Modern Datacenter | Security Offerings

1. **Identity and Access Management** should provide controls for assured identities and access management. Identity and access management includes people, processes and systems that are used to manage access to enterprise resources by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution. Redapt focuses on Microsoft Active Directory (including Azure AD)

2. **Data Loss Prevention** is the monitoring, protecting and verifying the security of data at rest, in motion and in use in the cloud and on-premises. Within the cloud, data loss prevention services could be offered as something that is provided as part of the build, such that all servers built for that client get the data loss prevention software installed with an agreed set of rules deployed.

3. **Web Security** is real-time protection offered through software/appliance installation or via cloud native tools. This provides an added layer of protection on top of things like AV to prevent malware from entering the enterprise via activities such as web browsing. Policy rules around the types of web access and the times this is acceptable also can be enforced via these web security technologies. These tools are sometime called layer 7 or next generation firewalls

4. **E-mail Security** should provide control over inbound and outbound e-mail, thereby protecting the organization from phishing and malicious attachments, enforcing corporate policies such as acceptable use and spam and providing business continuity options. The solution should allow for policy-based encryption of e-mails as well as integrating with various e-mail server offerings. Digital signatures enabling identification and non-repudiation are features of many cloud e-mail security solutions.

5. **Security Assessments** are audits of cloud services or assessments of on-premises systems based on industry standards. Traditional security assessments for infrastructure and applications and compliance audits are well defined and supported by multiple standards such as NIST, ISO and CIS. Redapt used Rapid7 and other tools to provide these services one time or on a reoccurring basis.

    Cloud Security Audit
    Cloud Security Assessment
    Cloud Security Governance

Redapt, Inc.
14051 NE 200th Street
Woodinville, WA 98072
redapt.com

6. **Intrusion Management** is the process of using pattern recognition to detect and react to statistically unusual events. This may include reconfiguring system components in real time to stop/prevent an intrusion. The methods of intrusion detection, prevention and response in physical environments are mature; however, implementing these in the cloud and leveraging cloud native capabilities can be more complex.

7. **Security Information and Event Management** systems accept log and event information. This information is then correlated and analyzed to provide real-time reporting and alerting on incidents/events that may require intervention. The logs are likely to be kept in a manner that prevents tampering to enable their use as evidence in any investigations.

8. **Encryption** systems typically consist of algorithms that are computationally difficult or infeasible to break, along with the processes and procedures to manage encryption and decryption, hashing, digital signatures, certificate generation and renewal and key exchange. Key vaulting services can be implemented in the cloud to allow more widespread use within the environment with little upfront costs.

9. **Business Continuity and Disaster Recovery** are the measures designed and implemented to ensure operational resiliency in the event of any service interruptions. Business continuity and disaster recovery provides flexible and reliable failover for required services in the event of any service interruptions, including those caused by natural or man-made disasters or disruptions. Cloud-centric business continuity and disaster recovery tools make use of the cloud's flexibility to minimize cost and maximize benefits. Good hygiene in BCDR practices will allow for recovery from ransomware attacks that are on the rise.

10. **Network Security** consists of security services that allocate access, distribute, monitor and protect the underlying resource services. Architecturally, network security provides services that address security controls at the network level Redapt always deploys best practices around “assume breach” architecture with every migration and disaster recovery project. This can be accomplished with cloud native and 3rd party tools.

Redapt, Inc.
14051 NE 200th Street
Woodinville, WA 98072
redapt.com