Use Case

Ahsay Backup Software

as the Silver Bullet to Ransomware Attack

1 Executive Summary

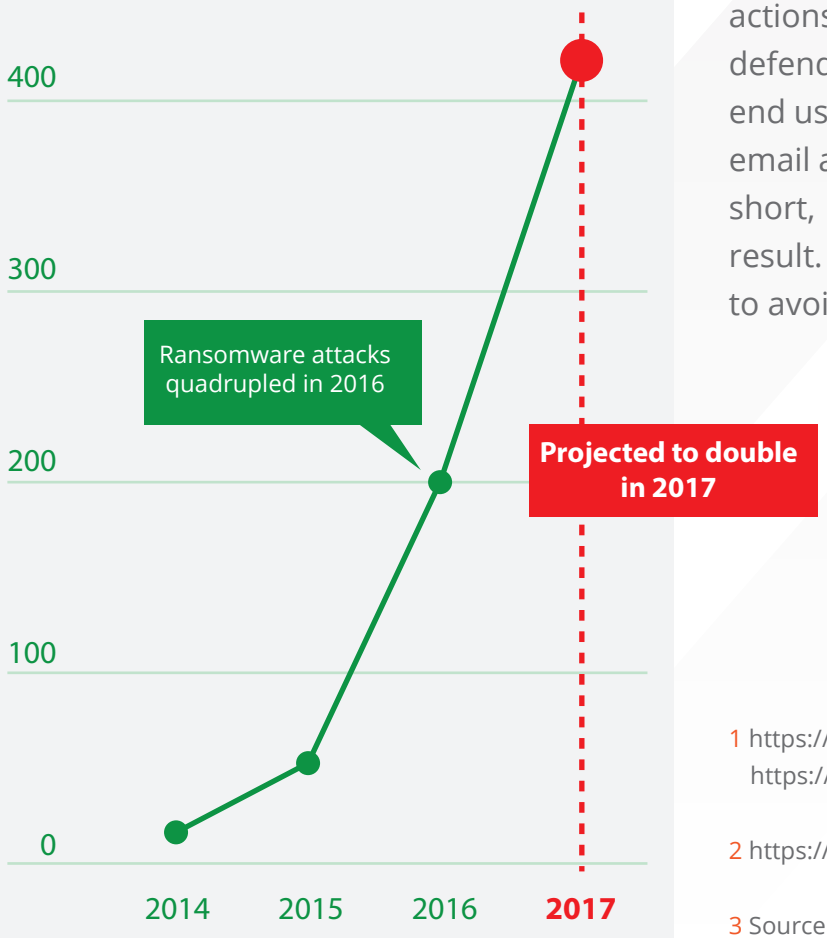
Ransomware is perhaps the most talked-about topic in the IT Industry. While IT Administrators can provision a high budget for tools to protect their environment with the best of breed preventive measures, a comprehensive backup strategy coupled with a cost-effective backup software will provide the protection required to effectively and quickly recover from a ransomware attack.

2

Trend in Ransomware

With the rising frequency of ransomware attack (with WannaCry[1] being the most recent attack at the time of this writing), IT Administrators need to take preventive actions to protect their environment. There are various tools in the market to defend your network but these tools fail to address the weakest link, which is the end user. In a recent report by Spiceworks[2] , Social Engineering Attack (e.g. phishing email attachment) is the second reason why ransomware is spreading so quickly. In short, spending a high budget on preventive measures may not yield the desired result. Instead, a speedy recovery on mission critical data is essential for enterprise to avoid ransomware attack.

Ransomware attacks are soaring [3]

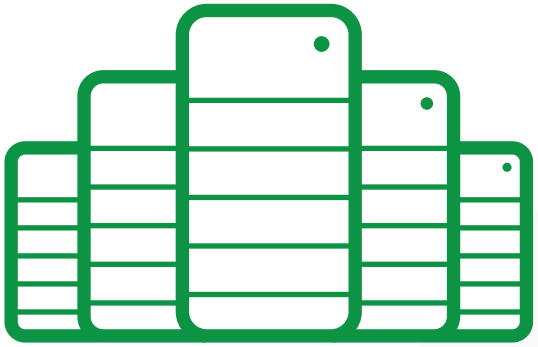


1 https://labsblog.f-secure.com/2017/05/13/wcry-knowns-and-unknowns/
https://www.ahsay.com/blog/2017/05/22/7-facts-about-wannacry-ransomware/

2 https://community.spiceworks.com/topic/1967355-2017-trends-in-ransomware-5-disturbing-predictions

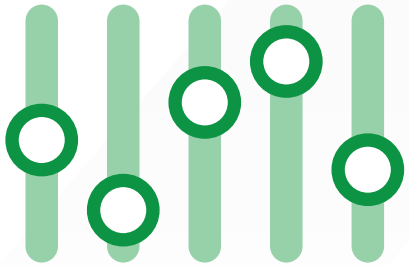
3 Source: https://www.beazley.com/news/2017/beazley_breach_insights_january_2017.html

3 Backup Strategy



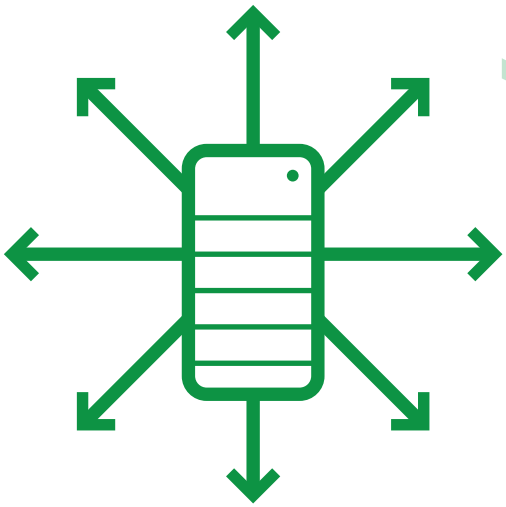
3.1 Centralized Servers for instant recovery

Daily backup of mission critical data resided in centralized servers is important to ensure the ongoing operation in case of ransomware attack. With the increasing processing power on a physical server, virtualization is a norm in the industry. Therefore, it is important that the backup software is equipped with instant recovery capability.



3.2 Company-wide backup policy

IT Administrators have minimal control on what the end user can work on their machines and therefore this is the weakest link. It is important that the IT administrator can control the backup of computers of individual users remotely and ensure any missed backup is caught in time and corrective action is taken.



3.3 Multiple Destination including Public Cloud Storage

While traditional backup software will back up data to one single destination, the contemporary ones should be equipped with the capability to back up to multiple backup destinations that include public cloud destinations if local regulations allow. By utilizing public cloud infrastructure, IT Administrators can provision storage in a low cost while maintain the elasticity for a robust storage.

3.4 Replication

In addition to standard backup that is stored in a centralized location, it is also important a replicate copy of the backup data is stored in a separate location to achieve better resilience in case the production backup server is attacked. Such replication should be carried out in near real time to ensure data integrity.

3.5 Reporting

While backup is conducted based on preset schedule, it is important that a comprehensive report is provided to ensure any exception or error is caught and corrective actions are taken to ensure data is intact.

4 Ahsay Backup Software

Ahsay Backup Software is a cost-effective backup solution with a centralized management console to allow IT Administrators full control of all endpoints in their network environment remotely. With the implementation of "VM Run Direct" in Version 7, user can restore their virtual machine within one minute[4] to minimize the downtime in case of cyber attacks. A full endpoint control down to individual user level ensures all laptops and personal computers are safeguarded. With the support of Microsoft, MacOS, and Linux/Unix environments together with common applications such as Microsoft Exchange, MS SQL, and MySQL, all client servers will be protected.

4 Based on Ahsay laboratory testing. Results may vary. Speed for Run Direct restore depends on factors such as VM size, network traffic, available CPU resource, free memory, disk I/O and number of delta.