

User Behavior Analysis: Gaining Real-Time Cost-Effective Visibility into Who Is Doing What, Where on Your Network



Executive Summary

If your company is like most, there are real business needs and compliance requirements compelling you to continuously monitor and verify:

- Who is accessing critical business systems?
- What are these users doing?
- Where on the network are they doing it?

To efficiently reduce risk inside the network and meet compliance requirements, it's vital to have continuous visibility into your network and critical business applications. The challenge is that, when manually attempted, this visibility is often nothing more than a static, after-the-fact "snapshot in time." It falls seriously short of a continuous, accurate, and cost-effective view of user access and behavior.

This lack of visibility and its corresponding lack of decision support send IT and security teams scrambling whenever threats impact the business. Such lack of visibility also frequently leads to audit findings regarding:

- Gaps in continuously proving the verification of third-party access
- Gaps in continuous monitoring of boundary conditions such as segregation of duties and international privacy laws
- Gaps in monitoring privileged user access

McAfee Network User Behavior Monitor Overview

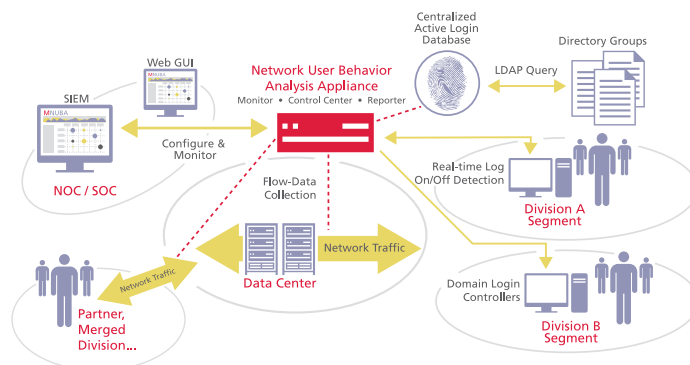
To solve these challenges, McAfee Network User Behavior Monitoring (Network UBA) (Security) provides automated, identity-based monitoring to keep you in compliance and in control. This comprehensive monitoring solution delivers complete visibility and verification of who is doing what and where on an automated, continuous, real-time basis. By identity, we mean the actual user name, group name, and role correlated to behavior and delivered in real time—not after the fact. Our out-of-band, network-based solution requires no endpoint agents or recoding of custom applications, and it can be deployed and running in hours.



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.



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.



Representative McAfee Network UBA solution deployed in front of a data center hosting critical business systems.

Solution Brief User Behavior Analysis: Gaining Real-Time, Cost-Effective Visibility into Who Is Doing What, Where on Your Network

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

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

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

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

Ultimately, companies measure the value they receive from McAfee Network UBA through a combination of:

- Reduced insider risk
- Dramatically improved efficiency through network visibility
- Continuous compliance metrics

Overarching Business Challenge: Lack of Visibility into the Network

According to McAfee estimates culled from interviews with dozens of Fortune 500 firms, up to 70 percent of projects today require manual discovery and analysis to determine who is doing what on the network and where. Yet manual processes such as log analyses, surveys, and other activities are historically inaccurate and labor-intensive. As a result, they are infrequently performed. Even when organizations do gain a snapshot of visibility, they are unable to continuously see and verify who is on their network, where each user came from, where each user is going, and what each user is doing once they get there.

The requirements for visibility and verification across three top IT initiatives are discussed below.

Challenge: Limited visibility into who is doing what and where on critical business systems (insider risk)

Unsecured and improper practices by authorized insiders can create substantial risk to critical business systems. Outsourcers, offshore developers, contractors, careless employees, partners, joint ventures, and others must be monitored. Yet monitoring security to the standards recommended by CERT and others is nearly impossible to do in real time with traditional security tools. And, using log data to get this level of information can drain valuable IT resources while still falling short of delivering real-time operational visibility and control.

McAfee Network UBA provides continuous, real-time visibility through monitoring the “who, what, and where” in your network to prevent risks and threats. Specifically, Network UBA enables you to:

- Use watch lists to monitor high-risk users in real time and receive alerts on misuse, such as leap-frogging or unauthorized outsourcing, custom to your unique business environment
- Detect anomalous, unsecured, and malicious behaviors by outsourcer and privileged users in real time
- Detect precursor activities to network misuse, such as network scans, service probe, failed logins, and worm propagation
- Detect when users exceed established thresholds for network bandwidth, system time, and other resources on a per-user basis
- Provide network context to detect unauthorized sources and bypassing of access systems
- Fill gaps in network access control (NAC) and content monitoring and filtering (CMF) deployments by verifying all relevant traffic, even if masked
- Monitor systems containing personally identifiable information (PII)
- Protect critical systems
- Securely connect and monitor the networks of partners and military coalition allies
- Reduce vulnerabilities and risks associated with the transition from IPv4 to IPv6

Challenge: Limited visibility increases workload substantially during infrastructure change and ongoing network operations

Be it a merger or acquisition, or a network segmentation, virtualization, or consolidation, companies require visibility into who is doing what on the network and where—before, during, and after complex infrastructure changes. Yet this level of visibility demands time-intensive manual processes and resources.

McAfee Network UBA readies your business with:

- Broad, cost-effective visibility into your network’s “as is” state for network and data center consolidation and legacy network migration, including:
 - Application usage for connecting and consolidating systems
 - Application and port usage to ensure system compatibility

Solution Brief User Behavior Analysis: Gaining Real-Time, Cost-Effective Visibility into Who Is Doing What, Where on Your Network

McAfee Network UBA Capabilities Continued

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

Certification

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

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

- » System usage for consolidations and decommissioning
- » Network and application conformance to security best practices
- » User migration status
- Improved bandwidth utilization
- An intuitive, real-time view of network traffic to resolve misconfigured firewalls, routers, and other devices

Challenge: Reducing cost and efforts for regulatory compliance and audit preparation

The lack of visibility discussed above is also partially responsible for the high costs and extra efforts associated with IT audits. These audits are typically driven by audit findings of bypasses or gaps in existing preventative controls, which are much more difficult to remediate during and after audits.

McAfee Network UBA helps simplify regular IT audits and provides for audit-readiness. It is also proven to help ensure regulatory compliance and prevent audit findings in the first place by filling gaps in existing preventive controls. McAfee Network UBA is most valuable to organizations that are governed by two or more regulations, including Sarbanes Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI), and other federal and state regulations.

McAfee Network UBA helps proactively address periodic IT audits, reduces audit prep time, and improves audit posture by providing:

- Monitoring for verification and compliance
- Verifying actual access by users, groups, and roles to ensure effectiveness of access controls
- Simplifying compliance monitoring and reporting
- Improving audit posture through detection of unauthenticated users and unapproved applications, and de-provisioning of users or privileges on non-integrated commercial applications
- Verifying access of privileged users with broad rights, such as outsourced IT staff
- Providing better proof for auditors, such as access verification, configuration management, and more
- Verifying access after implementing a logical access control system to meet HSPD-12
- Identification of assets and network access points
- Ongoing monitoring to ensure compliance with PCI, SOX, FISMA, and others

Challenges with existing solutions: manual, time-intensive, limited visibility

You could use multiple point solutions and manual processes to achieve the level of visibility and verification required for each IT initiative in the previous section. However, the cost and effort of such an attempt is prohibitive, and for resource-tapped IT teams, not realistic.

The following table provides a brief overview of typical solutions employed to gain visibility and some of the challenges in using these solutions:

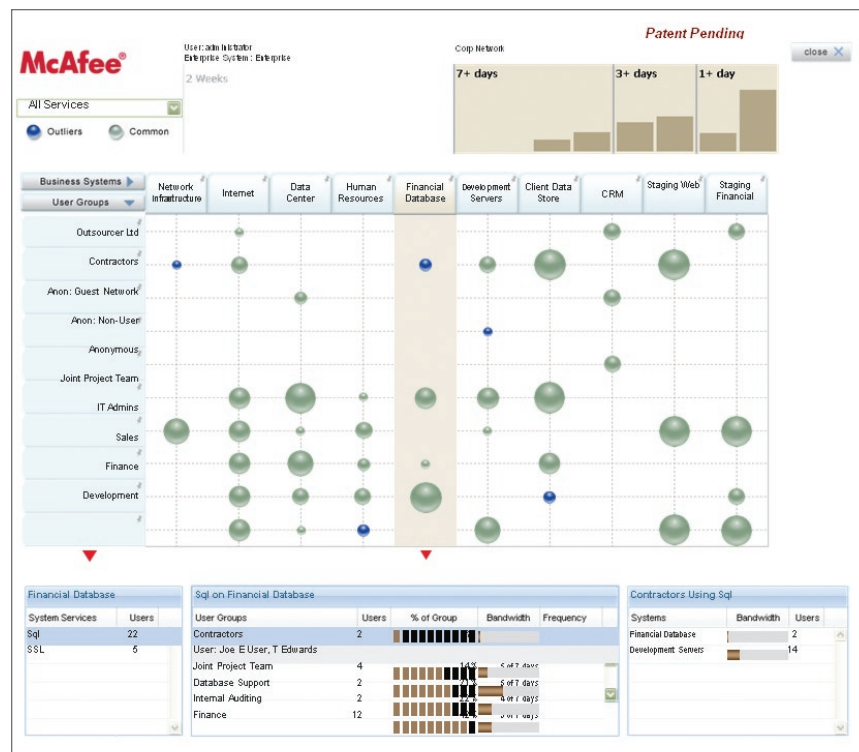
Existing Method or Solution	Challenges
Manual surveys and polls	Manual surveys and polls are an intrinsic part of running a network. However, when used for real-time visibility, they fall short. Due to multiple sources and human error, they are inaccurate. They are also inefficient and labor-intensive.
Security Information/Event Management (SIEM) and log collection tools	SIEMs are only as good as the underlying elements that preprocess data and send alerts to the SIEM console. SIEMs and log management solutions also process information available from application and database logs. But their primary focus is on collecting data for post-incident forensic analysis. SIEMs don't provide real-time visibility or verification.
Network Behavior Analysis (NBA)	Used for examining anomalous network usage, NBAs typically require setting a baseline. This is very difficult to do in a dynamic environment without creating too much noise. Also, NBAs typically don't look deep into application transactions, such as HTTP Get versus HTTP Put, or application data, such as the content of the URI field. They also don't typically tie the actual user name, group name, and role to an activity for proactive, real-time visibility.
Network Access Control (NAC)	While NAC is great for preventing compromised hosts from connecting to the corporate network and checking hosts for overall security posture, it is limited in its ability to track post-admission activity. The static snapshot approach doesn't monitor or enforce subsequent activities by that host once it has access.

Solution Brief User Behavior Analysis: Gaining Real-Time, Cost-Effective Visibility into Who Is Doing What, Where on Your Network

Unique Feature: Automated Discovery

McAfee Network UBA's automated discovery capability helps uncover the "who, what, and where" during the planning phase of change projects, without requiring any rule definition. The solution's Discovery Dashboard provides a single view of passively monitored traffic and correlates user groups and their associated activity on critical business systems. McAfee Network UBA's appliances require no agents and communicate directly with existing directories, leveraging existing groups and memberships. (Custom groups can be added if required.)

McAfee Network UBA also provides additional analysis capabilities, including the ability to focus on a single system. For example, you could concentrate Network UBA on a specific CRM or accounting system. Likewise, you can use Network UBA to discover all user groups or focus on a specific user group, office location, or network boundary. For instance, you could monitor for sales representatives accessing a particular system from headquarters. Additional information on what users are doing is also provided, including protocol decode, ports, bandwidth, URLs, and commands. This level of detail is extremely useful for network rezoning and segmentation, or application and server moves that might impact users' ability to access their applications.



The Network UBA Discovery View graphically provides enterprises an initial understanding of what users and groups are accessing which critical systems (automatically, without requiring a static baseline). This visibility can save significant time in gaining knowledge about usage of systems by users, protocols/services, bandwidth, etc.

Unique Feature: Automated Verification

McAfee Network UBA's verification capability builds on the discovery view. McAfee NUBA verification automatically verifies traffic against role-based controls and pre-built security best practices. McAfee Network UBA offers over 300 pre-built and customizable controls to verify what users are doing after gaining access to the network. McAfee Network UBA's appliances require no agents and communicate directly with existing directories, leveraging existing groups and memberships. (Custom groups can be added if required.)

Solution Brief User Behavior Analysis: Gaining Real-Time, Cost-Effective Visibility into Who Is Doing What, Where on Your Network

Unique Feature: Identities Based on Actual User Name, Group, and Role
 McAfee Network UBA tightly integrates with existing directory stores, such as Microsoft Active Directory, leveraging actual user, group, and role information to dynamically determine when a user accesses the network. McAfee Network UBA queries the directory in real time, and then correlates users and their groups with all related access and activity. Note that user identity credentials are detected in the traffic by McAfee Network UBA without the use of any agents on the client or server side.

Here's an example of McAfee Network UBA in action. A user named jsmith logs into the network. McAfee identifies this action and immediately determines that jsmith is part of the marketing group and has a job role that allows her access to the marketing database and a joint-venture database but not the finance database. McAfee Network UBA continues to monitor network traffic to ensure that jsmith's actions abide by this policy as well as all other established security controls.



Applying user-based policies, the Network UBA Control View graphically illustrates the network usage of users and groups to critical systems and clearly denotes what activity is acceptable, unacceptable and what activity merits a closer look by the security and operations teams.

McAfee Network UBA verification can instantly pinpoint and provide real-time alerts on the following representative examples:

- Access by non-authenticating users, such as terminated employees who have had their access privileges revoked
- Network access exceptions such as printers that are not behaving as expected
- Verifying access of users that should be on the network, such as reassigned employees or outsourcers who inappropriately, perhaps inadvertently, access systems they shouldn't
- Unsecured or malicious activities, including tunneling of services like FTP inside of HTTP to transit firewalls
- Verifying expected usage of administrative protocols or commands, such as web authoring

How McAfee Network UBA Is Deployed

McAfee Network UBA offers a tiered architecture that comprises McAfee Network UBA Monitors, McAfee Network UBA Control Center appliances, and McAfee Network UBA Reporter appliances. Our solution has the deployment advantages of an out-of-band, network-based solution without the need for agents or application integration and is proven at highly sensitive networks worldwide, monitoring hundreds of thousands of users for a single customer and monitoring over 3 million users in real-time across all customers.

McAfee Network UBA Monitor appliances 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:

- Monitors can 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.

Business Brief User Behavior Analysis: Gaining Real-Time, Cost-Effective
Visibility into Who Is Doing What, Where on Your Network

- Flow Monitors can leverage existing flow-based data from Cisco Netflow, Juniper J-Flow, and others 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.
- When using McAfee Network UBA management appliances, you can use Monitors in a “Mixed” mode that combines both DPI and flow-based data.

McAfee Network UBA Reporting appliances overview

Network UBA Monitors can perform analysis on a distributed basis. However, for longer-term reporting, McAfee Network UBA Reporter appliances can provide a data warehouse to capture and query data for up to one year. Network UBA Reporter appliances also deliver pre-built reports for compliance and forensics.

McAfee Network UBA Control Center appliances overview

For multi-Monitor deployments, consolidate information using McAfee Network UBA Control Center. McAfee Network UBA can also send automated, prioritized SNMP alerts to trouble ticket systems and incident response personnel when required.

This purposeful architecture accelerates deployment, scales to the largest organizations, and does not require Monitors at distributed user locations, such as divisional offices or branches, in order to monitor network-wide activity.

Summary

McAfee Network UBA’s identity-aware solutions enable lower cost and faster and broader deployment of visibility into “who is doing what and where” across applications and networks. More than 60 global enterprises and major federal agencies trust McAfee Network UBA to help improve their network visibility and the behavior analysis of more than 3 million users.

Ultimately, our solutions help.

Increase efficiency and compliance

- Replace time-intensive manual discovery surveys
- Dispense with the inaccurate manual verification of logs
- Decrease investigation time for access violations with correlated data
- Reduce disruption of erroneous infrastructure and access changes
- Minimize time and effort spent on application recoding

Reduce risk

- Detect inappropriate user behavior after admission
- Eliminate the bypassing of security gateways and access controls
- Compensate control for unprotected custom applications
- Detect abuses from deprovisioned users and users reassigned to new roles
- Monitor the use of privileged accounts

