

Introduction

With numerous news stories detailing public breaches that have led to sensitive user data getting released—on websites, stolen as part of a laptop theft, or even released accidentally over an email or instant messaging (IM) communications—organizations are increasingly under pressure to protect privacy data. Over the last few years, this challenge is compounded by increasing regulations related to compliance that enforce through fines or other penalties, like jail time, how privacy data is handled. California and other states that have enacted similar laws, organizations are now forced to publicly disclose if computerized data files have been compromised by unauthorized access, which can open up the risk for identity theft. The impact on privacy data leaks can impact an organization's brand and public reputation, not to mention put its customers, employees and partners at serious risk. Here's a top ten list of requirements your organization should consider when selecting a solution to protect privacy data:

Step 1: Identify known content risks

Whether Social Security numbers, credit card information or medical records, it's critical for organizations to have the tools to scan their network, including file shares, databases, content management stores and other repositories, for known risks. Often organizations will know where a portion of this data resides, like a server used by the Finance or Human Resource Department, but discovery mechanisms are required to find all instances of sensitive data. This might include a legacy server, desktops or another repository long since forgotten by the IT team. Furthermore, the discovery engine needs to have automation mechanisms for running over time, as new content is created or added to the network.

Step 2: Create Content Signatures and Filters

Once known sensitive content is identified, some mechanism needs to exist to create snapshots and generate filter rules that align with each of these unique files containing sensitive data. These signatures and related rules should be designed to enforce the movement of sensitive data on the network, such as being distributed externally either because of a broken business process, mis-configured IT system or in the worst case malicious end-user activity. It's important that the signatures and filter rules can logically

detect modifications to source content, such as detecting a single column exported from an Excel spreadsheet and then saved with a new file name.

Step 3: Port and Protocol Independent Analysis

When it comes to protecting privacy data flowing across the network and outside of an organization, monitoring needs to occur across the entire network and all traffic. It's not enough for an organization to monitor email, web or IM traffic alone. Furthermore, numerous techniques exist for exploiting holes and re-direction mechanisms on the network, such that applications can route SMTP protocol traffic (or FTP or IRC or peer-to-peer) over non-standard ports or over Port 80, typically the most open port in most organizations. The ideal content filtering and monitoring solution should take into account all traffic across all ports, but also do this analysis independent of the protocol being used for the communication since there is no guarantee the two are interconnected.

Step 4: Deep Content Inspection and Policy Definition

Inspection needs to be thorough enough to look at all content types from Excel documents to email messages to even meta-data embedded within a file. Furthermore,

sensitive data will take multiple forms and in some cases not be as easy to define as a certain known file or set of keywords, but more likely strings of content elements linked together that compromise a privacy record, and accordingly risk. For example, a medical record isn't just a Social Security Number, but it is also comprised of a patient's name, information on 'admission' or 'discharge' dates, as well as other details on insurance company or healthcare provider. Accordingly flexible mechanisms need to exist around defining policies around 'what is privacy data' and ensuring the inspection techniques and related policies align with the specific requirement a customer is trying to address for company brand protection, compliance or other security reasons.

Step 5: Alerting, Blocking and Enforcement

No security strategy is complete unless mechanisms exist to report and alert on its effectiveness, as well as take action in real-time to stop threats. For protecting sensitive data and addressing privacy, multiple mechanisms are required. Notifications for IT administrators, HR, legal or compliance officers can be important, but also end-user alerts can be valuable for educating and modifying user behavior to ensure appropriate handling of sensitive records. This could be as simple as an email notifying users of a privacy breach or more proactive mechanisms like forcing their email communications that include privacy data to get re-routed to an encryption server to be protected before it is sent out. Along these lines, various enforcement activities can be important for not only blocking and stopping risky traffic, but can be useful for removing the mechanisms, like public webmail services like Gmail or instant messaging services like Yahoo!, that are conduits for a breach.

Step 6: Delegated Controls and Remediation

In the course of identifying content risks, as well as establishing the monitoring that needs to take place on an organization's network and related actionable policies, delegation of control is a requirement. Clearly different owners need to exist for defining a policy, such as one for identifying sensitive records, but more important delegation is critical for the follow-on remediation steps if a breach does occur. Should HR address the incident or a compliance officer? What if a reconfiguration issue is required on end-user desktop and IT staff intervention is required? What if user training is a requirement and how is this remediation process managed and tracked to completion? Along the course of resolving an incident, an organization needs to ensure workflow procedures exist. They also ensure that the sensitive data that was at the epicenter of the incident is now safeguarded, and only accessible by a privileged few users or managers.

Step 7: Historical Capture Database

Security is by nature a journey and not a destination. Constant tuning and adjustments are required for the greatest effectiveness, so capturing network events in a database for later analysis can be helpful for constantly learning more about network activity and traffic patterns. After-the-fact analysis can not only lead back to the root cause of a sensitive data leak, but also point to unusual patterns, like traffic from malware programs on the network finding and sending data to remote destinations or emerging IT applications, like Skype, running on the network that expose the organization to risk. Capture can also be valuable for archiving historical network activity to audit compliance with industry regulations, like HIPAA, or provide a legacy record of how all sensitive data has been handled over time.

Step 8: IT Co-existence and Leveraging Existing Investments

Organizations have invested heavily over the last 15 to 20 years on various Internet technologies for building out their network, deploying applications on top of it, and then securing it. Accordingly, whatever solutions are selected for managing privacy data and intellectual property should leverage this existing IT investment in both hard dollars, but also internal skills and other competencies. For example, an ideal solution should plug into existing infrastructure elements like email gateways, network switches, web proxies and encryption servers for some blocking and enforcement. Similarly, the privacy solution should leverage intrusion detection systems (IDS), firewalls and vulnerability assessment solutions that may exist in the environment to further gain intelligence on low-level network activity and boost accuracy and overall effectiveness.

Step 9: Take a Phased Approach to DLP Solutions

Many customers find value in first deploying network-based components of their end-to-end security architecture as it helps them identify sensitive data and reveal risks. Then, as the value of data loss prevention becomes more evident, the same content analysis, detection, and prevention techniques can be deployed within the corporate desktop and laptop environments to ensure consistent protection for all data—whether the node is attached to the company network or not. McAfee has solutions for each stage of the process. First, McAfee Network DLP learning applications can help your organization "learn" about your sensitive data, your business process, and gain better insight into risks. Then, McAfee's ePolicy Orchestrator (ePO) ensures quick and easy deployment of McAfee Host DLP solutions to a broad and diverse workstation ecosystem.

Step 10: Appliance-based Solution

Many of the vendors in security have already standardized on the appliance approach since it delivers superior reliability and performance. The sheer design of appliances inherently has more built-in security than a software package deployed on a general-purpose server prone to hackers or malware. The firewall, IDS, email gateway and other security markets have all shifted to the appliance approach for this reason. For addressing privacy, an appliance solution provides the best cost of ownership since setup and management is easier, plus it simplifies upgrades of the privacy solution for the latest software releases including new policies and compliance filters delivered from the vendor on a periodic basis.

Why McAfee Network DLP solutions?

Only McAfee Network Data Loss Prevention (DLP) solutions provide learning applications to help eliminate the key information security challenges facing your organization with deploying DLP technologies. By indexing all content in motion and at rest, and making this information available through a simple and intuitive search interface, McAfee Network DLP allows you to quickly identify your sensitive data, who is using it, where it is being sent, and where it is stored, and investigate activity— whether a rule was configured or not. McAfee Network DLP doesn't expect you to "know" exactly what needs to be protected— or how. Nor does McAfee Network DLP expect you to "know" where your critical information is vulnerable and who or what your threats may be. Rather, McAfee Network DLP learning applications help you "learn" about your sensitive data, your business process, and gain better insight into risk.

For more information about McAfee Network DLP solutions please visit: www.reconnex.net or call us at 888.847.8766— 24 hours a day, seven days a week.

For more information about all of McAfee's Data Protection solutions please visit: www.mcafee.com or call us at 888.847.8766—24 hours a day, seven days a week.

About McAfee, Inc.

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world.

With its unmatched security expertise and commitment to innovation, McAfee empowers businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security. www.mcafee.com

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved.

5024_brf_10steps-privacy-data_1008