

Powering the Future
of Healthcare ▶

 **CitiusTech**

Cybersecurity for Payers

**Build Resiliency with next-gen
healthcare focused cybersecurity
solutions and accelerators**



www.citiustech.com

Who we are

As a strategic partner to some of the world's largest healthcare and life sciences organizations, we play a deep and meaningful role in accelerating digital innovation, driving sustainable value and helping improve outcomes across the healthcare ecosystem.



With 100% focus on healthcare, CitiusTech is well-positioned to empower health plans at every step of their digital transformation journey. We focus exclusively on delivering specialized solutions and services across the healthcare digital value chain – spanning interoperability, data & analytics, digital engineering, provider performance management and member experience management.

3 out of the 5

national plans are our customers

9 Blue plans

leverage our products and solutions

Cybersecurity: Industry Trends

As health plans stretch the boundaries of data integration, business models, and digitizing processes, cyber risks proliferate. Healthcare cybersecurity trends demonstrate the need for adaptable, timely, and robust tactics to defend, avoid, and respond.



Cybersecurity Governance

Organizations that undergo M&As have more than one security model to pick from, and it can be challenging to adopt one. A common eGRC framework works best for a variety of scenarios and sizes of organizations



Regulations & Compliance

Inconsistent and conflicting state and federal compliance standards pose major challenge to manage healthcare data. Staying on top of evolving regulations takes a methodical and consistent approach



Zero Trust Architecture

With more users connecting unmanaged devices over the Internet, there's a growing need for zero trust security. This requires a model that assumes no person, device, or application should be trusted



Remote Care Requires More Security

Business and care models that increasingly use remote, virtual, IoMT, and hybrid technologies require a comprehensive framework, including MFA and rebooting policies to mitigate risks



API Threats

Over six months, API traffic increased 141% and malicious traffic by 348%. Adhering to the OWASP Top 10 API vulnerability list and decommissioning outdated APIs are key to mitigating API threats



Cloud/SaaS and Open-source Adoption

While SaaS offerings and open-source models provide a wealth of benefits at lower costs, they are primary targets for attackers. Payers continue to take heightened security measures to avoid cyberattacks

Cybersecurity: Key Challenges

- Despite investment in training employees on data-hygiene practices, simple human errors still cause untoward cyber security breaches
- A limited pool of experienced cybersecurity specialists has created an increase for 24/7 outsourcing options to ensure continuous security monitoring and response
- As payer organizations increase Cloud adoption, they are asking for more training and security best practices to ensure applications and infrastructure are resilient to malware and ransomware
- AI/ML-based cybersecurity systems continue to evolve, systems can be tricked into falsely labeling malicious software as safe or normal, requiring continuous improvement in cybersecurity solutions and approaches



Payer Regulatory: Key Offerings

- **Cloud Security:** Implement zero-trust network security for hybrid and multi-cloud environments. Provide Cloud security and resilience strategies to achieve secure adoption.
- **Smart Digital Identity:** Increase identity and access management maturity with strict role-based access control and periodic access check audits.
- **Application Security Management:** Adhere to OWASP and other security guidelines, practicing DevSecOps for software engineering. Product security through vulnerability assessments, penetration testing, intelligent automation, and security analytics.
- **Risk Governance:** GRC framework provides a single-source-of-truth for organizational risks, controls, and remediation efforts, abiding to best practices like HIPAA, HITRUST CSF, and NIST, to ensure effective policies and practices are in place.
- **Resiliency Services:** Business resiliency, continuity, and disaster recovery planning maintains an acceptable level of operation for critical business functions in case of disruption from any cybersecurity threat or disaster.

CitiusTech's offers a host of mature cybersecurity solutions and accelerators that enable payer customers to operate "business as usual" while under persistent threats and sophisticated attacks.

Together, we make payers more resilient to any threat or disruption based on proven expertise and customer trust.

Cybersecurity: Capabilities Overview

Cyber Security Focus Areas



Cybersecurity Compliance

- Sustained compliance



Security Orchestration, Automation, & Response (SOAR)

- Automation of security monitoring and response



Application, API & Mobile Security

- Releasing secure applications
- Adherence to Open Web Application Security Project.



Cloud Security (CSPM & CWPP)

- Secure Cloud posture and workload
- Configuration review and vulnerability assessment



Vulnerability Assessment & Penetration Testing

- Vulnerability detection & continuous protection
- Penetration testing & Red Team attacks



SDLC & Medical Device Security

- Medical device
- Pre-market and post-market security



DevSecOps

- Shift Left security testing



Governance, Risk & Compliance (GRC)

- Establishing a risk management regime
- GRC tool implementation



Business Resiliency

- Business continuity planning
- Disaster recovery



Identify & Access Management (IAM)

- Identity & privileged access management and strategy
- Roles management
- Access provisioning

Success Stories: Value-driven Engagements with Leading Health Plans



National leader in providing integrated and innovative medical benefits management.

- Strengthened the application authentication process by defining a framework to calibrate security checks
- Automated assessment checks for internal and external applications and laid out structured mitigation plan to help resolve vulnerability issues



Leading health insurance company in southeastern Pennsylvania, serving more than 8M members.

- Reduced a significant number of vulnerabilities in the platform by identifying process gaps
- Leveraged the Lean Six Sigma (LS6) approach and prioritized 31 major client areas like governance and process improvement, etc.

About CitiusTech

With 6,500+ healthcare technology professionals worldwide, CitiusTech helps leading healthcare and life sciences organizations reinvent themselves by accelerating digital innovation, leveraging next-gen technologies, and driving data convergence across the healthcare ecosystem.

We provide strategic consulting, digital engineering, data, analytics & AI, specialized platforms and end-to-end solutions to over 130 organizations across the payer, provider, medtech and life sciences industries. Our key focus areas include healthcare interoperability data management, quality performance analytics, value-based care, omni channel member experience, connected health, virtual care delivery, real-world data solutions, clinical development, personalized medicine and population health management.

Our cutting-edge technology expertise, deep healthcare domain expertise and a strong focus on digital transformation enables healthcare and life sciences organizations to deliver better outcomes, accelerate growth, drive efficiencies, and ultimately make a meaningful impact to patients.

Key Contacts



Shyam Manoj
Sr. Vice President & Head, Payers
shyam.manoj@citiustech.com



Jeffrey Springer
Sr. Vice President & Head, Products
jeffrey.springer@citiustech.com

100%
healthcare focus

130+
healthcare clients

50M+
lives touched

4.5/5
Client Satisfaction Score

\$340M+
worldwide revenue

Powering the future of healthcare ▶



This document is confidential and contains proprietary information, including trade secrets of CitiusTech. Neither the document nor any of the information contained in it may be reproduced or disclosed to any unauthorized person under any circumstances without the express written permission of CitiusTech.