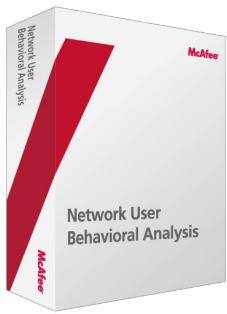


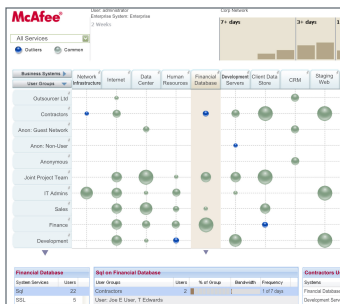
# McAfee Network User Behavior Analysis (Securify) Monitor



## Monitor Options

McAfee provides the following Network UBA Monitor options:

- Monitor SE – bandwidth up to 1 Gbps for heavy-traffic networks
- Monitor – bandwidth up to 400 Mbps
- Monitor LE – bandwidth up to 100 Mbps
- Monitor LE-50 – for monitoring small, remote office networks of 50 or fewer machines
- Flow Monitor SE – for flow-based monitoring across larger networks and segments
- Flow Monitor – for flow-based monitoring across smaller networks and segments



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, etc.

## Summary

Do you know who's doing what on your network? Do you want to cost-effectively improve your network visibility?

McAfee Network User Behavior Analysis (Securify) Monitor provides a continuous, real-time view of what business users are actually doing across your complex network environment. McAfee Network User Behavior (Network UBA) Monitor appliances leverage your existing infrastructure and the identity and role information in your existing directory to deliver cost-effective discovery, analysis, and control of user access and behavior across networks and systems.

Network UBA Monitors provide two intuitive views of network traffic:

- Pure "Discovery" mode, which requires no baselining
- "Controls" mode, which automatically verifies traffic against policy and role-based controls

## McAfee Network UBA Monitor Overview

McAfee Network UBA Monitor appliances are the cornerstone of the overall McAfee Network UBA solution. Monitors are network-based and designed to capture and analyze critical traffic data inside the network using one of three methods:

- Flow Monitors leverage existing flow-based data from Cisco Netflow and Juniper J-Flow for analysis. This broader network view is often useful for gaining a cost-effective, enterprise-wide view of who is doing what and from where across the entire network, including remote locations.
- Monitors passively capture, decode, and analyze traffic via native deep packet inspection (DPI). They use port mirroring or passive network taps to obtain full packet data for protocol decoding up to the application layer (layer 7). This level of

detail is often required to ensure a tamperproof view of network activity within critical data centers and critical business systems.

- When using McAfee Network UBA management appliances, you can use Monitors in a "Mixed" mode that combines both DPI and flow-based data.

Note that each Monitor is capable of performing its own analysis in a distributed manner, or you can choose to aggregate the data from your Monitors to a McAfee Network UBA management appliance, such as the McAfee Network UBA Control Center.

## Simplified Setup

Deployment takes only a matter of hours and you can gain improved visibility of 'who, what and where' in a matter of minutes after deploying. Monitors require no agents, no application integration, and no recoding. For identity-based monitoring, McAfee Network UBA Monitors leverage your existing directory information, such as that found in Microsoft Active Directory, including groups and memberships.



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.

**Benefits**

- 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 Monitoring Appliance Specifications**

**Technical Specifications**

- 1 Intel Xeon 5130, 2.00 GHz, 1,333 MHz, 4 MB cache, dual-core CPU (for Monitor SE, Flow Monitor SE, and Flow Monitor: 1 Xeon 5150 2.66 GHz CPU)
- Two 250 GB, 32 MB cache, 7.5K RPM SATA II, 3.5" hard drives
- 4 GB RAM

**Physical Data**

- Rack-mountable 1U device
- Height: 1.7 inches
- Width: 16.9 inches
- Depth: 28.6 inches
- Weight: 30 pounds

**Environmental Limits Overview**

- Operating temperature: 10° C to 35° C / 50° F to 90° F (maximum change rate not to exceed 10° C per hour)
- Non-operating temperature: -40° C to 70° C
- Non-operating humidity: 90%, non-condensing at 28° C

**Power and BTU Specs**

- Max surge amps = 9.5
- Max running amps = 8.5
- Avg running amps = 6.25
- Watts = 750
- BTU/hr = 2,550

**Safety Compliance**

- UL60950 – CSA 60950 (USA/Canada)
- EN60950 (Europe)
- IEC60950 (International)
- CE – Low-voltage Directive 73/23/EEE (Europe)

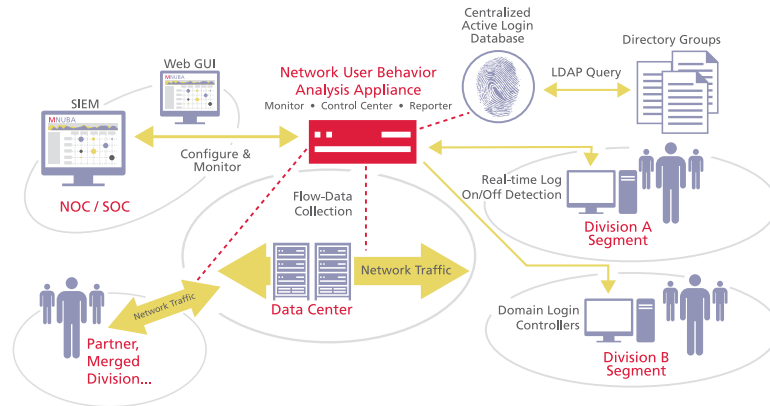
**Certification**

- Common Criteria EAL 3 Certified
- U.S. Department of Defense accreditations for operating in SIPRNet, NIPRNet, and JWICS

Technical information provided by Intel Corporation. Product specifications subject to change at any time without prior notice.



McAfee, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054  
888 847 8766  
www.mcafee.com



Representative McAfee NUBA solution deployment in front of a data center where critical business systems reside.

**McAfee Network UBA Capabilities**

**Network monitoring and analysis**

- Monitoring via port mirroring or passive network taps for deep packet inspection
- Monitoring via flow data from Cisco Netflow, Juniper J-Flow, and others
- Identity capabilities
- User identity tracking via real-time integration with existing directory infrastructure:
- Leverages existing user, role, and policy contexts
- All user activity is tracked from the instant a user accesses the network
- Continuous, non-invasive polling of directory
- Moves, adds, and changes done once in the directory, which then filter down to NUBA Monitors
- Identity-, group-, and role-based controls:
  - » Control granularity: user groups vs. network segments
- Controls expressed in easy-to-understand business contexts
- Supports typical, random address pool DHCP environments

**Application Decode**

- 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

**Controls**

- Over 300 pre-built network and application behavior controls:
- Includes URL and rates controls
- Wizard-based interface to define controls and control groups and one-click customizable control creation feature

- User-defined application layer thresholds by number of events and bandwidth by day and hour
- User-defined HT

**Detection Capabilities**

- Network scan detection
- Service probe detection
- Protocol anomaly detection
- Network behavior anomaly detection
- Application behavior anomaly detection
- Unauthorized services detection
- Unauthorized communication channels detection
- Native IDS signature detection:
  - » Custom signature deployment
  - » Regular and on-demand signature updates

**Integration**

- Integration with directories such as Microsoft Active Directory and LDAP-based directories
- Integration with network routers and switches for blocking actions
- Integration with flow-based data from Cisco, Juniper, and others
- Export event alerts to security information manager (SIEM) and other third-party systems such as ArcSight via:
  - » SNMP
  - » SMTP
- Integration with non-Windows based identity clients such as Centrify
- Import of vulnerability assessment

**Certification**

- Common Criteria EAL 3 Certified
- U.S. Department of Defense accreditations for operating on SIPRNet, NIPRNet, and JWICS