Information security in the age of collaboration

The data that flows across networks is boosting teamwork and highlighting the need to protect information at rest and in motion

Prateek Temkar
Symantec

"DATA NOW TRAVERSES PUBLIC NETWORKS INSTEAD OF BEING CONFINED TO THE CORPORATE PERIMETER, WHICH MAKES IT EASIER FOR MALICIOUS ACTORS TO INTERCEPT SENSITIVE INFORMATION."

Agencies are relying more heavily on cloud-based applications for a variety of reasons. Cloud apps are easier to manage than their on-premises counterparts, and there's no need to provision hardware or staff large teams. The user experience is better because cloud vendors iterate rapidly and push updates continuously. In addition, people can collaborate more readily across different devices, including personal ones, and with external partners, vendors and suppliers.

However, increased collaboration comes with risks. Data now traverses public networks instead of being confined to the corporate perimeter, which makes it easier for malicious actors to intercept sensitive information. And cloud apps are often accessed from unmanaged or personal devices that may not have the proper security posture.

Shadow IT compounds the problem. Employees can sign up for unsanctioned cloud apps without IT approval, making it harder to track and protect sensitive data. Additionally, not all cloud apps enforce strong security practices such as encryption, multifactor authentication or secure APIs.

Those risks highlight the growing need to protect data both at rest and in transit through policy enforcement, encryption and continuous monitoring.
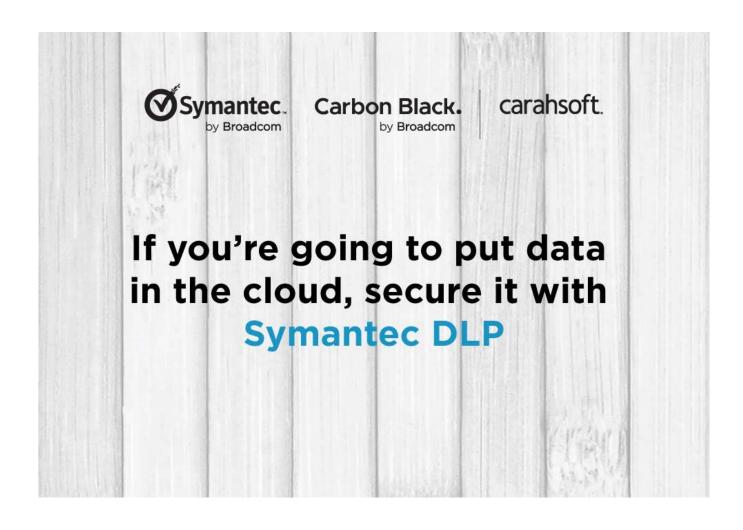
How to create a successful DLP strategy

There are some key steps agencies can take to create a successful data loss prevention (DLP) strategy. First, ensure that app owners, the legal and compliance teams, and agency leaders are on board by helping them understand the risks associated with data loss.

Start small by identifying the most sensitive applications and the types of data that need protection. Understand who has access to the data and how it flows—across email, endpoints, cloud apps and web traffic.

Determine which regulations apply to your agency and ensure your strategy aligns with those requirements. Label or classify sensitive data so it can be consistently tracked and protected, even as it moves across systems and users.

Identify who will manage incidents, how they'll be resolved and what remediation measures will be in place when a leak is detected. Also, define how employees will be coached, ideally through just-in-time feedback when a policy is violated.

Finally, establish clear success metrics, which might include how many violations are detected, the rate of false positives, response times, and how the organization's overall data protection posture improves over time.

Protecting data without affecting the user experience

Broadcom delivers seamless DLP without compromising performance. For cloud apps, we partner with a range of providers, including Microsoft, Google, Salesforce, Box, ServiceNow and Amazon Web Services. We integrate via APIs and receive near-real-time notifications when content is created or modified. As users collaborate, we inspect data behind the scenes and automatically delete, unshare or quarantine content based on policy without disrupting the user experience.

We've developed a high-performance content extraction library that accelerates DLP analysis, along with advanced fingerprinting that scans entire documents rather than just samples for high-accuracy detection without added latency. In addition, our scalable Exact Data Matching (EDM) technology allows precise detection of sensitive content based on customer-defined datasets, which drastically reduces false positives. Our EDM implementation supports up to 6 billion data cells and is one of the most scalable in the industry.

For large data scans, such as compliance audits across massive file shares, our solution delivers unmatched performance by scanning up to 1 terabyte per hour, which is among the highest in the enterprise DLP market.

With those technological innovations, agencies can protect even the largest datasets from attackers. ■

Prateek Temkar leads product management for Symantec's information and network security business at Broadcom.