ManageEngine
ADAudit Plus

Three challenges

IT admins face when it comes to defending against insider threats, and how **user behavior analytics (UBA)** helps overcome them

Security threats aren't exclusive to the external world. While administrators are busy protecting a company's perimeter, a trusted insider could be carrying out a malicious attack from within the boundary. In fact, insider threats are more dangerous than external attacks, because these attacks use legitimate credentials, machines, and access privileges.

Insider attacks require quite a bit of time and effort to contain and resolve. This may result in IT administrators spending weeks, if not months, dealing with the fallout of an insider attack rather than investing that time in business-driving tasks.

Traditional SIEM solutions are ill-equipped to tackle these threats. In this solution brief, we'll take a look at the main challenges IT administrators face while trying to fend off insider threats, malicious or otherwise, and the ways IT teams can overcome them.

Monitoring deviations in user behavior.

Traditional SIEM solutions fail to analyze user behavior and don't detect anomalies in this behavior. As a result, when an employee is working with sensitive data, it can be hard to know whether they are just doing their job or something malicious.

28 percent

of all breaches involved internal actors.

ManageEngine insider threat survey, 2019

ManageEngine
ADAudit Plus

False positives and delayed threat detection.

False positive alerts are a source of distraction that delay breach detection. Many security solutions tend to flood security professionals with insignificant warnings, making it difficult to find those that are critical and require immediate attention. Many organizations use simple rules-based monitoring that detects basic insider activities (such as emailing large files), but these are rarely capable of tracking advanced threats or more sophisticated insider threats.

68 percent

of all breaches in 2017 took a month or longer to discover.

ManageEngine insider threat survey, 2019

Identifying vulnerabilities and risks.

It only takes one person to carry out an attack that causes lasting damage. Traditional SIEM solutions don't usually offer any risk assessment to help enterprises take proactive steps to protect themselves against breaches.

55 percent

of all breaches involved internal actors.

ManageEngine insider threat survey, 2019

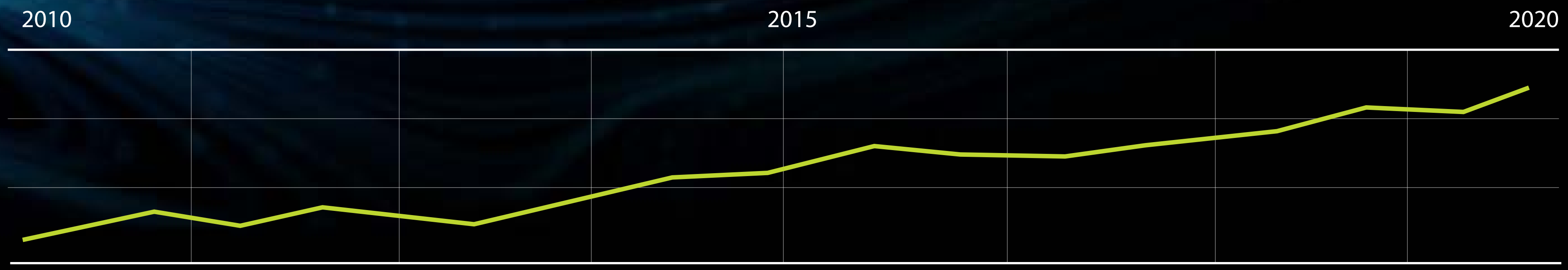
ManageEngine
ADAudit Plus

User behavior analytics in ADAudit Plus

Given how advanced many cyberattacks are, manually creating more alert rules in a traditional SIEM solution alone simply isn't an effective way of detecting threats. This is because existing security solutions use static threshold values to differentiate between what's normal and what's not.

Enterprises need to include anomaly-based analytics to strengthen incident detection mechanisms. User behavior analytics (UBA) helps you gain better insight into your users' activities so you can detect and respond to insider threats.

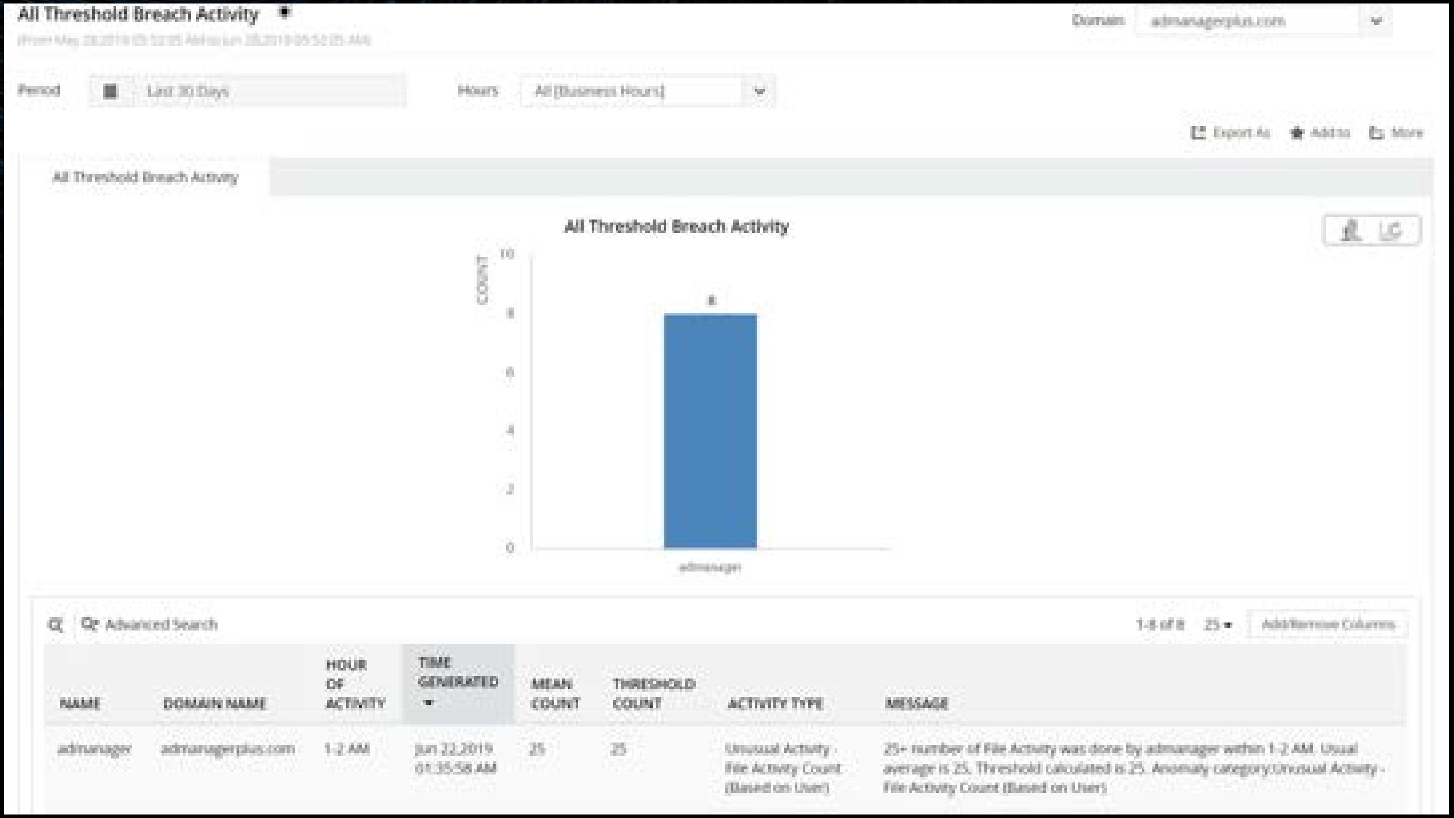
UBA creates a dynamic baseline of each user's activity and monitors user behavior continuously to detect anomalies. Any activity that deviates from the norm is detected using machine learning. Complementing your SIEM solution with UBA can help you avert a potential breach caused by a malicious insider.



Gartner predicts that the market for UBA will grow at a steep **48 percent** CAGR between **2015** and **2020.**

How ADAudit Plus' UBA engine can help you overcome these challenges

1. ADAudit Plus uses machine learning to create a baseline of normal activities that are specific to each user to detect potential insider threats. Focusing on your users' activities and looking out for deviations from their usual behavior gives you an important vantage point in identifying threats before they become damaging breaches.



All Threshold Breach Activity

(From May 28,2019 05:52:05 AM to Jun 28,2019 05:52:05 AM)

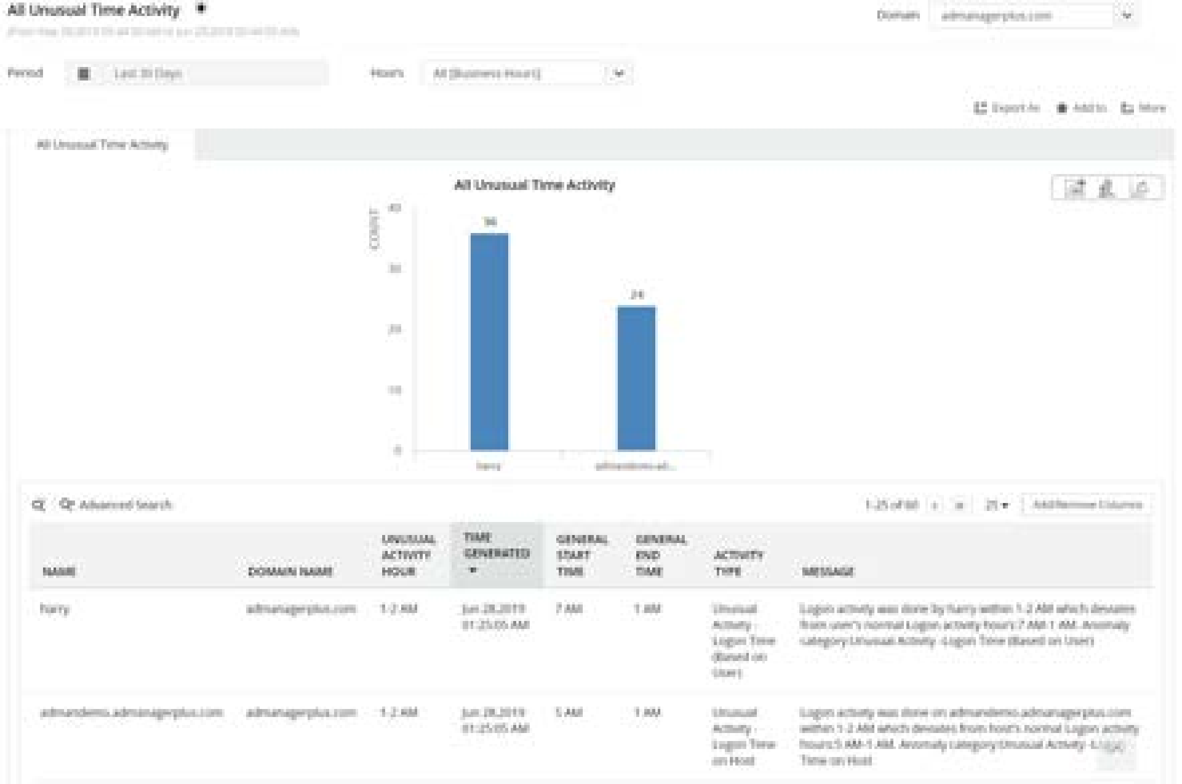
Domain: admanagerplus.com

Period: Last 30 Days

Hours: All [Business Hours]

NAME	DOMAIN NAME	HOUR OF ACTIVITY	TIME GENERATED	MEAN COUNT	THRESHOLD COUNT	ACTIVITY TYPE	MESSAGE
admanager	admanagerplus.com	1-2 AM	Jun 22,2019 01:35:58 AM	25	25	Unusual Activity - File Activity Count (Based on User)	25+ number of File Activity was done by admanager within 1-2 AM. Usual average is 25. Threshold calculated is 25. Anomaly category:Unusual Activity - File Activity Count (Based on User)

2. The longer it takes to discover an insider threat, the more costly it can be to fix. ADAudit Plus combines data analytics and machine learning to define dynamic thresholds based on real-world user behavior. With its alert thresholds, ADAudit Plus reduces the number of false positives, so security teams can easily spot the real indicators of compromise and quickly respond. In other words, what often takes weeks to investigate using traditional SIEM solutions can be accomplished in seconds with UBA.

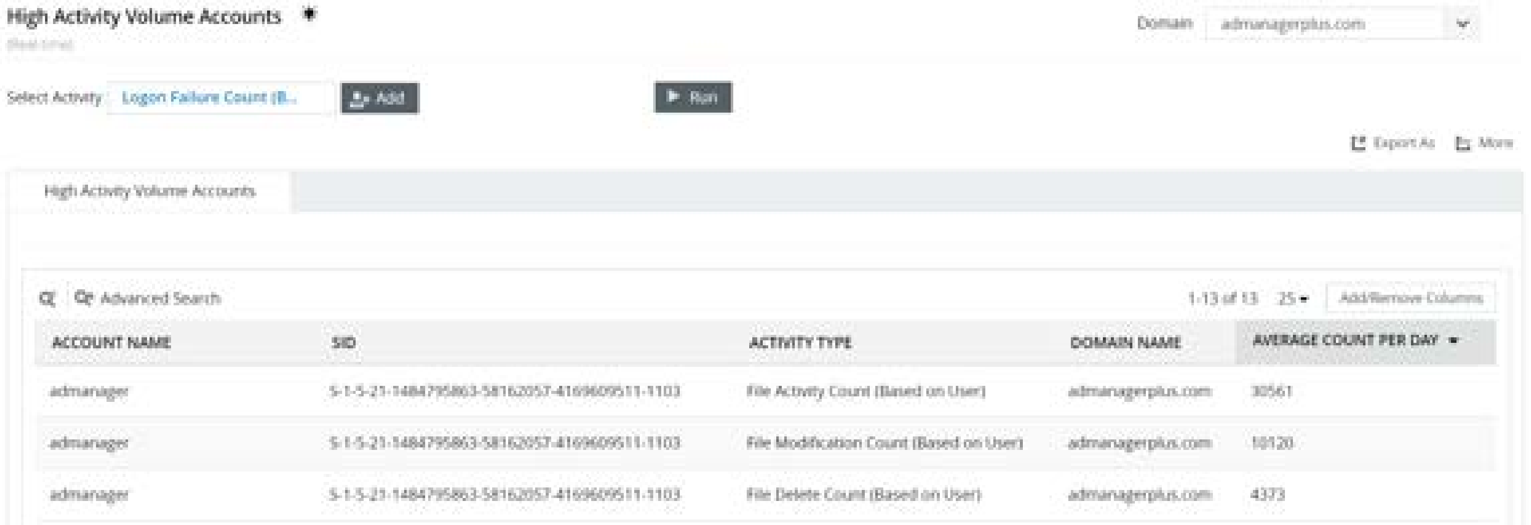


All Unusual Time Activity

[illegible]

NAME	DOMAIN NAME	UNUSUAL ACTIVITY HOUR	TIME GENERATED	GENERAL START TIME	GENERAL END TIME	ACTIVITY TYPE	MESSAGE
harry	admanagerplus.com	1-2 AM	Jun 28,2019 01:25:05 AM	7 AM	1 AM	Unusual Activity - Logon Time (Based on User)	Logon activity was done by harry within 1-2 AM which deviates from user's normal Logon activity hours 7 AM-1 AM. Anomaly category Unusual Activity -Logon Time (Based on User)
admandemo.admanagerplus.com	admanagerplus.com	1-2 AM	Jun 28,2019 01:25:05 AM	5 AM	1 AM	Unusual Activity - Logon Time on Host	Logon activity was done on admandemo.admanagerplus.com within 1-2 AM which deviates from host's normal Logon activity hours 5 AM-1 AM. Anomaly category Unusual Activity -Logon Time on Host

3. Enterprises need to scale their diligence and defenses appropriately to effectively detect and mitigate risks. In addition to this, they need to be able to quickly identify the culprit. Companies should foster an environment that prioritizes threats based on the risks they pose, so they can address the most glaring threats in the network first. With risk assessment reports, ADAudit Plus can help identify high risk users and weak points in your network by filtering the hyperactive accounts along with the users connected to the most assets. Monitoring these vulnerable accounts helps reduce the risk of insider threats within an organization.



High Activity Volume Accounts
(Real time)

Domain: admanagerplus.com

Select Activity: Logon Failure Count (B...

ACCOUNT NAME	SID	ACTIVITY TYPE	DOMAIN NAME	AVERAGE COUNT PER DAY
admanager	S-1-5-21-1484795863-58162057-4169609511-1103	File Activity Count (Based on User)	admanagerplus.com	30561
admanager	S-1-5-21-1484795863-58162057-4169609511-1103	File Modification Count (Based on User)	admanagerplus.com	10120
admanager	S-1-5-21-1484795863-58162057-4169609511-1103	File Delete Count (Based on User)	admanagerplus.com	4373

The various stages of UBA are:

- **Collect** information on users over an extended period of time.
- **Build** a baseline of normal activities specific to each user.
- **Define** dynamic thresholds based on real-world user behavior.
- **Find** deviations from the norm.
- **Notify** the concerned security personnel upon deviation.
- **Update** thresholds continuously based on recent data.

Benefits

- **Efficiency:** Improve detection speed, analyze the impact of security incidents, and respond quickly to them.
- **Precision:** Move beyond simple rules and utilize targeted attack detection capabilities for user credential theft and abuse to detect attacks quickly.
- **Reduced false positives:** UBA calculates the threshold value for each user based on their level of activity instead of using a blanket threshold across all users.
- **Better threat detection:** UBA solutions rely on the baseline activities of users to identify unusual user behavior that points to potential attacks.

E-BOOK

Other useful resources: Download UBA guide | Download UBA white paper | Download UBA ebook

ManageEngine

ADAudit Plus

ManageEngine ADAudit Plus is a real-time Active Directory change auditing solution that features file and folder monitoring, plus access and permission change capabilities. With more than 200 event-specific reports and real-time email alerts, it provides in-depth knowledge about changes made to both the content and configurations of Active Directory, Azure AD, and Windows servers. Additionally, ADAudit Plus provides thorough insight on workstation and file server access (including NetApp and EMC). For more information about ADAudit Plus, visit manageengine.com/active-directory-audit.

$ Get Quote

⭳ Download