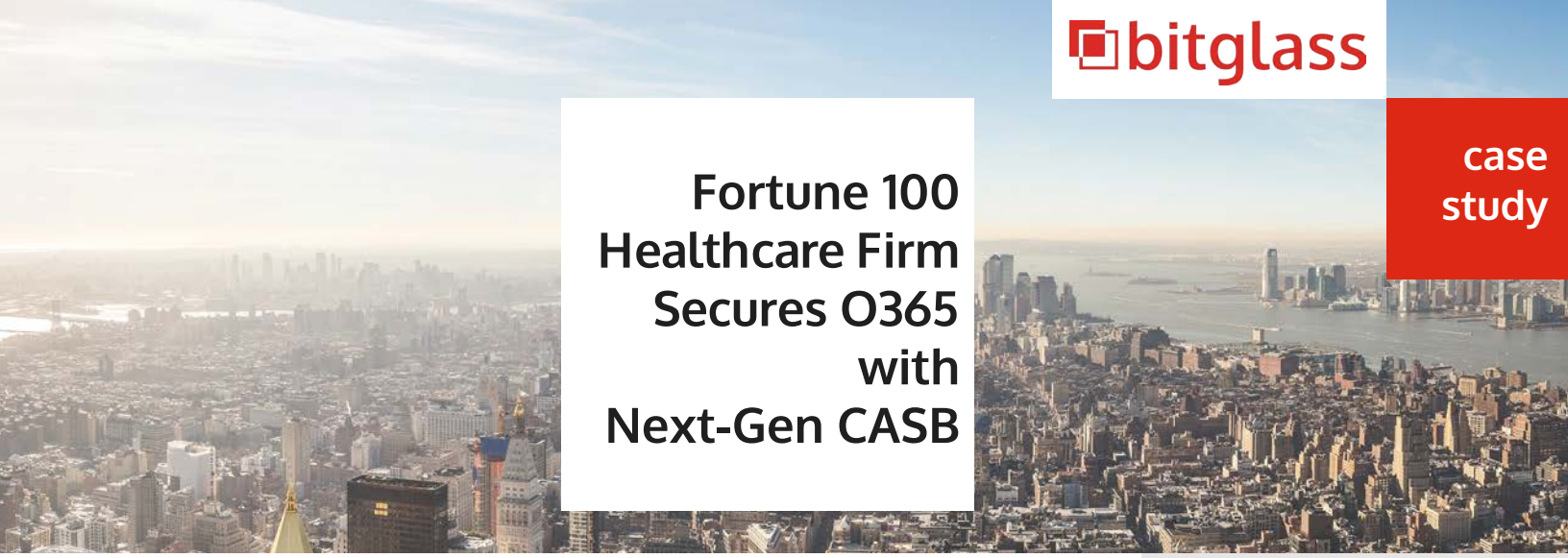

bitglass

case study

Fortune 100 Healthcare Firm Secures O365 with Next-Gen CASB

Based in the US, this healthcare firm was looking to fully transition its 30,000 global employees to a SaaS productivity suite. The firm's IT team had already deployed Office 365 for email only, but without proper security controls it refused to deploy file sharing and storage via OneDrive and Sharepoint. The firm's existing security architecture included next-gen firewall appliances, along with secure web gateways from Bluecoat and Symantec DLP appliances. This network-level security architecture was inadequate for protecting data in the cloud and allowing for access on any device.

With the firm's internal Office 365 productivity suite initiative set to rollout rapidly throughout the company, its enterprise security architecture team decided to deploy a cloud access security broker solution to enable secure cloud usage. Of particular concern was protecting PHI, PII, and corporate intellectual property in data flowing out of the cloud. The native Office 365 security controls did not provide an adequate level of data protection, especially in the case of data access by unmanaged and untrusted devices.

In its search for a solution, the firm conducted trials of Bitglass and two other major CASB vendors. In these trials, the IT security team ran the CASB solutions through a gamut of use cases – access control, discovery, API, and managed/unmanaged device access.

The firm ultimately chose Bitglass because of the distinctive ability of its solution to provide real time data protection. In its testing, the firm's security architecture team concluded that API-only approaches were not sufficient for complete Office 365 data protection. The team favored the proactive real time, inline data security enabled by Bitglass' hybrid architecture to the reactive, delayed security offered by API-only solutions. The limitations of the API solutions, which were only able to detect data leakage after the fact, were highly problematic. The ability of Bitglass' unique technologies – reverse proxy and AJAX-VM as well as Activesync proxy – to secure sensitive data on unmanaged devices and BYOD was key. Additionally, the integrated DLP engine of Bitglass' solution offered a clear system performance advantage over the external DLP via ICAP required by competing CASBs.

"In comparing the leading CASB solutions, we found that only Bitglass delivers a complete security solution for cloud and mobile with real-time inline data protection from any device – laptops or mobile."

– CISO, Healthcare Firm