



How Federal Health Agencies Can Step Up Their Cyber Defenses

Healthcare was one of the top 10 cyber targets in 2024, with 725 data breaches reported that year, according to a [HIPAA Journal article](#) summarizing the federal 2024 Healthcare Data Breach Report. Healthcare is a prime target for attackers, and the increase in ransomware, identity threats, and medical device vulnerabilities continues to elevate the risk.

The vast amount of personal health information held by federal healthcare organizations is often vital to national security, readiness, and disaster response efforts — making these agencies especially attractive targets for both criminal and nation-state adversaries.

In this report, we look at how an integrated, automated platform approach can help healthcare agencies identify threats, assess potential impacts, and mitigate risk.



Challenge: Architecture, Infrastructure Impede Security

Federal health agencies face a number of cybersecurity challenges as they seek to safeguard systems and data from both criminal actors and nation-state adversaries. Technological and organizational issues alike hinder the effectiveness of traditional cyber defense strategies.

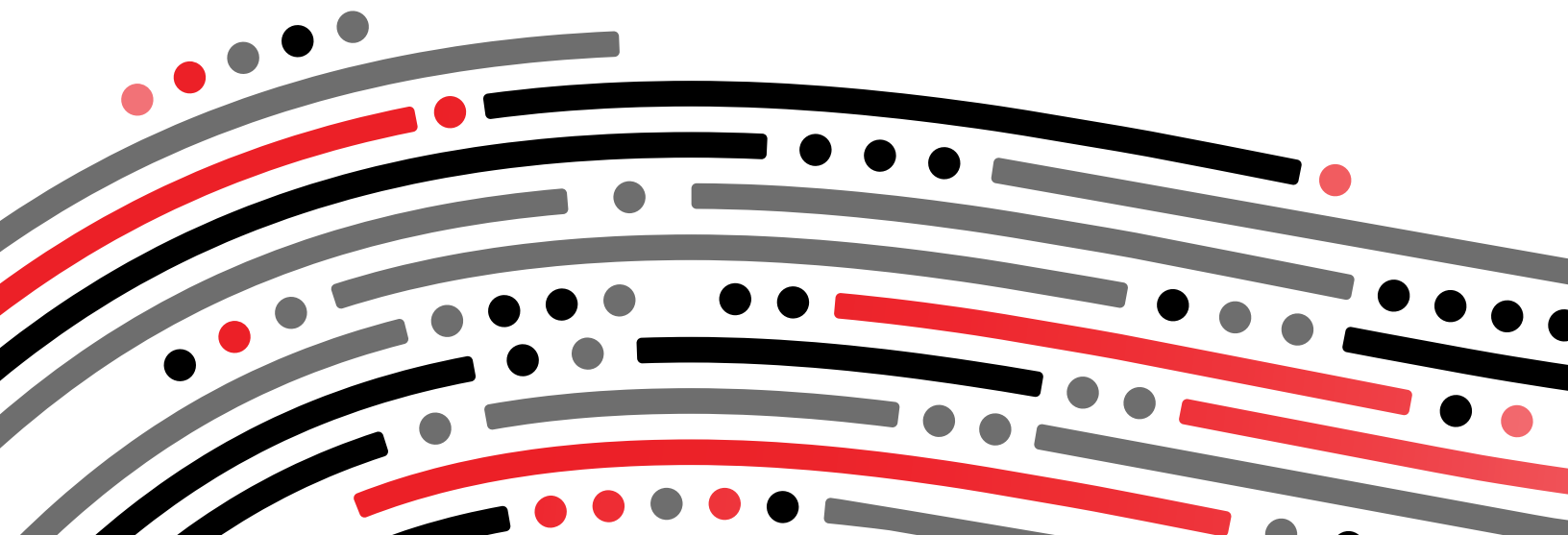
- In legacy architectures, a distributed and decentralized structure provides autonomy to subordinate organizations. That's as intended, but it results in a lack of standardization and visibility, which has a profound impact on cyber readiness.
- Complex IT infrastructure makes it difficult for health agencies to implement Zero Trust, a foundational approach to modern cybersecurity. Similarly, complexity makes it challenging for IT teams and cyber defenders to put in place modern security controls.
- Workforce and other organizational constraints factor into the overall cyber picture in federal healthcare. With limited staffing, stiff competition for top cyber talent, and competing budget priorities, health agencies cannot simply throw more people at the problem.

Solution: An Integrated, Automated Cyber Platform

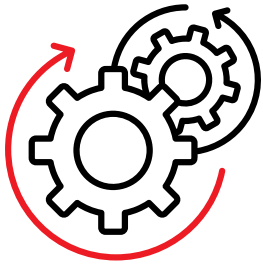
Agencies do not have the time or resources to juggle multiple cyber-defensive tools. In place of the outmoded "Swiss Army knife" strategy, they need an integrated, automated platform that integrates best-of-breed solutions.

Key attributes of a platform solution include:

- **Cloud-based:** A cloud-based solution empowers defenders to manage hybrid environments and hybrid cloud infrastructure. Speed is everything in healthcare, and instant updates deliver immediate protection. Centralization and scalability drive efficiency and reduce total cost of ownership.
- **Modular:** With modularity, healthcare agencies can take advantage of FedRAMP Moderate and High solutions based on their maturity, rather than having to make wholesale changes. Modularity enables federal health agencies to utilize the most appropriate tools to detect sophisticated endpoint-, identity-, and cloud-based cyberattacks.
- **Comprehensive:** A platform delivers a full suite of threat detection and investigation capabilities. This should include the use of artificial intelligence to detect anomalies and to spot cyber exploits in real time.



Best Practices in Risk Mitigation



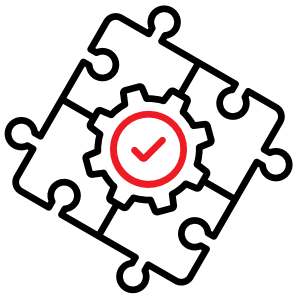
Leverage automation

A cyber platform will deliver automated threat detection and investigation processes, accelerating response times while also driving efficiency by reducing manual efforts. As adversaries develop new exploits, defenders can leverage these capabilities to automatically prioritize those vulnerabilities that matter most in defense of government healthcare agencies.



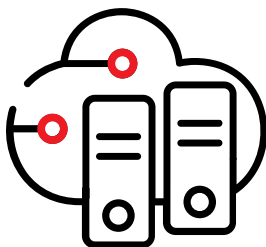
Elevate cross-domain protection

Adversaries have many avenues to the endpoint. Cloud, identity, networks, and SaaS applications are all interconnected. Health agencies can utilize a platform's cross-domain capabilities for timely and comprehensive defense. For example, they can develop a clear, accurate, up-to-date record of all known vulnerabilities, as they work to keep pace with monthly vulnerability reports.



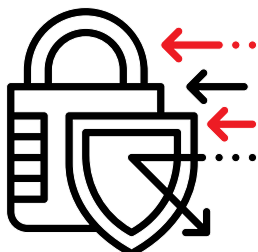
Take advantage of integration

Agencies can take advantage of a platform's ability to integrate endpoint, identity, workload, and unmanaged systems into one view to meet the current call for efficiency. With a consolidated approach to cybersecurity, agencies can reduce human labor while simultaneously improving outcomes. They can take advantage of integrations to gain the context they need to deliver effective protection across multiple domains faster than the adversary.



Tap into cloud readiness

As health agencies shift to cloud infrastructure in support of remote treatment and other advanced capabilities, new risks emerge. Organizations can leverage cloud detection and response for cross-domain threat hunting across cloud environments, identities, and endpoints. And they can make use of the scalability inherent in a platform that's purpose-built in the cloud to achieve superior protection, with reduced complexity and immediate time-to-value.



Pivot to comprehensive security

As IT teams look to utilize a robust platform, they should take advantage of complete code-to-cloud protection, utilizing the platform's ability to prioritize cloud and application risks while ensuring robust security across sensitive data assets in the cloud. This will eliminate blind spots, helping defenders discover all assets across clouds and apps and empowering them to detect threats, prevent exfiltration, and stop cloud breaches in real time.



Case Study: Accelerating Security Outcomes at Montage Health

Montage Health, a nonprofit healthcare system in California, serves a large community with a growing footprint of connected medical devices, virtual desktop environments, and cloud-based applications. Like many healthcare organizations, it faced the dual challenge of defending an expanding digital attack surface while modernizing outdated security infrastructure. With limited staff and rising adversary sophistication, Montage turned to CrowdStrike to consolidate and modernize its cybersecurity strategy.

The organization deployed the AI-native CrowdStrike Falcon® cybersecurity platform to unify endpoint, identity, and threat intelligence capabilities under a single lightweight agent and cloud-native console. CrowdStrike's modular platform architecture gave Montage Health the flexibility to adopt new capabilities over time — starting with extended detection and response (XDR), then expanding into identity protection, IT hygiene, and adversary intelligence. With CrowdStrike Falcon® Next-Gen SIEM, the healthcare provider gained the ability to conduct high-speed, low-cost security investigations at scale, dramatically accelerating response time while reducing operational complexity.

Montage Health also relies on CrowdStrike Falcon® Complete Next-Gen MDR for 24/7 managed detection and response, ensuring continuous protection across its environment. This comprehensive approach to cybersecurity has helped the organization cut monthly investigations nearly in half, reduce alert fatigue, and drop investigation time from hours to under a minute. For federal health agencies facing staffing and budget constraints, Montage Health demonstrates how a single, AI-native platform can transform cyber readiness — delivering speed, scale, and simplicity without compromise.

How CrowdStrike Helps

CrowdStrike and its leadership team have a long history supporting healthcare agencies, providing specialized expertise and advanced solutions. With FedRAMP Moderate and High authorizations, CrowdStrike's Falcon platform delivers real-time insights into attack indicators, threat intelligence, and evolving adversary tradecraft. It helps agencies meet Zero-Trust mandates, consolidate security operations, and stop breaches with pioneering detection and response, real-time identity protection, and all-domain security, all with a lightweight agent and unified platform that eliminates tool sprawl and gaps.

Want to learn more? Visit: crowdstrike.com/en-us/solutions/federal-government/

