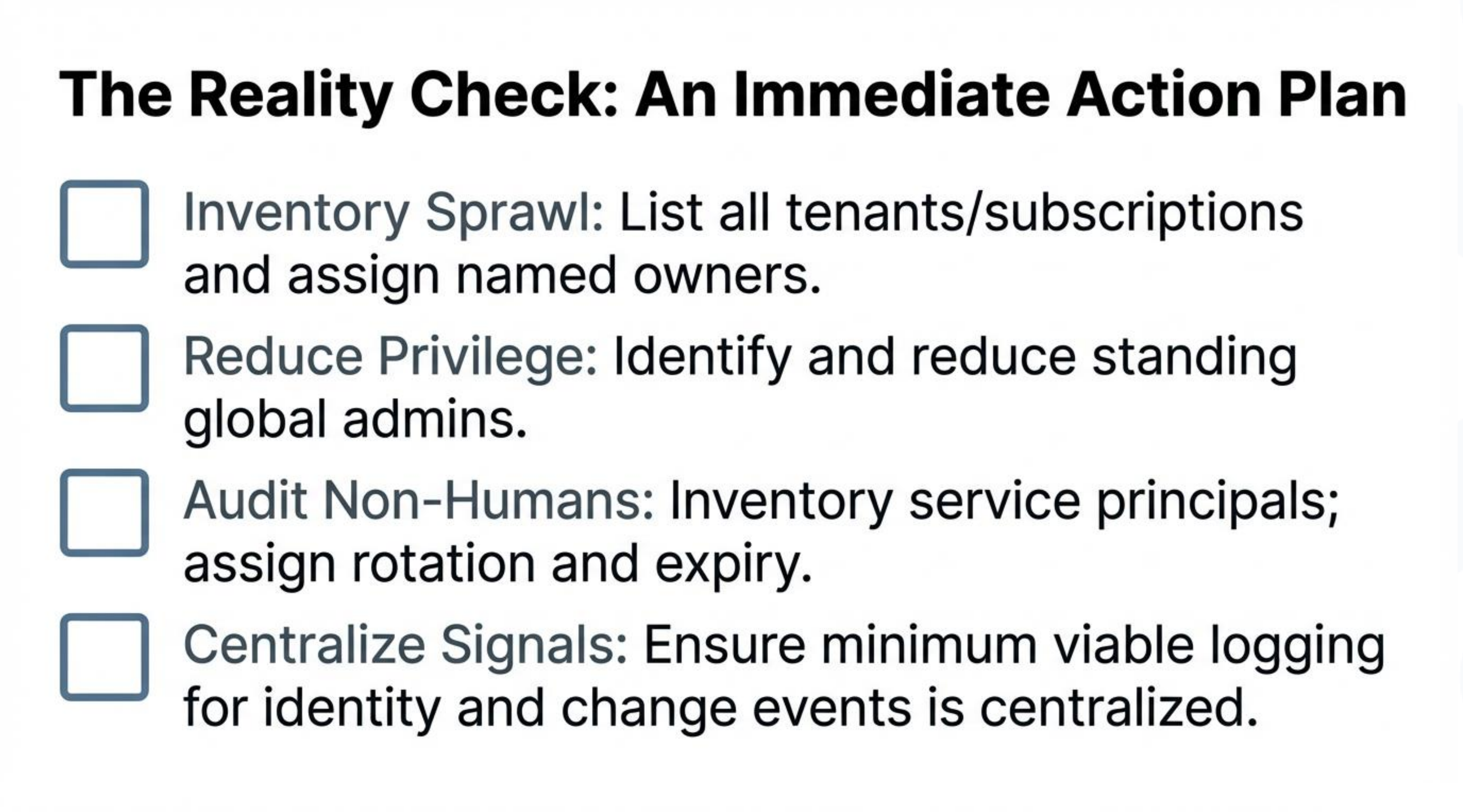


AI is an accelerant for data movement.

AI increases usage of new services and integrations. Leaders must establish boundaries now:

- Data Boundaries:
  Where does it flow?
- Access Boundaries:
  Who connects models?
- Third-Party Risk:
  API keys & Plugins.

The “Back to Office” Reality Check



The Reality Check: An Immediate Action Plan

- □ Inventory Sprawl: List all tenants/subscriptions and assign named owners.
- □ Reduce Privilege: Identify and reduce standing global admins.
- □ Audit Non-Humans: Inventory service principals; assign rotation and expiry.
- □ Centralize Signals: Ensure minimum viable logging for identity and change events is centralized.

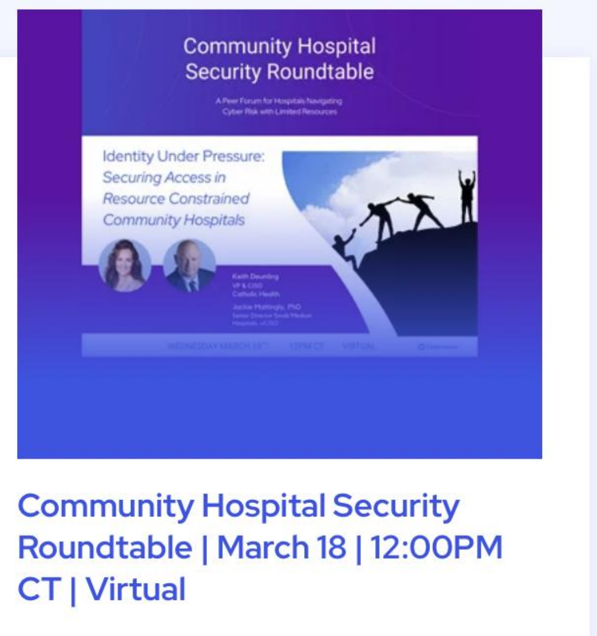
Q&A

Clearwater

Upcoming Webinars and Virtual Events

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

- Next session April 2nd
- VP, Privacy & Compliance Services, Andrew Mahler with CHIME executives discussing what's happening inside Washington & HHS
- Be on the lookout for the next quarter's invites (April, May & June) to come to your inbox next week



Community Hospital Security Roundtable

A Peer Forum for Hospitals Navigating Cyber Risk with Limited Resources

Identity Under Pressure: *Securing Access in Resource Constrained Community Hospitals*

Keith Deumling
VP & CISO
Catholic Health

Jackie Mattingly, PhD
Senior Director Small-Medium Hospitals, vCISO

WEDNESDAY MARCH 18TH 12PM CT VIRTUAL

Community Hospital Security Roundtable | March 18 | 12:00PM CT | Virtual

- Topic: Identity Under Pressure: Securing Access in Resource-Constrained Hospitals.
- Speakers: Keith Duemling, CISO Catholic Health + Jackie Mattingly, Clearwater

Save your spot

The Virtual Forty-Third National HIPAA Summit

- Clearwater experts will be speaking in multiple sessions during this premier industry conference, including a Cybersecurity Leaders Roundtable moderated by Senior Director of Consulting Services Jackie Mattingly; the conference is being presented April 7-10

View session information + register

Clearwater

Upcoming In-Person Events

HIMSS 2026 | March 9–12, 2026 | Las Vegas, NV

- Find CW in the Cybersecurity Command Center at our booth
- Dave Bailey, VP Consulting Solutions & Strategy will be speaking on AI in Healthcare on Wednesday at 10 am PT.

Learn more + book a meeting

Scale Community Gold Club Retreat | April 10-12, 2026 | Park City, UT

- Clearwater's David Kolb, VP, PPMG + Austin Holland AE, PPMG attending
- This exclusive gathering of senior leaders from Management Services Organizations (MSOs) in healthcare.

Learn more + book a meeting

HCCA Annual Compliance Institute | April 27-30, 2026 | Orlando, FL

- Clearwater is excited to participate in this premier conference for healthcare compliance and ethics professionals, bringing together industry leaders to explore best practices, regulatory updates, and emerging risk
- Several Clearwater experts speaking and visit us at booth 419

Learn more + view sessions

Cooley HealthTech Conference | April 28, 2026 | Palo Alto, CA

- Clearwater is proud to sponsor
- This invite-only event will spotlight the key forces driving innovation and growth industrywide, with focused discussions on strategies for healthtech, medical device, medtech and digital health companies.

Learn more + book a meeting

Upcoming In-Person Events

McGuireWoods Healthcare Private Equity & Finance Conference | April 29-30 | Chicago, IL

Health Tech Investment Forum 2026
April 30, 2026 | San Francisco, CA

McDermott Health Tech Investment Forum | April 30, 2026 | San Francisco, CA

- David Kolb, VP. PPMG, Dave Bailey, VP Consulting Strategy & Solutions and Richmond Donnelly, Senior Account Exec, Private Equity attending

- Clearwater is proud to sponsor this new event convening investors, c-suite operators and founders in healthcare tech.
- Alex Masten, VP, Digital Health & Jeff Englander, Executive Business Advisor, Business Development attending

Learn more+ book a meeting

Learn more + book a meeting

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.