

INFOBRIEF

# Five ways to maximize in-flight data security

## Big Data Can Lead to Big Vulnerabilities

Securing data has become increasingly important, and for good reason. A recent survey found that 43 percent of responding companies experienced a data breach within the last year.<sup>1</sup> That figure was even higher for targeted industries such as healthcare, finance, government, and education.

These breaches are expensive; the same study reported that the average cost per record lost in a data breach in the U.S. was \$217—with a cost almost double that for a loss of healthcare records. The average number of records exposed per data breach is 28,000, which means a single data breach can cost millions, without even taking into account potential criminal prosecution or the resulting damage to an organization's reputation.

At the same time, network traffic flow is growing. Driven by the demands of web-scale applications such as video and other on-demand services, the network must be able to scale to handle higher capacities. As a result, organizations need both high-capacity bandwidth and a security strategy to protect all critical data, both at rest and in flight, as it travels across the globe over metro, regional, and long-haul networks.

Finding the balance between high capacity, high security, and simplicity and scalability is not easy. Here are five factors to consider when securing the network.

### 1. Use third-party-certified encryption technology

Encryption makes information unreadable to anyone except those who possess the correct key to decipher the message. There are many ways to encrypt data, defined by various standards that specify the encryption requirements of the supporting products and keys, and set a certification process for network equipment. Standards for encryption include Advanced Encryption Standard (AES), published by the National Institute of Standards and Technology (NIST) in U.S. Federal Information Processing Standard (FIPS) publications. These standards assure service providers and end-users that the encryption solution complies with the defined requirements by passing rigorous laboratory testing and reviews. Testing performed externally by a reputable third party provides further assurance that the encryption solution is reliable and secure.

Data Security with Optical Encryption  
Download infographic now



### 2. Secure all at-rest and in-flight data

Most organizations protect data at rest, securing servers, databases, routers, and switches by managing user access and credentialing. However, in today's web-scale networks, large amounts of critical data are in flight as high-bandwidth communications occur beyond the walls of the data center, traversing a larger, potentially worldwide network. A comprehensive IT security approach therefore must

<sup>1</sup> Ponemon, IBM study: Cost of a Data Breach 2015; <http://ibm.co/1MkF24s>