Exponent®

THOUGHT LEADERSHIP

PUBLISHED 4Q 2019

Data Loss Prevention Strategies in the Era of the Cloud

December 17, 2019

Data loss prevention (DLP) is a broad term that refers to various aspects of data security, ranging from ensuring that data is properly stored without allowing unauthorized access, to preventing end users from transmitting sensitive or confidential data outside of an authorized network.[1] The goal of any typical DLP strategy is to establish secure systems and data practices so that users can access the data they need without compromising data security.[2]

A DLP strategy is often most effective when created based on the unique data needs of an organization. Unfortunately, due to the perceived complexity of DLP systems and policies, some organizations either may forgo DLP altogether or adopt an approach that is not bespoke to its situation and usage requirements. Implementing DLP in the era of the cloud requires numerous important considerations, including public versus private clouds, options for cloud encryption, and the role of cloud access security brokers.

Benefits of Cloud-Based Storage

Many organizations assume that storing data on its own network is more secure than using cloud-based storage; however, when incorporated properly into an appropriate DLP approach, cloud-based storage and services offer many benefits to an organization and can result in increased data security. Major cloud-service providers dedicate significant resources to maintaining their networks and servers, including teams of security engineers able to respond to the latest cyber threats. If an organization properly restricts access to its cloud, cloud-based resources can be more secure than an organization's on-premise resources that may be accidently misconfigured or may lack the latest security patches.[3]

Secure Design and Public vs. Private Clouds

Once an organization decides to replace in-house data storage and computing assets with cloud-based storage and computing, it will need to pick up the appropriate cloud models and configure them. One crucial decision is whether to set up a private cloud, use a public cloud service, or use a hybrid cloud approach. The best choice for an organization depends on its computational needs, security policies, and available budget.

As public clouds are hosted at vendor facilities, organizations who go this route can likely avoid investment in hardware or hardware maintenance. Organizations can quickly scale hardware to add more resources and are billed based on usage. Vendors typically host services for many

[1] https://whatis.techtarget.com/definition/data-loss-prevention-DLP and https://www.skyhighnetworks.com/cloud-security-blog/how-data-loss-prevention-dlp-technology-works/

[2] https://www.techradar.com/best/best-data-loss-prevention-service

[3] https://info.acloud.guru/resources/the-role-of-the-cloud-in-preventing-data-breaches

different organizations on the same hardware via virtual machines. The hypervisor software used to launch virtual machines and other software-based network components are supposed to segment and isolate the virtual machines. However, if the cloud vendor is attacked via a weakness in the hypervisor software, a data leak may occur between virtual machines. Moreover, organizations may lack control over the security policies of the physical systems used in a public cloud.[4]

In part due to these security challenges, organizations often opt for private clouds. Private clouds can be either on-premise or hosted. In an on-premise cloud, organizations own and maintain their own hardware. Such a cloud configuration provides an organization with complete control over security policies and data location. However, an on-premise cloud makes for a significant investment. Moreover, such clouds are not easily scalable and can suffer from security issues if not properly configured or regularly updated.

A private cloud can be hosted at vendor data centers where the vendor performs maintenance and timely updates, yet organizations have their own dedicated hardware. Compared to an on-premise private cloud, a hosted private cloud is generally considered less expensive and can be scaled more easily to handle user demand. Various vendors also offer "secure by design" default configurations that can lead to more secure services. The biggest challenge of a hosted private cloud is that the systems are not physically inside the organization perimeter and are managed by a third party, which may not be permitted by the organization's business policies or compliance requirements.[5]

Options for Cloud Encryption

Data encryption can help ensure data security in any type of cloud. Encryption scrambles content to make it effectively indecipherable without an encryption key. Cloud vendors offer a variety of options for cloud encryption and key management.[6] Similar to cloud selection, the best choice for an organization depends on its computational needs, security policies, and available budget.

One option is volume-based encryption, a process that encrypts data while the storage volume is unmounted or offline. When the volume is online, only authenticated users can access the data. This technology is generally more difficult to implement in a public cloud and is usually used for private clouds.

A second encryption option is application-specific encryption. This option encrypts data attached to the application and ensures that data can be accessed only by authorized users. The application itself is responsible for securely sharing the data across different cloud platforms.

A third option is file-based encryption, the encryption of individual files. This is the most flexible form of encryption that fits all cloud models. Encryption can be applied to files from within an organization and then uploaded to the cloud. Organizations can manage their keys either internally or via a third-party provider.

The Role of Cloud Access Security Brokers

Cloud access security brokers ("CASBs") are an important component of an organization's interface to a public cloud or hosted private cloud. CASBs examine network traffic to cloud services to ensure that data sharing is limited to approved cloud resources and that only approved devices can access the cloud services. CASBs also ensure that data is encrypted while in-flight and at rest (as designated by policy); that confidential information is de-identified or prevented from transferring to public clouds; and that an organization is alerted to security events.

CASBs can be implemented using a proxy server or an application programming interface (API). Proxies can take security action in real time, but they generally do not scale well, can cause significant delays, and can only secure known users who are communicating to cloud services via proxy. Alternatively, API-based CASBs are fully integrated with the cloud service and secure access to cloud resources from any device without impacting network performance. Because API-based CASBs are fully integrated with the cloud rather than being an isolated gatekeeper like proxy-based CASBs, they are better equipped to learn from cloud activity and provide enhanced security.[7]

contact informantion on next page

[4] https://www.datamation.com/cloud-computing/private-vs-public-cloud.html and https://www.ibm.com/blogs/cloud-computing/2013/07/29/how-your-data-leaks-from-a-virtual-machine/
[5] https://www.datamation.com/cloud-computing/private-vs-public-cloud.html
[6] https://digitalguardian.com/blog/what-cloud-encryption
[7] https://managedmethods.com/blog/api-vs-proxy-casb-which-is-right-for-you/

Exponent's Expertise

Exponent's multi-disciplinary team of electrical engineers and computer scientists have expertise in computer networks, computer security, and machine learning. We can help organizations build DLP strategies and select the cloud models, encryption options, and CASBs best suited to their computational needs, security policies, and budgets.

Brian D'Andrade, Ph.D., P.E.
Electrical Engineering & Computer Science
Principal Engineer
Bowie
(301) 291-2559
bdandrade@exponent.com

Sonal Kothari Phan, Ph.D., P.E.
Electrical Engineering & Computer Science
Managing Engineer
Atlanta
(678) 412-4824
skothari@exponent.com

Matthew Pooley, Ph.D.
Electrical Engineering & Computer Science
Managing Scientist
New York
(212) 895-8146
mpooley@exponent.com

Exponent Office Locations
Alexandria, Atlanta, Austin, Bowie, Chicago, Denver, Detroit, Houston, Irvine, Los Angeles, Maynard, Menlo Park, Miami, Natick, New York, Oakland, Pasadena, Philadelphia, Phoenix, Sacramento, Seattle, Warrenville, Washington D.C.

International Offices:
Basel, Switzerland; Derby, Harrogate and London, UK; Düsseldorf, Germany; Shanghai and Hong Kong, China; Singapore