bitglass

case study

Healthcare Leader Secures BYOD with Next-Gen CASB

This regional health insurance leader sought to provide mobile email access to their employees. The CISO sought to balance the security requirements of HIPAA regulations with the mobility demands of employees.

HIPAA requires that Protected Health Information (PHI) be in the control of the company at all times. In fact, Department of Health and Human Services data shows that three quarters of breaches in the healthcare sector can be attributed to lost and stolen devices. That said, BYOD is a reality with which IT leaders must contend.

This firm's first attempt at solving the BYOD challenge involved device management software from Good Technology, quickly rejected by employees over usability and privacy concerns.

They then deployed Bitglass to enable HIPAA compliant access to corporate email, all without agents. By leveraging Bitglass' Omni multi-protocol proxies, this firm was able to secure data in transit and on all endpoints. Deployment was painless, with no configuration required. Users simply added their corporate email accounts to the native email clients of their BYOD devices and data dynamically tracked, encrypted, redacted and blocked. Where the Bitglass data protection engine detected PHI, DLP policies were applied to limit leakage.

This organization also made use of Bitglass' rich visibility, analytics, and patented selective wipe capabilities. If a device is lost or compromised, IT can wipe corporate data from the device without touching end-users' personal data.

Bitglass enabled mobile email access on BYOD for the employees of this insurer while ensuring HIPAA compliance.

No software, no enrollment headaches.

“Bitglass enables secure mobile access for our employees while ensuring HIPAA compliance. Easy to deploy and transparent to users so they can focus on the well-being of patients.”

— CISO, healthcare firm