

User behavior analytics

Securing your network against the unexpected



User behavior analytics: Securing your network against the unexpected

As an IT administrator, you know how to ward off outsiders trying to breach your security and gain access to organizational data. However, internal threats make things a little more complicated since disgruntled employees are already within your network premises, and they might have access to critical resources. With almost [28 percent of data breaches](#) involving trusted insiders, it's high time you strengthen your detection systems to identify malicious activity within your network.

User behavior analytics (UBA) is your best bet for gaining better insight into your domain users' activities and detecting any insider threats. UBA creates a dynamic baseline of each user's activity and will monitor user behavior continuously to detect anomalies. Any activity that deviates from the norm is detected using machine learning.

Why are traditional security solutions weaker than UBA?

- ▶ **Inability to detect abnormalities:** Traditional auditing techniques can't accurately detect unusual user behavior. Alert thresholds are subjective and unique to each network, plus they change over time, so you can't rely on alerts to spot threats, especially slow attacks. You can detect deviations using machine learning without setting any threshold values. Machine learning analyzes user behavior over time and spots any minor user abnormalities.
- ▶ **False positives mask the real threats:** In spite of organizations keeping their perimeters secure and carefully scrutinizing every step of insiders and outsiders alike, almost [68 percent of all breaches in 2017 took a month or longer to discover](#). This is because most administrators miss the indicators of compromise amidst an overwhelming volume of false alarms. UBA uses machine learning to spot anomalies, so you don't have to spend time and effort configuring rules to avoid false positives.

How UBA strengthens insider threat detection

UBA employs different artificial intelligence methods to study user behavior patterns over time. When a UBA solution detects a suspicious incident that deviates from the user's normal behavior, it alerts administrators.

For example, if a user logs in to a machine they generally don't log in to, the UBA engine will classify this event as anomalous activity and alert the administrator who can further investigate the incident.

The ADAudit Plus advantage

ADAudit Plus, real-time Active Directory change monitoring software, doesn't stop with just auditing your domain controllers. It goes a step further by incorporating UBA to detect insider threats more efficiently. Its built-in UBA engine helps you:

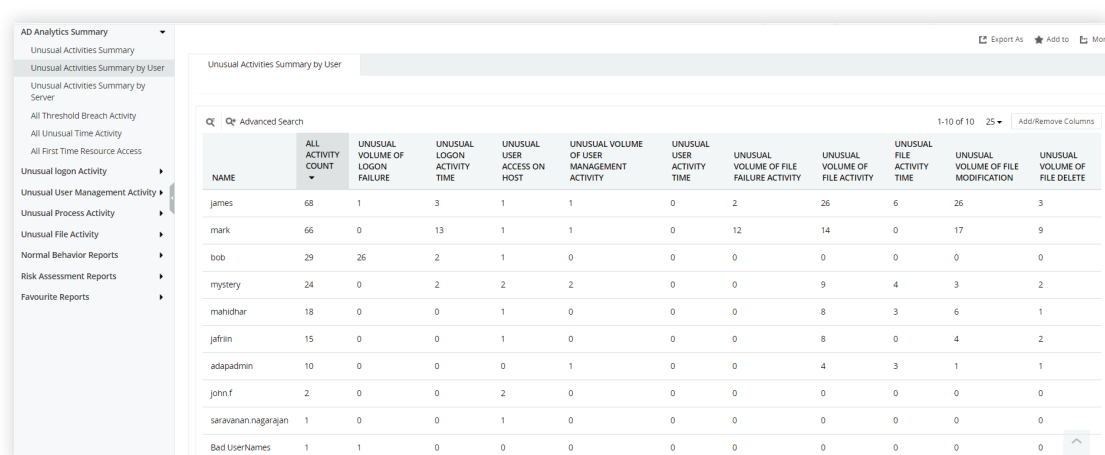
- ▶ Detect abnormalities.
- ▶ Detect privilege abuse.
- ▶ Spot external threats caused by users' mistakes.

Detecting abnormalities

Any deviation from a user's daily routine is immediately detected with ADAudit Plus.

These abnormalities include:

- ▶ Unusual volume of a specific routine event, such as a logon.
- ▶ Abnormal time of logon or object access.
- ▶ Logging into a machine a user doesn't typically use.
- ▶ Attempting to access a specific resource for the first time.
- ▶ Unusual file activity, including modification, copying, and deletion.



NAME	ALL ACTIVITY COUNT	UNUSUAL VOLUME OF LOGON FAILURE	UNUSUAL LOGON ACTIVITY TIME	UNUSUAL USER ACCESS ON HOST	UNUSUAL VOLUME OF USER MANAGEMENT ACTIVITY	UNUSUAL USER ACTIVITY TIME	UNUSUAL VOLUME OF FILE FAILURE ACTIVITY	UNUSUAL VOLUME OF FILE ACTIVITY	UNUSUAL FILE ACTIVITY TIME	UNUSUAL VOLUME OF FILE MODIFICATION	UNUSUAL VOLUME OF FILE DELETE
james	68	1	3	1	1	0	2	26	6	26	3
mark	66	0	13	1	1	0	12	14	0	17	9
bob	29	26	2	1	0	0	0	0	0	0	0
mystery	24	0	2	2	2	0	0	9	4	3	2
manidhar	18	0	0	1	0	0	0	8	3	6	1
jafrin	15	0	0	1	0	0	0	8	0	4	2
adapadmin	10	0	0	0	1	0	0	4	3	1	1
john.f	2	0	0	2	0	0	0	0	0	0	0
saravanan.nagarajan	1	0	0	1	0	0	0	0	0	0	0
Bad UserNames	1	1	0	0	0	0	0	0	0	0	0

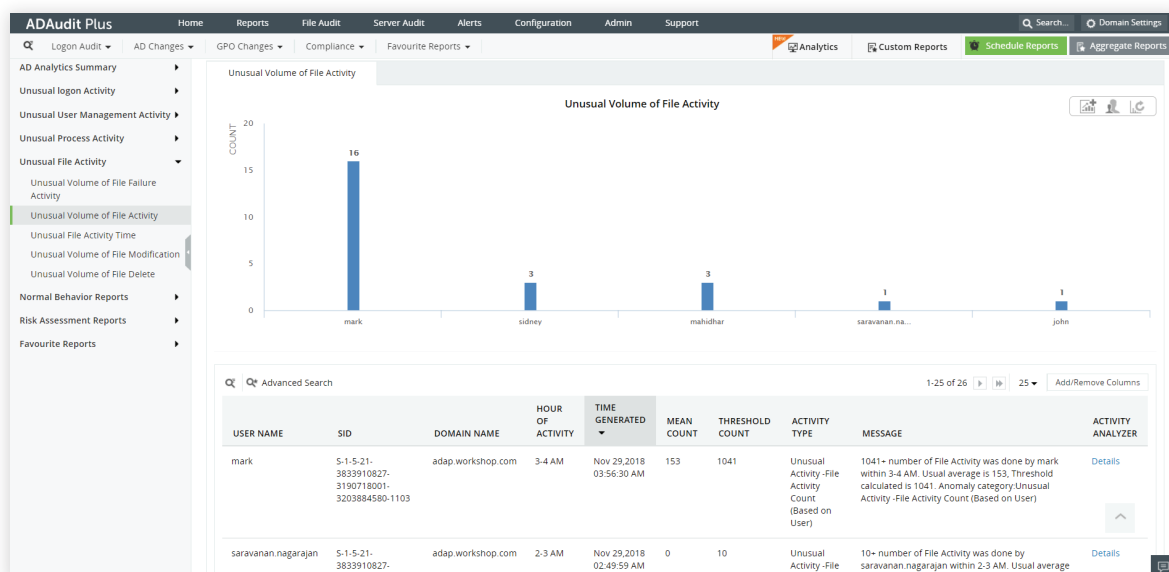
Detecting privilege abuse

ADAudit Plus' UBA module detects abnormal user behavior from privileged users to protect sensitive data. For instance, if a privileged user tries to access a critical file or folder and perform an unusually large volume of file modifications, ADAudit Plus will flag this event and alert you about the possible threat.

Advanced Search										
USER NAME	SID	DOMAIN NAME	HOUR OF ACTIVITY	TIME GENERATED	MEAN COUNT	THRESHOLD COUNT	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER	
james	S-1-5-21-3833910827-3190718001-3203884580-1105	adap.workshop.com	2-3 AM	Oct 24, 2018 02:19:46 AM	10	10	Unusual Activity - File Modification Count (Based on User)	10+ number of File Modification Activity was done by james within 2-3 AM. Usual average is 4, Threshold calculated is 10. Anomaly category: Unusual Activity - File Modification Count (Based on User)	Details	
james	S-1-5-21-3833910827-3190718001-3203884580-1105	adap.workshop.com	1-2 AM	Oct 24, 2018 01:21:43 AM	10	10	Unusual Activity - File Modification Count (Based on User)	10+ number of File Modification Activity was done by james within 1-2 AM. Usual average is 0, Threshold calculated is 10. Anomaly category: Unusual Activity - File Modification Count (Based on User)	Details	
james	S-1-5-21-3833910827-3190718001-3203884580-1105	adap.workshop.com	12-1 AM	Oct 24, 2018 12:19:47 AM	10	10	Unusual Activity - File Modification Count (Based on User)	10+ number of File Modification Activity was done by james within 12-1 AM. Usual average is 2, Threshold calculated is 10. Anomaly category: Unusual Activity - File Modification Count (Based on User)	Details	
james	S-1-5-21-3833910827-3190718001-3203884580-1105	adap.workshop.com	10-11 PM	Oct 23, 2018 10:13:51 PM	10	10	Unusual Activity - File Modification Count (Based on User)	10+ number of File Modification Activity was done by james within 10-11 PM. Usual average is 0, Threshold calculated is 10. Anomaly category: Unusual Activity - File Modification Count (Based on User)	Details	
james	S-1-5-21-3833910827-3190718001-3203884580-1105	adap.workshop.com	9-10 PM	Oct 23, 2018 09:17:50 PM	10	10	Unusual Activity - File Modification Count (Based on User)	10+ number of File Modification Activity was done by james within 9-10 PM. Usual average is 0, Threshold calculated is 10. Anomaly category: Unusual Activity - File Modification Count (Based on User)	Details	
james	S-1-5-21-3833910827-3190718001-3203884580-1105	adap.workshop.com	8-9 PM	Oct 23, 2018 08:17:30 PM	10	10	Unusual Activity - File Modification Count (Based on User)	10+ number of File Modification Activity was done by james within 8-9 PM. Usual average is 0, Threshold calculated is 10. Anomaly category: Unusual Activity - File Modification Count (Based on User)	Details	

Spotting security threats caused by users' mistakes

If a user accidentally opens the door for a breach or damages data by mistake, ADAudit Plus' UBA engine can catch the anomaly immediately. Consider a user who accidentally grants everyone in the organization permission to access a sensitive file. ADAudit Plus will detect the unusual volume of file activity and trigger an alert. An admin can then take a look into why this file was suddenly accessed so many times, and detect the data breach.



Risk assessment reports

You can identify the weak points in your network by filtering the users connected to the most assets, as well as hyperactive accounts. ADAudit Plus offers risk assessment reports for monitoring these vulnerable accounts. For instance, you can find out which accounts have the highest activity count (eg. high file activity) by running a query in the risk assessment reports.

The screenshot shows the ADAudit Plus web interface. The sidebar on the left contains a navigation menu with categories like 'Logon Audit', 'AD Changes', 'Unusual logon Activity', 'Unusual User Management Activity', 'Unusual Process Activity', 'Unusual File Activity', 'Normal Behavior Reports', 'Risk Assessment Reports', 'Users connected to most assets', 'High Activity Volume Accounts', 'Hyper Active Accounts', and 'Favourite Reports'. The main panel is titled 'High Activity Volume Accounts' and shows a table of user activity data for the domain 'adap.workshop.com'. The table has columns for 'USER NAME', 'ACTIVITY TYPE', 'DOMAIN NAME', and 'AVERAGE COUNT PER DAY'. The data is sorted by 'AVERAGE COUNT PER DAY' in descending order.

USER NAME	ACTIVITY TYPE	DOMAIN NAME	AVERAGE COUNT PER DAY
mark	File Failure Count (Based on User)	adap.workshop.com	195
mark	User Management Activity Count	adap.workshop.com	193
mystery	User Management Activity Count	adap.workshop.com	182
james	File Failure Count (Based on User)	adap.workshop.com	138
james	User Management Activity Count	adap.workshop.com	82
jafrin	File Failure Count (Based on User)	adap.workshop.com	75
ADAP_admin	User Management Activity Count	adap.workshop.com	54
jafrin	User Management Activity Count	adap.workshop.com	54
mystery	File Failure Count (Based on User)	adap.workshop.com	24