CONSTOR SOLUTIONS

DELL Technologies

Early Detection and Recovery from Ransomware Attacks

Every week a new cyberattack dominates the headlines. Organisations deploy the most advanced firewalls and real-time protection solutions, often engaging dozens of endpoint solutions at once. Clearly, these are not 100% effective. Attacks still happen and there must be a plan for when an attack penetrates the data centre so companies can quickly recover before significant damage and downtime occurs.

With companies supporting more and more users choosing to work remotely, IT networks and VPNs are vulnerable to attack.

The pain and suffering due to cyberattacks is growing. Why? It is all about the money, cyber criminals make a lot of it. It is estimated that high earners make up to £2 million annually, mid-level criminals make up to £900,000 and entry-level hackers make £42,000. They are highly motivated and well compensated.

Beyond launching their own cyberattacks, these criminals are expanding their business to include cyber-as-a- service, targeting corporate networks too. Cyber criminals are stealing sensitive data here and threatening to publish this data on the internet, they are asking for higher ransoms due to the increased exposure. The business of cyberattacks is not going away. In fact, it’s becoming more sophisticated and costly.

Most organisations are focused on security solutions at the edge. These solutions look to block or find malware before it can penetrate the firewall and inflict damage. Cyber criminals are circumventing them using new and advanced techniques to get into networks. These edge solutions are critical, but they are not enough.

What about disaster recovery solutions?
They are architected to backup user files, databases, critical infrastructure, etc. daily to ensure the content is available in case of a disaster. But how do you know the backup data is good? When did the attack start – last week, month or year? What data has been corrupted? What about attacks that destroy backup catalogues? Disaster recovery needs to be extended to support cyber recovery.

Introducing CyberSense

CyberSense from Dell Technologies detects signs of data corruption in backup images using a patented, unique technology that directly indexes data in backup images without the need for the original software. CyberSense supports disk-based and tape-based backup images created using Dell EMC Networker/Avamar, Veritas NetBackup, IBM Spectrum Protect/TSM, and Commvault and additional formats. As backups are scanned, CyberSense checks the integrity of the files, databases, and even critical rebuild materials (AD, DNS, LDAP, etc.)

CyberSense has two unique use cases. Proactively, with existing data protection software, CyberSense analyses data in backups to identify files and databases that have been unknowingly corrupted by ransomware. If it has, an email with pertinent information is sent. CyberSense detects corruption utilising a combination of full-content-based analytics and machine learning. CyberSense analytics are indicative of all common attack vectors including entropy changes, known ransomware extensions, data corruption and deletion, and over 100 other statistics.

If an attack occurs within an organisation that was not actively running CyberSense, it can also be implemented post attack. CyberSense leverages its machine learning and forensic tools to diagnose and recover quickly with less downtime and no need for a clean room. Using a corrupted and pre-attack backup image, CyberSense can go back in time and create a view into how the data has changed. This includes reports on files that were impacted so they can be replaced with the last known good version, the type of attack vector, and with analysis of event logs the specific users accounts and executables or malware that performed the attack.

CyberSense is designed to stay ahead of today's cyber criminals. CyberSense can help you determine when an attack occurs, the breadth of the attack, and how to recover quickly. With CyberSense attacks can be detected quickly and recovery can turn a process that typically takes weeks and months down to hours and days.

Contact Constor Solutions today and discover how CyberSense is the ideal choice to protect your companies data.

CONSTOR SOLUTIONS

Tel: +44 (0) 20 3004 8446
Email: info@constor.co.uk
86-90 Paul Street, London, EC2A 4NE

DELL Technologies
PLATINUM PARTNER

Dell EMC Service Delivery Partner of the Year 2018