Abstract

The changing landscape of the data protection industry has evolved from backing up data in order to recover from hardware and network failures, software bugs and human errors, to fighting a mounting wave of cybercrime. Over the years, hardware and software have significantly improved their reliability and resiliency levels. However, cybercrime has now become a bigger threat to data protection and the stakes are getting higher as anonymous individuals seek to profit from other's valuable digital data. With a cease-fire in the cybercrime war unlikely, we are witnessing *the convergence of data protection and cybersecurity* to counter rapidly growing cybercrime threats, including ransomware.

Cybercrime and Ransomware on the Rise

Though digital extortion is not new, the growing use of ransomware is the latest crypto-viral digital extortion technique that locks the system's screens by encrypting selected users' files unless a ransom or extortion fee is paid (typically into an anonymous bitcoin account) in exchange for the deciphering key. A ransomware attack typically begins when an end user clicks on a website link or opens a file attachment in a malicious email that is part of a phishing (random) or spear-phishing (targeted) campaign. Emails deliver over 60% of all malware infections and initially land on HDDs or SSDs -- but not on tape.

According to the findings in a report by Symantec Corp., hackers successfully stole or extorted an estimated $172 billion in 2017 with ransomware leading the way. Presently ransomware is growing unabated with over 4,000 attacks estimated daily. Nathan Thompson, CEO and founder of leading storage provider Spectra Logic, states in his recent book, Society's Genome, that "manufacturers of antivirus products have reservations about their ability to keep pace with this malware tidal wave". Thompson also states that "the aging power grid infrastructure in the United States is particularly vulnerable to cyber-