Data Protection: Building a Comprehensive Strategy

February 2013

Data loss remains a top challenge and concern among organizations of all sizes as IT struggles with the influx of technologies aimed at making sensitive corporate data flow more freely between trusted and untrusted computing environments (e.g., mobile devices and the cloud). At the same time, targeted attacks on enterprises, as well as on individuals inside organizations, are now primarily aimed at stealing sensitive information from individuals’ machines or infiltrating networks for deeper data theft purposes. According to IDC's 2012 Security Survey, preventing exposure of confidential information, increasing sophistication of attacks, and mobile clients and unmanaged devices were cited as the top 3 challenges facing enterprises in the coming year.

The following questions were posed by Trend Micro to Phil Hochmuth, program manager for IDC’s Security Products research, on behalf of Trend Micro’s customers.

Q. **What trends in enterprise networks and computing are creating challenges for data security?**

A. One of the biggest trends creating data security challenges is the use of employee-owned and consumer-grade mobile devices in the workplace — a phenomenon now commonly known as “consumerization” and “BYOD” (bring your own device).

Another major trend creating data security risks is the growth not just in consumerized devices but also in cloud applications, such as online storage, collaboration tools, video, chat, and social media. Employees are increasingly adopting these nontraditional business tools for work as well as personal use. Examples include LinkedIn to connect with colleagues or potential hires, or Facebook for marketing purposes, or storing sensitive information in cloud services such as Dropbox.

All these trends might be summed up in a single megatrend: the introduction of untrusted end-user environments in the enterprise. The basic fact is that sensitive information, which once rarely, if ever, left the sealed and safe confines of the enterprise or the endpoint, is now moving into these untrusted environments — whether an employee’s personal iPhone, Dropbox, or Google Docs account — which can put organizations and their end users at risk.

Q. **What are organizations doing differently now compared with five years ago regarding these changing trends? Are they deploying new technology, changing strategy, or implementing new practices and processes?**

A. Faced with these trends, organizations are moving security closer to end users and their point of interaction with company data. This means allowing security policy and security controls to follow end users, as well as data, as they move from a corporate-owned PC or smartphone to a
personally owned tablet, smartphone, or even laptop, depending on where they are working and what they need to accomplish. Because the fact is, end users are accessing sensitive data with a more diverse and wide-ranging set of devices than ever before.

So the old approach of building a strong perimeter around your data assets and relying primarily on firewalls, VPNs, and gateways to confine your sensitive data and the activities of your workers to a company-issued laptop or desktop that is used primarily on the LAN is no longer as effective.

This is not to say that those technologies do not play a role in this new type of security deployment trend that we're seeing. The gateway still has a vital role in terms of protecting people in an office environment, whether or not they are using personal or corporate devices. More recently, we're seeing that perimeter tools can be effective at helping identify and apply controls to end-user application activity based on context, but in the end, the controls and visibility need to be oriented around the end user rather than tied to a specific device.

It's just a more balanced approach, whereas in the past, there was a heavy emphasis on "perimeterization" of the enterprise as the only way to protect sensitive data. Today organizations are deploying tools that put the protection where it is being accessed by end users, whether within or outside the confines of the "trusted" IT environment.

Q. Should data loss prevention (DLP) technology be the focus of an enterprise data initiative?

A. When DLP came on the market six years ago, it was promoted by some vendors as the answer to data loss issues or leaks. People have now realized that while DLP solutions are vital pieces of the larger data protection puzzle, they are not the be-all and end-all of a data protection strategy.

Organizations want to complement DLP with other tools that may already be in the enterprise but that may not be integrated with DLP, such as encryption, mobile device management (MDM), or enterprise rights management — and particularly identity and access management. We're seeing a lot of integration and coupling of DLP security technologies with identity, for example, to make policy enforcement stronger and to make the controls, and the way that DLP can block or stop a leak, be tied more closely to end-user activity and end-user privileges and roles.

At the same time, DLP is also becoming a more integrated and fundamental feature in the applications and data resources themselves. Platforms such as messaging servers, as well as collaboration tools such as SharePoint, are adopting DLP-like controls at the application level or integrating with third-party DLP tools to provide such capabilities. Features built into Web gateways and other perimeter platforms are increasingly being leveraged to scan outgoing content — bound for cloud-based sharing, collaboration, and storage apps — for DLP and data governance policy compliance. In short, we're seeing a mix of DLP with a lot of other technologies that is moving data protection schemes forward for many organizations.

Q. How should organizations think about security and data protection technologies over the next three to five years?

A. Given the trajectory of the megatrend of the untrusted IT environment, as well as the changing approaches to end-user protection and DLP, it follows that data protection will fit under the broader umbrella of security technologies. IDC calls this "information protection and control," or IPC — DLP being a part of that. It also includes technologies such as encryption, rights management, and identity. The basic idea is that data protection technologies should live almost everywhere in the network and on almost every type of IT asset where sensitive data could traverse or be stored.
Increasingly, IPC and DLP are becoming more integrated — either from an overall functionality standpoint or as direct IPC/DLP product tie-ins — with adjacent IT management platforms, such as MDM and cloud application/SaaS gateways and cloud brokering agents in the enterprise.

It's possible to do this now given that many products support advanced filtering, traffic recognition, detection, and inspection. Overall, now there's simply the bare horsepower on endpoints to allow at least some IPC features on the devices. So we're no longer relying on one or two critical inspection points in the network, or on an endpoint, to catch a data leak or identify a sensitive piece of data.

Over the next three to five years, we will see data protection capabilities almost everywhere, really integrated into the fabric of the network and the computing environment. We refer to this as a "ubiquitous IPC" strategy.

Q. How does an organization get started with the ubiquitous IPC concept?

A. The first step is to assess the existing tools in an enterprise that could be classified as IPC. Get a sense of what's in the IPC toolbox of your organization. Is there already wide deployment of whole disk encryption technologies, for example, on laptops or mobile devices? Could there be DLP features or add-on capabilities in existing gateways, such as email gateways or Web security gateways, that aren't being utilized or are underutilized?

Look at things such as identity platforms, and try to figure out if there are ways to tie identities in directories, such as Microsoft Active Directory, LDAP, or other types of repositories of information. Link users to roles and rights to sources of data, whether databases or file servers. Start thinking more of a connection between the identity of an employee and the types of data he or she can access and manipulate.

The next step is a big one, but you need to tie the disparate IPC features together. This can be done through integration with a strategic partner — sometimes a DLP provider or a security vendor that already offers many pieces of the IPC puzzle.

Regardless, have a framework in terms of IPC technology, and know what would fill the gaps in terms of new products that can tie things together. Then keep in mind where you want to go in terms of what this overall architecture will look like in the end. What types of data are you trying to protect? What is your most valuable asset to the organization from a data or information standpoint?

Organizations that think about these questions as they work toward a goal of ubiquitous IPC can devise a strategic approach to addressing the challenges of consumerization, cloud services, and the rise of the untrusted IT environment.

ABOUT THIS ANALYST

Phil Hochmuth is the program manager of IDC's Security Products service. In this role, he conducts primary research and provides insight and analysis on a range of enterprise security markets, including data loss prevention (DLP), information protection and control (IPC), messaging security, and Web security. His research also examines the convergence of these security technologies, and others, as enterprises address new and evolving data security challenges.