Anti-virus Management

Helps prevent and detect malicious code

Over the past year you have invested in anti-virus software for your user workstations. You thought you had established a widespread and far reaching approach to protect your company from malicious code. Then it happens—you receive a phone call. The network administrator from one of your partner companies tells you that your Web Server is transferring viruses their way. How could this have been avoided? Was there a better way to prepare? Was there a more beneficial approach to deployment?

Through its Managed Security Services, IBM can offer anti-virus management to provide complete outsourcing of key activities at various points in your infrastructure. This provides a multi-tiered and in-depth approach to help protect against malicious code.

Anti-virus workshop

The anti-virus workshop is designed to assist with a malicious code security assessment of your business environment. The intended result of the workshop is a suggested action plan to protect your business assets from risks of unwanted malicious code intrusions.

The anti-virus planning session will be conducted at your site by an IBM consultant who is experienced and skilled in dealing with malicious code security matters in today’s business environment. This session is intended to assist in exploring various aspects of virus security. The anti-virus workshop is completely customized to meet your needs. After the session, IBM will provide a final written report.

Managed anti-virus perimeter defense

Managed anti-virus perimeter defense will allow for the installation and configuration of software, owned by you, on your firewalls and/or gateways. The technology will work with the firewall to scan various protocols in and outside of your company for malicious code. Virus definition updates will occur on schedule or as required and virus event logs will be monitored weekly for events requiring attention.

IBM consultants will provide advice on virus activity, providing limited incident response, and real-time response to ‘threshold monitoring’ at an additional cost.

Managed URL filtering

This filtering will monitor and prevent users from visiting undesirable Web sites that could lead to malicious code activity.

Your URL filtering software will be installed and configured on your servers. IBM will support URL filtering software that automatically obtains rule updates from the software vendor. URL rule updates will occur on schedule and software will be updated as required. Logs will be monitored weekly for events requiring attention and your requests will be reviewed as they arise.

Managed anti-virus vendor product updates

Though tested prior to release, anti-virus software updates may require additional testing against your infrastructure to validate its effectiveness in your environment. IBM will provide virus pattern updates that have been properly tested with a scripted quality assurance test on your client workstation for the protection of malicious code penetration. We will support customer anti-virus client products such as Symantec’s Norton Anti-Virus, McAfee, and Trend that have a defined virus definition update delivery system.

These tests are performed against six images that you provide. Any required updates to the product will be rolled out to your clients or gateways.
**Managed anti-virus enterprise defense**
A comprehensive anti-virus management solution for your entire network is your best defense against malicious code penetration. IBM can provide installation assistance, management, configuration, updates, and notification services for clients, servers, firewalls, gateways, and URL filter servers. Managed anti-virus enterprise defense also includes emergency notification of new viruses, scheduled anti-virus software definition updates, and an annual on-site workshop.

**Threshold Monitoring**
Early detection of virus activity can minimize the impact of a virus infection. IBM offers 24 hours, 7 days a week monitoring of alerts generated by the anti-virus software when predetermined thresholds are exceeded. Personnel from the IBM Security Operations Center will analyze the incident(s) and initiate an agreed upon escalation process.

**Relying on our experience**
The people of IBM Global Services—comprising the largest professional security community in the world—offer broad experience and a proven track record of successful engagements. IBM can help reduce your risk and exposure in today’s interconnected world by leveraging our extensive intellectual capital and best practices models to develop superior business continuity and security programs.

**For more information**
To learn more about managed security services or other IBM security services, contact your local IBM sales representatives or Business Partner, or visit: [ibm.com/services/continuity](http://ibm.com/services/continuity)