DATA LOSS PREVENTION

STRATEGY CHECKLIST

FILECLOUD

WWW.GETFILECLOUD.COM

Executive Summary

"FileCloud enables data infrastructure modernization scenarios, thanks to its flexible cloud implementation, backup and disaster recovery support"

Gartner magic quadrant report

"FileCloud is deployable in a private cloud (FileCloud Server), a public cloud (FileCloud Online) and hybrid architectures. Organizations can choose to implement FileCloud on public cloud infrastructure, such as that of AWS and Microsoft Azure, or private data centers."

Gartner magic quadrant report

The start of the digital revolution was solidified by the radical shift in the way information is moved and stored within organizations. In today's complex digital world, communication within the enterprise takes place in a more agile way. However, this new digitalized business environment is exposed to advanced threats on top of evolving regulatory compliance controls. The thought of losing confidential, critical, or highly restricted data strikes fear into the heart of businesses, large and small alike, and with good reason. Data loss and the resulting downtime can have severe ramifications on an enterprise's finance and operations. To address this looming fear, a security concept known as Data Loss Prevention (DLP) has evolved.

The DLP market is not new in any way, shape, or form. It has evolved to include advanced threat protection, cloud functionality, and managed services among other things. All this advanced protections combined with the upward trend in data breaches has seen a prodigious uptick in DLP adoption as a way of securing sensitive data. Despite the fact that DLP ties into other facets of data security, it remains a crucial part of comprehensive data-centric security. DLP technologies are designed to perform both contextual analysis and content inspection in order to prevent the loss of data. These technologies rely on rules that look for sensitive information included in electronic communication. They can be used to discover personally identifiable information (PII) within your environment, from phone numbers and names to credit card numbers and social security numbers. They can also identify Intellectual Property (IP), end encrypt or block any attempts to copy, print, or email this sensitive data.

The Threat is Real

As companies continually rely on bits and bytes, the value of data rises. Lost data directly translates to expensive downtime, lost productivity, and long-term damage to reputations. Additionally, there are costs associated with recovering the lost data and regulatory costs. The harsh reality is that business data is vulnerable at all hours of the day. One-in-five enterprises will deal with a major data loss incident, and here's why.

Data Breaches Wreak Havoc

2017 was a prodigious year for data breaches. The number of breaches rose by 44.7 %. Organizations in the utilities, trade, hospitality, and retail sectors accounted for 55% of breaches, followed by the healthcare and medical industry, with 23.7%. A 2017 study on the cost of data breach by the Ponemon Institute revealed that out of the 1,200 US enterprises surveyed, 71%reported suffering at least one data breach. However, while the breaches increased, the average cost of a single data breach went down by 10% to $3.62 million. The study also surmised that the number of days it took organizations to contain a breach averaged 66 days. Breaches that were as a result of criminal or malicious attacks typically took longer to contain (77 days) and even longer to identify, compared to breaches caused by human error (64 days).

Disaster Strikes (the Same Place) More than Once

Data loss isn't limited to massive breaches and malicious hackers. It goes way beyond that. Natural disasters can happen more commonly than you think. If you are not in a Hurricane zone, you may be in an earthquake zone. Other disasters include fires and theft which can occur regardless of your geographical location. Disaster strikes two out of 1,000 company data centers each year, with 43% of those companies closing immediately, and another 29 % gone in the span of two years. For most organizations, the question is not if an outage or disaster could happen, but when it will occur and its subsequent severity.

It's a Mobile First World

Mobility is on a steady rise as a business. The more mobile you are, the more competitive you can be. However, having a mobile workforce comes at a steep price. You will have to compromise on certain aspects of your data security. As it turns out, your employees are the greatest cause of data loss, even more than malicious attacks by hackers. In fact, human error and technology failure are the major culprits in most data loss cases. The growing popularity of bring-your-own-device (BYOD) increases the chances of device damage, software corruption, and theft. On top of losing corporate data, laptop theft also poses a threat of data breach. The device risk is evinced by the fact that 40 percent of all data breaches from 2005 to 2015 were as a direct result of a lost mobile device.

First The Plan!

DLP is not going away anytime soon. Gartner experts recently predicted that 85 percent of organizations will implement at least a single form of 'integrated DLP' by the year 2020. Gartner also forecasted that DLP spend in 2018 will surpass a billion dollars with a solid compound annual growth of 20 percent from 2015 to 2021.

Most organizations are typically enthusiastic to implement data loss prevention in order to improve compliance efforts, better protect intellectual property(IP), and address the risks associated with the internet of things (IoT), mobility and the cloud. However, without a well thought out strategy, organizations have a propensity for going all-in and attempt to deploy all facets of a DLP solution – cloud, network, and discovery endpoint – simultaneously. This rushed approach usually introduces an overwhelming number of false positives and alerts.

The ideal DLP strategy should take a data-centric approach to security. This strategy enables users to enforce data-access control policies based on content, context, user tags, and input, all without disrupting existing business process or impeding user productivity. This white paper explores some of the key items on a DLP checklist that should be addressed before a data-centric strategy is deployed.

Data-Centric DLP Strategy Checklist

Classify Data Accordingly

- Confidential Data in Motion
- Confidential Data at Rest
- Confidential Data in Use
- Consequence if breached

Align Information Flow With Business Requirements

- Map out data endpoints
- Map out data storage
- Map out data on networks
- Third-party access
- User data transmission capabilities
- Business data exchanges

Establish and Maintain Policies and Practices

- Establish and Maintain Policies and Practices
- Monitor policies for effectiveness
- Develop specific controls for risks identified
- User training to stop accidental leaks

Integrate With Additional Security Controls

- Data protection in the Cloud
- Data protection in mobile devices
- Rights management
- Anti-malware apps
- Encryption
- Removable media controls

Test the DLP Solution First

- Progress from small workloads to full production
- Business communications not disrupted
- Performance of storage networks OK
- Create deployment documentation

Prepare an Incident Response Plan

- Breach recognition
- Damage recovery
- Evidence integrity
- Maintenance

Classify Data Accordingly

Before we establish what data is sensitive and can't be leaked, we have to identify the data we have. The first thing every organization should do is identify all the restricted and highly confidential data it has across the following three channels:

Data in Motion – data that is being moved, copied or sent over the local network or across the internet.

Data at Rest – data that is stored on database servers, hard drives, thumb drives, or any other storage media. This category also includes backup copies of data.
Data in Use – data that is created and synchronized to external storage devices like thumb drives or the cloud.

Not all data is equally exigent. The first step of a DLP strategy is determining, for each type of data, the consequences if stolen. This should be measured based on availability, integrity and confidentiality. Thus the prospective impact from a security breach could result in: unauthorized leakage of information (loss of confidentiality); unauthorized alteration of information (loss of integrity); disruption of use or access of information (loss of availability).

Classifying data is typically seen as a harrowing challenge in data loss prevention. A simple yet scalable approach is to classify by context; linking a classification with the data store, source application, or user who created it. By focusing your DLP protections on high-risk areas, you will make a notable positive impact on your organization's risk profile.

Align Information Flow With Business Requirements

Not all data movement constitutes data loss, but it is very important for organizations to identify their business information flow. The key parts of the organization, endpoints, storage, and network components, should be clearly mapped out. This makes it easier to understand where data is going and how it flows. You data mapping should include third-party data access, end-user data transmission capabilities, and business driven data exchange. A detailed network map helps you establish where you have to deploy specific

DLP solution components such as:

1. *The egress points present in your network*
2. *The source and destination of identified data*
3. *The processes in place to govern the flow of information*

Once the flow of information and business requirements are aligned, using a DLP solution to monitor endpoint activity becomes easier. IT administrators will be better positioned to ensure that employees, partners, contractors, and third-party vendors are prevented from leaking your data – inadvertently or intentionally. Furthermore, having a clear understanding of how information flows across the organization lays the groundwork for more comprehensive governance over your own information.

Establish and Maintain Policies and Practices

Before a system for data leakage prevention and data loss can be implemented, you have to clearly establish what to enforce. Unless you specifically know what you want to accomplish with your DLP solution, its arduous to evaluate varying options and know which best suits your needs. Setting up data usage controls may be easy at the start of a DLP initiative when you are targeting the most common risky behaviors. However, as the data loss prevention program matures, the policies should be monitored for effectiveness. Organizations can then develop more granular, fine-tuned controls to alleviate specific risks. This will greatly diminish the chance of interruption to business operations and will guarantee a swift return to productivity in the event of any data loss.

Once an organization understands the conditions under which data is moved, user training should be the next logical step towards curbing the risk of accidental data loss by insiders. Employees usually don't recognize that their actions can lead to data loss, and will self-correct when educated. A risk-based approach is the most ideal way to go about it. Those with regular access to confidential data should be rigorously trained in their responsibilities. Users have to understand the risk of data loss and its aftermath on their organization.

Integrate With Additional Security Controls

Cloud and mobile technologies have brought convenience to the enterprise, but in most cases, it's at the cost of data security. Data loss prevention in a cloud and mobile combined world has several innate challenges, the most critical being the shift in focus from securing just the network to securing the endpoints. Today's DLP solutions have to be able to protect data in accordance with corporate policies and regulatory requirements even when the data is on devices that are outside the corporate network. Successfully implementing Endpoint DLP requires an array of technologies: rights management, anti-malware apps, encryption, and content-aware removable media controls among others.

DLP is the most effective part of an overall data-centric security program, and integrates well with other security solutions to augment its capabilities. When used with complementary tools like monitoring, discovery, reporting, and network tools, DLP helps to prevent the accidental exposure of confidential information across all devices. Wherever data resides, in use, at rest in storage, or in transit on the network, a properly integrated DLP solution can significantly reduce the risk of data loss.

Test the DLP Solution First

DLP is a powerful technology and if poorly deployed it could impact key components of your communications. Despite the fact that you have tested your DLP solution, it is crucial to test it once more against your business requirements. Deploying consciously and cautiously involves testing components of the strategy against different scenarios to establish workflow efficiency. You may have to test the DLP solution to ensure it's using the right ports and protocols to efficiently handle network traffic, in addition to testing its performance on the storage networks. To start off, the solution can be implemented on small workloads, then as confidence with the solution grows, it can be expanded into every facet of the organization. Make sure everything related to the deployment and architecture of DLP is documented. If your DLP solution was completely burnt to the ground, your documentation should be comprehensive enough to guide you through full re-deployment.

Prepare an Incident Response Plan

An incident can be defined as any activity that disrupts the normal activities of a system and that may trigger some level of crisis. You can use technology to track and prevent incidents. However, no system, no matter how skillfully or thoroughly implemented can prevent 100% of all incidents. A careful and organized reaction to an incident could mean the difference between total disaster and complete recovery. In an increasingly complex world, understanding how best to respond to a security breach can be hard. Incident handling involves breach recognition, damage recovery, evidence integrity maintenance, investigation, and prosecution.

A 2018 study by the Ponemon Institute revealed that despite heightened concerns over data breaches, more than 75% of surveyed organizations don't have a formal process for handling one. An Incident Response (IR) is just as important an element of your security policy as are firewall deployment and physical security. IR demands preparation, planning, training, and evaluation. A good IR plan incorporates logical repeatable processes and can also decrease an organization's liability in the event of data loss. For example, your IR plan should allow you to offer supporting documentation to claim data breach insurance. In an era of increasingly stringent and more punitive privacy laws, having a plan in place will help IT staff respond to incidents and give them more time to prevent and mitigate damage. An IR plan can save the organization from incurring possible fines and legal costs, not to mention the brand damage associated with a data breach.

Summary

Today's digital revolution includes more technologies than ever before, from embedded systems to mobile devices, social media applications, hypervisors, and the proliferation of connected devices. These technologies have created a *borderless* network perimeter with multiple points of attack. According to a 2017 report by Check Point Software Technologies Limited®, 100% of organizations from a sample of 850 companies with at least 500 mobile devices experienced a mobile attack. In fact, the organizations were attacked an average of 54 times in one year. It's quite clear that convectional approaches to security continue to prove ineffective against current threats. Enterprises have to adjust to this digital transformation by shifting towards a security model that focuses on data protection at its core.

A data loss prevention strategy is mandatory for any organization that creates, stores, uses, accesses, or moves any type of data that is confidential, sensitive, or is governed by regulatory privacy-protection laws. DLP is an ideal preventive and defensive technology that if properly implemented has the potential to provide peace of mind to organizations concerned about protecting both their data and their client's data. Nonetheless, the most crucial element of a successful DLP implementation is understanding that the solution is a process. DLP implementation is not a solution that provides a quick fix – it is a process, and deploying is just the start.

In a mobile- and cloud-first world, FileCloud Server offers a suite of features that can simplify the complexities of DLP deployment. With unique capabilities to monitor, prevent, and repair data leakage, organizations are assured that their corporate data will be protected across all devices.

About Us

"FileCloud is used by 1000s of customers around the world including Global 2000 enterprises, government organizations, educational institutions, and managed service providers."

"We liked FileCloud's pricing, comprehensive feature set (branding, encryption) and the responsive support"

Stewart

A privately held software company, headquartered in Austin, Texas, USA. Our company offers two products – Tonido for consumers and FileCloud for businesses – used by millions of customers around the world, ranging from individuals to Global 2000 enterprises, educational institutions, and government organizations, and managed service providers.

To read more about how FileCloud can help keep your information secure as it is shared, visit www.getfilecloud.com