What three things to know about Veritas Solutions for Ransomware?

Ransomware has quickly emerged as one of the most dangerous cyberthreats facing organisations today and is now a $30 Billion business for criminals. There is now an attack every 14 seconds, so organisations need to protect against the **Ransomware threat**, but also ensure they have a **Ransomware recovery plan**. Providing your customers with a Veritas solution, delivers the unified approach to data management that is needed.

This edition of What Three Things provides a simple perspective to the Veritas cross-portfolio approach to protecting, detecting and recovering from ransomware.

VERITAS™ Partner Force

1. Prevent – Protect your last line of defense - The Backup

We encourage customers to have the 3:2:1 strategy to ensure that they protect their last line of defense, the backup copy. 3:2:1 simply means that customers should keep 3 copies of their data in 2 different locations ensuring 1 copy is offsite and "air-gapped". Veritas provides the industry's best 'Ransomware Protected' data protection solution.

1. Veritas supports +150 storage locations, including Tape – which is an 'immutable' (cannot be altered) copy of data. Many of the new backup and recovery solutions on the market cannot support tape technology. In addition to tape support, Veritas Access is a great alternative for Long-term retention.
2. Veritas integrated backup appliances are unique in providing additional security hardening to protect against Ransomware infecting backup data
3. Veritas provides cross site replication that can be air-gapped for additional security with orchestrated recovery.

2. Detect Ransomware activity

It's important to detect ransomware infection activity as quickly as possible so that you can isolate the infection and take steps to remove it and recover. Veritas provides solutions that can help organisations detect ransomware quickly.

1. Veritas Information Studio and Veritas APTARE provide visibility to critical data and applications, this allows customers to protect these assets accordingly and prioritize the recovery process.
2. Data Insight provides early detection to Ransomware encryption activity.
3. APTARE and NetBackup can help report on unusual changes in data so that customers can investigate to see if the data has been infected.

3. Recover – Don't pay the ransom!

Ransomware attacks occur every 14 seconds, therefore there is no such thing as 100% safe. Recovering quickly after an infection is key so you do not need to negotiate with criminals! Veritas is the market leader in backup and recovery solutions and provide several ways in which organisations can recover data quickly and safely

1. Veritas Resiliency Platform (VRP) – provides single click recovery from a single system to a complete site. VRP integrated with NetBackup, VRP data movers and third-party array replication.
2. Veritas NetBackup provides Instant access to virtual machines and certain databases so that organisations have rapid access to their critical systems, whilst the recovery takes place in the background.
3. Veritas provides the ability to automate DR testing so that organizations can be confident that they can recover in the event of a ransomware infection.

Find our more information from the links below:

Link to the **Veritas Ransomware solutions page**

Ransomware **whitepaper**

Ransomware Marketing Campaigns – **Partner Marketing Centre**

VERITAS™ Partner Force