WHITE PAPER

SECURING THE FUTURE OF HEALTHCARE INSURANCE: A CYBER-RESILIENT APPROACH

Abstract

As healthcare insurance organizations accelerate their digital transformation, the regulatory and cybersecurity landscape grows more complex and intertwined. Traditional compliance programs are no longer sufficient in an environment driven by real-time data, value-based care, and increasing cyber threats. This whitepaper outlines how Infosys supports its customers to transform into forward-thinking insurers by building a proactive, risk-based compliance program that integrates cybersecurity innovation to protect patients, ensure regulatory alignment, and strengthen operational resilience.

Infosys®
Navigate your next

Executive Summary

As large healthcare insurance providers move toward a fully cloud-centric, digitized, AI-enabled service model, cybersecurity is no longer just a backend function, but it is a core strategic differentiator. From processing millions of claims to managing sensitive health, financial, and behavioral data, insurers sit at the intersection of some of the most valuable and vulnerable information in the healthcare ecosystem. Leveraging the AI advancements to find innovative ways to improve quality of care, decrease costs, and retain top talent across a distributed business environment has led to evolving threats in an ever-changing technological landscape due to the unification of SaaS and PaaS offerings.

Patient and provider trust has become the new currency of competitive advantage. Ensuring that trust requires continuous investment in intelligent, adaptive cybersecurity frameworks that go beyond traditional perimeter defenses and regulatory compliance mandates. With the rise of AI, real-time health data, and value-based care models, insurers must safeguard a web of interconnected systems; from member portals and mobile apps to third-party platforms and data-sharing APIs spanning SaaS and PaaS platforms distributed across cloud service providers.

A single breach can trigger not only financial penalties but long-lasting reputational damage and legal exposure under HIPAA, HITECH, and emerging state-level data privacy laws. More critically, it can disrupt access to care, delay reimbursements, and erode member confidence, undermining the very foundation of trust that healthcare insurers strive to build.

Infosys supports its healthcare insurance customers by embedding cybersecurity into the design of digital products, care coordination tools, and claims automation platforms by bringing in its "Secure by Design | Secure by Scale | Secure the Future" strategy and tailored security frameworks with Cyber Resiliency at Core. Done effectively, this more holistic approach has effectively helped our customers reduce overall cybersecurity risks, not just due to external threats but internal as well; further reducing costs, increasing compliance and elevating customer confidence.

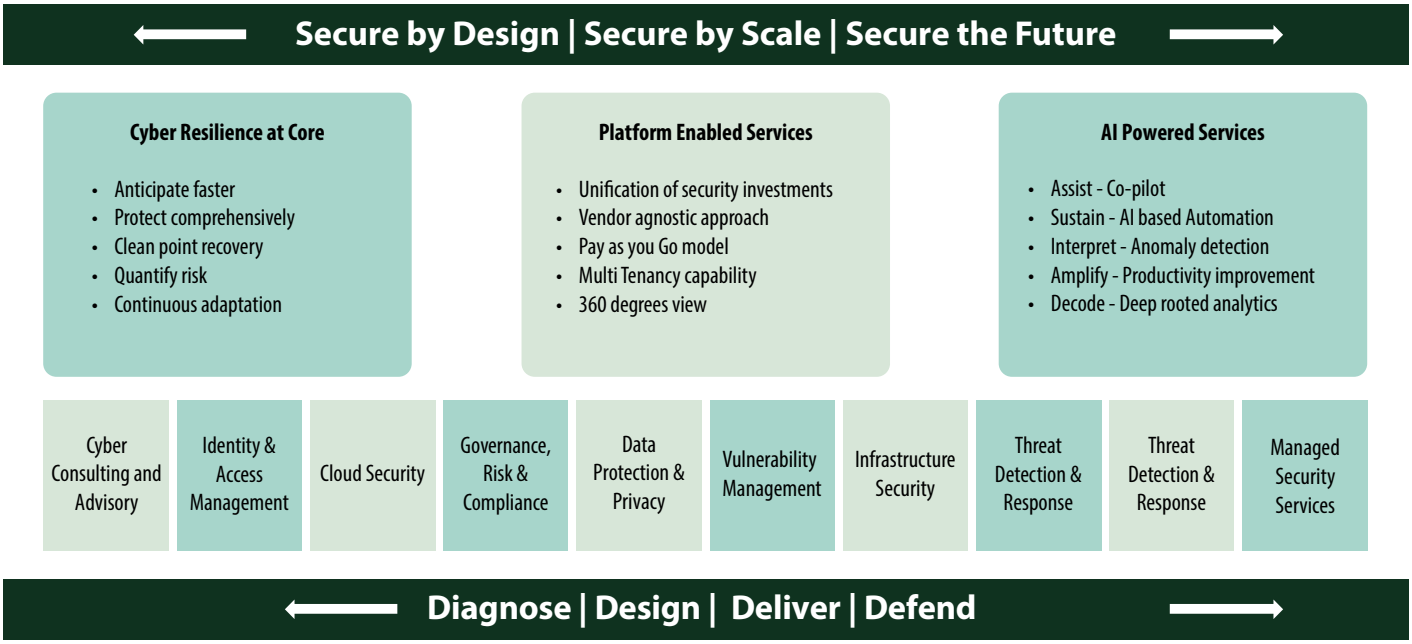

Fig. Infosys Strategy for Cybersecurity

In this white paper, we will delve into the unique set of challenges faced by healthcare insurance providers, and how Infosys supports its customers by leveraging its cybersecurity-driven compliance framework in managing these complex challenges across evolving ecosystems and demands.

Most pressing cybersecurity challenges

Cybersecurity in the healthcare provider space presents a unique set of challenges due to the sensitive nature of patient data, complex IT ecosystems, and growing reliance on third-party services. The requirements for secure enterprise architecture are evolving rapidly, driven by increasing interconnections among hospitals and clinics, physicians' remote offices, contractors, suppliers, university networks, and other external entities. In this dynamic environment, traditional security measures, viz. firewalls, antivirus software, and intrusion detection/ prevention systems no longer offer the necessary granularity, protection, or enforcement capabilities.

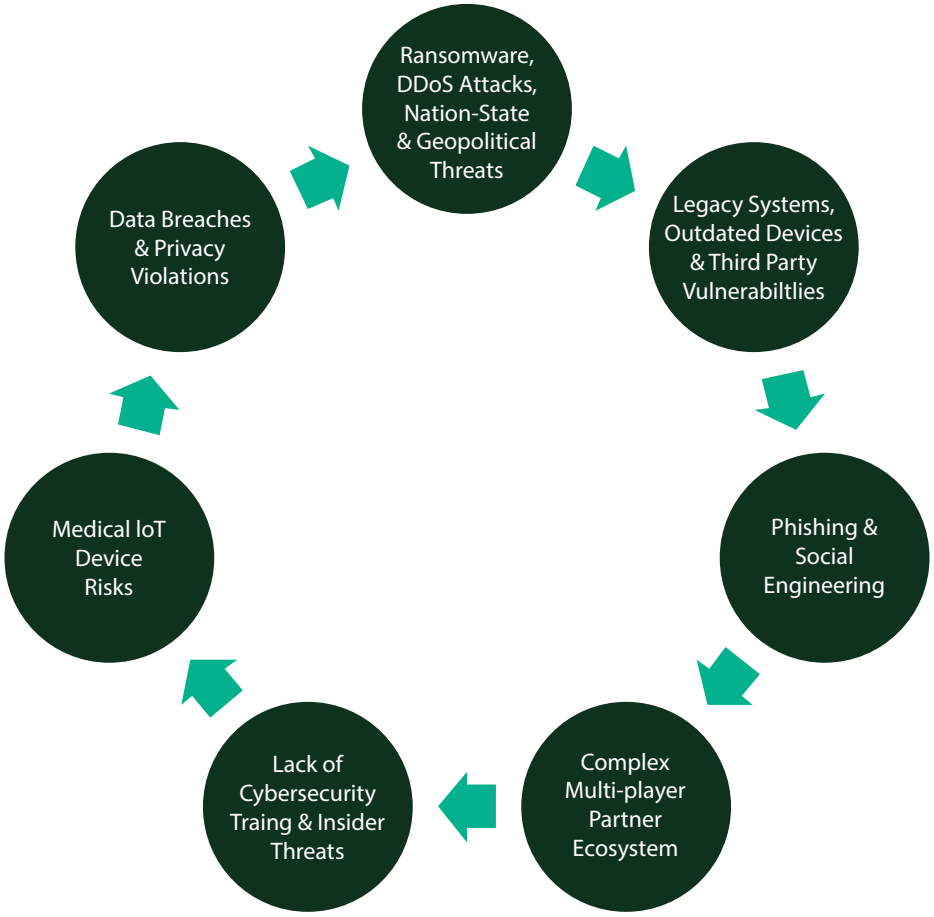

Fig. Cybersecurity challenges in healthcare

Ransomware, DDoS attacks, nation-state & geopolitical threats

- These are no longer just data-theft incidents, they are threat-to-life crimes. Such attacks can shut down hospital systems, delay patient care, and disrupt entire regional healthcare networks.
- The Change Healthcare attack in 2024 is a prime example, affecting every hospital in the U.S. and halting billions in payments.
- Distributed Denial of Service attacks can disable access to EHRs, scheduling systems, and other critical services. They damage reputation and delay care, making mitigation strategies essential.
- Increasing collaboration between nation-state hackers and ransomware groups (e.g., Iran and Russia) poses a growing threat.

Legacy systems, outdated devices, and third-party vulnerabilities

- Many hospitals still rely on 20-year-old systems that are difficult to patch or update. These systems often force newer technologies to lower their security standards to maintain compatibility, creating significant vulnerabilities.
- Healthcare providers heavily depend on vendors for EHRs, billing systems, diagnostics, and IoT devices. However, many of these vendors lack robust security measures, making them prime targets for cyberattacks.

Phishing and social engineering

- Deceptive emails targeting healthcare staff are increasingly common, often impersonating government agencies or insurance providers to gain unauthorized access.
- These attacks can lead to credential theft, ransomware infections, and data breaches.

Complex multi-player partner ecosystem

- Supply chain breaches and attacks on third-party associates have significantly risen since 2022.
- The evolution of a connected digital health ecosystem now involves a wide range of stakeholders, including patients, physicians, healthcare providers, payers, health IT vendors, pharmaceutical companies, R&D and biotech firms, and medical device manufacturers.
- Coordination with federal and local government agencies is essential to ensure compliance, data security, and effective incident response across the healthcare ecosystem.

Lack of Cybersecurity Training & Insider Threats

- Frontline staff often lack awareness, making them vulnerable to social engineering and poor security hygiene.
- Insider threats have risen by 47% over the past two years. These threats, whether malicious or accidental, often involve staff with privileged access misusing or mishandling sensitive data.

Medical IoT Device Risks

- Devices such as infusion pumps and patient monitors continuously stream data, often without encryption or proper access controls.
- These vulnerabilities can be exploited to gain persistent access to hospital networks or to exfiltrate sensitive patient data.

Data Breaches & Privacy Violations

- Patient data is a high-value target for identity theft and insurance fraud.
- Failure to comply with HIPAA regulations often leads to breaches.

Core Pillars of Infosys CyberSecurity Program for Healthcare providers

With the recent surge in data breaches targeting healthcare providers, Infosys realizes the impact of the proliferation of health data from digital health, mobile apps, and APIs. Mounting regulatory pressures, viz. HIPAA, HITECH, CMS, and state-level data privacy laws like CCPA and CPA, combined with growing expectations from members and providers around data security and trust, present significant challenges. Addressing these require a modern compliance program powered by cybersecurity innovation—one that goes beyond merely meeting legal requirements. We understand that compliance can no longer operate in isolation. Traditional compliance is reactive, checklist-driven, and siloed, while cyber threats require dynamic, integrated risk management.

Infosys CyberSecurity-driven compliance program delivery focuses on leveraging risk-based compliance frameworks, Zero Trust architecture, continuous monitoring, and incident response with AI/Automation for threat detection and compliance, while ensuring well-structured and tailored practices for periodic third-party risk assessments.

Risk-Based Compliance Frameworks

- NIST, HITRUST, and ISO 27001 integration
- Prioritizing based on data criticality and threat intelligence

Zero Trust Architecture

- Identity and access management as compliance foundations
- Real-time user behavior monitoring to detect anomalies

Continuous Monitoring and Incident Response

- Logging, SIEM, and automated alerts
- Regulatory reporting requirements (e.g., OCR breach notification timelines)

AI/Automation for Compliance & Threat Detection

- Real-time claims fraud detection
- Automated evidence gathering for audits

Third-Party Risk Management

- Securing the extended enterprise (vendors, TPAs, cloud services)
- Contractual safeguards and routine cybersecurity audits

For a Managed Service Provider like Infosys, our role is evolving beyond basic Infrastructure, Application or Security Operations support. We are now strategic partners—safeguarding our customers through patient trust, ensuring compliance, and enabling digital health innovation. Our approach transcends reactive threat management; we design and operate secure environments tailored to the unique demands of healthcare, where uptime can mean the difference between life and death, and data breaches carry life-altering consequences.

Our cybersecurity services catering to the healthcare industry are backed by a suite of AI-enabled service offerings.

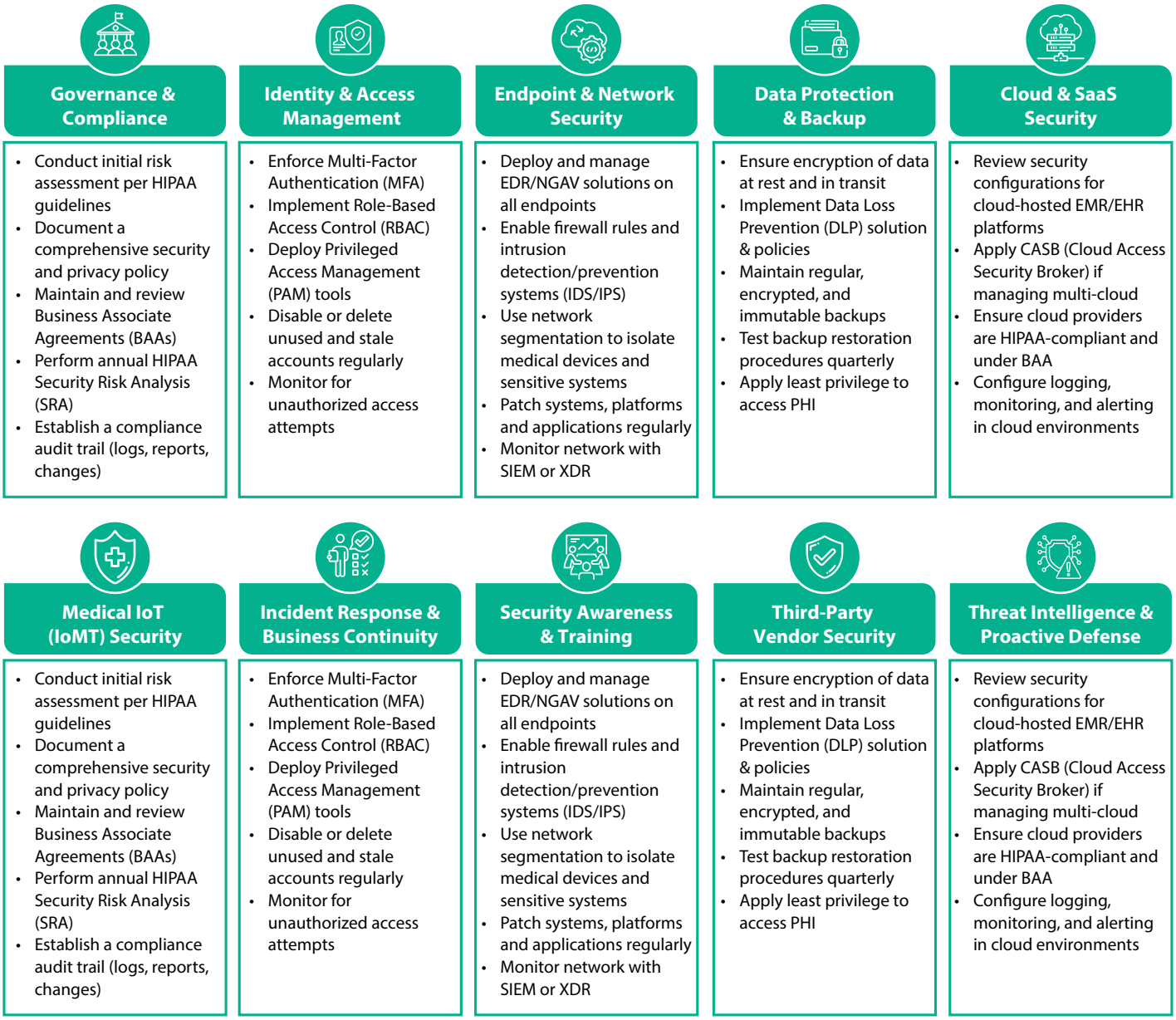

Fig. Infosys CyberSecurity services catering to healthcare industry

Threat and Vulnerability exploitation

Infosys' strategy to stay ahead of threat and vulnerability exploitation is led by the establishment of a dedicated Risk Management Office under the CISO. This initiative aims to mature vulnerability management practices using AI and Automation. The program focuses on clear roles and responsibilities (RACI), well-defined policies, exception processes, and clear remediation workflows for governance.

The program ensures:

1. **Regular Scanning and Assessments:** Conduct frequent vulnerability scans to identify weaknesses in your systems, software, and network components. Consider using a combination of vulnerability scanners, software composition analysis tools, and penetration testing.
2. **Leveraging Threat Intelligence:** Stay informed about the latest threats and vulnerabilities by subscribing to threat intelligence feeds and monitoring reputable cybersecurity resources. This allows you to anticipate potential risks and proactively address them.
3. **Prioritizing Vulnerabilities:** Not all vulnerabilities pose the same level of risk. It's important to prioritize them based on factors listed below:
   a. **Severity:** Use scoring systems like CVSS as a guide but also consider the context of your specific environment.
   b. **Exploitability**: Assess how likely a vulnerability is to be exploited in the wild, referencing platforms like CISA KEV.
   c. **Asset Criticality & Exposure**: Focus on vulnerabilities impacting high-value assets (e.g., critical data, production systems) and their proximity to the periphery/edge.

4. **Timely Patching and Remediation**: Apply patches and updates promptly to address known vulnerabilities. Consider integrating patching into your software release cycles to streamline the process. When immediate patching is not feasible, implement mitigating controls such as network segmentation or access restrictions to reduce risk.
5. **Continuous Monitorin**g: Employ continuous monitoring to detect new vulnerabilities or changes in your environment.

Additionally, Zero-Day Exploit Prevention practices focus on:

a. **Behavioral Analysis**: Use tools to detect unusual patterns in the system and user activity that might indicate a zero-day exploit.
b. **Heuristic Analysis**: Employ heuristic tools to analyze code and identify suspicious characteristics, even for previously unknown malware.
c. **AI and Machine Learning**: Utilize these technologies to predict and flag anomalies that could point to zero-day attacks.
d. **Implement a Robust Web Application Firewall (WAF)**: WAFs can help monitor and regulate network traffic to block unauthorized access and prevent zero-day exploits.

Impact of AI-induced Threats in Healthcare

Another critical area that Infosys CyberSecurity is focused on is the impact of AI-induced threats in healthcare services. With the increasing demand for AI-led transformations to improve the patient care experience and keep costs low, AI adoption has gained rather alarming momentum. This has further led to threats that are multifaceted and pose significant risks to patient safety, data privacy, and systemic equity. Infosys is already leading this space with a clear vision to proactively identify these threats and drive mitigations to eliminate or reduce the impacts of this exponential technology adoption outburst.

Some of the key AI-Induced threats that we consider for our solutions are:

1. **Algorithmic Bias and Misalignment**

- AI systems may perpetuate or amplify existing social inequalities due to lack of insufficient data.
- Examples include racial bias in care recommendation algorithms and underdiagnosis in minority populations that may be due to selective exclusion during data collection.

2. **Automation Bias and Overtrust**

- Clinicians may overly rely on AI recommendations, potentially ignoring clinical judgment when urgency and timelines are pressing, especially in emergency care scenarios. This can lead to diagnostic errors or inappropriate treatments.

3. **Lack of Transparency and Interpretability**

- Many AI models operate as "black boxes," making it difficult to understand or challenge their decisions.
- Some of this isolation may be a voluntary motivation by the service providers for a competitive edge.

4. **Regulatory and Ethical Challenges**

- Fragmented regulatory oversight across jurisdictions further complicates compliance.
- Ethical concerns may include consent, accountability, and equitable access.

5. **Data Privacy and Security Risks**

- AI systems rely heavily on sensitive patient data, making them prime targets for cyberattacks.
- Risks include unauthorized access, data breaches, and misuse of personal health information.

To address the above increasingly evolving challenges, Infosys has designed tailored solutions by bringing in its Secure by Design, Secure by Scale, and Secure the Future strategy using its AI-Powered platforms and solutions that are tailored to AI-focused security frameworks. Some of the mitigation strategies adopted through our services and recommended are:

1. **Robust Oversight and Governance**

- Implement scalable human oversight and ethical review boards.
- Use techniques like inverse reinforcement learning and mechanistic interpretability to align AI behavior with human values.

2. **Data Protection Measures**

- Employ strong encryption, multi-factor authentication, and secure data storage capabilities.
- Adhere to regulations like HIPAA, GDPR, and HITECH to safeguard patient data.

3. **Bias Auditing and Inclusive Training Data**

- Regularly audit AI systems for bias and fairness, with a metric-driven approach.
- Ensure training datasets are diverse and representative of all patient populations, with due consideration to voluntary exclusions.

4. **Transparent and Explainable AI**

- Develop models that provide interpretable outputs to support clinical decision-making that can be measured over time through metric trending.
- Encourage the use of explainable AI (XAI) frameworks.

5. **Education and Training**

- Train healthcare professionals to understand AI limitations and ethical implications, especially in critical care scenarios.
- Promote interdisciplinary collaboration between clinicians, data scientists, and ethicists.

6. **Regulatory Harmonization**

- Advocate for unified global standards and sector-specific regulations.
- Monitor developments like the EU AI Act for guidance on responsible AI deployment.

Shift in Mindset for mature practices

At Infosys, we firmly believe that mature cybersecurity practices stem from a fundamental shift in mindset; from treating security as a reactive, isolated function to embedding it as a proactive, business-integrated strategy. This transformation is critical to defending against increasingly sophisticated threats and building long-term organizational resilience. We ensure:

1. **Continuous enablement and enforcement of Secure Development practices**

- **Define Security Requirements**: Incorporate security requirements throughout the Software Development Lifecycle (SDLC).
- **Secure Coding Practices**: Train developers to follow secure coding practices to reduce the likelihood of introducing vulnerabilities during development.
- **Code Review and Analysis**: Review code and use static analysis tools to identify and remediate vulnerabilities early in the development process.
- **Secure Default Settings**: Configure software with secure default settings to reduce the risk of deploying with weak configurations.
- **Enforced Gating**: Ensure security gates for code and configuration movement from Development to QA and further into controlled environments.

2. **Continuous testing and refining of Incident Response practices**

- **Develop and Test Incident Response Plan**: Have a well-defined and tested plan for responding to security incidents, including zero-day exploits.
- **Train Employees**: Educate staff on security awareness and their role in preventing and responding to incidents.
- **Random Test**: Conduct periodic red, blue and purple team exercises

3. **Leverage of investments in Security Solutions**

- **Endpoint Security**: Deploy endpoint security solutions that can detect and prevent malicious activity, including zero-day threats.
- **Intrusion Detection and Prevention Systems (IDS/IPS)**: These systems can monitor network traffic and block potential attacks in real-time.
- **Security Information and Event Management (SIEM)**: SIEM solutions can help you monitor and analyze security logs to detect suspicious activity.
- **Visibility**: Ensure all security logs and feeds from security solutions are ingested into SIEM for visibility and correlation.
- **Automation**: Utilize automation to streamline vulnerability management tasks, such as scanning, prioritization, and patching and Security Orchestration, Automation, and Response (SOAR) for incident response.

Conclusion

A modern compliance program that is AI-driven, powered by cybersecurity innovation, does more than meeting legal requirements; it enables insurers to build trust, reduce risk, and deliver secure digital experiences on a scale. By embedding security at the core of compliance, healthcare insurance providers can not only meet today's demands but also anticipate tomorrow's challenges, including those induced by AI adoption. Infosys is making significant investments in its partner ecosystem and leveraging AI for real-time threat detection, Zero Trust architectures, and AI-powered platforms for scalable protection and Responsible AI practices. At Infosys, we believe that in the future of healthcare insurance, security will be synonymous with value—because better care, faster claims, and personalized plans cannot be delivered without a secure and resilient ecosystem.

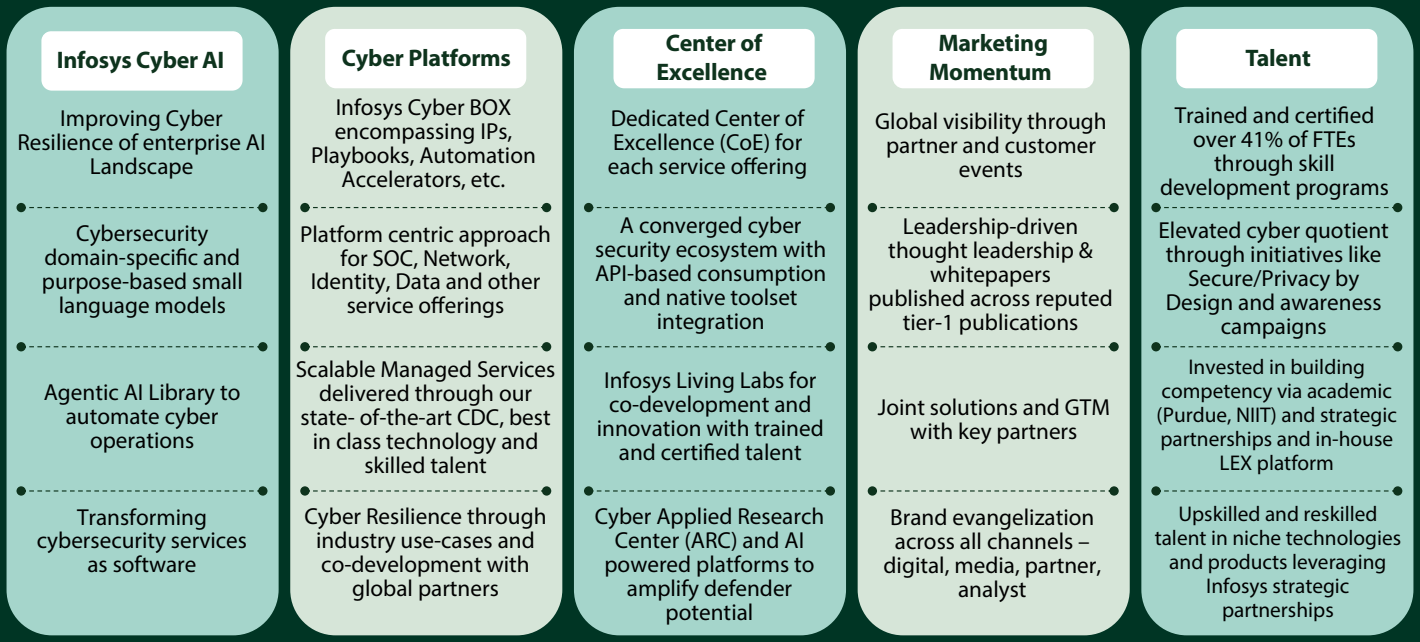

Fig. Infosys' Investments and Innovations for Cyber Resilience

About the Author

Satish Kumar Koyali
Delivery Manager

Satish is a Cybersecurity Strategist and Service Delivery Leader with over 26 years of experience at the intersection of IT, Security, and business strategy. He specializes in leading end-to-end cybersecurity initiatives that not only protect enterprise environments but also drive measurable business growth. He engages directly with CxO stakeholders to align cybersecurity strategies with business priorities and has led global teams across Security Operations (SOC), Identity & Access Management (IAM), Cloud Security, Application Security, Data Security and Risk Management—delivering transformation/engineering programs, managed services, to drive operational excellence and strategic outcomes. As a trusted advisor and servant leader, he's passionate about enabling secure digital transformation through innovation, collaboration, and a sharp focus on customer value.

For more information, contact askus@infosys.com

Infosys®
Navigate your next