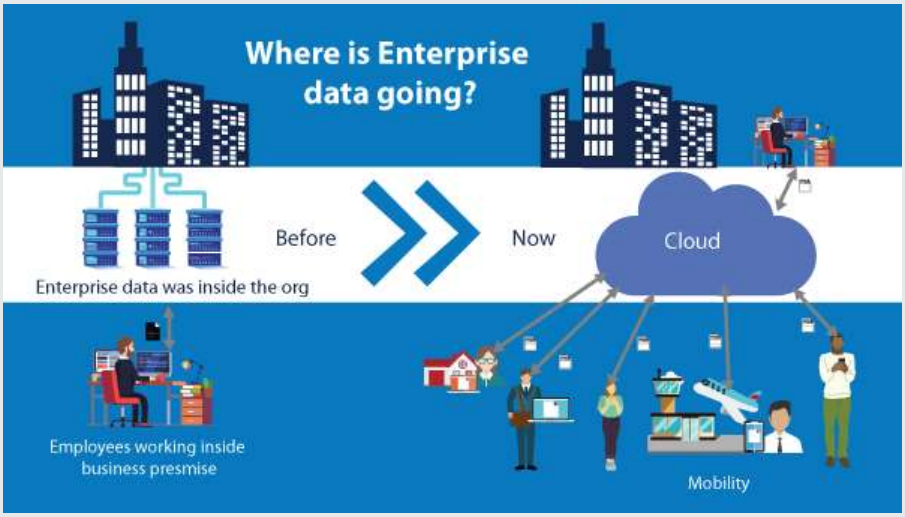
PARABLU

Ransomware is here to stay

In the last two decades, data has travelled from the constraints of flashy glass buildings that hold all information in one place, into the homes of every person. We carry our workplace in our pockets and backpacks. On-premise data has also made way for cloud computing to help businesses save money and time while solving problems at scale.

According to Gartner, by 2022, as a result of digital business projects, 75% of enterprise-generated data will be created and processed outside the traditional, centralized data centre or cloud, which is an increase from less than today's 10%.

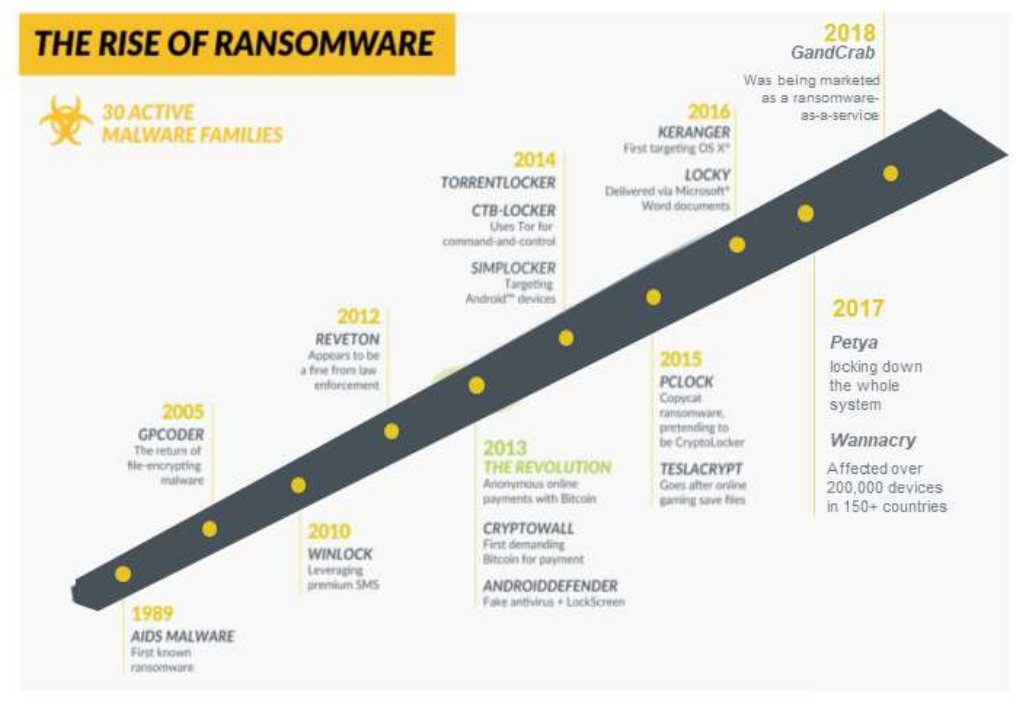
While this has meant a giant leap for organizations who strive to meet client requirements on the go, it has also opened up the threat surface of a typical organization to malicious actors. Loss of enterprise data could spell trouble in the form of expensive lawsuits and misuse of proprietary information.



The increased attack surface means a bigger target for malware authors to go after. They have re-doubled their efforts not just in attacking cloud repositories, but also endpoints where a lot of end-users and knowledge workers keep working sets of their data

Sadly, in spite of their best efforts, existing anti-malware solutions cannot be relied upon to detect and stop all malware. The quick moving malware underground ensures that anti-malware vendors are always playing catch-up

Organizations are evolving from the (now) archaic notion of data in secure data-centers to data "on-cloud" and data "on endpoints". But, the evolution in thinking to consider the security ramifications of this data shift has been slower than expected. There still seems to be a unhurried approach to security in several industry verticals, especially considering that ransomware damages alone might have costed the world more than $8 billion in 2018. This notion that security can be bolted on later, as an afterthought, has been costing organizations money in the form of losses due to phishing, ransomware and several other attack variants.



Ransomware has been the popular headline lately, giving even the Kardashians a serious run for their TRPs! Sonic wall reports that "There have been 181.5 million ransomware attacks year to date", and that was in the first six months of 2018 alone!

PARABLU

It's no surprise that ransomware is on the list of top concerns for Enterprise security. Ransomware is a form of malware that has existed for well over a decade, but has really taken on a visibly destructive form over the last couple of years. It operates by encrypting files on the infected computer and then demanding a bitcoin ransom in return for the decryption key.

While ransomware can attack any type of computer, in most cases, the infected computer is an end user's laptop or workstation. Therefore, any data stored on local disks, file shares and mapped network drives are vulnerable. Most popular cloud storage solutions also become vulnerable due to the replicative nature of their working. Since ransomware deletes the original files and replaces them with their encrypted versions, most cloud storage solutions faithfully replicate these changes in their repositories as well. While some of these solutions have file versioning capabilities, they don't usually have an option to perform a bulk restore of large amounts of data.

Ransomware accounts for 85% of all malware in the Healthcare sector making it the vertical with the highest incidents of ransomware attacks. With 750 incidents, and 536 with confirmed data disclosure in 2018, it would seem that the healthcare industry should be working harder at staying healthy!

This last year has definitely made many organizations sit up and take notice of the different ways their data can be misused and many are actively trying to defuse this oncoming threat. If you're an organization seeking to secure data on your end-points and are looking to learn about ways to combat ransomware, we have more coming your way. Watch this space!