PROTECT:
Protect Today, Secure Your Future.

BEST PRACTICES

Confidence in a connected world.

symantec™

CURRENT BUSINESS SCENARIO

For medium-sized and large enterprises, preventing data breaches is a primary challenge. In the past, data protection was simpler because controls focused on one major risk: the network perimeter. By locking down the perimeter, organizations could repel most attacks and keep their information, data, and devices fairly safe.

Those simple days are gone forever. Today, enterprise data flows freely both inside and outside the network and over portable devices such as laptops and smartphones. Pervasive use of devices like these has contributed to a diminishing perimeter that is no longer marked by the boundaries of your corporate network or the edge of your parking lot. The byproduct is that data is increasingly exposed to greater risk, including a growing array of threats—not only criminal opportunists, but also your own employees. The enterprise today demands a more robust strategy and deployment of integrated solutions that automatically protect all devices and enterprise data, whether they're on or off the corporate network. In addition, organizations need to be able to manage all these risks from one central platform to reduce complexity and cost, and to enable IT professionals to do more with less.

The first step toward addressing the growing risk of data loss is to deploy strong controls for endpoints and data loss prevention (DLP). At the same time, organizations must also ensure that they have business processes defined that follow industry best practices for protecting the enterprise. Symantec™ solutions enable companies to adopt such best practices and help them build a robust security program for effective enterprise data protection. These best practices also enable companies to demonstrate compliance with both internal policies and key government regulations.

ENDPOINT PROTECTION BEST PRACTICES

As much as 60 percent of a corporation's information resides on its endpoints. Symantec's research has shown that four out of five companies have lost confidential data through laptops, and one in every two companies has lost data through USB drives. The following best practices can help reduce the risk of loss or breaches of sensitive data on endpoints.

- **Encrypt sensitive data.** Identify which endpoint devices have confidential data stored on them and encrypt those devices. To increase efficiency and reduce costs, deploy a solution that automatically encrypts the entire disk on each endpoint.
- **Protect systems from malware.** Antivirus alone is not enough to protect your systems against today's threats. With the diminishing perimeter, traditional gateway technologies like intrusion prevention systems (IPS) and firewalls should be implemented on every endpoint.
- **Enforce access controls.** Enforce the use of strong passwords for access. Use network access controls to ensure mobile endpoints such as laptops and smartphones are safe to reenter the corporate network, and do not connect to public networks when they are vulnerable to infection.
- **Control use of USB devices.** Permit only the use of company-owned USB devices on enterprise endpoints, and block data transfers to or from them unless authorized. Deploy controls for live USB and portable applications. Ensure that data on USB devices is encrypted and password protected.
- **Control endpoint configurations.** Enforce standard configurations on endpoints for authorized operating systems and applications. If someone modifies an endpoint, enforce reversion to the authorized configuration before the endpoint is granted network access.
- **Regularly back up endpoints.** Provide users with an easy way to recover lost data.
- **Include personally owned endpoints in your plans.** Protect against endpoint devices owned by home workers that can be used to access the enterprise network, such as PCs, laptops, and any other portable device used for business as well as pleasure. Use incentives to encourage the use of security technology and ensure these endpoints are running up-to-date antivirus and antimalware protection, plus other controls for protecting your enterprise.
- **Build a contingency plan that addresses potential loss.** Despite their best intentions, workers will occasionally lose mobile endpoint devices. Establish clear policies and procedures for dealing with equipment loss, including steps to neutralize a stranger's ability to use lost devices for access. Ensure the organization also has a process and technology in place to determine whether confidential data was stored on the endpoint.

MESSAGING PROTECTION BEST PRACTICES

Messaging systems are the modern lifeblood of business, so many attacks attempt to exploit their vulnerabilities. IT security professionals can nip most attacks in the bud by adhering to the following best practices:

- **Create a baseline policy for spam.** Block obvious spam, but permit delivery of potentially useful messages such as newsletters or product marketing. Control message delivery by business role with user- or group-specific filtering policies. For example, messages containing executable files might be permitted for Engineering but dropped for other groups. Centralizing the management of messaging security will also save users the time they would otherwise spend managing their own spam.
- **Use integrated messaging solutions.** Email security and management requires the integration of all components, such as antispam, message transfer agent (MTA), content control, and archiving.
- **Implement connection management.** Techniques include blacklists, whitelists, sender reputation, rate controls, and recipient verification. These will eliminate the bulk of potentially problematic messages, allowing for selective use of deep-content analysis downstream. One way to boost performance is by blending in-the-cloud solutions with on-the-premises components.
- **Manage bounce notifications.** To thwart spam and potential message attack vectors, limit the number of external bounce notifications for unreachable addresses. Your antispam solution should support implementation of this practice.
- **Use a broad strategy for content security.** Your messaging security solution should allow implementation of other aspects for content control and compliance, such as enterprise policies for email retention and regulatory mandates (the Payment Card Industry Data Security Standard [PCI DSS], the Health Insurance Portability and Accountability Act of 1996 [HIPAA], and so on).
- **Educate users.** Automated messaging and other security controls must be supplemented by safe practices used by everyone in the enterprise (see sidebar).

BEST PRACTICES FOR “REGULAR” EMPLOYEES

Everyone in an organization shares some responsibility for preventing a data breach—especially nontechnical employees. But it’s difficult to automate security controls for every potential scenario, such as stopping an employee from giving their access information to a phisher. Here are some best practices all employees can follow to strengthen their organization’s data security.

- **Be vigilant with email.** Email is a conduit for malicious vulnerabilities, most of which come in attachments that contain a virus or worm. Do not open unexpected or suspicious attachments—especially in spam or from unknown senders outside the company. Delete all spam and never forward email about virus alerts. Don’t use your company email address to register at websites unless they are work-related. Double-check outgoing addresses before you send sensitive information. Never send sensitive information through email unless it is encrypted and you are authorized to send it. Do not send or store sensitive information through Web-based email.
- **Secure mobile devices.** Always lock your mobile device when it’s not in use. Never leave it in plain view or unattended. Do not give access to your mobile devices unless the requester is authorized. Obtain a privacy screen if you travel or work with sensitive information on a mobile device. Don’t use nonsecure public wireless access points to access or transmit sensitive data. Double-check taxis, airport lounges, and other public places when you leave, so you don’t forget a mobile device.
- **Beware of scams.** Thieves steal sensitive data by tricking people into disclosing user names and passwords. Such “phishing” scams can be attempted over the telephone when they pretend to be someone trustworthy (e.g., the helpdesk or an in-house developer). Do not disclose access information over the phone unless you know who you’re talking to and they are authorized to have the information. Watch for external email that asks you to click on a link to what appears to be a legitimate site, but could be a ploy to steal your access credentials. Double-check the URL of a suspicious page to spot a rogue site. Alert the IT security staff if you suspect a scam. Be careful.

DATA LOSS PREVENTION BEST PRACTICES

Data loss prevention (DLP) is essential to discover, monitor, and protect confidential data across network, storage, and endpoint systems. The following best practices have been proven to help IT security teams achieve effective risk reduction.

- **Gain complete protection.** In order to achieve complete protection, an organization should deploy all three aspects of data loss prevention:

  1. *Discover:* Find confidential data wherever it is stored (on laptops, desktops, file shares, databases), create an inventory of sensitive data, and automatically manage data cleanup.
  2. *Monitor:* Understand how confidential data is being used, whether the user is on or off the corporate network. Monitor email, Web mail, instant messages, FTP streams, copies going to a USB drive or CD/DVD, and printing, and gain enterprise visibility.
  3. *Protect:* Automatically enforce security policies to proactively secure data and prevent confidential data from leaving your organization.

  Organizations should also set policies on one unified platform so they can set a data protection policy once and enforce it everywhere.

- **Ensure accuracy.** Increase accuracy by leveraging detection technologies that can “fingerprint” structured or unstructured data (documents, databases) to look for exact matches of sensitive data.
- **Fix broken business processes first.** Reduce your risk of data loss by identifying broken business processes, the person who “owns” or is responsible for defining that process, and a secure way to fix the process and get business done.
- **Stop policy violations.** Monitoring and tracking policy violations is not enough. DLP must also be able to stop data transmissions that violate corporate policy before they leave the network.
- **Continuously measure your risk reduction.** Track and measure your progress with a four-step process:

  1. Establish a baseline of visibility on confidential data.
  2. Remediate incidents of data loss to identify where to target education and training efforts.
  3. Notify employees of policy violations in real time.
  4. Stop policy violations by preventing confidential data from leaving the organization across the network, storage, and endpoints.

- **Educate and train users.** Automated data loss prevention and other security controls must be supplemented by education and awareness training to enable employees to understand their corporate policies (see next page).

CONCLUSION

By implementing best practices for endpoint security, messaging security, and data loss prevention, your organization will reduce the risk of a data breach. Symantec invites you to consider our comprehensive offering of solutions for protecting the enterprise. Please contact your Symantec sales representative or one of our partners for more information.

SYMANTEC SOLUTIONS FOR ENTERPRISE PROTECTION

Effective security controls are essential in order to stop a catastrophic data breach. Symantec provides best-of-breed security solutions that automatically protect your data from external and internal threats—all while consolidating licenses and cutting operational cost and time. We invite you to consider the following solutions:

- **Symantec™ Protection Suite,** which creates a protected endpoint and messaging environment that is secure against today's complex security threats, and recovers your data quickly in the event of failure.
- **Symantec™ Data Loss Prevention,** which uses centrally managed policies to discover, monitor, and protect sensitive data wherever it is stored or used through deep content analysis.
- **Altiris™ Client Management Suite from Symantec,** which tightly integrates industry-leading technologies to reduce the total cost of owning client systems. It automates the tasks of deploying, managing, securing, and troubleshooting endpoints.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices andcontact numbers, please visitour website. For information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com