Cyber risks and regulatory pressures are escalating for healthcare organizations, making it harder to maintain patient trust. Already a lucrative target, stretched resources and multiple technology touchpoints increase the attack surface for nefarious cyber criminals to target providers with ransomware.

Too often, healthcare organizations are reacting to problems. That’s because:

- It’s not sustainable to keep managing problems the same way. Healthcare organizations need a more scalable, collaborative approach to better identify and mitigate security and compliance risks.
- The healthcare industry predicted to spend $125 billion by 2025 to beef up its cyber defenses, security automation will be a critical area to temper the costs and consequences of security gaps.

SILOED SYSTEMS make it difficult for healthcare IT teams to quickly assess threats and vulnerabilities.

POOR VISIBILITY leads to impromptu prioritization and delays, attention away from efforts to improve patient and clinician experiences.

MANUAL PROCESSES create delays when responding to issues and lead to increased time in patient care and safety.

LACK OF INSIGHT leads to blind attack responses which can be inefficient and result in ineffective remediation efforts.

It’s not sustainable to keep managing problems the same way. Healthcare organizations need a more scalable, collaborative approach to better identify and mitigate security and compliance risks. And with the healthcare industry predicted to spend $125 billion by 2025 to beef up its cyber defenses, security automation will be a critical area to temper the costs and consequences of security gaps.

ServiceNow works across your existing tools and systems to bring everything together in one place for case management. We deliver a single data model and system of intelligence, along with cross-functional digital workflows and automation to deliver powerful results:

- Move from reactive to proactive using a single, cloud-based platform that centralizes interoperable workflows and delivers end-to-end visibility for vulnerability and incident remediation.

Reduce compliance costs by escalating exceptions and recording audit data on a centralized platform.

Accelerate reaction times by connecting healthcare IT, risk, and security teams with digital workflows and a single system of action.

$12M in savings over three years using risk management applications.

85% mean time to contain improvement.

80% reduction in open vulnerabilities.

75% efficiency gain for risk and compliance activities and vendor risks.

VIEW OUR EBOOK