NetApp ransomware solutions for healthcare

Protecting valuable data from multiple threats

■ NetApp

The challenge

As healthcare providers, you are charged with keeping people well and healing them when they are sick. Technological advances such as digital imaging, precision medicine, and the electronic health record (EHR) empower you to better treat your patients for what ails them now and to prevent future ill health. With these advances in technology has come an incredible increase in data collected. Managing and protecting data can be difficult in the best of times, even for companies where technology is their focus. For most healthcare companies, technology efforts are afterthoughts, not integrated with each other. That disjointedness leads to vulnerabilities. There is a rise in the number of bad actors looking to capitalize on the wealth of personal and private information in the EHR and throughout a hospital system. The need for security and protection is pressing.

Persistent and growing threat

Ransomware attacks are on the rise in healthcare, especially in the Americas. Why? Because it's lucrative: Health records fetch about US$1,000 each on the black market and ransom demands are typically higher than $1 million. Because it's easy: Ransomware kits can be bought for $200, and the kits simplify the hack tremendously. Healthcare organizations are notorious for being behind the curve when it comes to security. There has been a marked increase in ransomware and other hacking attacks since the onset of COVID-19 — and that's in addition to the already projected fivefold increase of attacks over the next 5 years. This threat is not going away or decreasing. With downtime costing a hospital system more than $8,000 a minute — even if a ransom isn't demanded — the impact on the organization can be huge. The average return to normal takes more than a week.

The NetApp solutions

NetApp brings you innovative and specific security solutions. From assessment to prevention to remediation, capabilities that we provide can ward off villains and return you to operations if they do get through. NetApp Data Protection and Security Assessment (formerly Ransomware Risk Assessment) provides valuable insight immediately and helps you to improve your ransomware and data protection strategy. NetApp detection and prevention solutions include warning and security mechanisms to help

you prevent as many threats as possible. With NetApp remediation and restoration solutions, if your data and systems go offline, they get back online with minimal interruption to service. NetApp Data Protection and Security Assessment The NetApp Data Protection and Security Assessment service identifies potential gaps in current data protection and security policies and defines and documents security risks. The service also creates actionable plans to remediate exposure and provides valuable insights that help you be ready for a threat, recover from an attack, and maintain compliance to avoid future risks.

Detection and prevention

NetApp FPolicy™ software provides granular file-level monitoring and control to secure your information from malicious actors. FPolicy allows you to approve and deny users natively or externally and integrates with many third-part SIEM vendors. NetApp Cloud Insights and NetApp Active IQ® proactively provide you information about file changes and resource consumption to quickly alert you to potential risks and breaches. NetApp SnapLock® compliance software and write once, read many (WORM)

technologies back up your systems and secure them from external and internal threats. They give you confidence that you can restore your systems at any time — without data corruption.

Remediation and restoration
NetApp SnapLock and SnapCenter® solutions allow you to back up and restore at nearly any point. Getting back to normal operations is as easy as restoring to a NetApp Snapshot™ copy that was created before the ransomware infection. SnapLock software employs the WORM immutability technology that is native in ONTAP. Immutable backups ensure that administrators can't delete Snapshot copies. Hackers, who are an increasingly devious and common threat, can't delete or ransom your backups. The SnapCenter tool manages the movement and restoration of Snapshot copies, further speeding up return to operations and minimizing complexity for your staff.

Closing thoughts
NetApp's native tools and technologies provide you unmatched capabilities and fill gaps in security implementations that are typically filled by expensive third-party applications. In response to the rise of ransomware in healthcare, NetApp delivers proven solutions to protect your brand and your patients.

"We recently experienced a ransomware event, and when we saw what Cloud Insights ransomware detection provides, we were sold."
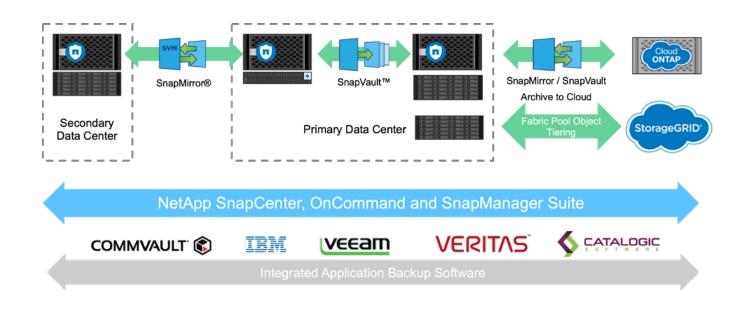
Director of IT, Transportation Company

About NetApp
In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services and applications to the right people—anytime, anywhere. www.netapp.com

Figure 1: NetApp's solutions stretch from edge, to core, to cloud