

# McAfee Network User Behavior Analysis Studio

Monitoring user behavior is one of the surest ways to reduce insider risk and improve audit-readiness. So how do you actually implement it within your network? Where do you get the necessary tools for defining and testing policies, and automatically monitoring user behavior against these policies?

McAfee® Network User Behavior Analysis (Network UBA) Studio enables corporate security architects to quickly create and refine user-based policies, perform detailed traffic analysis, and associate users and critical business systems with policy violations. This application is included and used with Network UBA Monitor or Network UBA Control Center for real-time traffic analysis and investigation.



## McAfee Network UBA Studio Overview

Through a graphical object-oriented development environment, security and network architects have access to all the tools they need to prototype, develop, test, and edit user-based policies (based on business and security policies) and automated security analyses. Network UBA Studio also provides a network topology view, where administrators can quickly model the network to be monitored and define how the known network assets interact with each other.

After initially defining a user policy, administrative staff can evaluate it against packets captured from the network (via span port or network tap or via flow data like NetFlow and JFlow) to see if it performs as expected. Network UBA Studio's Analyzer feature can be employed to examine the

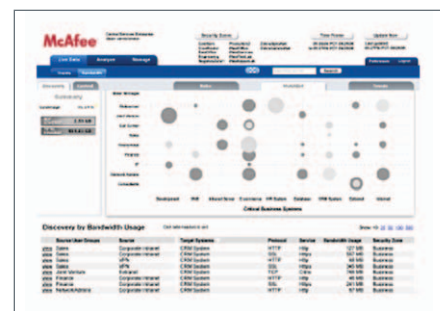
results and refine the user policies. Also, Network UBA Studio lets security teams manage native user-based behavioral signature functionality.

## Pre-Built Controls and One-Click Control Creation

Network UBA Studio delivers hundreds of pre-built control templates, which enable simple selection of network usage controls for verifying that the relationships between users, assets, and applications conform to security best practices and enterprise policies. Controls at the application command/transaction level provide deep granularity to enforce who can do what on the network. In addition to pre-built controls, users can also utilize a one-click option to add new controls in discovery mode.



The Discovery View graphically provides enterprises an initial understanding of what user groups are accessing which critical systems. This visibility can save significant time in gaining knowledge about usage of systems by users, protocols/services, bandwidth, and others.



Utilizing role-based controls, the Control View graphically illustrates the network usage of users to critical systems and clearly denotes what activity is acceptable, unacceptable and what activity merits a closer look by the security and operations teams.

**Rapid, Simple Deployment**

- Network appliances provide easy, centralized deployment
- Passive monitoring with no network reconfiguration minimizes risk
- No dependency on server agents or logs minimizes IT effort
- Distributed analysis provides real-time results and enterprise scalability

**McAfee Network UBA Solution Capabilities (Monitor/s plus Studio)**

<p><b>Network Monitoring and Analysis</b></p> <ul style="list-style-type: none"> <li>• Monitoring via port mirroring or passive network taps for deep packet inspection</li> <li>• Monitoring via flow data from Cisco Netflow, Juniper J-Flow, and others</li> </ul>	<p><b>Detection Capabilities</b></p> <ul style="list-style-type: none"> <li>• Network scan detection</li> <li>• Service probe detection</li> <li>• Protocol anomaly detection</li> <li>• Network behavior anomaly detection</li> <li>• Application behavior anomaly detection</li> <li>• Unauthorized services detection</li> <li>• Unauthorized communication channels detection</li> <li>• Native IDS signature detection:                         <ul style="list-style-type: none"> <li>» Custom signature deployment</li> <li>» Regular and on-demand signature updates</li> </ul> </li> </ul>
<p><b>Identity Capabilities</b></p> <ul style="list-style-type: none"> <li>• User identity tracking via real-time integration with existing directory infrastructure:</li> <li>• Leverages existing user, role, and policy contexts</li> <li>• All user activity is tracked from the instant a user accesses the network</li> <li>• Continuous, non-invasive polling of directory</li> <li>• Moves, adds, and changes done once in the directory, which then filter down to Network UBA Monitors</li> <li>• Identity-, group-, and role-based controls:</li> <li>• Control granularity: user groups vs. network segments</li> <li>• Controls expressed in easy-to-understand business contexts</li> <li>• Supports typical, random address pool DHCP environments</li> </ul>	<p><b>Integration</b></p> <ul style="list-style-type: none"> <li>• Integration with Microsoft Active Directory and LDAP-based directories for user identity information</li> <li>• Integration with network routers and switches for blocking actions</li> <li>• Integration with flow-based data from Cisco, Juniper, and others</li> <li>• Export event alerts to security information manager (SIM) and other third-party systems such as ArcSight via:                         <ul style="list-style-type: none"> <li>» SNMP</li> <li>» SMTP</li> </ul> </li> <li>• Integration with non-Windows-based identity clients such as Centrify</li> <li>• Import of vulnerability assessment</li> </ul>
<p><b>Application Decode</b></p> <ul style="list-style-type: none"> <li>• Packet capture and decode at command level for 20 key applications, including: DHCP, AIM, DNS, FTP, HTTP, IRC, Kerberos, POP, SIP, SMTP, SSL, TLS, YIM, and more</li> </ul>	<p><b>Certification</b></p> <ul style="list-style-type: none"> <li>• Common Criteria EAL 3 Certified</li> <li>• U.S. Department of Defense accreditations for operating on SIPRNet, NIPRNet, and JWICS</li> </ul>
<p><b>Controls</b></p> <ul style="list-style-type: none"> <li>• Over 300 pre-built network and application behavior controls:                         <ul style="list-style-type: none"> <li>» Includes URL and rates controls</li> <li>» Wizard-based interface to define controls and control groups and one-click customizable control creation feature</li> <li>» User-defined application-layer thresholds by number of events and bandwidth by day and hour</li> <li>» User-defined HT</li> </ul> </li> </ul>	

