

What Is L.O.C.S

~ and ~

Why Do You Need It?

This is the year of ransomware. And it is proving to be seriously profitable. Ransomware has quickly become the most lucrative type of malware ever seen. The FBI has said ransomware is on the way to becoming a \$1 billion annual market. Research shows that a single ransomware campaign can generate up to \$60 million annually. Attackers have the funds and the desire to continue innovating ransomware strands that will become far more virulent. We believe that ransomware will become more capable of self-propagating, with the aim of locking up vast swaths of corporate networks. That would effectively knock corporate IT functionality back to the 1970s. Current responses to ransomware tend to revolve around single point products. We must consider bringing a more architectural approach to bear given the various vectors that ransomware targets. This solution overview addresses the various vectors and methods that attackers use if this attack was triggered internally or externally.

Defenders must:

- Secure their backups as these will be infected
- Prevent lateral movement of ransomware should an infection occur
- Have a robust High Availability Solution not just a failover

L.O.C.S assists Companies in a event of a internal or external Ransomware attack, in 6 areas

L.O.C.S.

1



LOCATES

Granular filtering targets and Contain ransomware in worst-case scenarios should it enter the network

2



Organizes

Setup, Management, Implementation, Migrations, Sizing, Support 7 x 24, High Availability.

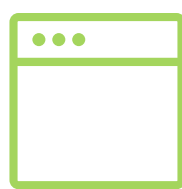
3



Controls

Analyzes streams in real time and Manipulates the attack surface enforcing good behaviour.

4



Secures

Physical security personal, IP-DVR cameras, Biometric Scanners, Mantraps, locking cages & cabinets, DDoS. and Compliance

5



Stores

Metro-scale and Geo-Archive storage distribution amongst multiple datacenters using a unique Network Connected Error Connection Code with high efficiency and resilience.

Key capabilities:

- Block ransomware from getting into the network
- Contain ransomware in worst-case scenarios should it enter the network
- Have a high availability network on standby

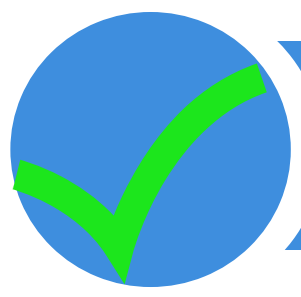
6



Cost Less

Use this High Availability solution to safe guard your data. You also have the ability to use this as a Test/Dev, or simple reduce your current hosting costs.

Contact us for a Free Trail



800-272-4309
THREATREMOVAL@braintreegroup.com

SOURCES

<http://www.braintreegroup.com/business-continuity>

CREATED BY

The Braintree Group

info@braintreegroup.com

1-800-272-4309

