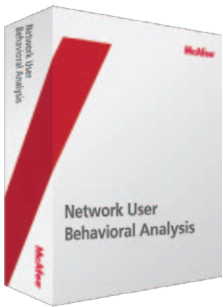


# McAfee Network User Behavior Analysis (Securify) Control Center



### Deployment Options

McAfee offers two types of Network UBA Control Centers:

- One Control Center SE can accommodate up to 25 Network UBA Monitors.
- One Enterprise Control Center can consolidate activity from up to 10 Network UBA Monitors.

Thanks to the flexibility of Network UBA Control Centers, you are able to mix and match any of the different Monitor family members: Monitor SE, Monitor, Monitor LE, Monitor LE-50, Flow Monitor SE, and Flow Monitor. This way, you can take advantage of varying bandwidth needs and data collection methods, and still have a single point of management for discovering and controlling network activity.

### Benefits

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

### Summary

McAfee Network User Behavior Analysis (Securify) Control Center is a complementary technology to McAfee Network User Behavior Analysis (Network UBA) Monitors. Control Center (formerly Enterprise Manager) simplifies your IT tasks by concentrating management of multiple Network UBA Monitors in one place. As a result, you are able to more efficiently administrate multiple Monitors with a minimum of personnel and hassle and gain a broad, cost-effective view of ‘who is doing what and where’ on your network.

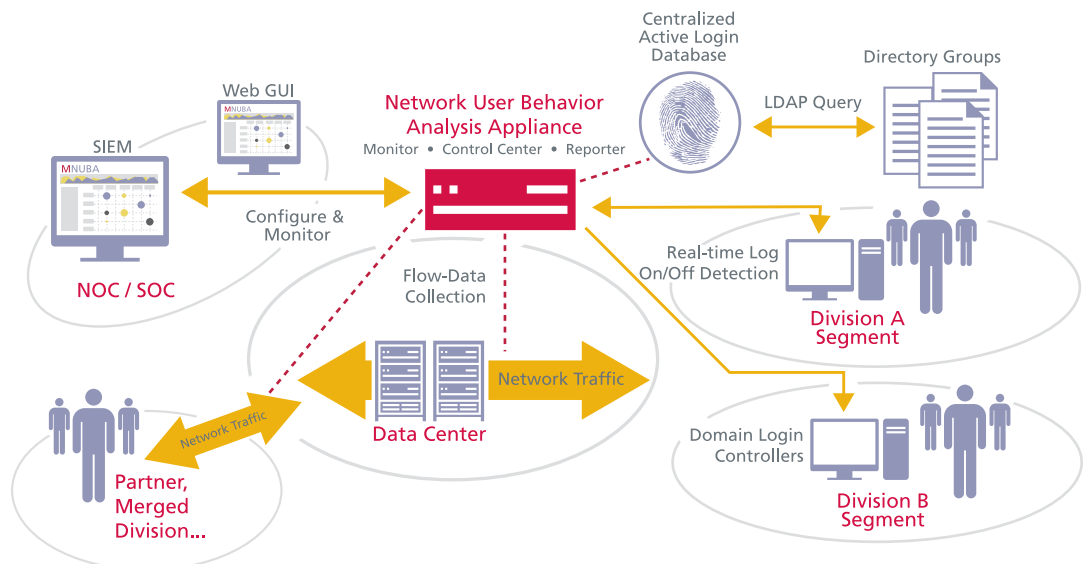
### McAfee Network UBA Control Center Overview

McAfee Network UBA Monitors provide a continuous, real-time view of what business users are actually doing across your complex network environment. They can 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.

McAfee Network UBA Control Center appliances are capable of consolidating and centralizing the ongoing monitoring, analysis, and management of all sizes of deployments—everything from a few Network UBA Monitor appliances at a single site to a worldwide McAfee Network UBA solution deployment.

In addition, large entities can easily stratify and delegate their management capabilities with Network UBA Control Center. For example, you could retain the ability to analyze and control network activity at an overall organizational level while also allowing your various operating divisions or security zones to monitor and manage network activity that’s specific to their group.



Representative McAfee Network UBA Control Center and Monitor appliances deployed in front of a data center where critical business systems reside.

**McAfee Network UBA Control Center Appliance Specification**

**Technical Specification**

- 1 Intel Xeon 5150, 2.66 GHz, 1,333 MHz, 4 MB cache, dual-core CPU
- Two 150 GB, 16 MB cache, 10K RPM SATA 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)
- IE60950 (International)
- CE – Low-voltage Directive 73/23/EEC (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.



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.

**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 Network UBA 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



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.

- 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 (SIM) 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

