

A 5-step plan for **effective data** **protection**



Presented by, Jay
IAM & IT Security Expert | ManageEngine

Protecting critical data: The stakes have never been higher



Recent **data breach** attacks that made headlines

- 250 Million – Microsoft, January 22
- 5.2 Million – Marriott, March 31
- 47.5 Million – Truecaller, May 27
- 160,000 – Nintendo, April 24
- 28,000 – GoDaddy, April 23

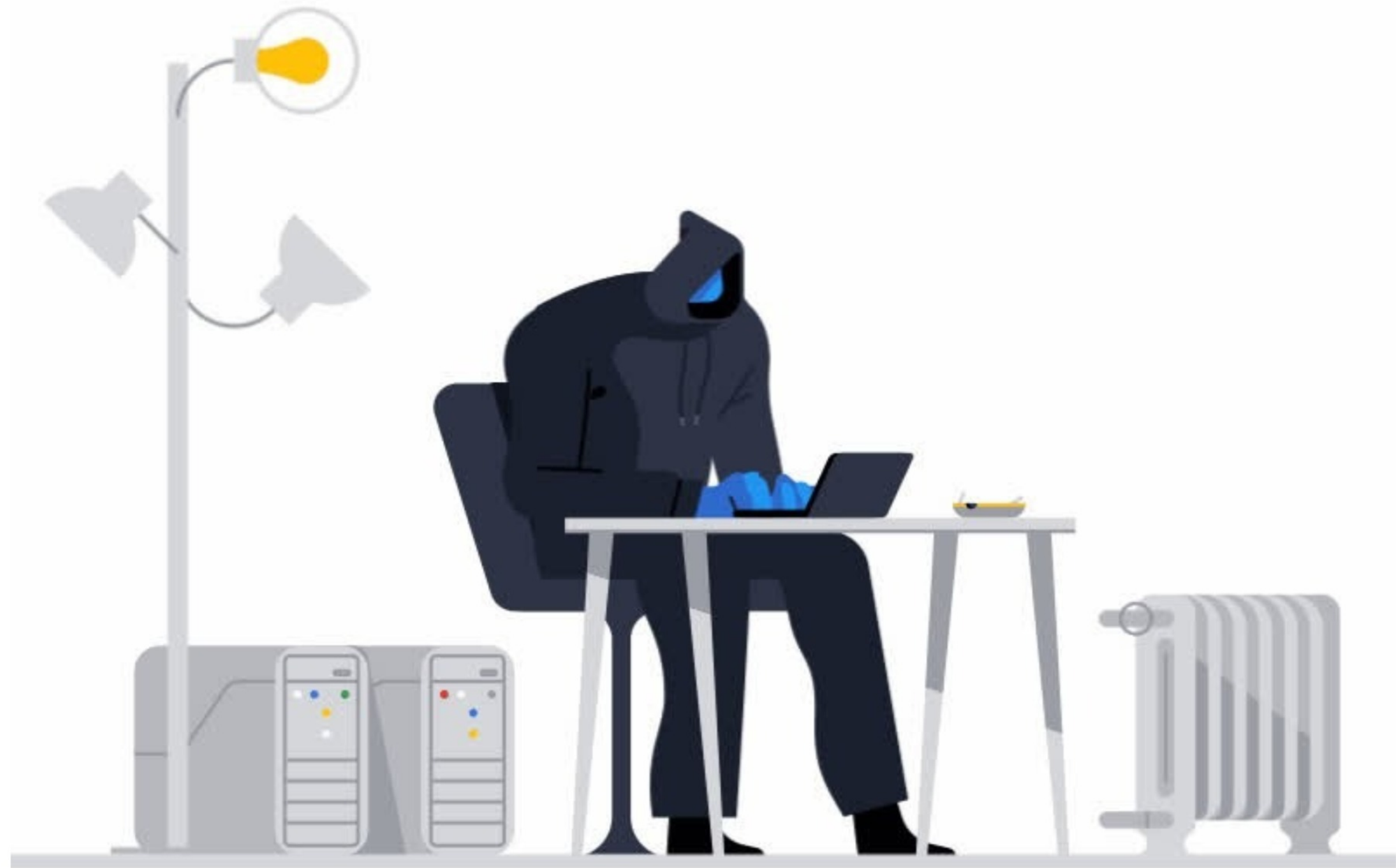
WHAT WE'LL DISCUSS TODAY:

- Implement Zero Trust access and impose the principle of least privilege.
- Leverage around-the-clock user behavior monitoring to detect anomalies.
- Identify malicious events and potential security risks such as malicious insiders, compromised accounts, and malware infections with threat detection.
- Configure real-time alerts, and automate your incident response.
- Overcome any disasters caused by data losses with a comprehensive backup plan.

A **zero trust network** is built upon five fundamental assertions

- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.

Why you need to adopt zero trust



■ Targeting Identity

81% of breaches involved compromised credentials

■ Targeting Apps

54% of web apps vulnerabilities have a public exploit available

■ Targeting endpoints and devices

300% increase in IOT and endpoints malware variants

Enabling **secure access**



Prevent risks

Reduce the risk of a breach before it happens.



Gain visibility

Identify risks and indicators of a breach of trust.



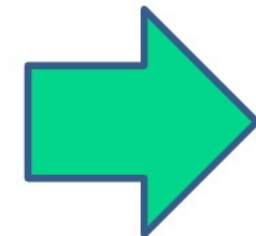
Reduce attack surface

Contain breaches and stop attacker lateral movement.

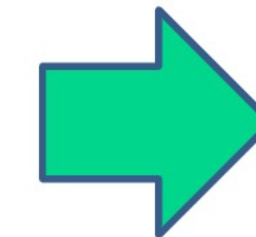
What's different in a **zero trust** approach

The traditional approach

Trust is based on the network location that an access is coming from.



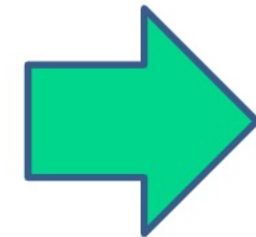
Enables attackers to move laterally within a network to get to the golden seat.



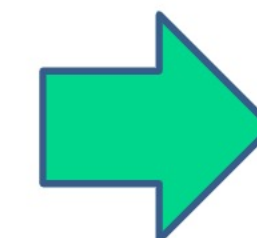
Doesn't extend security to the new perimeter.

The zero trust approach: **Never implicitly trust, always verify**

Trust is established for every access request, regardless of where it is coming from.



Secures access across your applications and network. Ensures only right users and devices have access.



Extends trust to support a modern enterprise with BYOD, cloud apps, hybrid environment and more.

Challenges addressed by zero trust



Insider threats

Zero Trust can prevent a compromised account or system from accessing resources by enabling MFA for network access.



Network visibility

Zero Trust approach can help collect encrypted traffic metadata and analyze it to detect malware or attackers on the network.



Policy gaps

An attacker exploits the gaps between different access policies that apply to the same asset. Zero Trust applies fine-grained contextual access policies.



Vulnerable endpoints

Zero Trust reduces the attack surface by protecting the vulnerable systems and prevents lateral movement of threats.

Provisioning and modifying users the zero-trust way



AD management mistakes that could cost you dearly

- 1) Granting excessive permissions to users and groups
- 2) Failing to clean up stale accounts
- 3) Not monitoring privilege creep

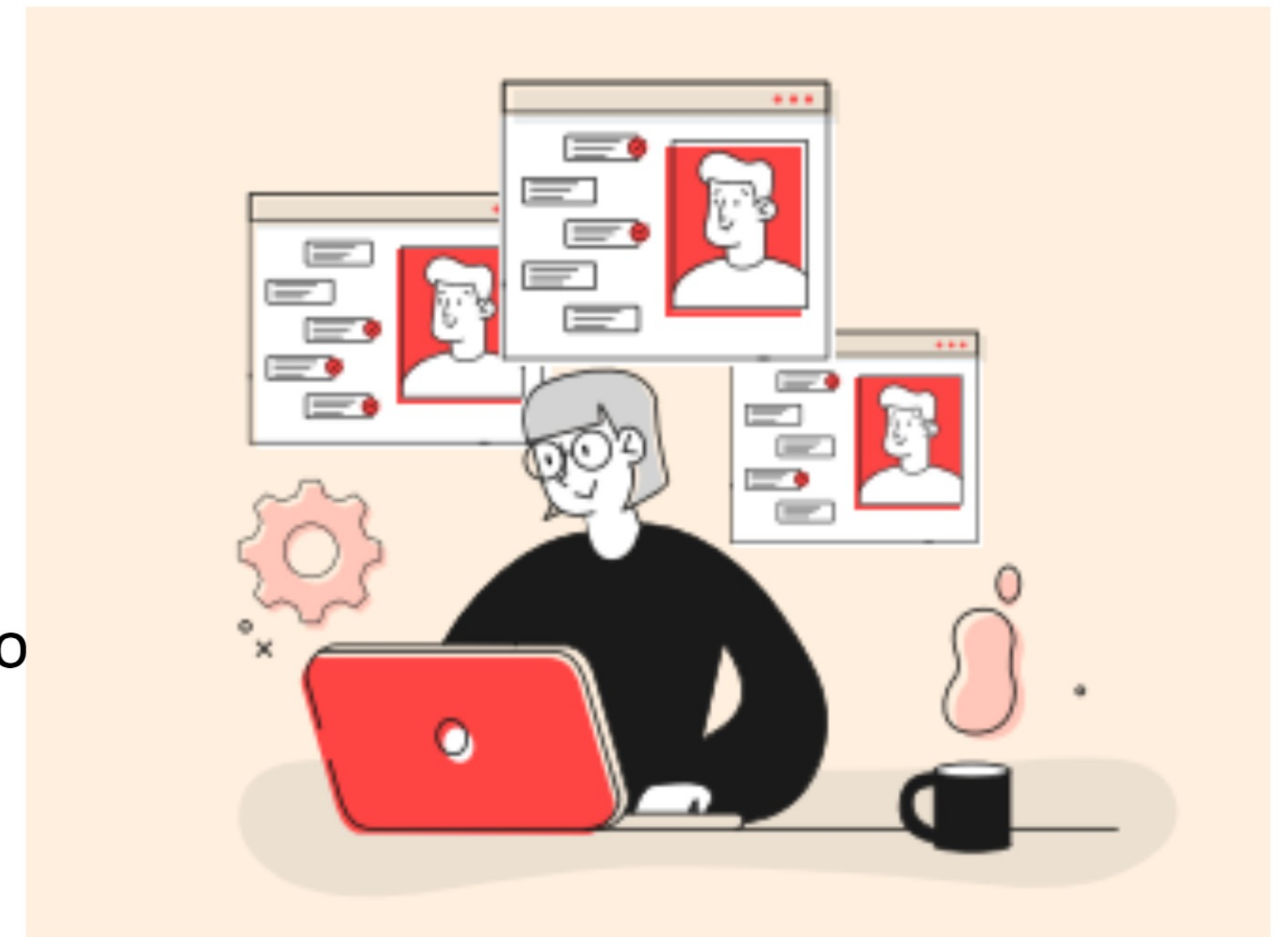
Tackling **excess privileges**

Delegating tasks to IT technicians can be really helpful when you are hard-pressed for time.

However technicians with excess privileges can cause more harm than good.

With AD360, delegate IT technicians to work on tasks without elevating their native AD permissions

1. Set boundaries on what technicians can and cannot do
2. View all the permissions assigned to or revoked from help desk technicians
3. Establish an audit trail to identify administrators performing changes on help desk technicians and see which roles were modified.



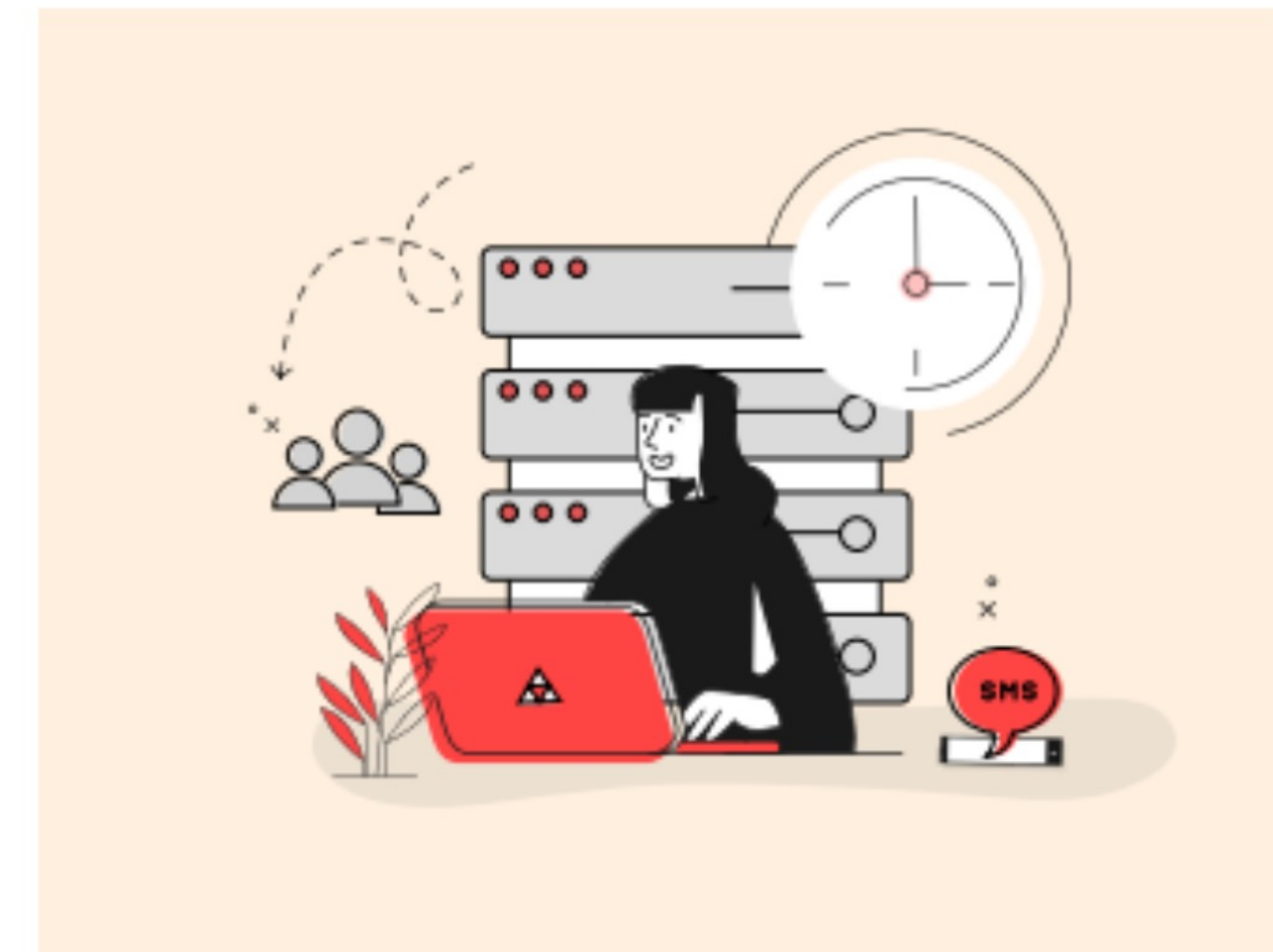


Cleaning up stale accounts

- When an employee leaves an organization, their account should be stripped of its privileges, then deprovisioned
- Malicious insiders could leverage stale accounts to access your organization's resources.
- Software licenses don't come cheap. Identify stale accounts and strip them of their licenses.
- Generate reports to identify stale accounts and strip them of their group memberships, revoke all their permissions, remove Office 365 licenses, and delete or disable them.

Monitoring **privilege creep**

- Overtime certain users will accumulate access to certain sensitive files even if they no longer need it.
- Grant time-bound access rights to important file servers for a limited time, after which the permissions will be automatically revoked.



Tell-tale signs of security breaches

- Multiple logon failures followed by a successful logon and a high volume of activity
- Unusual logon time followed by activities like security group membership changes/critical file changes/user account changes/GPO changes
- Dormant admin account becoming active
- Unusual volumes of file activity
- High frequency of account lockouts

How are you **tracking** these events?

Manually keeping track of these events are next to impossible. Is there a better way to keep these tell-tale signs of security breaches in check?

Enter User Behavior Analytics

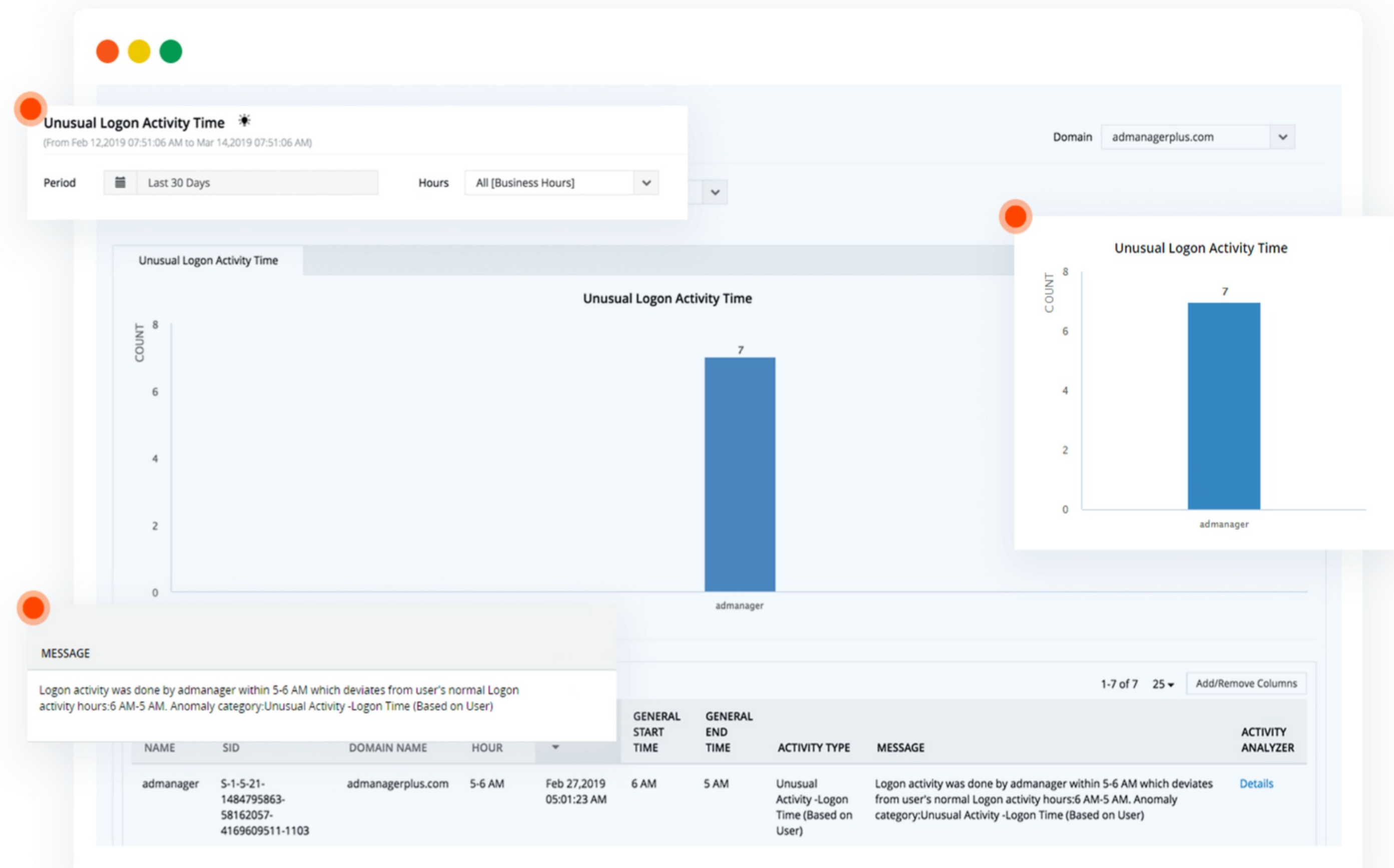


How **UBA** can help your organization

- Monitor user behavior continuously to spot anomalous activities and get instant alerts in case of malicious behavior
- Keep track of all file/folder access and permission changes made by the user to prove compliance
- Correlate unusual activity volume and time to spot threats
- Get details on user idle time and productivity by tracking user logon/logoff, startup/shutdown, and screensaver invokes/dismissals

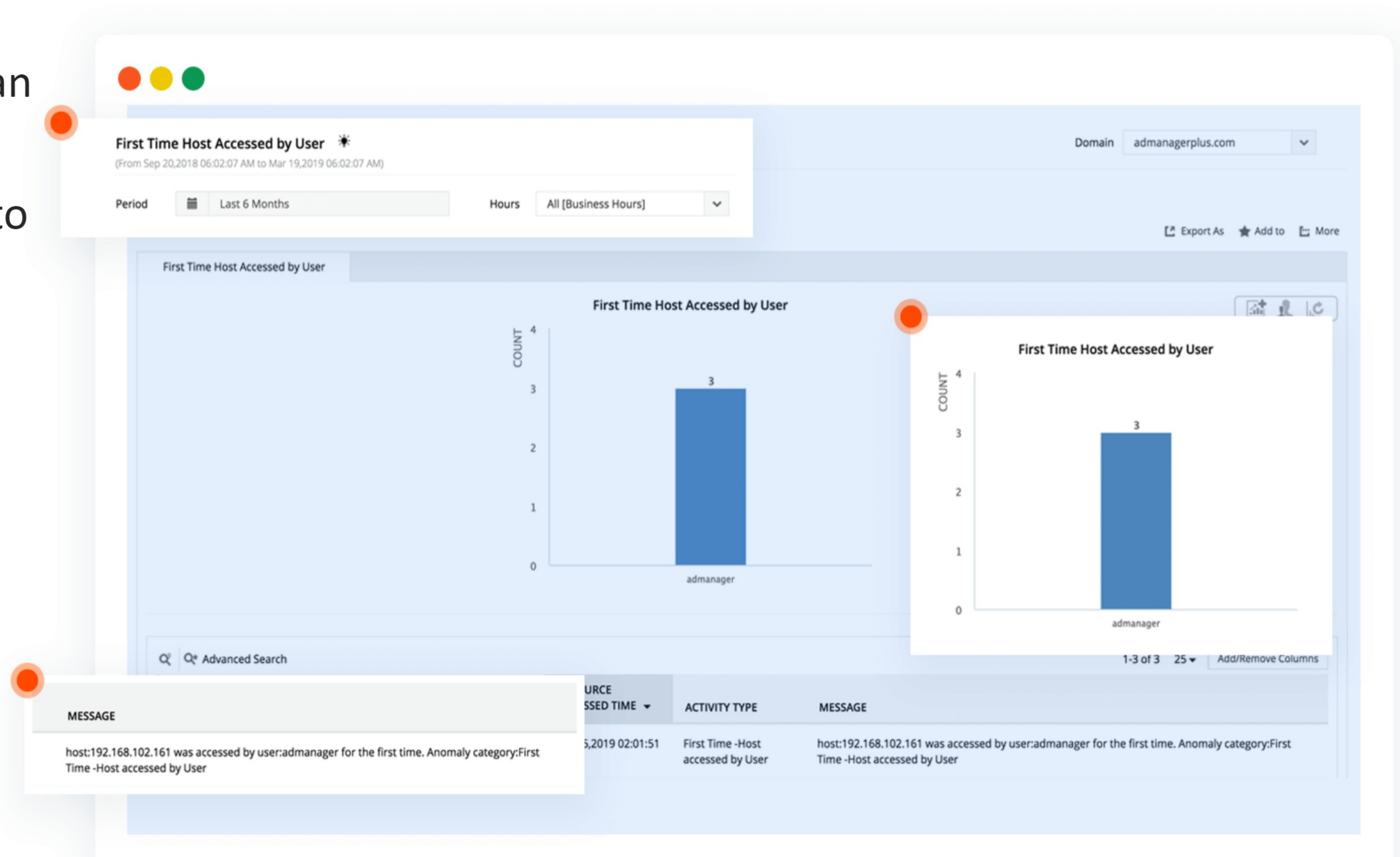
Identifying malicious logins

This critical data in the event of an unauthorized entry or regular monitoring is at the utmost ease to view with detailed reporting which helps prevent further wrong doing at the earliest.



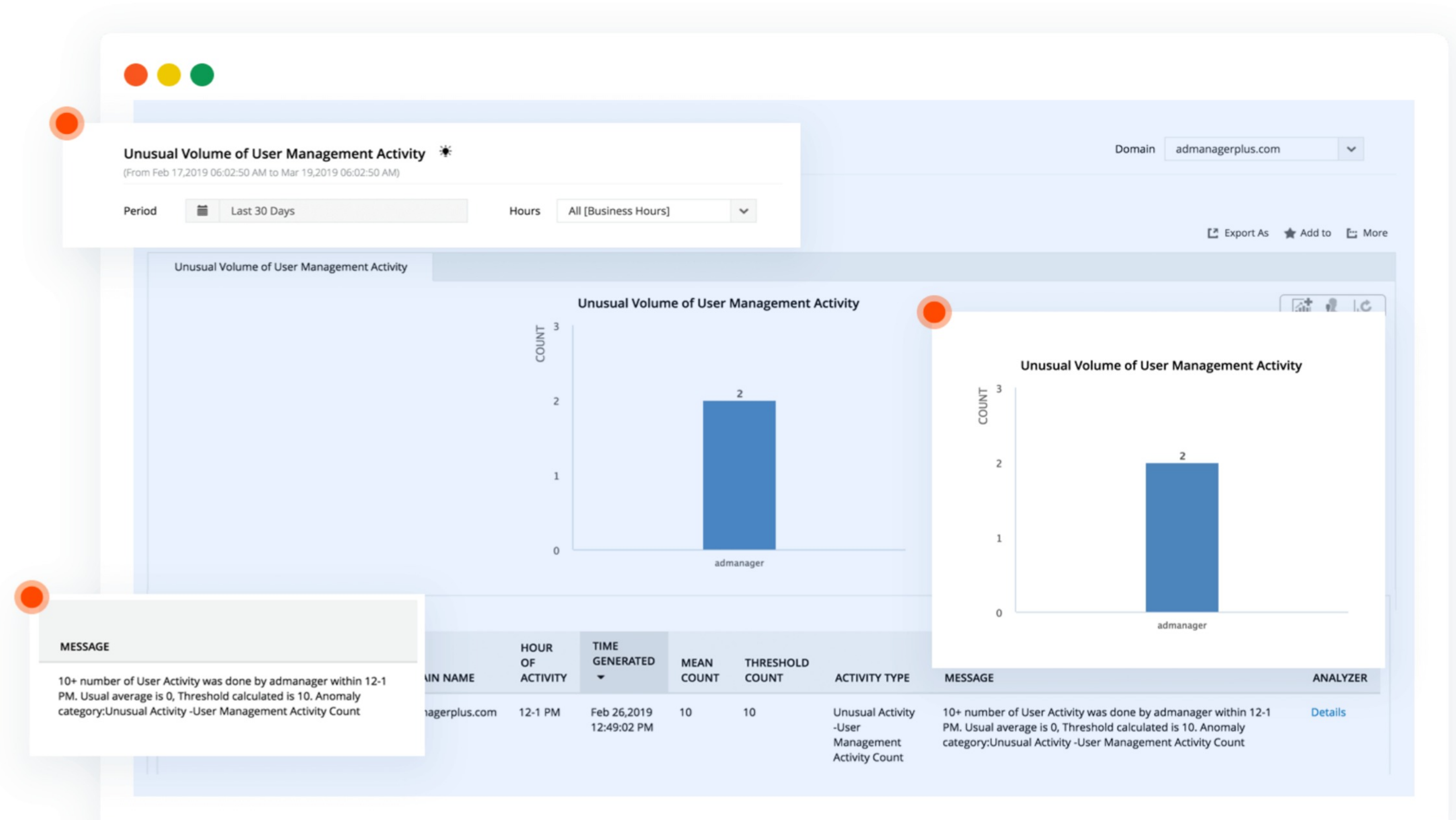
Detecting lateral movement

In a Lateral Movement attack, an attacker typically propagates in the network by gaining access to a non-sensitive account, leveraging that account to gain access to additional accounts/assets, until reaching the target.



Identifying **privilege abuse**

Privilege abuse is the direct result of poor access control: Users have more access rights than they need to do their jobs, and the organization fails to properly monitor the activity of privileged accounts and establish appropriate controls.



Spotting signs of data breaches

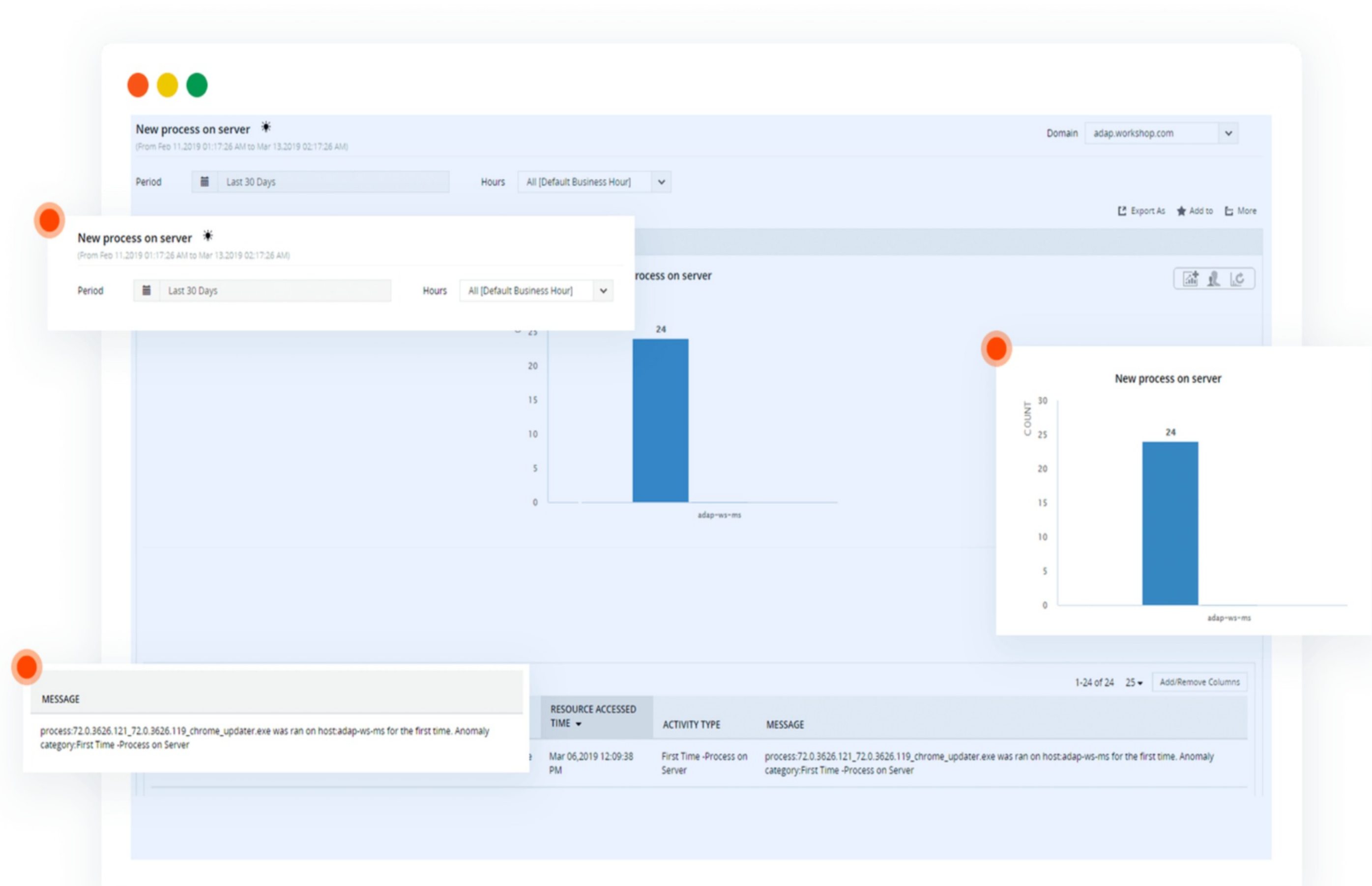
Detect USB devices plugged in to domain controllers, servers, or workstations, and receive alerts when files are copied to them.

The screenshot displays the ADAudit Plus interface for a 'File Copy and Paste (Removable Storage/USB)' report. The report covers the period from Jan 01, 2020 10:35:00 AM to Jan 31, 2020 10:35:00 AM. The interface includes a navigation menu, search bar, and various filters. A bar chart titled 'Top Users who modified files/folders' shows that user 'John-5887' has the highest count of 15. A detailed view of this user's activity shows a table of file operations.

SERVER	FILE / FOLDER NAME	LOCATION	TIME MODIFIED	MODIFIED BY	MESSAGE
John-5887	product\Copy (4).conf	\Device\HarddiskVolume17\	Jan 25, 2020 06:39:20 AM	John-5887	User 'John-5887' Copy-N-Pasted the file/folder '\Device\HarddiskVolume17\product - Copy - Copy (4).conf'.
John-5887	product\Copy (2).conf	\Device\HarddiskVolume17\	Jan 25, 2020 06:39:20 AM	John-5887	User 'John-5887' Copy-N-Pasted the file/folder '\Device\HarddiskVolume17\product - Copy - Copy (2).conf'.

Detecting malware

Look for new programs that are installed automatically and monitor modifications done to executable files.



Investigate anomalies

Identify suspicious activities such as an unusually high volume of events and file activities carried out at unusual times.

The screenshot displays the ADAudit Plus software interface. The main window shows a report titled "High Activity Volume Accounts" (Real-time). The report is generated for the domain "adapdev". The interface includes a navigation menu with options like Home, Reports, File Audit, Server Audit, Analytics, Alerts, Configuration, Admin, and Support. A search bar is visible at the top left. The report content is displayed in a table format with the following data:

ACCOUNT NAME	ACTIVITY TYPE	DOMAIN NAME	AVERAGE COUNT PER DAY
Mark	File Activity Count (Based on User)	adapdev	133
Lee	File Activity Count (Based on User)	adapdev	102
John	File Activity Count (Based on User)	adapdev	79
Mark	File Delete Count (Based on User)	adapdev	77
Mark	File Modification Count (Based on User)	adapdev	77
John	File Delete Count (Based on User)	adapdev	37

Below the main table, there is a section for "Favourite Reports" with a list of reports including "Privileges Utilized by user", "Privilege Escalation - First time Utilizing a Privilege", and "Shared Account Based on Remote Logon". A search bar is also present at the bottom of the interface.

Actively respond to threats

Once anomalies are detected, it is time to look at how you should respond to them, instantly.

Automating your incident response

- It's only a matter of time until an employee clicks on a link or a piece of unknown malware infects our systems, or a zero-day exploit is used to target us. What then?
- Alert fatigue is real. the number of alerts our detection tools generate is becoming overwhelming.
- Analytics systems simply just don't scale well. Even with advanced analytics platforms that help sift through the noise, we're drowning in manual tasks and processes that take up valuable time

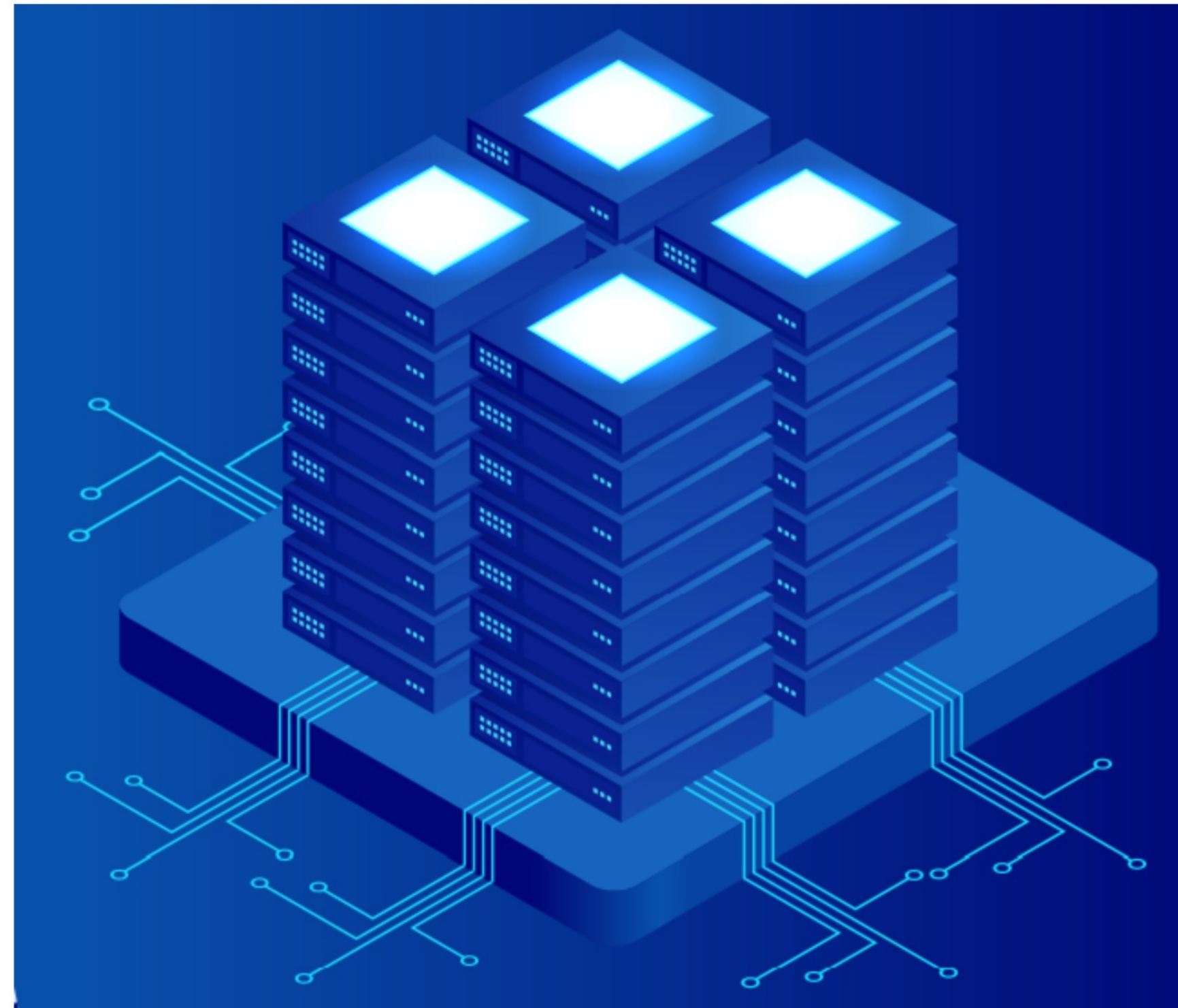
Three pillars of incident response

- Continuous data collection
- Aggregating and applying threat intelligence
- Streamlining live response capabilities

Continuous data collection

- Audit all AD object changes: Track changes made to OUs, users, groups, computers, and other AD objects with details such as the old and new values of the changed attributes
 - Track GPO setting changes: Audit changes made to GPOs and their settings, including computer configuration changes, password and account lockout policy changes, etc.
 - Monitor user logon activity: Get detailed reports on users' successful and failed logon attempts
 - Troubleshoot account lockouts: Detect account lockouts quickly with alerts, and identify their source from an extensive list of Windows components
 - Gain visibility into privilege use: Keep a close eye on privilege use in your enterprise by continuously auditing privileged user accounts and maintaining a detailed audit trail
- Audit hybrid AD environment: Get a single, correlated view of all activities happening across hybrid environments with alerts for critical events

File server auditing



File server auditing

- Monitor file and folder accesses: Track all file activity—including read, delete, modify, copy-and-paste, move, and more—in real time
- Detect failed file access attempts: Receive reports on failed attempts to access files or folders
- Audit permission changes: Track NTFS and share permission changes along with details such as their old and new values
- Monitor file integrity: Easily detect critical events such as changes made to a specific file, by a particular user, or more with email and SMS alerts on these events
- Audit file shares: Track every access and change made to shared files and folders in your domain with details on who accessed what, when, and from where

Windows server auditing



Windows server auditing

- Audit Windows servers: Monitor changes to local administrative group memberships, local users, user rights, local policies, and more
- Track scheduled tasks and processes: Audit the creation, deletion, and modification of scheduled tasks and processes
- Monitor removable device usage: Identify USB plug-ins and file transfer activities to removable storage devices
- Audit PowerShell processes: Monitor PowerShell processes that run on your Windows servers along with the commands executed in them
- Audit AD federation services (ADFS): Report on successful and failed ADFS authentication attempts in real time

Workstation auditing



Workstation auditing

- Audit logon and logoff activity: Track logon and logoff activity across your Windows network, record logon duration, and identify users who are currently logged on
- Track user logon history: Record every logon activity, identify users logged on to multiple machines, monitor RADIUS logons, and more
- Identify logon failures: Track all failed logon attempts with information on who attempted to log on, what machine they attempted to log on to, when, and the reason for the failure
- Monitor file integrity: Receive detailed reports on all changes made to system and program files
- Measure employee productivity: Track employees' idle time and actual work hours to ensure high productivity across your enterprise

Aggregating and applying threat intelligence - UBA

- Process logs from across your environment: Collect and process logs from configured DCs, member servers, and workstations
- Identify a safe baseline: Processed log data is used to create a user-specific baseline of normal logon, file, user management, and process activities
- Identify anomalies and alert admins: Incoming log data and processed baselines are compared to detect anomalies and notify admins, so they can investigate further
- Detect potential security threats: Quickly spot potential cases of malicious logons, privilege abuse, privilege escalations, data exfiltration, malware attacks, and more
- Automate incident responses: Reduce the time it takes to mitigate damage by instantly shutting down devices, terminating user sessions, or more based on the security incident

Threat detection capabilities that UBA offers

- 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 events early in the attack.
- Reduced false positives: With false positive alerts being a source of distraction that delay breach detection, dynamic alert thresholds—which are specific to each user in the organization—become important. 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.

UBA versus **real-world** scenarios

UBA versus bad actors.

USER NAME	SID	DOMAIN NAME	HOUR OF ACTIVITY	TIME GENERATED	MEAN COUNT	THRESHOLD COUNT	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
X	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:32:38 AM	0	10	Unusual Activity - File Activity Count (Based on User)	10+ number of File Activity was done by X within 1-2 AM. Usual average is 0, Threshold calculated is 10. Anomaly category:Unusual Activity -File Activity Count (Based on User)	Details

UBA versus **real-world** scenarios

UBA versus compromised accounts.

USER NAME	SID	DOMAIN NAME	UNUSUAL ACTIVITY HOUR	TIME GENERATED	GENERAL START TIME	GENERAL END TIME	ACTIVITY TYPE	MESSAGE	ACTIVITY ANALYZER
X	S-1-5-21-992173265-572275416-1555582462-203614	adap.internal.com	1-2 AM	Apr 12,2018 01:26:38 AM	10 AM	7 PM	Unusual Activity - Logon Time (Based on User)	Logon activity was done by X within 1-2 AM which deviates from user's normal Logon activity hours:10 AM 7 PM. Anomaly category:Unusual Activity -Logon Time (Based on User)	Details

UNUSUAL REMOTE ACCESS FROM COMPUTER	DOMAIN NAME	SERVER NAME	RESOURCE ACCESSED TIME	ACTIVITY TYPE	MESSAGE
ws.adap.internal.com	adap.internal.com	ADAP-ms1.adap.internal.com	Apr 24,2018 10:20:04 AM	First Time -Remote Access on Host	host:ADAP-MS1.adap.internal.com was accessed from host: ws.adap.internal.com for the first time. Anomaly category:First Time -Remote Access on Host

UBA versus **real-world** scenarios

UBA versus external threats

COMPUTER NAME	DOMAIN NAME	UNUSUAL PROCESS	RESOURCE ACCESSED TIME ▲	ACTIVITY TYPE	MESSAGE
ADAP-MS3	adap.internal.com	{2648CB07-372F-1A1D-241F-147FAAD0CEF3}.exe	Jun 12,2018 01:44:18 PM	First Time -Process on Server	process:{2648CB07-372F-1A1D-241F-147FAAD0CEF3}.exe was ran on host:ADAP-MS3 for the first time. Anomaly category:First Time -Process on Server

A **roundup** of what UBA does

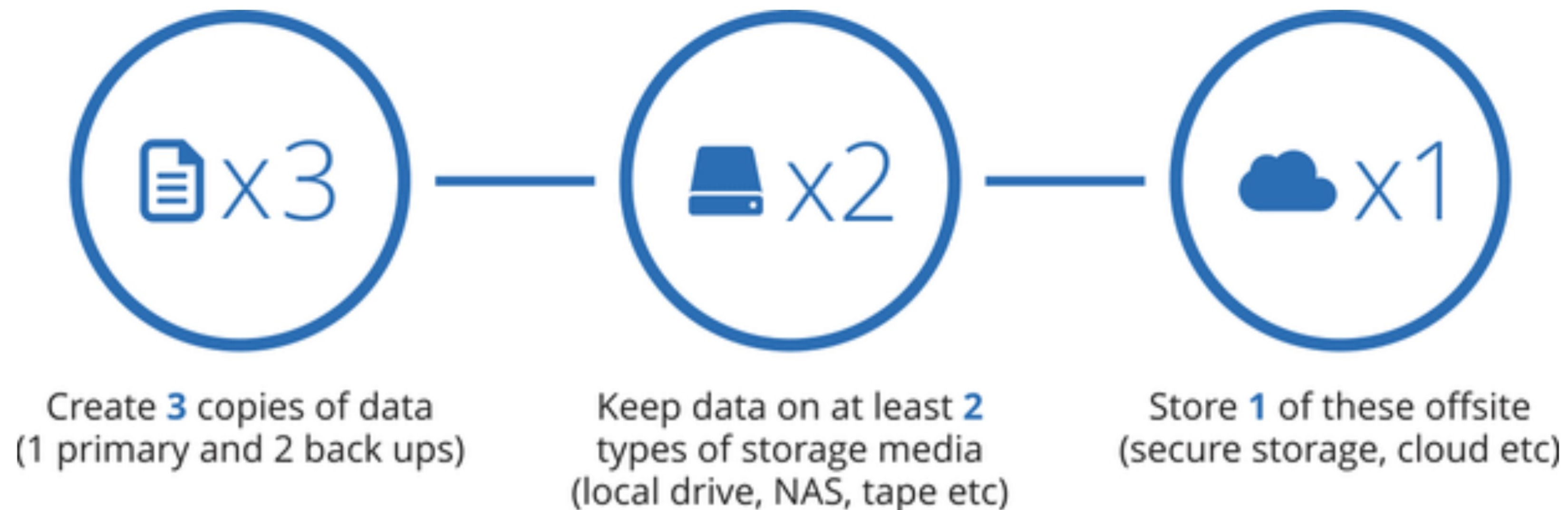
- Collect information on users over an extended period of time.
- Build a baseline of normal activities specific to each user.
- Define dynamic thresholds based on real-world user behavior.
- Find deviations from the norm.
- Notify the concerned security personnel upon deviation.
- Update thresholds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

We insure our cars, why overlook our businesses?

- Disasters happen every day: It's not a matter of IF, but WHEN
- In addition to all these security measures in place, it is advisable to have all your data backed up securely. The thumb rule of backing up data is the 3-2-1 rule.

Preventing valuable **data loss**

- Data loss risk can be mitigated with a backup plan in place. Thumb rule of a good backup plan is the 3-2-1 rule
- 3-2-1 rule, Backup 3 copies of your data, with copies stored in 2 different types of media and keep 1 of these copy offsite.



All-important features of a **B&R**






- Unified backup solution: Legacy backup tools are siloed, which makes it impossible to get a unified view of the backup infrastructure. A holistic solution lets you get a unified view of your IT infrastructure.
- Automation: Automation greatly reduces the chance of human error. The solution should let administrators schedule backups of the most recent version of your environments.
- Delegation: Modern backup solutions should allow non-admin users to initiate backup operations.

How **AD360** helps you backup data

- Unified backup solution: Configure multiple AD domains, Office 365 tenants, and Exchange organizations for backup, and manage them from a single dashboard.
- Automation: Schedule backups at fixed intervals to ensure you've backed up the most recent version of your AD, Office 365, and Exchange environments.
- Delegation: Delegate non-admin users with privileges to initiate backup operations and audit their actions.

The **AD360 backup** advantage

Overcome any disaster caused by unwanted change in your IT environment

-  Unified backup solution
-  Quick and easy deployment
-  Ransomware threat mitigation
-  Automate AD, O365 & Exchange backups
-  Backup job delegation & auditing

A quick recap on what we've discussed so far

- Enabling zero-trust and the challenges it can address
- Provisioning and modifying users the zero-trust way
- Tracking security events with UBA
- How can incident response be automated and what are its benefits
- Importance of data backup and how you can choose a comprehensive backup solution

Thank you.

Write to me to get our resources on data protection, UBA, and much more

jay@manageengine.com

ManageEngine 