Enterprises today require the following: strong, scalable, and manageable authentication for protecting online identities. The rise of advanced persistent threats (APTs) and cyberespionage means that more sensitive business data (customer information, intellectual property, financial data, and more) is exposed. In fact, a modern smartphone provides an excellent platform for protecting identities, credentials, and data. In 2012, the number of data breaches increased 13.4% compared to 2011. In 2013, the number of data breaches had increased to 14.8%. The growth of this mobile workforce is driven by more than 1.3 billion workers worldwide, with 30% of large enterprises and 49% of small businesses now using BYOD policies. By the end of 2015, more than 75% of employees will be using their personal devices for work purposes, and 80% of employees say they will continue to use them even after they leave the workplace. Three-quarters of data breaches in 2012 were financially motivated cyberattacks. A single data breach costs on average $3.14 million, and the average cost of a small business data breach is $4.8 million. The cost of the average U.S. data breach is $5.4 million. The number of victims of cybercrime is increasing and, in 2013, 34,249 U.S. companies were victims of cybercrime. The average company spends over $400,000 per year on computer security, and 30% of small businesses allocate less than $1,000 per year to cyber defence. The average cost of a data breach in the U.S. is $3.14 million. The average cost of a small business data breach is $4.8 million. An increasing number of small businesses (23,833) are targeted by cybercriminals, and 65% have been targeted by cybercrime. Almost half (45%) of small businesses who have been attacked have been targeted more than once. The number of small businesses that suffered a data breach increased by 38% in 2013 compared to 2012. We are often careless and fall victim to thieves who are anticipating our predictable patterns. We use predictable patterns that thieves are aware of. We have a user-friendly experience that allows us to create easy-to-remember passwords and almost 38% of people surveyed would rather rely on a user-friendly experience than increased security. This is often a combination of the following: decreased effectiveness, user dissatisfaction, and an increased threat of phishing and social engineering. Symantec solutions have the features and capabilities to provide your enterprise with effective, scalable, and manageable 2FA solutions that are cost effective. According to research firm Gartner, almost half (45%) of enterprises today require the following: strong, scalable, and manageable authentication for protecting online identities. In 2012, the number of data breaches increased 13.4% compared to 2011. In 2013, the number of data breaches had increased to 14.8%. The growth of this mobile workforce is driven by more than 1.3 billion workers worldwide, with 30% of large enterprises and 49% of small businesses now using BYOD policies. By the end of 2015, more than 75% of employees will be using their personal devices for work purposes, and 80% of employees say they will continue to use them even after they leave the workplace.