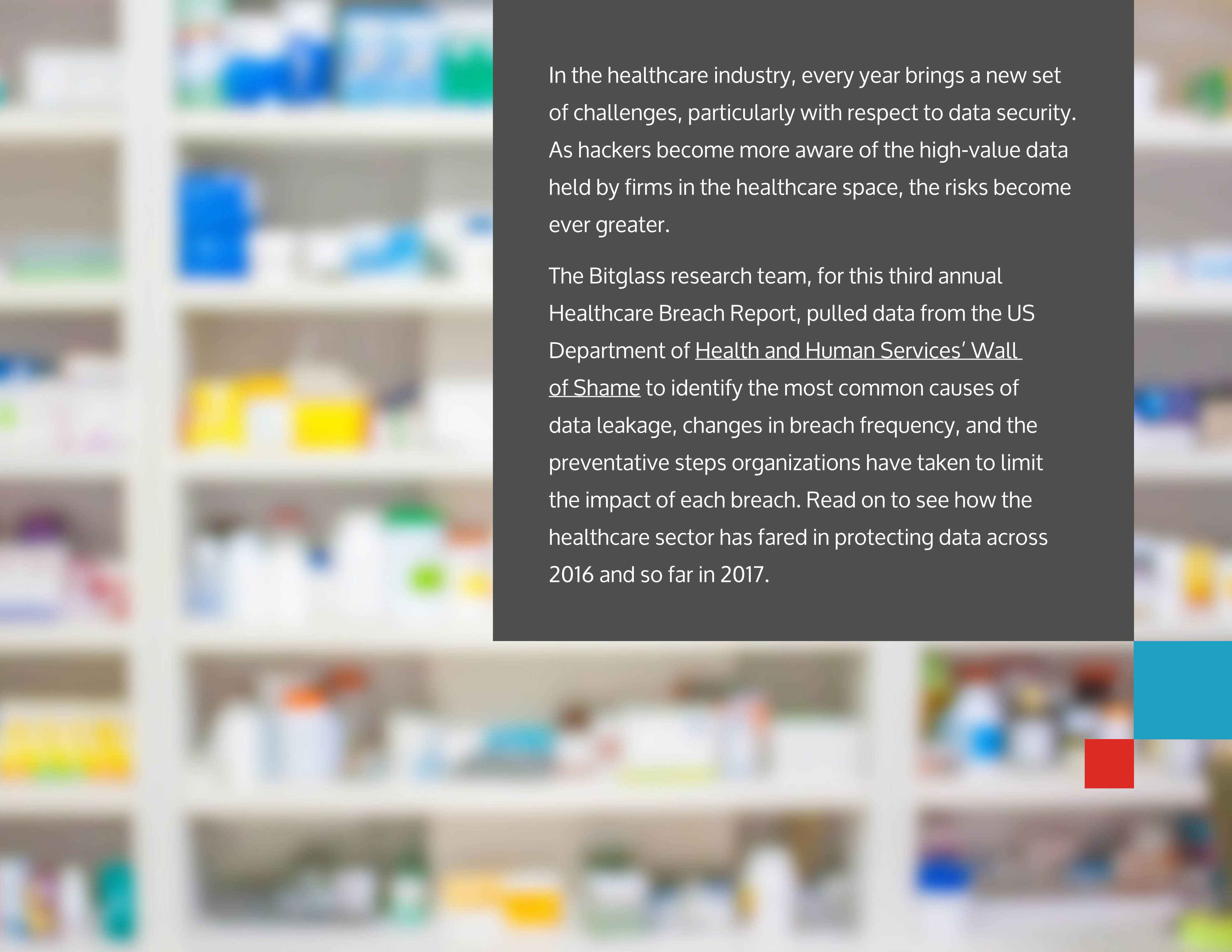
Healthcare Breach Report 2017

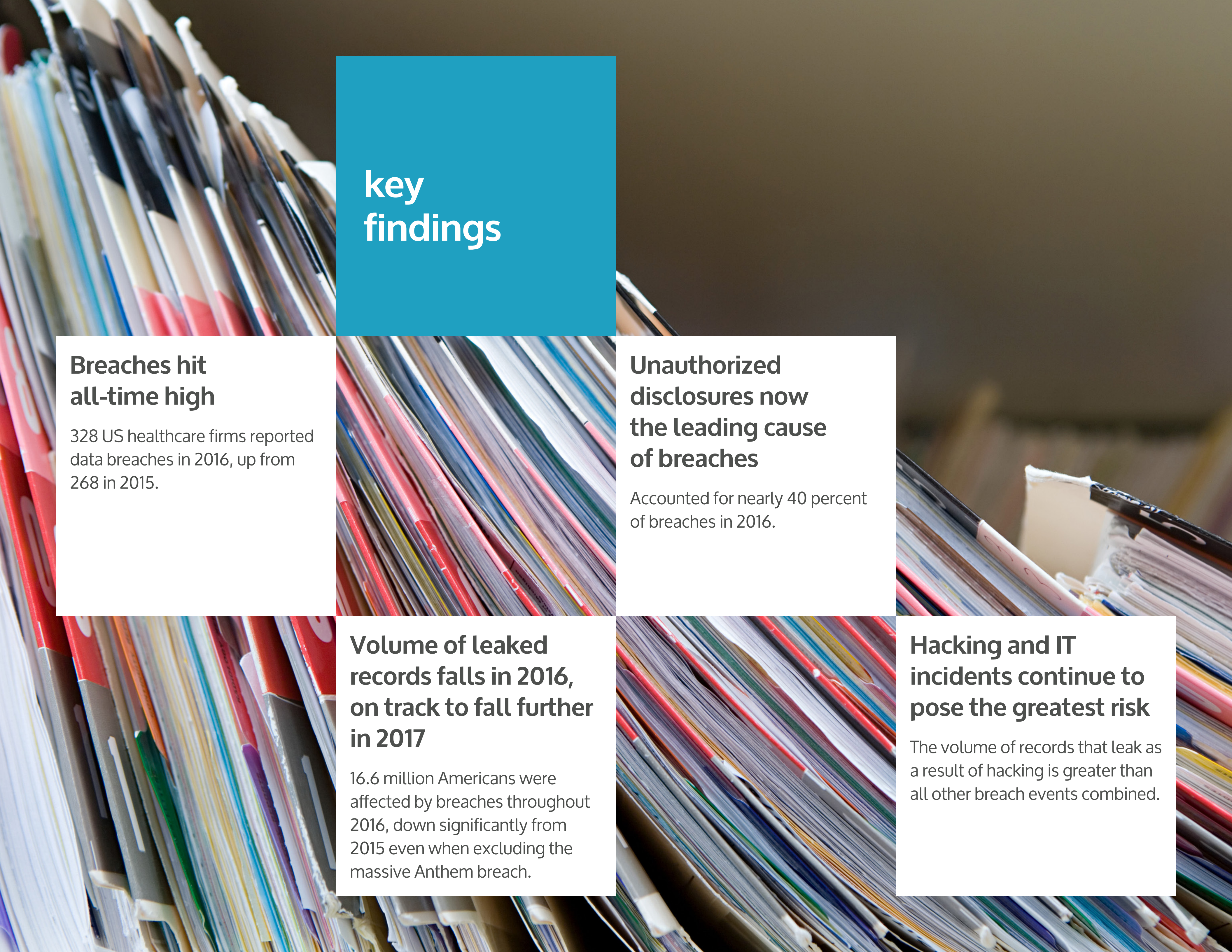
Is your data at rest or at risk?

bitglass



In the healthcare industry, every year brings a new set of challenges, particularly with respect to data security. As hackers become more aware of the high-value data held by firms in the healthcare space, the risks become ever greater.

The Bitglass research team, for this third annual Healthcare Breach Report, pulled data from the US Department of Health and Human Services' Wall of Shame to identify the most common causes of data leakage, changes in breach frequency, and the preventative steps organizations have taken to limit the impact of each breach. Read on to see how the healthcare sector has fared in protecting data across 2016 and so far in 2017.



key findings

Breaches hit all-time high

328 US healthcare firms reported data breaches in 2016, up from 268 in 2015.

Unauthorized disclosures now the leading cause of breaches

Accounted for nearly 40 percent of breaches in 2016.

Volume of leaked records falls in 2016, on track to fall further in 2017

16.6 million Americans were affected by breaches throughout 2016, down significantly from 2015 even when excluding the massive Anthem breach.

Hacking and IT incidents continue to pose the greatest risk

The volume of records that leak as a result of hacking is greater than all other breach events combined.

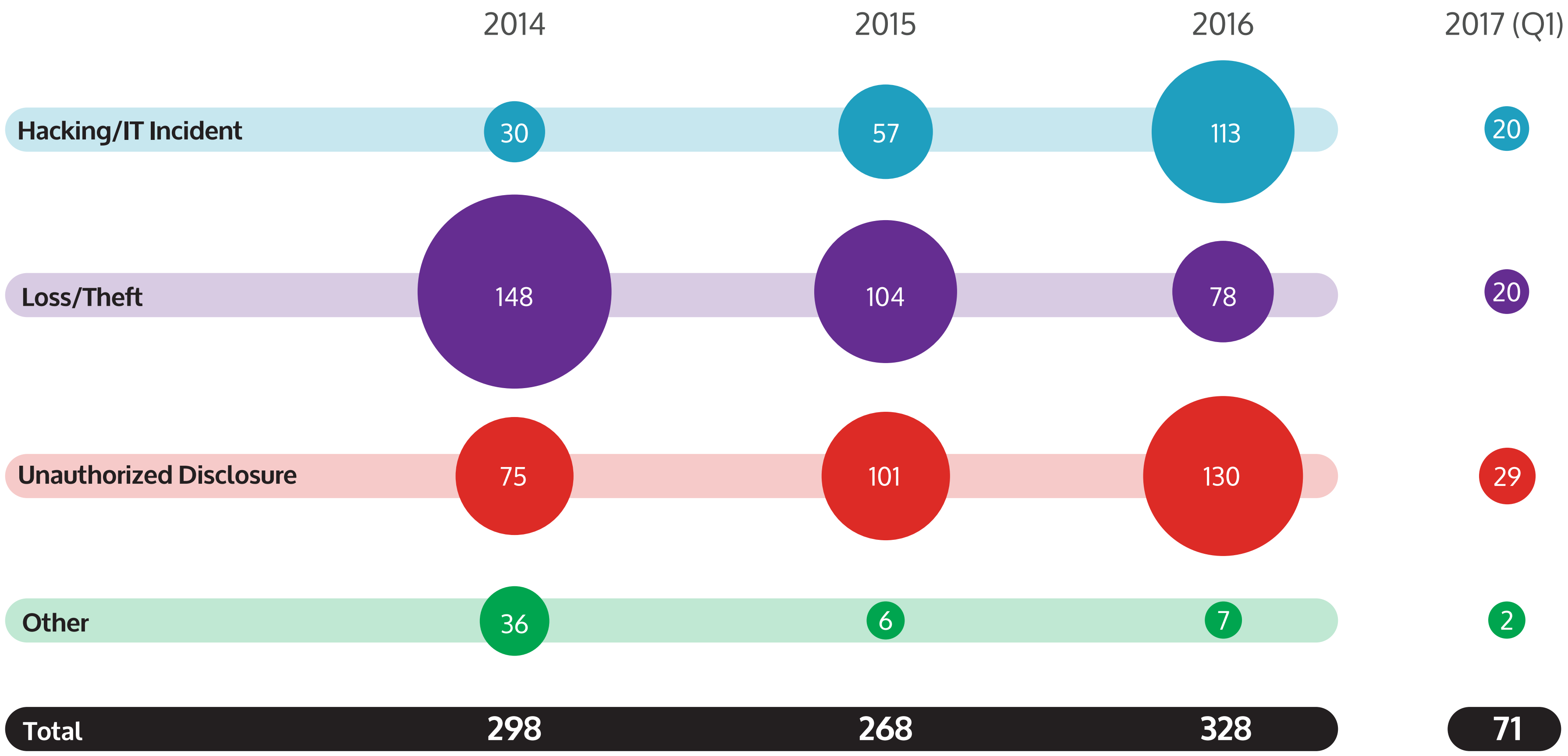
Has healthcare become a bigger target?

Through 2016, many organizations took steps to limit the impact of data breaches. While the total number of breaches has risen, fewer patients and clients were affected as organizations have fortified their defenses.

Unauthorized disclosures continue to tick up and are now the leading cause of breaches as data moves to cloud and mobile and as external sharing becomes easier. Unauthorized disclosures includes all non-privileged access to PII or PHI.

Hacking and IT-related incidents doubled year-over-year an indication that malicious actors are not letting up and are increasingly aware of PHI's high long-term value.

Number of breaches

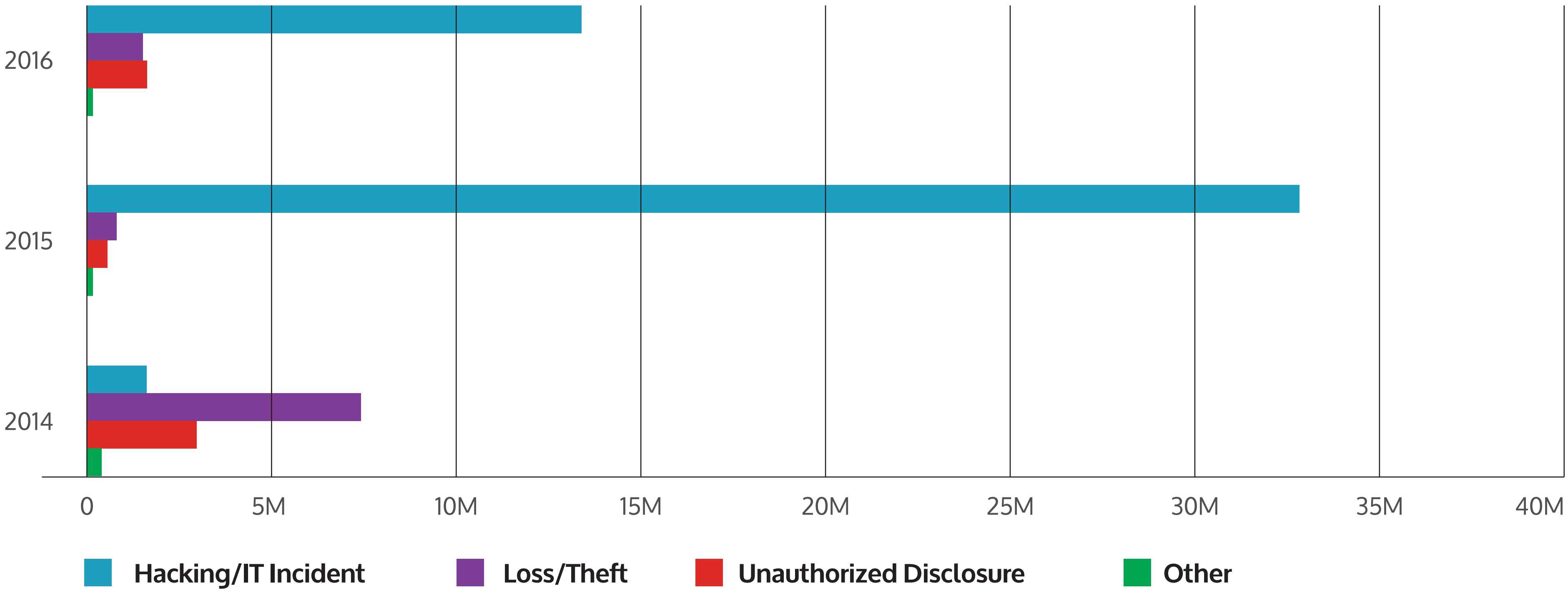


16.6 million Americans' records leaked in 2016, 1.5 million leaked so far in 2017.

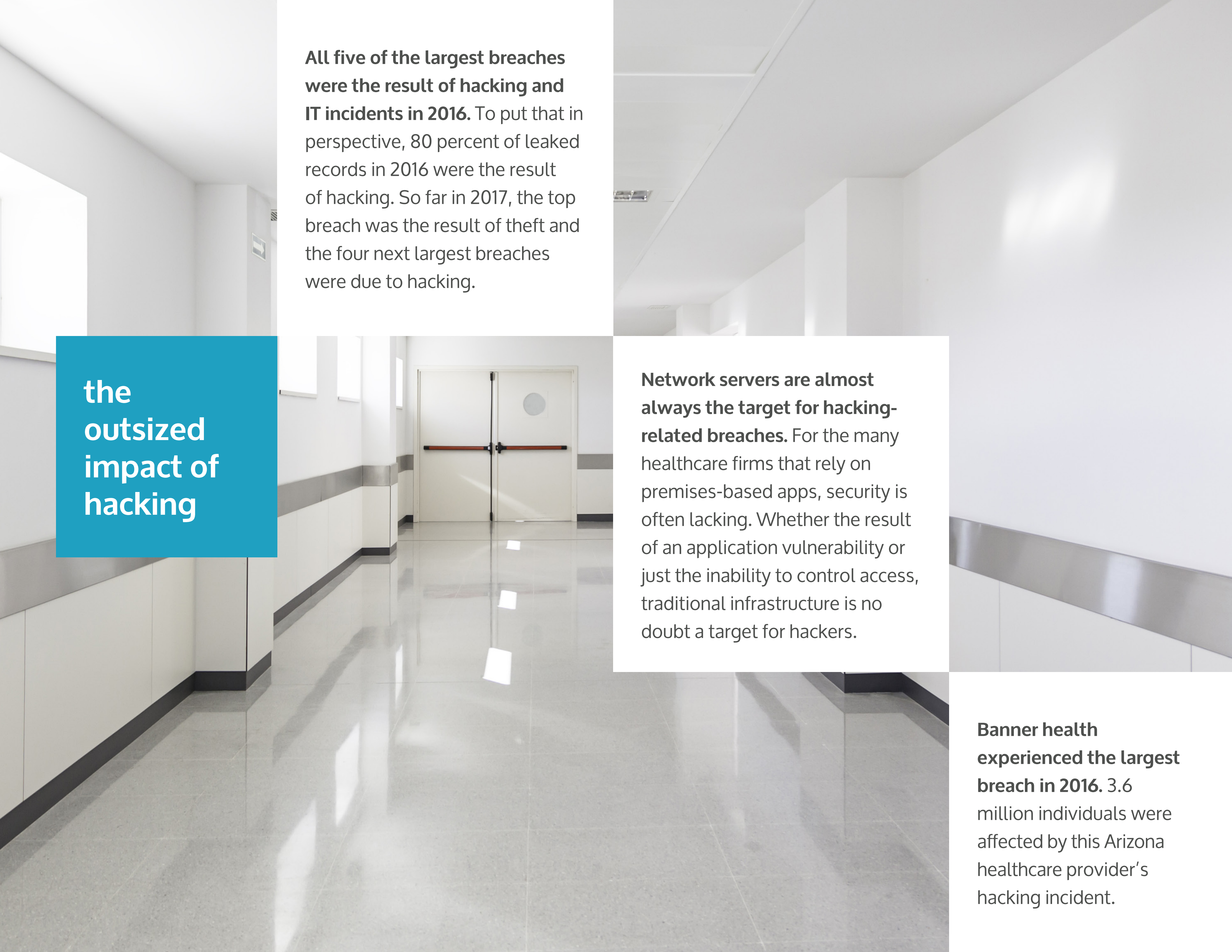
While the number of individuals affected fell dramatically from 2015 to 2016 and appears on track to fall again in 2017, healthcare firms are still a target and must stay one step ahead of malicious users and new workflows that threaten data security.

The Anthem breach that affected 78 million Americans skewed the numbers in 2015, but even if you exclude that outlier less than half as many customer records were leaked in 2016 as in 2015.

Individuals affected *



*This graph does not include the 78.8M individuals affected by the 2015 Anthem breach



the outsized impact of hacking

All five of the largest breaches were the result of hacking and IT incidents in 2016. To put that in perspective, 80 percent of leaked records in 2016 were the result of hacking. So far in 2017, the top breach was the result of theft and the four next largest breaches were due to hacking.

Network servers are almost always the target for hacking-related breaches. For the many healthcare firms that rely on premises-based apps, security is often lacking. Whether the result of an application vulnerability or just the inability to control access, traditional infrastructure is no doubt a target for hackers.

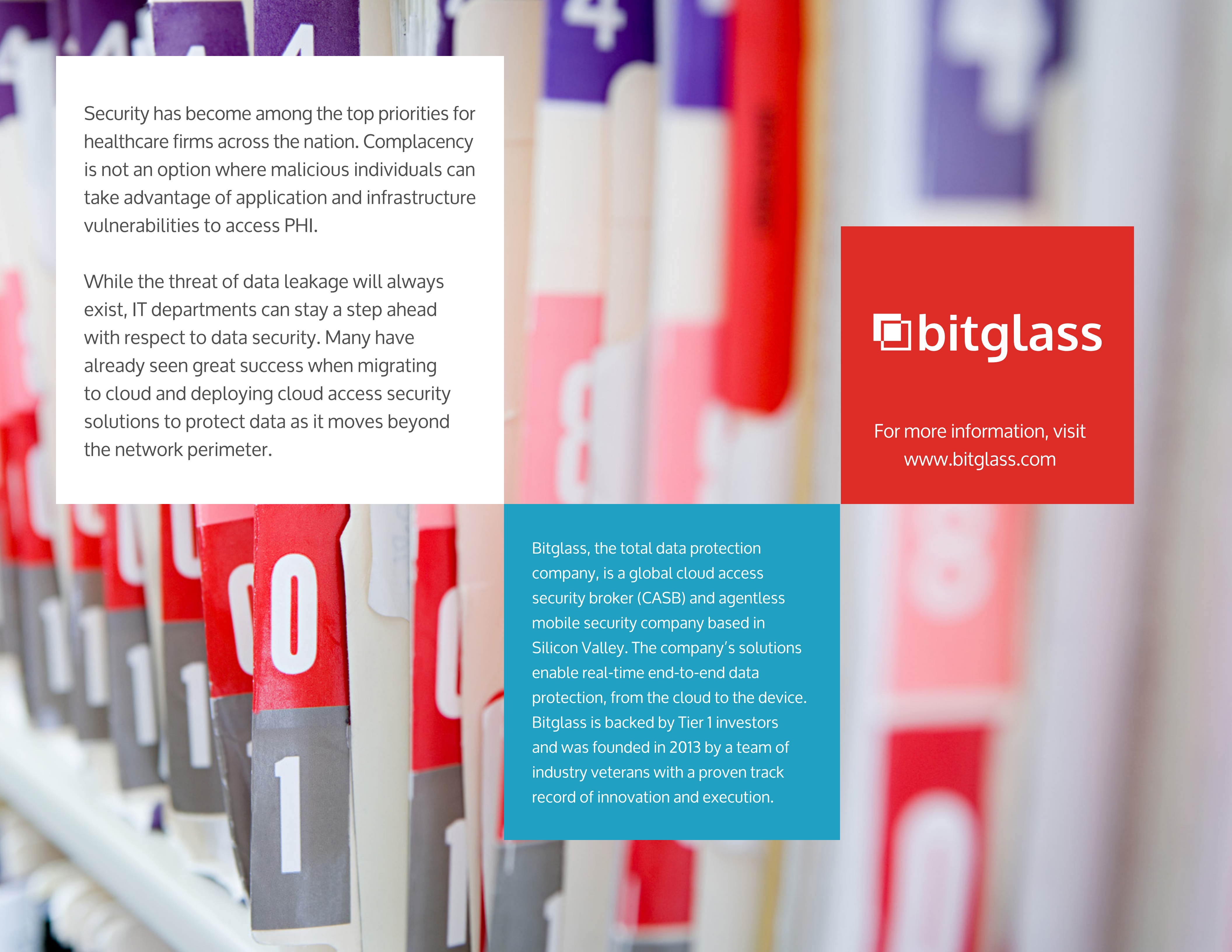
Banner health experienced the largest breach in 2016. 3.6 million individuals were affected by this Arizona healthcare provider's hacking incident.

breach costs hit record high

According to data from the Ponemon Institute, the average breach costs US companies $221 per lost record, up from $217 per record in 2015.

The cost per leaked record for healthcare firms topped $402 in 2016. A massive cost given the number of records lost as a result of each hacking-related breach.

Given the high value of healthcare data—Social Security numbers, treatment records, credit information, and more sensitive personal information—the cost of a breach to a hospital or health system can be devastating.



Security has become among the top priorities for healthcare firms across the nation. Complacency is not an option where malicious individuals can take advantage of application and infrastructure vulnerabilities to access PHI.

While the threat of data leakage will always exist, IT departments can stay a step ahead with respect to data security. Many have already seen great success when migrating to cloud and deploying cloud access security solutions to protect data as it moves beyond the network perimeter.

bitglass

For more information, visit
www.bitglass.com

Bitglass, the total data protection company, is a global cloud access security broker (CASB) and agentless mobile security company based in Silicon Valley. The company's solutions enable real-time end-to-end data protection, from the cloud to the device. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.