The Antivirus Defense-in-Depth Guide

View all security guidance topics
Server Security
Desktop Security
On This Page

Introduction

Although many organizations have deployed antivirus software, malicious software such as computer viruses, worms, and Trojan horses continue to infect computer systems around the world. There is no single reason for this apparent contradiction, but the current situation indicates that the standard approach of deploying antivirus software on each computer in your environment may not be sufficient.

The Antivirus Defense-in-Depth Guide provides an easy to understand overview of different types of malware, or malicious software, including information about the risks they pose, malware characteristics, means of replication, and payloads. The guide details considerations for planning and implementing a comprehensive antivirus defense for your organization, and provides information on defense-in-depth planning and related tools that you can use to help reduce your risk of infection. The final chapter of the guide provides a comprehensive methodology to help you quickly and effectively respond to and recover from malware outbreaks or incidents.
Top of page
Guide Chapter Summary

The Antivirus Defense-in-Depth Guide consists of four chapters:
Chapter 1: Introduction

This chapter presents a brief introduction to the guidance, an overview of each chapter, and the intended audience of the guide.
Chapter 2: Malware Threats

This chapter defines the primary types of malware and specifies what types of programs are included — and excluded — in this category. It also provides information about malware characteristics, attack vectors, means of propagation and payloads.
Chapter 3: Antivirus Defense-in-Depth

This chapter details considerations for establishing a comprehensive antivirus defense for your clients, servers, and network infrastructure. It also discusses user policies and general security measures that Microsoft recommends considering when forming your overall security plan.
Chapter 4: Outbreak Control and Recovery

This chapter provides a step-by-step approach to resolving and recovering from malware attacks, based on

industry best practices and internal operations at Microsoft.
Top of page
Give Us Your Feedback

We would appreciate any feedback you might have on this guidance. In particular, we would be grateful for any feedback on the following topics:

- How useful was the information provided?
- Were the step-by-step procedures accurate?
- Were the chapters readable and interesting?
- Overall, how would you rate the guidance?

Send your feedback to secwish@microsoft.com. We look forward to hearing from you.