bitglass

Case Study

John Muir Health Secures Cloud & Mobile with Next-Gen CASB

JOHN MUIR HEALTH

John Muir Health is a nationally recognized, not-for-profit healthcare organization serving patients in the San Francisco Bay Area. It includes a network of more than 1,000 primary care and specialty physicians and over 6,500 employees across medical centers in the San Francisco Bay area, including a trauma center and a behavioral health center. The health system offers a full-range of medical services and a leader in several specialties – neurosciences, orthopedics, oncology, cardiovascular treatment, trauma care, pediatrics and high-risk obstetrics.

John Muir Health needed a solution for data security and HIPAA compliance across cloud applications such as Office 365 and ServiceNow, accessible from a range of managed and unmanaged end-user devices. As with other health systems, John Muir must comply with complex federal regulations including HIPAA for protected health information (PHI), PCI-DSS for billing information, and local state regulations around personally identifiable information (PII). As an organization with a complex network of physicians, member hospitals, and wide-ranging services, protecting data on all devices, was of great concern.

John Muir needed a security solution that could control the flow of PHI, PII and PCI in the cloud, at access and on any device, managed or unmanaged. Initially, John Muir Health adopted a combination of a traditional Mobile Device Management (MDM) solution and an agent-based Cloud Access Security Broker (CASB). Installation of agents was rejected by users at large who resented the invasion of privacy on their personal devices. Furthermore, many users had multiple affiliations, and it was technically impossible to deploy multiple agents on their devices, one for each affiliated institution.

After researching data protection solutions, John Muir Health chose Bitglass for its unique agentless Next-Gen CASB and mobile security solutions. With Bitglass, John Muir Health was able to rapidly achieve security and compliance for cloud applications including Office 365 and ServiceNow, across any device, without the need for agents on endpoints. Furthermore, Bitglass' Next-Gen architecture delivered Zero-Day protection, future proofing security for John Muir Health's evolving cloud footprint..

The Bitglass Next-Gen CASB delivers visibility, compliance, identity and access control at scale. John Muir Health is also able to define granular data loss prevention (DLP) policies and prevent unauthorized access in compliance with HIPAA. Bitglass earned John Muir Health's trust because of its unique Next-Gen capabilities of rapid deployment and Zero-Day protection, and easy-to-deploy agentless architecture.

"We have hundreds of unmanaged devices in use by clinicians at John Muir Health, however, we need to properly manage the PHI and PII data within our environment. New applications like Office 365 could pose security and compliance risk. Fortunately, Bitglass' next-gen CASB solution provides the security, manageability and, flexibility that we need to protect data across our environment, including our cloud-supported applications, protecting and securing our patient's data."

–Bill Hudson, VP of IT Operations and ACIO, John Muir Health