Executive summary the microsoft information technology

Business, Company

The Microsoft InformationTechnology(Microsoft IT) group needed an antivirus solution to adequately address the growing threat from the many types of Internet-borne malicious software, also known as malware. When Microsoft IT assessed its requirements for an enterprise anti-malware solution, the group realized the challenge of the ever-changing landscape of client security.

Centralized management, rapid reporting, and a positive user experience for clients were some features that Microsoft IT sought in a client security solution. A product group within Microsoft consulted with the security staff of Microsoft IT for the initial development of a new anti-malware solution, Microsoft® Forefront™ Client Security. As the new product emerged, Microsoft IT volunteered to test it, first in a labenvironment, and then in an enterprise production environment. Microsoft IT developed and tested a server management group for administering the new system. Testing revealed that the server choices more than sufficed, but they required more advanced storage. For this reason, the server management group attached to a storage area network (SAN) for use by data collection and reporting services. Lab testing was successful, so Microsoft IT rolled out the solution into a production environment in a limited-participant pilot.

The initial pilot was successful, and soon 10, 000 participants were using the product. The ability to quickly see reports on the security status of all participating clients quickly facilitated executive queries. Moreover, a centralized console simplified client management. If a report on the console alerted Microsoft IT security staff to a misconfiguration that exposed a vulnerability or a possible malware infection, the team could easily resolve

the issue. The team could quickly move through console reports and remotely correct the misconfiguration. Or, the team could initiate an anti-malware scan on the client computer without involving the end user. Microsoft IT worked with the Forefront Client Security product development team to expand the pilot to 50, 000 worldwide users.

Microsoft IT also integrated the management server group services used by Forefront Client Security into the existing network infrastructure wherever possible. This white paper shares architecture, design, and deployment considerations. This paper briefly discusses the advantages of advanced Forefront Client Security features. The paper also describes how Microsoft implemented the Forefront Client Security solution in its environment. This paper assumes that readers are technical decision makers and are already familiar with the following:•Anti-malware security technologies Microsoft server products such as Microsoft SQL Server® 2005 database software, Microsoft Operations Manager 2005, and Microsoft Systems Management Server (SMS) 2003 •Windows Server® technologies such as Windows Server Update Services (WSUS) IT groups can employ many of the principles and techniques described in this paper to manage risk in their organizations. Similarly, the design considerations for anti-malware security infrastructure can be applied to most enterprise-scale IT environments that use