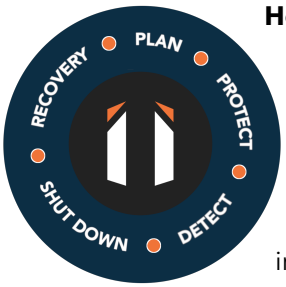
ORIIUM

Why businesses need a ransomware 'bubble'

Ransomware attacks have increased in both volume and sophistication since the COVID outbreak and organisations often overlook a critical aspect; these ever-evolving threats can, and do, target backup data as well as production data sets. The often adopted approach to mitigate this risk is to keep data stored offline on removable tape or disk, however this approach also carries risk of a different sort.

By adopting an offline data approach organisations swap the data breach risk with severely degraded data access, governance or compliance headaches and significant management costs. The associated management overhead to conduct removable media backups is more often than not detrimental to organisations IT budget and productivity. Costs include the manual labour required to move media, recording and cataloguing media whereabouts and expensive third party storage costs. Perhaps the highest price paid though, is that the business creates huge barriers to access, audit or control their data on demand. For most organisations this is not an acceptable trade off and simply isn't necessary with the right solution adoption.



How to mitigate ransomware efficiently and effectively in 5 simple steps

By adopting truly modern data protection technology and strategies, real time ransomware detection, and coupling this with a data isolation and rapid recovery capability, it is possible for organisations to have their cake and eat it. Achieving data security confidently with the convenience of instant access to data and no associated management burden. This is a perfect illustration of how cloud solutions benefit businesses in the modern era.

1) Plan: Always have a plan. 2020 has taught us all, that business continuity preparation, planning and testing is required universally. Whilst at times it may seem like a horror movie the current situation isn't sci-fi or scaremongering on social media. Organisations have a duty to their shareholders to be prepared for all scenarios, and taking action to ensure that DR and business continuity plans are robust is the first step. This includes regular system restores and DR invocation testing. How quickly could your business recover in a systems wide attack or DR scenario?

2) Protect: ORIIUM's Cloud Store security model protects data and works in the same way as offline protection. Permanently replicated data is held in an 'air gap' and provides instant customer access and disaster recovery invocation using Commvault Live Sync technology. This allows customers to instantly 'spin up' Virtual Machines in a location of their choice, including separately hosted virtualised infrastructure or public cloud such as Microsoft Azure / Amazon AWS in the event of an attack.

3) Detect ransomware attacks: ORIIUM baselines what "normal" looks like in your organisation and monitors for any variance. This means change rates can be used to detect abnormal behaviour, trace the anomaly and report instantly.

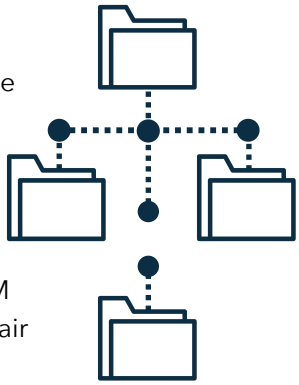
4) Shut down: In the event of a live attack, ORIIUM can trigger intelligent workflow and actions to shut down key systems and prevent further damage or infiltration. These flexible automation mechanisms can be employed to isolate and contain compromised data. By shutting systems down or disabling network access, the spread of ransomware throughout an estate can be prevented.

5) Recovery: Initiate rapid data and systems restoration from the air gapped Cloud Store environment. Perform instant recovery of Virtual Machines using Commvault Live Mount technology, which involves spinning up a Virtual Machine from backup data in order to make it instantly accessible. This process is much quicker and simpler compared with restoring data block by block in the absence of a Disaster Recovery solution.

Offline standard security – in the cloud

ORIIUM Cloud Store provides the 'best of both worlds' by employing modern threat protection at all levels. All data stored in our cloud is striped in a proprietary format, encrypted at source for transmission and at rest when stored. These measures ensure that any other application, or interception, such as ransomware, cannot read customer data. The solution contains multiple security layers with orchestration adopting a broad range of security technologies and platform hardening.

Air gap



An air gap data storage strategy means ensuring that at any given time, one copy of a company's data is completely disconnected from any network and cannot be accessed externally. If the data or systems have no connection to the Internet or networks, it cannot be remotely accessed, hacked or corrupted. This solution is unlike most cloud target backup technologies which require permanent connectivity and security considerations to ensure they cannot be infiltrated.

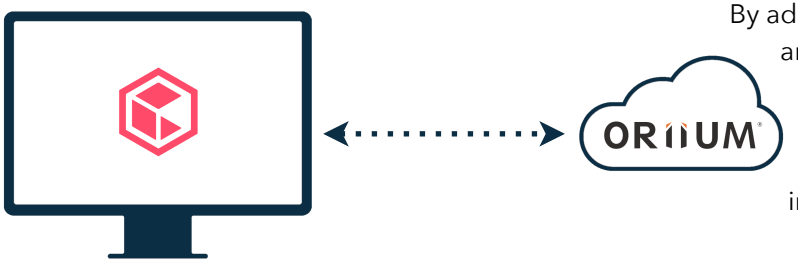
To ensure reliable backup and recovery, ORIIUM adopts the National Cyber Security Centre's 3-2-1 backup plan. The "1" is a copy of your data that is stored offsite in the ORIIUM cloud and is only accessible via encrypted, application driven tunnels. This creates a virtual air gap and is tamper proof from external threats with continuous replication producing two offsite copies adding an extra layer of protection.

Secure Multi-Tenancy

The ORIIUM Cloud is a secure multi-tenant environment, providing an isolated Virtual Cloud for each customer with complete isolation of customer metadata, backup data and network traffic.

At-rest data is encrypted using a 256-bit Encryption Key, used in conjunction with a 256-bit Key-Encrypting Key (KEK). This allows encryption keys to be secured within a customer's domain and gives them control over who has access to their data. In the event of a ransomware attack, these keys can be removed in order to prevent access to the data.

Data-in-transit also adopts robust encryption en route between Customer environments and the ORIIUM Cloud. Encrypted tunnels are used to authenticate and protect all data in transit using TLS and a 256bit cipher suite. With this approach, data is protected at all stages and IT teams can be confident that encryption keys and access to data is fully secure.



By adopting this approach to security and this solution architecture, ORIIUM Cloud Store Customers are able to benefit from an always available, offline data environment. No more removable media, no more media management overhead and instant access to critical business data.

Learn more at https://www.oriium.com/data/storage/commvault-storage/

Email: partner.sales@oriium.com

Tel: 0800 021 6555

CLOUD STORE
DESIGNED FOR