It's a familiar refrain: Cloud services and mobile devices have made the challenges of safeguarding company data even more acute. Sensitive information now travels far beyond the relative safety of in-house networks into consumer cloud storage services where it's accessed by employees using unsecured mobile devices.

Yet while these risks are well understood, the number of data breaches continues to rise. A combination of greater security complexity and motivated cybercriminals has made the management and protection of corporate data increasingly more challenging.

One way to maximize protection against data loss and theft is the deployment of an advanced data loss prevention (DLP) solution. To help you effectively protect your organization, we've listed the following seven key features to look for when evaluating a DLP system.

1. **Content-aware detection capability**

   One of the cornerstones of sound security is the ability to detect, with great accuracy, all of the confidential information in an organization — whether that information is at rest, in use, or in motion. More specifically, advanced DLP systems should possess the ability to fingerprint structured data sources, use fingerprinting techniques to uncover confidential information in unstructured data (such as Microsoft Office documents, PDFs and JPEGs) and detect content by looking for matches between keywords, expressions, patterns and file properties.

   Additionally, the most advanced DLPS employ vector machine learning to protect intellectual property that may be challenging to describe due to subtle characteristics (think source code or financial reports). This type of rare or difficult-to-describe content is detected using the statistical analysis of unstructured data to compare it to similar content or documents.

   By employing these content-aware detection capabilities, organizations can find confidential data stored virtually anywhere and in any format, while greatly reducing false positives.
These days data is dispersed across a variety of devices and storage environments, making the ability to consistently define and enforce policies imperative. The best DLP solutions combine a unified management console with a business intelligence reporting tool, providing the ability to write policies and enforce them everywhere while reducing information risks.

This setup provides the functionality to define data loss policies, review and repair any incidents, and conduct basic system administration across all endpoints, mobile devices, cloud services, and on-premise systems. Additionally, the best solutions provide a robust analytics tool that allows for ad hoc analysis and advanced reporting. Users can extract and summarize system data to create reports and scorecards for various organizational stakeholders.

These features ensure consistent policy application and the ability to take action, when the need arises, to safeguard sensitive data.

2 The ability to define and enforce policies across an entire environment

These days data is dispersed across a variety of devices and storage environments, making the ability to consistently define and enforce policies an imperative. The best DLP solutions combine a unified management console with a business intelligence reporting tool, providing the ability to write policies and enforce them everywhere while reducing information risks.

An advanced DLP solution should also have the capability to monitor and protect sensitive information transmitted via email, making sure of quick detection of sensitive data and the subsequent notification of users creating policy violations. Suspect emails should be redirected to a secure encryption gateway or blocked in real time to prevent leakage of the most sensitive information.

4 Securing data on traditional endpoints

The emergence of mobile and cloud hasn’t lessened the need to protect traditional endpoints, which continue to serve as a critical repository for confidential business data. The best DLP solutions include the functionality to monitor, discover, and protect information on desktops, whether traditional or virtual, as well as off or on corporate networks.

The right DLP solution should include features for local scanning, detection, and real-time monitoring for a variety of events across a range of operating systems. It should also enable the monitoring of confidential data that is being copied, downloaded, or transmitted between laptops and desktops, whether it involves applications, email, cloud storage, or removable storage.

Additionally, the use of multiple scanning options (such as
idle and differential scanning) to increase performance, and pop-up notifications in the event of a policy violation, are desirable features that help ensure endpoint users are fully protected.

5 Full protection for mobile devices

Today the line between our business and personal lives has grown very blurry, thanks in large part to our mobile devices. Users want (and expect) to be able to access sensitive business data where they want and how they want — which often means they'll use personal devices to do so.

A powerful DLP solution can help businesses make concessions to today's evolving business norms without sacrificing security by offering monitoring and protection functionality to all iOS and Android devices, regardless of ownership. The ability to monitor and detect when users are downloading confidential material to their iOS and Android devices — and to prevent such transmission when necessary — is imperative for full mobile security.

The best DLP solutions then have the power to automatically secure any exposed files that are detected, making sure to quarantine or move files, or apply policy-based encryption and digital rights to specific files. Custom file remediation options — and easy integration with third-party security solutions — are also key features.

Finally, a data governance tool that's designed with unstructured data environments in mind can offer you highly actionable intelligence into data ownership and usage. By discovering confidential files, identifying data owners and understanding access history and file permissions, you can illuminate "dark data" by shining a light on the data in your environment, ultimately gaining the ability to see who owns it, who can access it and how it's being used.

6 An answer to the problem of unstructured data

Unstructured data presents a real challenge — it represents the vast majority of all data and it's growing at a rather jaw-dropping rate of 70 percent annually. Given this growth, it's no surprise that organizations find it difficult to manage and protect this data effectively.

The most advanced DLP solutions, however, help tackle this problem by letting organizations take control of their unstructured data, making it less vulnerable to cybercriminals and less-than-diligent employees. The first step is a rigorous scan of databases, network file shares and other repositories, using cutting-edge technology that can recognize hundreds of different file types based on the binary signature of the file.

Studies show that half of all employees use personal accounts to handle work email. Given this, it's hardly surprising that emails and the web are where most data gets lost. By investing in an advanced DLP solution, however, you can significantly reduce the odds of this occurring by monitoring a wide range of network protocols and preventing...
users (both authorized and otherwise) from mishandling data.

The right DLP solution can detect confidential information over a range of protocols (HTTP, FTP, SMTP, custom port-specific protocols, etc.) while providing thorough content inspection of all communications without packet loss (some solutions will sample packets during peak loads, but this creates a greater risk for false negatives).

Additionally, inspections of business email and outbound web traffic for confidential data — with subsequent notifications for policy violation — are a fundamental feature for protecting moving data.

The takeaway

Cloud and mobile have conferred profound benefits on today’s organizations — yet they’ve also raised the ante in terms of security. To give your business maximal protection against data loss and theft, make sure your next DLP system offers the seven core features outlined above.

Joshua Carter is a senior system engineer and DLP architect for Symantec. Joshua has held technical architecture and consulting roles at a number of major corporations, including Accenture, American Express and Case, LLC. He also served for five years in the US Navy as an information system technician.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.