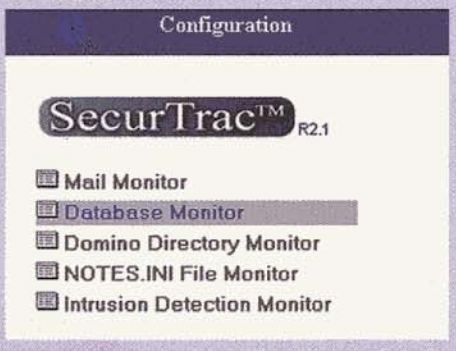
SecurTrac

BY JASON COLLIER

SecurTrac, a Domino server add-on product from Extracomm Technologies, Inc., takes Domino security to the next level by providing enterprise-level auditing and tracking features in an easy-to-use, affordable product. SecurTrac monitors changes in several Domino-environment areas, including Notes documents, database Access Control Lists (ACL), application designs, and the server's Notes.INI file.

FIGURE 1

SecurTrac monitors user-selected databases and objects for unauthorized changes



It also monitors e-mail messages and can identify possible intrusion attempts as soon as they begin.

SecurTrac uses two Notes databases that reside on the Domino server. The SecurTrac Configuration Database, SCTCFG.NSF, helps administrators configure which databases, Notes documents, fields, and other resources SecurTrac will monitor (Figure 1), such as changes to the server's Notes .INI file and possible intrusion attempts. SecurTrac logs all changes to the monitored resources in the SecurTrac Log Database, SCTLOG.NSF.

Not only does SecurTrac monitor resources for changes, but it also provides detailed monitoring of the changes within those resources. If a field value has been changed on a Notes document, for instance, the change is stored in the SecurTrac Log Database, and the Administrator can readily identify the change and take appropriate action. SecurTrac accomplishes this by tracking several key aspects of any change, such as who made the change, when the change occurred, what the change was, and where the change happened. In particular, it records whether the change occurred on a local server or via replication from another server or workstation.

SecurTrac provides logging information on all areas of data access, such as e-mail messages, including what users have opened, added, updated, or deleted from any Notes database. Administrators can extend SecurTrac to monitor all or certain aspects of the Domino Directory. The administrator can also specify multiple Domino Directories for monitoring and the types of changes to monitor. Changes can be defined as additions, updates, and deletions. SecurTrac configuration options include monitoring only certain document types within the Domino Directory.

SecurTrac's most important feature is the ability to detect intrusion attempts. In a large environment, a malicious user could add him or herself to the Domino Directory, access secure resources, and delete his or her access before detection. This is where SecurTrac's ability to configure event notifications is invaluable.

SecurTrac can send immediate notifications to administrators and other designated users via e-mail alerts when any specified conditions occur. Alerts can go to an e-mail address, a Simple Messaging Service (SMS) device such as a mobile phone, or to a pager. SecurTrac also generates a detailed log of the activity as it occurs so the administrator can respond appropriately.

Authorized users can configure and administer SecurTrac using a Lotus Notes Client 5.0 or greater, Microsoft Internet Explorer 4.0 or greater, and Netscape Navigator 4.5 or greater. ❍

Jason Collier is a senior systems engineer with Wireless Knowledge, Inc. He is a Certified Lotus Professional in application development and system administration for both R4 and R5 and a Certified Lotus End-User Instructor. You can reach him at jcollier@WirelessKnowledge.com.

SecurTrac

Platforms: Windows NT/2000, Domino R5. Requires 10 MB available RAM, 50 MB minimum disk space (200 MB recommended).

Vendor: Extracomm Technologies
(416) 222-5280
Fax (416) 222-7371
http://www.extracomm.com