Outsmart the Bad and Safeguard The Good: Data Loss Prevention Strategies

Perry Hutton, Fortinet Africa regional vice president

Preventing the loss of critical or sensitive data has been an issue for as long as there has been proprietary information and intellectual property. But recent developments both in regulatory requirements and in the evolution of network infrastructures, including BYOD, virtualization, sophisticated applications, shadow IT, and cloud environments, make it imperative that organizations take a new look at how they control and protect critical data. Most of the time, data loss is unintentional, attributed to employees that unknowingly violate security policy or attempt to get around email based security solutions by using a personal Web-based e-mail, IM, or online file sharing application to transmit sensitive documents.

Regardless of the method or intent, the consequences of lost or stolen data can be disastrous for an organization. Valuable information, such as intellectual property, blueprints, or trade secrets acquired by a competitor or sold on the black market can potentially cost an organization millions in losses. Classified government information that falls into the wrong hands can compromise a nation's safety and security. Exposure of customer data can leave an organization susceptible to law suits, customer attrition, and damage to brand and reputation. And data leakage is often a red flag that signals other compliance violations that can cost an organization hefty fines or loss of credit card processing rights.

That's where Data Loss Prevention (DLP) solutions come into play. DLP is more than a product, or even set of products. It is a systems-based solution that needs to be applied across the entire distributed network, including endpoints, local and distributed networks, data centres, cloud services, applications, and web and e-mail services in order to prevent end users from sending sensitive or valuable information to unauthorized users and devices. An effective DLP strategy can also be a valuable tool for IT administrators, enabling them to create, refine and enforce policy, gain broad visibility into data flow, filter data streams on the network, and protect data at rest, in motion, or in use.

IT Transformation and DLP

Network infrastructures are entering a period of dramatic transformation. Customers, employees, contractors, and business partners have an unprecedented need to access critical business data and network resources. The number and kinds of devices used to access this data are expanding rapidly, from smartphones, tablets to personal laptops that are increasingly not controlled by IT. At the same time, critical data is being stored offsite on a variety of third-party platforms, something known in the industry as Shadow IT.

In this evolving environment, the traditional perimeter of the data centre, and the network itself, is fundamentally changing. Users expect to be able to access any information, from any location, at any time, using any device. The result is that the corporate network is expanding beyond its traditional borders to include web and cloud-based access.

Securing data in this environment can be a complex process because that data no longer simply exists behind the iron doors of the data centre. The flow of data transactions into and out of the data centre, between data centres, or that is used and stored on a wide variety of devices is increasing at a dramatic pace. During this process, the nature of the data changes, and comprehensive data loss security strategies need to address these different states.

Add to this complexity the dramatic rise in regulatory requirements. Increasing numbers of regulations have been imposed by government or industry, or even self-imposed as best practice standards or legal defence hedges. Most regulatory compliance mandates are focused around the need to protect data - from personal information related to customers, patients or clients, to protecting sensitive or secret information from falling into the wrong hands. This means that existing data security practices and policies need to be reviewed and updated on a regular basis, especially as the environment within which this data exists continues to undergo significant transformation.

The common security thread across all of these changes is the need to protect and preserve critical, sensitive, or confidential data in the midst of a rapidly expanding environment where traditional security solutions are less and less relevant.

Cyber Criminals are Getting More Organized. Your Data Loss Protection Strategy Needs to Outpace Them

The profile of high-tech criminals has changed from one of vandals and mischief-makers to organized criminals who exploit weaknesses in your

security strategy to steal data for profit. Securing data against these criminals, both outside of and inside your organization, requires implementing a security strategy across the entire breadth of the environments within which your data may exist.

It is important to remember that data loss prevention is achieved through the coordination of many different components. The first, and most essential, is a strong policy and governance strategy. Utilizing the resources of an expert is essential in creating a comprehensive strategy that not only secures your data, but which can also withstand scrutiny from compliance regulators.

After a policy is in place, it is essential to design a network that is able to discover, analyze, and secure data. This can be achieved through a combination of specific data management and control tools, content-aware security devices and solutions, and the ability to leverage the devices, intelligence, and services that already exist in your network. As with policy creation, utilizing the services of data loss prevention IT experts can help you design and implement a secure architecture that meets both your data policy and governance requirements as well as any external regulatory mandates.

Many security solutions are inadequate in addressing data loss prevention requirements.

[if !supportLists]· [endif]No central policy, command, management, orchestration, or control

[if !supportLists]· [endif]Poor visibility into the larger security solution

[if !supportLists]· [endif]Inability to collect and share critical event information between solutions

[if !supportLists]· [endif]Little to no collaboration between discrete security elements

[if !supportLists]· [endif]No real integration between various security devices and the network

[if !supportLists]· [endif]High IT overhead for managing and maintaining siloed security elements

An effective data loss prevention strategy needs to address such areas as data management solutions, perimeter control, network segmentation and security zones, access control, identity of both users and devices, connectivity and VPN, data encryption, mobile devices, cloud services, content control such as web and email, application management and content inspection, and secure storage.

As networks, devices, and data itself continues to change, it is important to understand what your existing data loss prevention strategy can and can't do. Many attacks seek to compromise new technologies that have often been adopted and implemented without a data loss strategy being implemented. Others, like advanced persistent threats, are designed to operate below the radar of most security solutions, often carving data up into unrecognizable chunks to be reassembled later.

An effective data loss prevention strategy, therefore, needs to participate in an active lifecycle security strategy, which includes 1) preparation and planning as new network technologies, strategies and devices are being considered, 2) designing and implementing collaborative and adaptive security as an integral part of your network architecture, 3) continuous assessment and automated response to threats as they occur, and 4) the implementation of forensic tools that allow you to immediately trace an event to its source, identify bad actors or compromised devices inside your network, and optimize your environment to prevent future breaches.