

Ransomware Forces Healthcare Organizations to Modernize Their Approach to Resilience

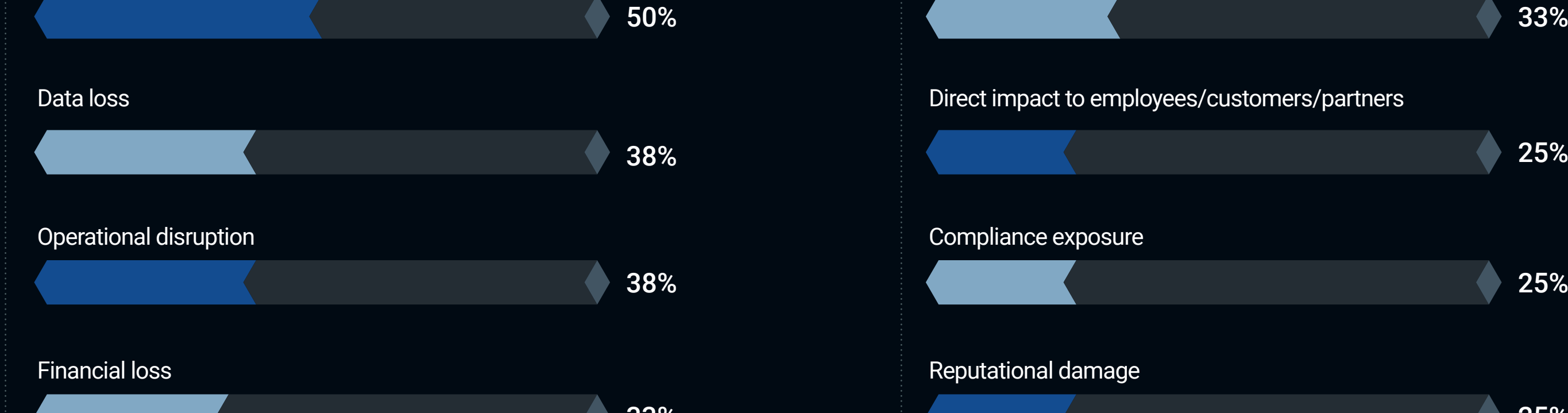
When it comes to ransomware attacks, healthcare organizations often find themselves in the crosshairs. Disruptions not only impact financials but also place lives at risk. As technology enters the era of AI, ransomware attacks are poised to increase in frequency. It is the responsibility of technology leaders in healthcare to ensure the right technology, tools, and processes are in place to best defend against ransomware and ensure uninterrupted patient care. Cloud-based modernization offers a path for healthcare organizations to strengthen their resilience and address the increased threat of ransomware.

This Infographic from Enterprise Strategy Group was commissioned by Commvault and Microsoft and is distributed under license from TechTarget, Inc.

Beyond Disruption, Successful Ransomware Attacks Often Expose Business and Patient Data

For healthcare organizations, ransomware is a matter of when, not if. Additionally, a ransom payment is not the only objective for the perpetrators of an attack. Ransomware attacks also target sensitive data in an attack, such as financials and patient records, increasing the cost and risk generated by an attack. For healthcare organizations, electronic health record (EHR) systems are prime targets for cybercriminals due to the wealth of sensitive information they store, including detailed patient data, which is highly valuable for identity theft, extortion, and fraud on the dark web.

» Top Impacts of Successful Ransomware Attacks on Healthcare Organizations



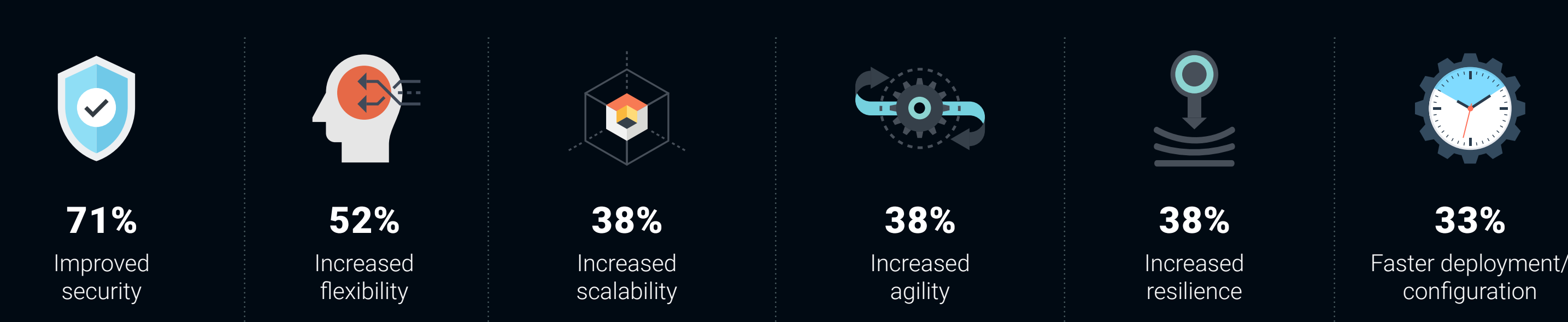
“Resilience in healthcare is crucial. Without it, timely and reliable access to data is compromised, which can critically impact patient care. **Any disruption can significantly hinder healthcare delivery, degrading the quality of patient care and, in the worst cases, jeopardizing patient safety.**”

- David Houlding, Director of Global Healthcare Security and Compliance Strategy, Microsoft

Cloud-based Modernization for an Effective Ransomware Protection Strategy

As healthcare organizations evaluate options to improve their ransomware readiness, immutability and cloud integration are among the top recovery solution considerations. When addressing ransomware concerns, organizations should look to cloud-based modernization for EHR systems and other mission-critical data, as improved security is the most commonly sought benefit of cloud adoption by healthcare organizations.

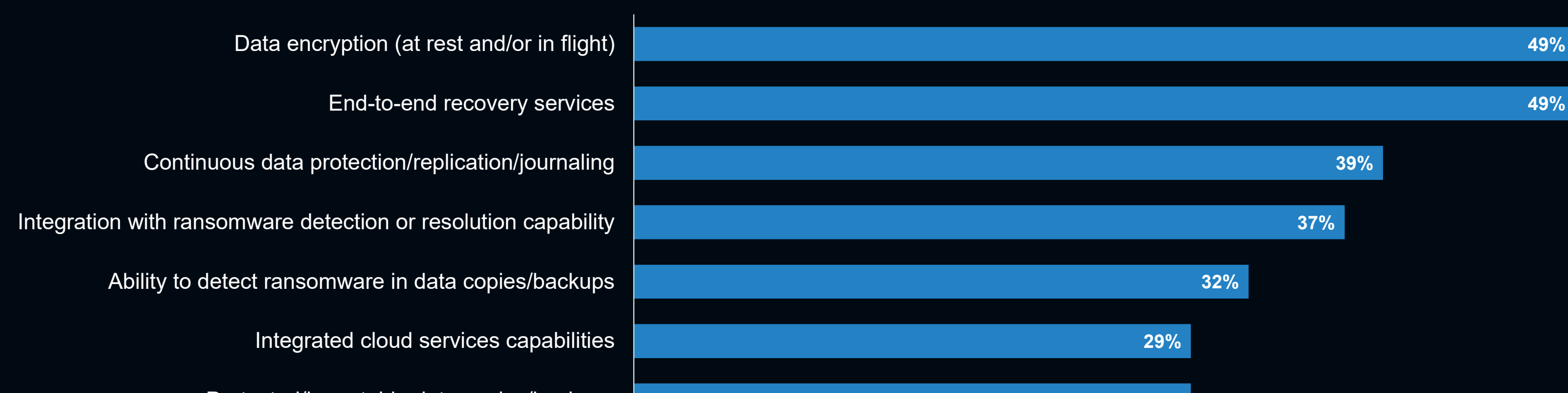
» Top Technology-related Benefits of Public Cloud Services for Healthcare



“Cyber recovery isn’t like a typical outage—you need to be sure your data is safe and uncompromised before restoring it or you risk making things worse. Microsoft and Commvault seamlessly share threat signals, enabling security and IT teams to work within their usual tools without switching apps. Commvault Cleanroom Recovery allows teams to practice secure data recovery, ensuring readiness for real incidents. Microsoft Copilot for Security further accelerates response, helping analysts work faster and sharpen their skills. **These tools prepare teams to handle cyberincidents with confidence and precision.**”

- Peter Hands, Chief Information Security Officer, British Medical Association (BMA)

» Top Considerations for Healthcare When Selecting a Ransomware Recovery Solution



Microsoft Azure Plus Commvault Cloud Deliver Cyber Resiliency for EHRs On Azure

As healthcare organizations modernize their mission-critical systems, cloud services, such as Microsoft Azure, enhance scalability, agility, and innovation while reducing technical debt. When combined with Commvault Cloud, healthcare organizations gain access to advanced security and rapid recovery capabilities, helping to deliver the combined benefits of resilience, rapid recovery, and cost efficiency to healthcare organizations.


» Cyber Resiliency Benefits of Microsoft Azure Plus Commvault Cloud for Critical Healthcare Data

- 1. EHR co-developed integration**
The solution is purpose-built with EHRs to provide seamless protection and compliance with regulatory standards.
- 2. Comprehensive backup and recovery for all data**
Application-consistent backups safeguard EHRs and other mission-critical data from cyberattacks, errors, and failures, providing both data integrity and reliability.
- 3. Immutable and indelible air-gap protection**
With a zero-trust framework and unique preemptive early warning deception technology, SaaS-based air-gapped storage shields EHR backups from threats.
- 4. Cleanroom recovery for safe testing and recovery**
Isolated recovery environments allow for recovery testing, investigation, and recovery without affecting production.
- 5. Azure-optimized and cost-effective**
Resilience and recovery instances of both data and the application leverage Azure’s scalability, on-demand cost optimization, and unparalleled performance.

Choosing the right strategic technology and services partner can help ensure that healthcare organizations maintain cyber resilience by enabling operational best practices.


» Best Practices for Operationalizing Cyber Resilience

#1 RISK ASSESSMENTS




Identify vulnerabilities and focus resources on mitigating high-impact threats.

#2 ROBUST CYBERSECURITY POLICIES AND PROCEDURES



Strengthen network segmentation, enforce multifactor authentication (MFA), and secure medical devices.

#3 INCIDENT RESPONSE PLANNING AND PRACTICE



Conduct regular periodic testing to prepare for cyber-events and needed rapid recovery.

“In healthcare, integrated security is essential to reducing the inefficiencies and risks associated with multiple, disjointed security tools. Microsoft’s suite, combined with Commvault Cloud’s cyber resilience and recovery capabilities, delivers integrated, AI-powered security. Cloud-based cyber recovery allows for efficient, cost-effective preparedness, enabling healthcare providers to recover quickly from ransomware and other threats while avoiding the costs of on-premises backups.”

- John Doyle, Global CTO of Healthcare and Life Sciences, Microsoft

Conclusion

Given the ever-increasing threat of ransomware, healthcare organizations must continue to ensure that they are doing everything necessary to protect patient care and the financial state of their organization. Commvault and Microsoft Azure’s integrated solutions can help deliver ransomware protection and rapid recovery, while enabling uninterrupted patient care and continuous healthcare operations. Integration with Microsoft Azure delivers greater flexibility in both data resilience and restore options, further helping to ensure uninterrupted patient care.

These highly integrated solutions deliver to healthcare organizations tools tailored to meet the compliance and privacy needs of the healthcare industry, while also offering the scale to serve remote healthcare locations as well. The result is a stronger and more resilient environment that is better equipped to reduce the risk, cost, and interruptions of an attack.

LEARN MORE

