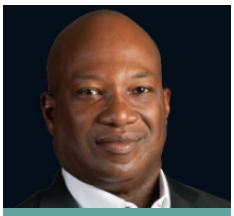
precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume 6: Issue No. 2 February 2022



Dr. Ronald Walcott
Managing Director

Today, we continue looking at another common vulnerability in cybersecurity, Unsecured communication channels. Communication channels are the means of transmission of information between devices and users on a network. Emails are one of the most common channels of communication to exchange information. To secure your business, the use of a DLP would be the best option in ensuring risk is kept low.

WHAT IS DLP?

Data loss prevention (DLP), per Gartner, may be defined as technologies that perform both content inspection and contextual analysis of data sent via messaging applications such as email and instant messaging, in motion over the network, in use on a managed endpoint device, and at rest in on-premises file servers or cloud applications and cloud storage. These solutions execute responses based on policy and rules defined to address the risk of inadvertent or accidental leaks or exposure of sensitive data outside authorized channels.

DLP technologies are broadly divided into two categories – Enterprise DLP and Integrated DLP. While Enterprise DLP solutions are comprehensive and packaged in agent software for desktops and servers, physical and virtual appliances for monitoring networks and email traffic, or soft appliances for data discovery, Integrated DLP is limited to secure web gateways (SWGs), secure email gateways (SEGs), email encryption products, enterprise content management (ECM) platforms, data classification tools, data discovery tools, and cloud access security brokers (CASBs).

HOW DOES DLP WORK?

Understanding the differences between content awareness and contextual analysis is essential to comprehend any DLP solution in its entirety. A useful way to think of the difference is if the content is a letter, context is the envelope. While content awareness involves capturing the envelope and peering inside it to analyze the content, the context includes external factors such as header, size, format, Etc., anything that doesn't include the content of the letter. The idea behind content awareness is that although we want to use the context to gain more intelligence on the content, we don't want to be restricted to a single context.

Once the envelope is opened and the content processed, multiple content analysis techniques can be used to trigger policy violations, including:

In this Issue:

Rule-Based/Regular Expressions: DLP's most common analysis technique involves an engine analyzing content for specific rules such as 16-digit credit card numbers, 9-digit U.S. social security numbers, etc. This technique is an excellent first-pass filter since the rules can be configured and processed quickly, although they can be prone to high false-positive rates without checksum validation to identify valid patterns.

Database Fingerprinting: Also known as Exact Data Matching, this mechanism looks at exact matches from a database dump or live database. Although database dumps or live database connections affect performance, this is an option for structured data from databases.

Exact File Matching: File contents are not analyzed; however, the hashes of files are matches against exact fingerprints. Provides low false positives, although this approach does not work for files with multiple similar but not identical versions.

Partial Document Matching: Looks for a complete or partial match on specific files, such as multiple versions of a form that different users have filled out.

Conceptual/Lexicon: Using a combination of dictionaries, rules, etc., these policies can alert on completely unstructured ideas that defy simple categorization. It needs to be customized for the DLP solution provided.

Statistical Analysis: Uses machine learning or other statistical methods such as Bayesian analysis to trigger policy violations insecure content. Requires a large volume of data to scan from—the bigger, the better, else prone to false positives and negatives.

Pre-built categories: Pre-built categories with rules and dictionaries for common types of sensitive data, such as credit card numbers/PCI protection, HIPAA, etc.

There are myriad techniques in the market today that deliver different

types of content inspection. One thing to consider is that while many DLP vendors have developed their content engines, some employ third-party technology that is not designed for DLP. For example, rather than building pattern matching for credit card numbers, a DLP vendor may license technology from a search engine provider to pattern match credit card numbers. When evaluating DLP solutions, please pay close attention to the types of patterns detected by each solution against a fundamental corpus of sensitive data to confirm the accuracy of its content engine.

Data protection is one of the primary concerns when adopting cloud services. The average enterprise uses 1,427 cloud services, and employees often introduce new services independently. Analyzing cloud usage data for 30 million users, McAfee (formerly Skyhigh Networks) found that 18.1% of documents uploaded to file-sharing services contain sensitive information, such as personally identifiable information (PII), protected health information (PHI), payment card data, or intellectual property, thus creating compliance concerns. It follows that employing the right DLP solution in the cloud encompassing accuracy, real-time monitoring, data analysis in motion, incident remediation, and data loss policy authoring is essential for successful cloud adoption.

Frequently Asked Questions:

WHAT ARE THE MOST COMMON CAUSES OF DATA LOSS?

The primary causes of data loss are:
- Human error;
- Malware infection and computer viruses;
- Theft;
- Hardware destruction.

WHAT ARE THE MOST COMMON USE CASES FOR IMPLEMENTING A DLP SOLUTION?

The most relevant use cases when organizations should consider implementing Data Loss Prevention software are:

- Insider threat management;
- Customer data protection;
- Meeting compliance requirements;
- IP protection.

WHAT CAN DLP DETECT?

DLP can detect potential data breaches and data exfiltration attempts; it can also prevent them by discovering, monitoring, and controlling confidential data. When DLP rules find a policy violation, alerts are triggered.

DLP policies can block prohibited activities, like inappropriate sharing of sensitive information via email, messaging apps, etc, thus reducing the risk of insider threats.

Frequently Asked Questions Cont'd:

As you plan your DLP policies, it's essential to identify the business processes that touch your sensitive items.

HOW CAN A DLP TOOL HELP WITH COMPLIANCE?

Data Loss Prevention solutions can assist organizations in meeting compliance requirements by discovering PII stored on computers, stopping unauthorized sensitive data transfers through a multitude of exit points such as USB storage devices, file sharing applications, cloud storage, email, instant messaging applications, and more.

Some DLP tools offer predefined compliance profiles for data protection regulations such as the GDPR, CCPA, LGPD, HIPAA, or PCI DSS, thus ensuring an easier way to safeguard customer data. Organizations can also customize detection rules and contextual conditions that align with compliance requirements.

DOES DLP PROTECT DATA WHEN AN ENDPOINT GOES OFFLINE?

When employees work remotely, they may not always have a continuous internet connection. Without a DLP, you risk data loss and non-compliance with data protection laws and industry standards. By using a DLP solution that applies policies at the device level, you can ensure that data continues to be protected whether a computer is online or not. This means that DLP policies remain active, blocking unauthorized data transfers and storing logs locally until they reconnect to the company network.

Upcoming Events

HYBRID CANADA SUMMIT
March 8, 2022

PACIFIC NORTHWEST US CYBERSECURITY SUMMIT
March 22, 2022

CLOUD DATA SECURITY SUMMIT
March 29, 2022

HEADLINE NEWS:

Feds Advise 'Shields Up' as Russian Cyberattack Defense

The U.S. Cybersecurity and Infrastructure Security Agency, along with the FBI, issued a joint advisory on Saturday pointing to Russian state-sponsored activity using WhisperGate and HermeticWiper malware to target Ukrainian organizations. The agency has also updated the Shields Up webpage to include new information, recommendations for corporate leaders and actions to protect critical assets.

In the advisory, U.S. officials say that such destructive malware can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. The advisory states that there is no credible threat to the United States at this time, but warns all organizations to assess and bolster their cybersecurity.

Jen Easterly, director at CISA, says in the wake of continued denial of service and destructive malware attacks affecting Ukraine and other countries in the region, CISA has been working hand-in-hand with partners to identify and rapidly share information about the malware that could threaten the operations of critical infrastructure in the U.S.

"Our public and private sector partners in the Joint Cyber Defense Collaborative (JCDC), international computer emergency readiness team (CERT) partners, and our long-time friends at the FBI are all working together to help organizations reduce their cyber risk," Easterly says.

Source: https://www.databreachtoday.com

868-610-7237
salesinfo@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad