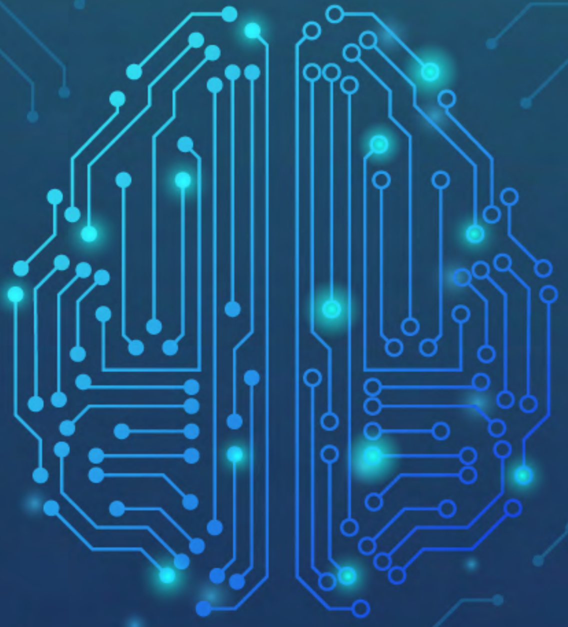
Fortified
HEALTH SECURITY

2025 MID-YEAR HORIZON REPORT

The state of cybersecurity in healthcare

Contents



CEO's Message

"Think differently."

I was getting a new headshot, which is always a bit awkward, when the photographer suggested I pose with my hand in my pocket. My first instinct was to say no, but I decided to do it. The result? It was the first time I actually liked how my picture turned out.

It was such a small moment but an important reminder that sometimes the best results come from getting a little uncomfortable, listening to feedback, and being open to a new approach. The same holds true in how we evolve as healthcare's cybersecurity partner: We have to think differently.

What does thinking differently look like for healthcare organizations like yours? It means not settling for the status quo. Expecting more from your MSSP: More specific insights, communication, and collaboration. It means finding the right partner who listens to your feedback, evolves with your needs, and focuses on outcomes that protect your patients, data, and mission.

That mindset led to the launch of EscalationIQ, our enhanced module within Central Command that gives clients a more transparent, collaborative threat response experience. Born from direct client feedback and custom-built by our experts, EscalationIQ is another example of how we're improving workflows and redefining them.

That commitment to going next level also helped us earn the title of Best in KLAS for Security & Privacy Managed Services for the fourth year in a row.

Thinking differently isn't just a catchphrase for my mid-year message; it's a genuine commitment to being bold and leading with agility, creativity, and a deep understanding of the mission that drives healthcare cybersecurity forward.

For the rest of 2025 and beyond, let's keep making healthcare safer, protecting patient data, and changing the game.

Warm regards,

Dan L. Dodson

2025 Mid-Year Cybersecurity Check-In

Meaningful progress regarding healthcare cybersecurity posture is underway, but some serious gaps remain. At the midpoint of 2025, Fortified Health Security's rolling NIST Cybersecurity Framework (CSF) data (2023–present) reveals a sector steadily gaining maturity, but with critical vulnerabilities still unresolved.

Five Areas Showing Signs of Momentum

According to Fortified Health Security's data, the following categories show signs of improvement:

01

Governance

Executive and board-level engagement in cybersecurity is at an all-time high. Leaders no longer treat cybersecurity as an afterthought; it's becoming a formal part of governance structures. Across the industry, we've seen the establishment of dedicated committees focused on information security and privacy that include organizations previously disengaged. Even the most reluctant healthcare entities are launching their first governance bodies this year, signaling meaningful progress among longstanding holdouts. In parallel, organizations are proactively aligning with upcoming HIPAA updates and NIST expectations, formalizing areas of oversight that were once loosely managed or deprioritized.

02

Response Planning

Once considered isolated IT issues, healthcare organizations now treat cyber incidents as enterprise-wide disasters. Leaders are increasingly aligning their incident response plans with broader disaster recovery and business continuity strategies. This shift is being driven both internally and by external pressures, particularly from cyber insurers who now require evidence of preparedness and often include tabletop exercises as part of policy conditions. As a result, executive leaders and technical teams regularly rehearse response scenarios to minimize confusion, accelerate decision-making, and improve resilience during actual events.

03

Risk Assessment

Risk assessments have matured from checkbox exercises to tools that drive strategic insight. Many healthcare organizations are now adopting NIST-based maturity assessments instead of HIPAA Risk Assessments, which has resulted in a more comprehensive and measurable view of their cybersecurity posture. Leaders use year-over-year score analysis to justify security investments and drive business process improvements. Most notably, risk is now recognized as an enterprise-wide responsibility, extending beyond the IT department and into the core organizational strategy and governance models.

04

Continuous Response Improvement

Healthcare organizations are placing greater emphasis on accelerating operational recovery following cyber incidents. Many now conduct multiple tabletop exercises each year, covering technical and executive levels, testing and refining their response processes and readiness. There is a growing commitment to adopting best practices and implementing incremental improvements, even when comprehensive overhauls are not immediately feasible. This shift reflects a more mature, agile approach to building long-term cyber resilience.

05

Identity and Access Management (IAM)

While IAM remains a heavy lift, healthcare organizations are starting to make progress. Many are conducting discovery exercises to assess their readiness for comprehensive IAM solutions, uncovering common issues like outdated and overgrown Active Directory environments. Despite the hurdles, many healthcare organizations are still actively discussing phased IAM strategies, a huge step forward for a historically neglected area.

Continued Risk Areas

Despite the progress, gaps still exist in critical areas. According to our data, the following NIST categories represent the top five continued risk areas:

01

Risk Management Strategy

Most organizations still lack a defined, unified approach to risk management. Risk tolerances wildly vary, and because of that, responsibility for managing that risk is often unclear. This leads to decision-making delays and inconsistent practices. A solid governance structure is essential to fix this, yet many healthcare organizations resist prioritizing it.

02

Supply Chain Risk Management

While some healthcare organizations make Third-Party Risk Management (TPRM) part of procurement decisions, many still treat it as a checkbox activity. There's a wide gap between those optimizing third-party risk practices and those just starting. That said, more clients are now using risk insights to reject vendors with poor scores, proof that progress is possible, albeit uneven.

03

Maintenance Security Controls

Maintenance has shown improvement but remains a high-risk area. While cybersecurity investments are gaining more executive-level attention in the budget, funding often favors new technology over maintaining legacy systems. As a result, many organizations are left cobbling together outdated platforms on aging hardware. Some now recognize that decommissioning obsolete systems may be safer than trying to keep them running. Still, decentralized patching and limited visibility, especially across Internet of Medical Things (IoMT) devices, continue to present significant challenges.

04

Asset Management

Asset management remains a universal and foundational challenge across the healthcare sector. Without a complete and up-to-date inventory, organizations lack a clear understanding of what they protect, making effective risk management nearly impossible. In many cases, producing current-state inventories cannot be done easily, particularly when clinical assets are tracked separately by BioMed teams. This fragmentation creates blind spots, especially when identifying which assets store or process electronically protected health information (ePHI). Without unified asset visibility, organizations are prone to false positives, delayed responses, and missed threats that could otherwise be contained.

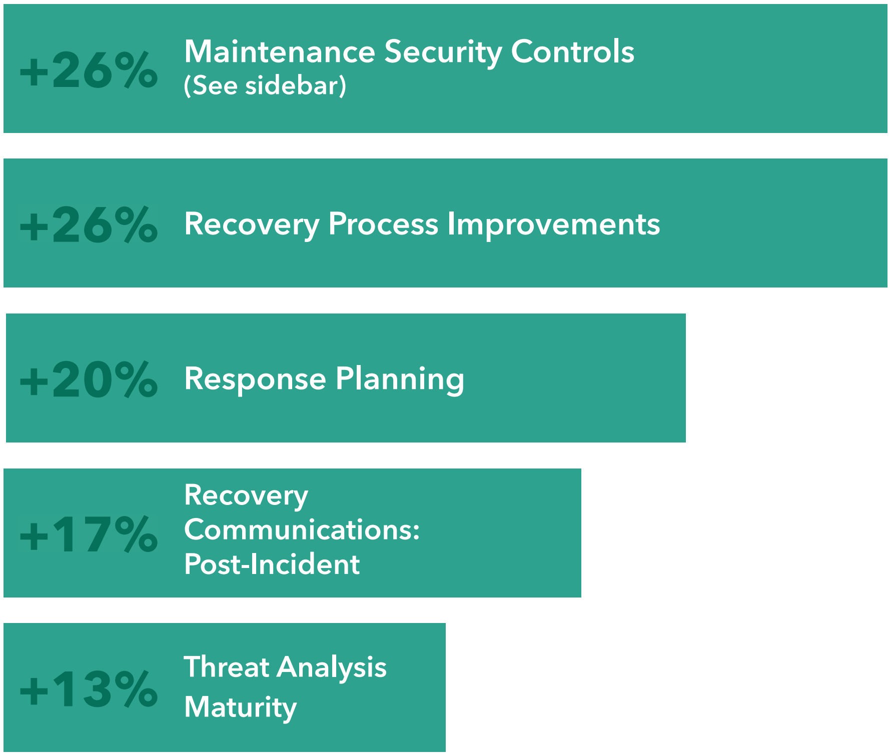
05

Awareness Training

While there is progress, training is too often limited to annual refreshers or new hire orientation. Yes, phishing simulations and role-based modules help, but cultural change is needed. Cybersecurity must become part of the organizational DNA, and many companies have not yet accomplished that. You can encourage active engagement by rewarding and/or recognizing engaged employees and sharing real-world stories.

Most Improved: Signs of Resilience

These five NIST categories saw the most significant year-over-year score increases. While they remain below full maturity, the sharp improvements could signal a turning point in healthcare cybersecurity posture.



Maintenance is Improving, but the Risk Remains

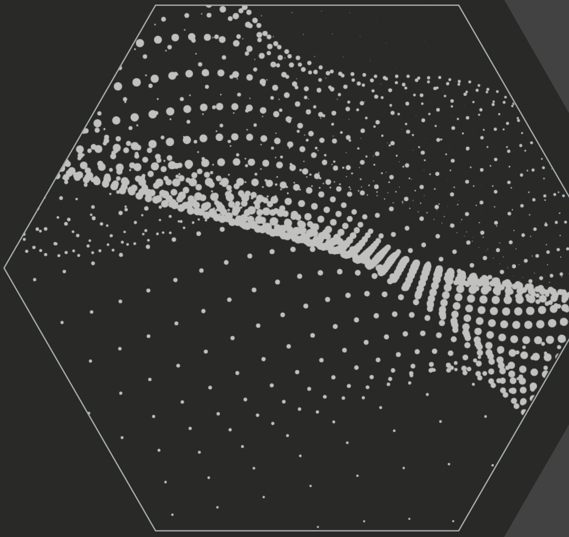
Maintenance may be "most improved," but it still ranks among the lowest overall scores, highlighting a crucial truth: while organizations are catching up, many started from a dangerously low baseline. Despite the progress, legacy systems, IoMT patching limitations, and decentralized responsibility make this an ongoing risk vector.

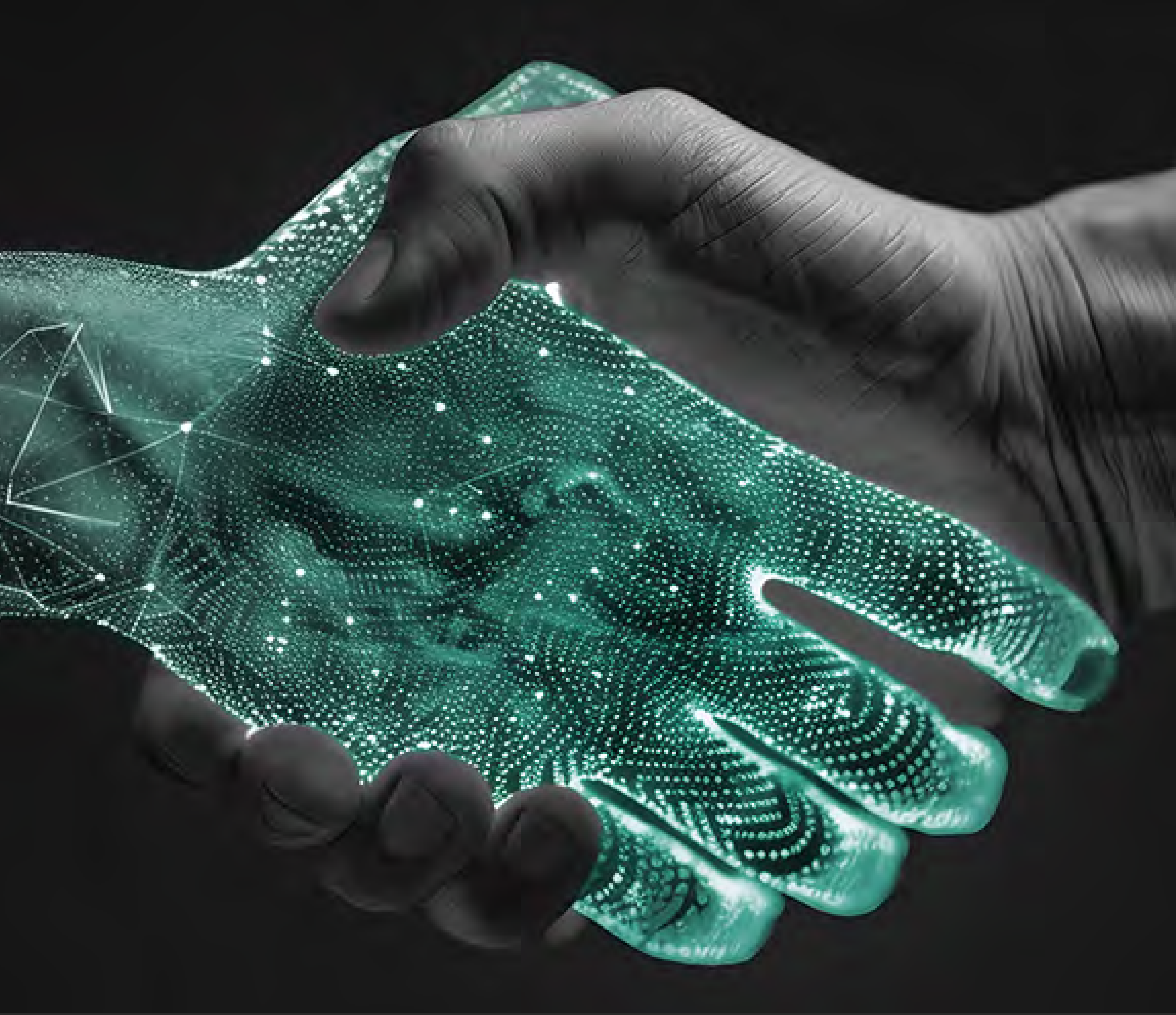
The Bottom Line

Framework sets the most resilient healthcare organizations apart. But so does mindset.

It's important to treat cybersecurity as an enterprise-wide responsibility, invest in awareness as seriously as infrastructure, and celebrate behavior reinforcing a strong security posture. **Real progress happens when organizations teach people to see through a different lens**, where every story, simulation, or phishing test becomes a chance to build smarter, more secure habits.

To close the remaining gaps, healthcare must shift from reactive compliance to proactive resilience. The organizations that will lead in the years ahead are those embedding cybersecurity into decision-making, culture, and care delivery.





The IQ of AI:

Why Human Intelligence Still Leads in Cybersecurity

By Preston Duren

Artificial Intelligence. No other topic generates more excitement, confusion, and fear, especially in healthcare cybersecurity, where patient safety and sensitive data are always top of mind. AI is an exciting topic, but in my experience, the best use case is to augment human intelligence, not replace it.

The misconception that AI can fully replace a Security Operations Center (SOC) analyst is one of today's most persistent myths. Much of that belief stems from marketing hype that positions AI as a miracle cure for staffing shortages or complex cyber threats. But reality paints a different picture. AI handles specific tasks quickly, but it still falls short in the adaptability and context awareness that human analysts rely on to make the right call during alerts, something that's critical in healthcare environments.

Healthcare: Raising the Stakes for AI

In healthcare, cybersecurity risks can have serious impacts. AI's lack of real context can turn an automated response into a life-or-death situation.

Consider a scenario that happens in real-life healthcare environments: A device on the network, like a radiation therapy machine, exhibits unusual behavior. AI might recognize patterns based on past incidents and, following its training, automatically isolate the device from the network to prevent the spread of perceived malware.

While that seems like a proactive move, an experienced analyst would dive deeper before taking action. They'd ask critical questions:

» What VLAN is this device on?

» What is the device connected to?

» Is it currently being used in patient care?

If the device is actively delivering radiation therapy, taking it offline would jeopardize a patient's treatment, a risk that far outweighs the cybersecurity threat at that moment.

In healthcare, availability isn't just a convenience; it's often a matter of life or death. This prioritization reflects a critical healthcare cybersecurity principle rooted in the CIA triad: confidentiality, integrity, and availability.

While confidentiality is often an emphasis in traditional IT environments, availability frequently takes precedence in healthcare. As I often say, "I would rather all of my personal data be leaked to the Internet than die on the operating table because a critical system went offline."

Clinical context further complicates these decisions. Whether a system is treating a patient, hospital capacity surges during full moons or major holidays, or the influx of new, less-phished-resilient medical residents in July all shape appropriate responses. No AI model operating in a vacuum can replace human awareness of these environmental, clinical, and operational dynamics.

Moreover, healthcare organizations face additional privacy obligations under HIPAA, PCI, and GDPR. Data sensitivity and the difficulty in verifying how AI models handle protected health information add to the need for human oversight.

> ”
>
> AI handles specific tasks quickly, but it still **falls short in the adaptability and context awareness** that human analysts rely on to make the right call during alerts.

AI is an extraordinary tool for accelerating well-defined tasks. **It's not a replacement for human judgment.**

The Right Balance: Humans and AI, Together

Healthcare organizations should view AI as a powerful partner instead of a replacement. It should handle the heavy lifting for those routine tasks that take up time.

In our SOC, we view AI as "the new Google." Analysts use AI to accelerate research, validate hypotheses, and perform preliminary investigations. But final decisions, escalations, and incident responses remain firmly in human hands.

This collaborative model between AI and human analysts significantly boosts both speed and effectiveness. AI filters out false positives, allowing analysts to focus their expertise on real threats. Over time, continuous feedback from analysts helps fine-tune the automation, creating a smarter system without replacing human judgment or clinical insight.

Practical Guidance for Healthcare Organizations

If you're a healthcare organization exploring AI investments in cybersecurity, focus on tools, not self-built models. Companies like CrowdStrike and SentinelOne are embedding AI into their endpoint detection platforms in ways that complement human workflows. Leveraging mature vendor ecosystems reduces risk while still providing innovation.

Key metrics to track when integrating AI include:

- Mean Time to Acknowledge (MTTA)
- Mean Time to Respond (MTTR)
- True Positive vs. False Positive Rates

If these metrics improve without diminishing analysts' ability to tell meaningful, contextualized stories about incidents, then your AI investments are adding value.

Future-Ready SOCs: Built on Human Intelligence

You cannot build a future-ready SOC in healthcare on AI alone; you must build it with teams that leverage AI smartly, enabling speed, scale, and deeper analysis without losing the human factor that ensures patient safety through operational resilience.

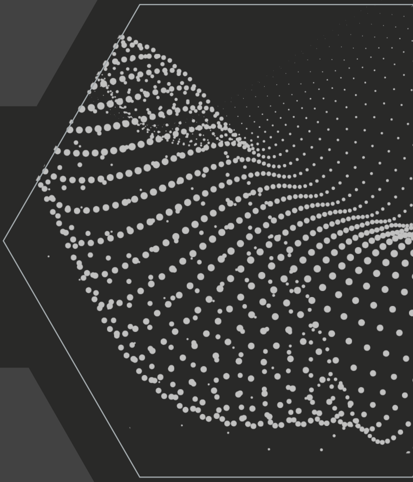
Building that team culture requires intentionality. Analysts should be encouraged to use AI to sharpen their work, but they also need to learn how to verify outputs and challenge assumptions. **SOC leaders must foster an environment where AI is a trusted tool, not an unquestioned authority.**

The Smartest Use of AI in One Sentence

"If I had to summarize the smartest use of AI in a single sentence, it would be this:

With a partnership of humans and artificial intelligence, we can do more, faster, and better… **together**.

That's AI's real IQ and how healthcare cybersecurity must evolve to meet the challenges ahead."



Rethinking ASM:

A Strategic Perspective on Healthcare’s Expanding Attack Surface

By T.J. Ramsey

In an era where adversaries are increasingly sophisticated and persistent, healthcare organizations must evolve from reactive postures to informed, anticipatory defense strategies. One critical evolution in this shift is the proper implementation and understanding of Attack Surface Monitoring (ASM), a capability often referenced, frequently misunderstood, and inconsistently applied.

As someone who has spent a career in military intelligence and healthcare cybersecurity, I've seen firsthand how easily the terminology around ASM becomes diluted by marketing buzzwords. The result? Leaders are left to decipher solutions that promise everything yet deliver only fragments. My intent here is to clarify not only what ASM is, but what it is not, and why it must be viewed through a more strategic and mature lens in the healthcare sector.

Understanding the Evolution: From Dark Web Monitoring to Comprehensive ASM

Dark web monitoring was one of the earliest forays into proactive external threat awareness. Initially, its value was most evident when federal agencies would notify hospitals of sensitive information discovered in criminal forums (credentials, patient records, insider communications), often long after the point of compromise. That model was inherently reactive.

To address that lag, a wave of vendors emerged offering indexed visibility into the dark web. Think of it as building a search engine for adversarial chatter. By monitoring for mentions of organizational assets, early indicators of intent, and data exposure, these tools helped organizations shift from victim to early responder.

Yet even this only captured a narrow slice of the risk landscape. Parallel to this, another capability matured: attack surface monitoring. Where dark web intelligence observes hostile intent and actor behavior, ASM evaluates what your organization looks like from the outside, or your perimeter exposure in near-real-time.

Evolution Snapshot

Dark Web Monitoring

Watches for stolen data or chatter about your organization

Attack Surface Monitoring

Continuously scans your external digital footprint–websites, portals, IPs, credentials

ASM with Dark Web

The complete picture: visibility + intent signals

If you haven't mastered patching, password policies, and access control, you're not ready for ASM. **Fundamentals come first.**

Over time, the industry began to integrate the two, but that merger isn't universal. Not all ASM platforms include dark web intelligence.

A truly mature program accounts for both, and healthcare leaders must demand that level of completeness.

The Prerequisite: Operational Maturity

Before investing in ASM, organizations must first ensure that foundational cybersecurity controls are sound. If your password policies are weak, patching cycles erratic, or role-based access poorly enforced, an ASM solution will only highlight the symptoms of those failures, not protect you from them.

Once that baseline is in place, ASM becomes an indispensable component of strategic defense. It enables visibility into risks that traditional tools won't catch, risks that sit just beyond your firewall, where most opportunistic actors first look.

Healthcare's Digital Perimeter: Where Exposure Happens First

The external attack surface in healthcare is broader and more fragmented than most realize. Beyond the core systems, exposure often originates from:

- Patient portals hosted by third-party vendors
- Public-facing websites with outdated content or insecure configurations
- Conference registration pages where staff use/reuse work credentials
- Remote employee access points and login portals
- Business applications tied to legacy medical device platforms

What ties these together is visibility: many of these assets exist outside the core IT environment and are therefore overlooked during traditional risk assessments. ASM restores that visibility and, with integrated dark web intelligence, offers contextual insight into whether adversaries are actively targeting these vulnerabilities.

Strategic Value: Precision Without Noise

One of the greatest misconceptions is that ASM should be dramatic with constant alerts, high-stakes indicators, and red-flashing dashboards. The reality is more nuanced. Properly tuned, an ASM platform delivers targeted, actionable intelligence. It has signals that matter to your specific organization and nothing more. It also shields your security team from the darker realities of the open web, filtering content to ensure the focus remains on risk, not distraction.

ASM becomes a force multiplier when incorporated into broader threat management frameworks, particularly Vulnerability Threat Management (VTM) or outsourced Security Information and Event Management (SIEM) services. It provides the external perspective needed to validate assumptions, anticipate threats, and prioritize remediation efforts based on how adversaries actually perceive your environment.

Consider ASM if:

01

You're already investing in Vulnerability Threat Management

02

You're outsourcing SIEM or MDR services

03

You've mastered the security basics and need external threat context

04

You want to anticipate, not just react, to cyber risk

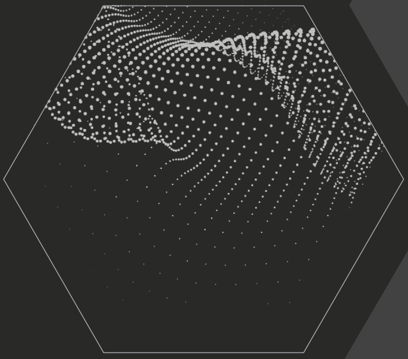
Demand Accuracy Over Hype

In an industry where buzzwords often outpace clarity, security leaders must challenge what's being sold. Not all ASM is created equal. Some platforms offer deep insight into attack surface exposure but omit dark web monitoring entirely. Others specialize in dark web intelligence but lack real-time scanning of externally facing assets.

Ask the right questions. Insist on transparency. And most importantly, ensure any ASM investment complements, and does not replace, your organization's broader risk management maturity.

ASM is not a silver bullet, nor is it a commodity tool. It is a strategic asset when deployed with purpose.

Healthcare deserves more than hype. It deserves solutions that work.



Navigating the Fog:

Healthcare Cybersecurity in a Year of Regulatory Uncertainty

By Russell Teague

As we cross the midpoint of 2025, the healthcare cybersecurity landscape feels more like a fog-covered road than a well-lit highway. Threats are accelerating—louder, faster, more coordinated. Meanwhile, the regulatory landscape grows murkier by the month.

For CISOs and healthcare security leaders, this moment demands more than technical controls. It requires conviction, clarity of purpose, and the courage to keep moving forward even when the federal roadmap is incomplete.

A Tense, Transitional Time

In April, I wrote about what felt like a tipping point in healthcare cybersecurity policy. Sweeping layoffs across HHS, FDA, and CDC, not to mention structural changes under Secretary Robert F. Kennedy Jr., signaled a step back in centralized oversight. At the same time, testimony from industry leaders like Erik Decker and Greg Garcia reinforced the role of the private sector in stepping up.

Now, in the last half of 2025 we remain suspended in that tension. There's been no sweeping federal clarity. Proposed regulatory changes remain stuck in draft or debate. Questions swirl around DOGE restructuring, future funding for cybersecurity initiatives, and what minimum cyber standards will look like, if they materialize at all.

However, one significant development arrived in June. President Trump issued Executive Order 14306, titled "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity." This EO reversed several Biden-era mandates, such as those requiring software bills of materials and digital identity adoption, while preserving protections for critical infrastructure. It also introduced new timelines for federal agencies like NIST and CISA to deliver on software development frameworks, post-quantum cryptography guidance, and AI/quantum security strategies. At the same time, it narrowed the scope of federal sanctions, limiting their application to cyberattacks on critical infrastructure.

The EO marks a return to decentralized federal oversight, placing more responsibility on agencies and industry consortia to drive forward secure software, AI risk mitigation, and next-gen encryption practices. It reinforces the message: regulatory ambiguity isn't going away anytime soon. For healthcare, this EO marks a return to decentralized oversight. Without mandates like SBOMs, the burden shifts to hospitals and clinics to self-govern software risk. Strong internal policies are no longer optional; they're essential.

The reality? Healthcare is operating in uncertainty and that is having ripple effects on policy strategy and practical decisions. As an MSSP, we've seen organizations delay investments, pause vendor evaluations, and hesitate to implement new frameworks because they're waiting to see where the regulatory winds blow next.

Legislative Spotlight

The Healthcare Cybersecurity Act of 2025

A bipartisan bill introduced on June 9 aims to strengthen healthcare cybersecurity by creating a **deeper collaboration between CISA and HHS**. If enacted, it would provide technical assistance, workforce training, and funding for at-risk hospitals. The bill must pass committee reviews in the House before advancing to a full vote The threat environment has outpaced the policy cycle. **Hospitals and health systems can't afford to sit idle while Washington catches up or decides on a direction for us to take.**

Waiting Comes at a Cost

Let's be honest: threat actors aren't waiting. LockBit 4.0 isn't waiting. AI-powered phishing campaigns are already bypassing traditional defenses. Meanwhile, delayed DOGE restructuring and HHS staffing gaps have stalled much-needed updates leaving organizations in limbo.

Hospitals are short-staffed or uncertain about government direction. In 2024, 92% of healthcare organizations reported cyberattacks, and nearly 70% saw patient care impacted.

What To Do in the Absence of Clarity?

My message to healthcare leaders is simple: Stop waiting for regulatory clarity to do what you already know is necessary. Cybersecurity fundamentals haven't changed. You don't need a mandate to adopt a framework, mature your incident response plan, or enforce strong identity and access controls.

Pick a framework: NIST, HITRUST, 405(d), whatever best fits your organization, and execute. Stay the course on your cybersecurity roadmap. Your responsibility is to ensure patient safety, operational resilience, and the protection of critical systems that your community relies on.

The Path Forward: Proactive, Not Prescriptive

In times like this, resilience requires initiative. Move from compliance-driven security to mission-driven security. It means investing in talent, tools, and partnerships that support continuous improvement, even when the rules aren't fully defined.

It also means embracing collective action. Public-private partnerships, cross-sector collaborations, and information sharing are now strategic necessities. If the federal government is taking a step back, the private sector must be ready to step forward.

And we can. I've seen firsthand how mature organizations working with MSSPs and vendors create self-governing ecosystems that are more agile and scalable than any centralized model.

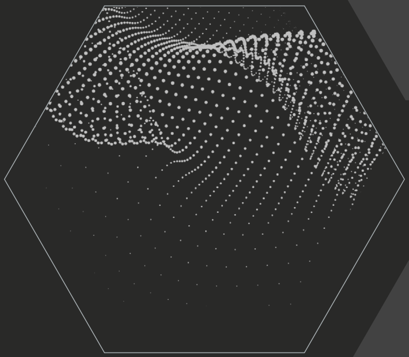
> In 2024, **92%** of healthcare organizations reported cyberattacks, and nearly **70%** saw patient care impacted.

Let's Keep Moving

While uncertainty can be paralyzing, it can also be clarifying. It forces us to ask: What really matters? What are we waiting for? And what do we already know we should be doing?

We are at an inflection point. If we lead well now, healthcare can become the model for adaptive cybersecurity; built not just to withstand today's threats, but to evolve with tomorrow's.

So, keep moving. Keep leading. And most of all, don't let the fog fool you into thinking you're lost. The destination remains unchanged: a defensible, proactive, and patient-first cybersecurity posture.



Creating Environments to Think Differently:

The Untapped Power of Peer Collaboration

By William Crank

Isolation is a liability in cybersecurity. Yet across healthcare, many security leaders remain siloed, operating without a trusted peer network to exchange ideas, challenge assumptions, or validate strategies. That needs to change.

Cyber adversaries are not working alone. They collaborate, evolve, and adapt faster than most organizations can keep up. If defenders are going to have a chance, we must embrace that same spirit of connection—not just through shared technology or frameworks, but through real, human conversation and collaboration. In my experience, creating an environment for those interactions is one of the most powerful yet underutilized tools in our cyber defense arsenal.

The Reality of Silence… and the Cost

Healthcare security leaders face immense pressure. We carry the expectation of perfection charged with protecting patient safety, care continuity, and sensitive data in environments often constrained by resources or bureaucracy. At the same time, we're held accountable when cyber incidents occur, even when we lack full authority over funding or prioritization.

That pressure creates a chilling effect. Legal and reputational concerns make leaders hesitant to speak openly about incidents, even with peers. The fear of exposing internal risk or appearing weak often outweighs the potential benefit of dialogue. As a result, many in our field feel like they're solving complex, evolving problems in a vacuum.

But here's the truth: silence doesn't make us safer. It makes us stagnant. And in an industry where attackers are constantly innovating, standing still is the same as falling behind.

A Better Way: Peer Dialogue as a Strategy

One of the most overlooked advantages we have as defenders is each other. Real progress happens when healthcare security leaders come together outside of vendor pitches or compliance checklists to discuss what's happening in their environments. Not sanitized versions. Not after-action reports crafted for legal review. But honest, candid, "here's what we tried and here's what worked (or didn't)" conversations.

Over the years, I've learned that sometimes the best ideas don't come from the biggest budgets or the most sophisticated tech. They come from small insights exchanged in trusted settings. I once heard a CISO explain how their team improved awareness simply by rotating the design of external email banners, changing font color, size, and location monthly so users didn't become blind to the warning. That simple idea cost virtually nothing to implement but created a measurable impact in reducing risky click behavior.

That's the power of perspective. When peers bring different backgrounds (technical, operational, governance) you get a broader, more resilient view of risk. You see possibilities you may have missed, you may entertain opportunities you never envisioned. You challenge your own assumptions. And you make more informed and better decisions.

> ”
>
> Silence doesn't make us safer.
>
> **It makes us stagnant.**

> We need **transformational spaces** that foster strategic dialogue, encourage creative problem-solving, and shift the mindset from **reactive defense to proactive anticipation.**

Trust is the Prerequisite

These conversations don't happen without trust. That's why any environment designed for honest collaboration, whether a regional working group or a national executive roundtable, must be built on shared values and clear guardrails.

At Fortified, we've spent several years developing a roundtable environment rooted in Chatham House Rule. Nothing leaves the room. No attribution. No agenda beyond shared learning.

Our Roundtables didn't happen overnight. Our first session had our CEO, Dan L. Dodson, me, and one guest. But we stayed with it. We showed up. We listened. And over time, we earned the trust of peers who now return regularly, contribute openly, and bring forward real-world challenges without fear of judgment or exposure.

Moving from Transactional to Transformational

Much of the healthcare cybersecurity ecosystem still centers around transactional engagements like compliance updates, vendor pitches, and breach headlines. However, the problems we face are bigger than any single solution. We need transformational spaces that foster strategic dialogue, encourage creative problem-solving, and shift the mindset from reactive defense to proactive anticipation.

These spaces don't require a national platform. It can start locally. Invite a handful of peers to breakfast. Join your ISSA or (ISC)² chapter. Host a lunch-and-learn in your organization and set ground rules for privacy and openness. You may only have one person show up the first time. That's okay. Building trust takes time, but the payoff is exponential.

Small Starts, Big Impact

How to Launch Peer Dialogue

01 **Start small**
One coffee conversation is enough

02 **Set expectations**
Trust and discretion are non-negotiable

03 **Focus on learning**
No pitches, no presentations

04 **Be consistent**
Trust builds over time

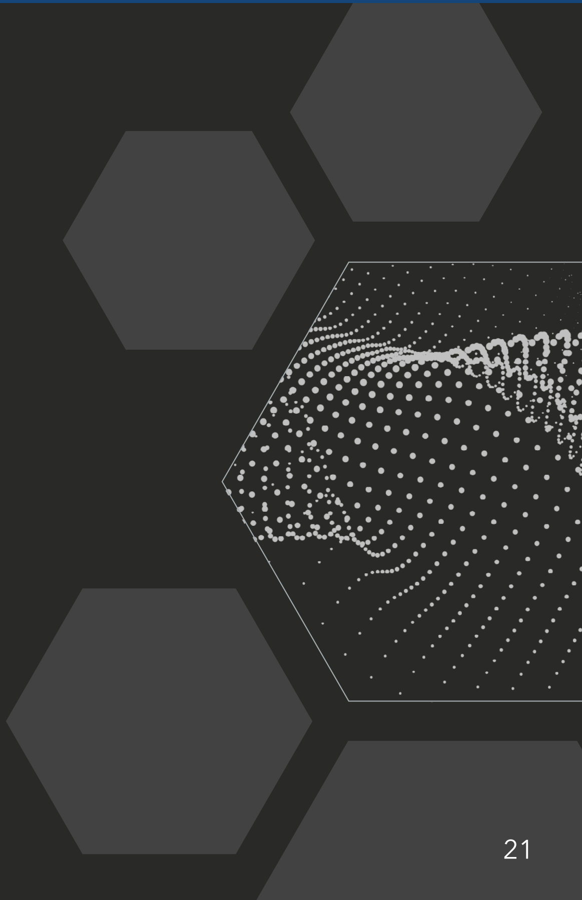
05 **Stay local**
Your best collaborators may be right down the road

A Community that Defends Together

Cybersecurity in healthcare is not a zero-sum game. We're not competing for patients in the SOC. We're fighting to preserve care, protect dignity, and ensure access for everyone. That means we share a mission—and, with it, a responsibility to help one another.

When we create space to think differently, we create space to defend differently. And in that space, we can shift from isolated expertise to collective strength. That is how we stay ahead, not just of threats but of the status quo.

Because if we want to outmaneuver the adversary, we must be willing to out-collaborate them.



JOSHUA DOSTIE
MaineGeneral Health
Senior IT Analyst

We're All Patients

Risk assessments, training, incident response: these are the solutions we talk about when protecting healthcare organizations. But, at the heart of it all, we're not just securing buildings or systems. We're protecting people.

Patients are the why behind the decision to improve your cybersecurity posture.

Their lives are at stake during every decision, every investment, and every cyber threat response you make. No one understands that better than MaineGeneral Health's Senior IT Analyst, Joshua Dostie.

Unlike his team members, Dostie's connection to MaineGeneral didn't start with a job application. It began with a birth certificate.

"I was born in this very building I'm sitting at right now," Dostie says. "Then I started volunteering here when I was 16 years old."

MaineGeneral Health isn't just where Dostie works; It's where his life began, where his community gets care, and that's why his mission to protect others as a senior IT analyst feels most urgent.

He says keeping his organization secure isn't just about stopping bad actors; it's about protecting the people who depend on those systems to survive.

"Every alert, every threat, and every action we take has the potential to impact someone's life," he explains. "Yes, we need to protect the data and technology. But there are people connected to those computers. Before I take any action, we have to make sure it won't impact a patient."

> Hackers are going to target the most vulnerable. And in my view, that's the person lying in a hospital bed, hooked up to technology. **My job is to protect them.**

Dostie says he profoundly understands the responsibility that comes with every decision he makes. "Behind every device is a person who depends on it. These are my neighbors, my friends, my family. When I make a decision, I'm thinking about them."

His connection to the hospital and the people in it has shaped how he sees cybersecurity. Rather than a back-office function, he views it as a direct extension of patient care.

"Hackers are going to target the most vulnerable. And in my view, that's the person lying in a hospital bed, hooked up to technology. My job is to protect them."

Nearly two decades into his IT career, with the last ten years focused on security, Josh has seen technology evolve. But his reason for doing the work hasn't changed. "I've grown with this place. I've seen it change and helped it stay safe through those changes. And I take that personally."

Because when it comes down to it, he says, it's not just about systems or strategy. It's about people. "We're all patients someday. And when it's our turn, we all deserve to be protected."

About the Contributors

Dan L. Dodson

CEO
Fortified Health Security

As CEO of Fortified Health Security, Dan L. Dodson brings nearly 20 years of leadership experience in healthcare and insurance. He has held key roles across the industry, including Executive Vice President at Santa Rosa Consulting, Global Healthcare Strategy Lead at Dell Services, and leadership positions at Covenant Health System, The Parker Group, and Hooper Holmes. In 2022, he was elected to the Association for Executives in Healthcare Information Security (AEHIS) Board.

A recognized thought leader in cybersecurity, data privacy, risk management, and threat mitigation, Dan is a frequent speaker at top industry events such as CHIME, HIMSS, and HIT Summits. In 2025, Dan became the creator and host of Cyber Survivor, a podcast that explores the human impact of cybersecurity in healthcare through real-world stories and expert interviews.

William Crank

COO
Fortified Health Security

William Crank serves as COO of Fortified Health Security. For more than 20 years, he's driven the successful execution of cybersecurity strategies and tactics for the healthcare industry, including managing the Information Security Risk Management (ISRM) team at Hospital Corporation of America (HCA) and serving as Chief Information Security Officer (CISO) at MEDHOST.

He currently holds multiple certifications in the areas of Information Security and Information Technology, has served as Sponsorship/Programs Director and Vice President of the Middle Tennessee chapter of the Information Systems Security Association (ISSA), and retired after serving more than 20 years in the United States Navy.

Russell Teague

Chief Information Security Officer
Fortified Health Security

With over 20 years of experience, Russell Teague's expertise spans Information Security across industries such as Healthcare, Pharma, Financial, Retail, Technology, and more. A U.S. Army Intelligence veteran, he has held senior leadership roles, including CSO and CTO, and worked with top cybersecurity service providers. Russell has consulted with the White House on the National Cybersecurity Healthcare Strategy, contributed to key publications, and has been a prominent voice at major industry events, including Blackhat, HIMSS, and Health Connect Partners (HCP).

Preston Duren

VP of Threat Services
Fortified Health Security

Preston Duren brings more than 16 years of IT/security expertise to his role as VP of Threat Services at Fortified. His experience spans threat and vulnerability management, security engineering, security program development, digital forensics, and SOC. Previous roles include engineering/architecture at Community Health Systems & Information Security Officer at RCCH Health.

T.J. Ramsey

Senior Director, Threat Operations
Fortified Health Security

T.J. Ramsey is a seasoned IT security professional with nearly 20 years of experience focused on healthcare and defense intelligence. He served as a U.S. Army Military Intelligence Analyst for the Department of Defense, and held security roles at Obsidian Solution Group and SAIC/Leidos. T.J. has shared his cybersecurity expertise in publications like TechTarget and Chief Healthcare Executive and presented at industry events, including Health Connect Partners (HCP), CHIME, and THIMA.

Jason Stewart,

Manager, vCISO Services
Fortified Health Security

Jason Stewart is Manager of the Virtual Information Security Program for Fortified Health Security. He has more than 25 years of progressive experience in the information technology, information security, and cybersecurity industries covering the healthcare, technology, and manufacturing sectors. He excels in complex business management environments with aggressive growth targets and has extensive expertise in advisory services, managed services, strategic governance, threat management, incident response, risk management, education strategies, and board-level advisement.

About Fortified Health Security

Fortified Health Security is healthcare's cybersecurity partner, trusted by healthcare organizations nationwide to deliver tailored, high-touch programs that reduce risk, simplify complexity, and protect what matters most: their patients. As a four-time consecutive Best in KLAS winner, Fortified provides specialized managed security services built exclusively for healthcare.

Fortified understands the full spectrum of healthcare cybersecurity, from rural providers to enterprise networks, third-party vendors, and connected medical devices. The company's award-winning Central Command platform, featuring innovations, like EscalationIQ, translates client feedback into action, enabling smarter, faster security decisions that strengthen every layer of defense.

Fortified doesn't just guard the perimeter. The team embeds with clients, bringing context to every alert and helping healthcare leaders move from reactive to resilient, 24/7, 365.

Because in healthcare, cybersecurity isn't just an IT issue. It's a patient safety issue.

Learn more at fortifiedhealthsecurity.com.

Fortified
HEALTH SECURITY

www.fortifiedhealthsecurity.com

connect@fortifiedhealthsecurity.com

120 Brentwood Commons Way
Building 4, Suite 500
Brentwood, TN 37027

BEST IN KLAS® SECURITY & PRIVACY MANAGED SERVICES 2025
BEST IN KLAS® SECURITY & PRIVACY MANAGED SERVICES 2024
BEST IN KLAS® SECURITY & PRIVACY MANAGED SERVICES 2023
BEST IN KLAS® SECURITY & PRIVACY MANAGED SERVICES 2022