TOP 5 IDENTITY AND ACCESS MANAGEMENT CHALLENGES OF 2021 AND HOW TO OVERCOME THEM

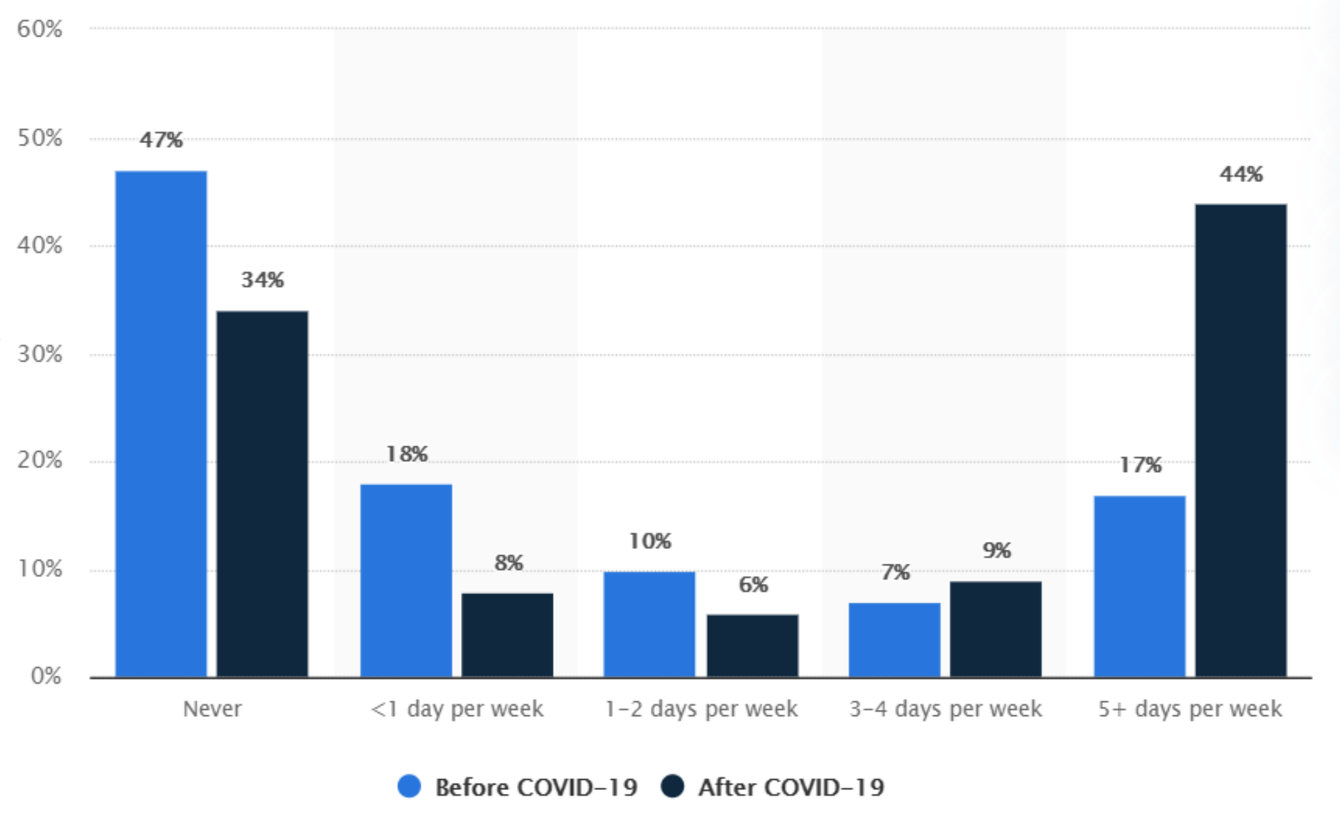
Presented by,
Jay Reddy
IAM & IT Security Expert | ManageEngine

What we'll discuss today:

- The shift from 'workplace' to 'workspace'
- Identity: The new perimeter.
- 5 Identity and access management challenges of 2021
  - **Prediction #1** - Accelerating cloud adoptions
  - **Prediction #2** - Bottlenecks in the employee onboarding process
  - **Prediction #3** - Legal risk associated with expanded employee data collection
  - **Prediction #4** - Increase in contingent workers
  - **Prediction #5** - New working conditions may drive up the risk of human error
- How AD360 can help overcome these challenges

The shift from 'workplace' to 'workspace'

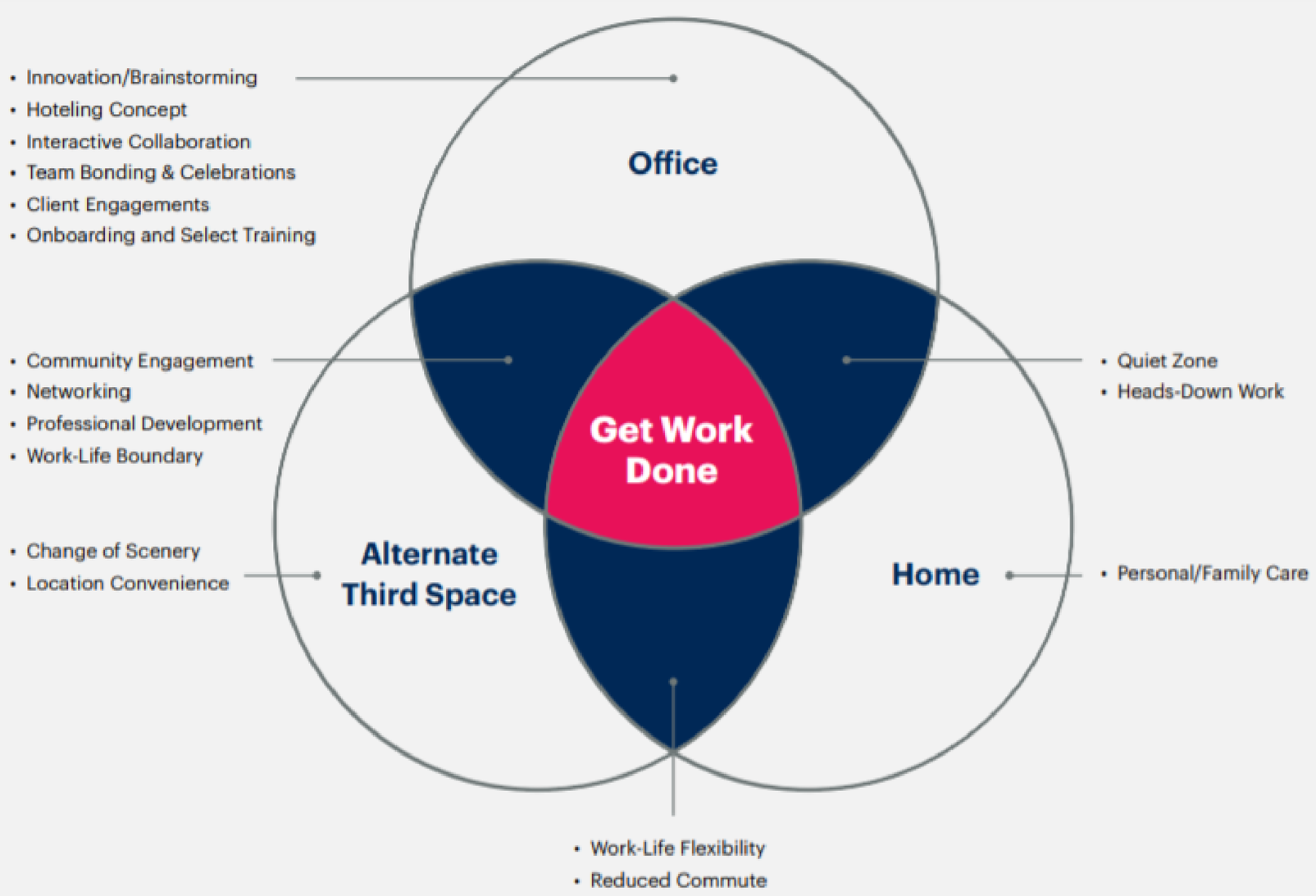
Post-COVID-19 era: what is different?



The virus has broken through cultural and technological barriers that prevented remote work in the past, setting in motion a structural shift in where work takes place, at least for some people.

Source: Statistia, McKinsey

Rethinking how (and where) work is done



300 percent

increase in remote work compared to pre-COVID levels

Source: Forrester

- Due to the disruptions caused by the pandemic last year, an estimated 2.7 billion people, or **more than four out of five** workers in the global workforce, have been affected by lockdowns and shelter-in-place orders.

- Businesses and governments were challenged to respond to the crisis quickly and in real time —forcing them to prioritize **service availability over security.**

Source: International Labour Organization

Result?

Cyber scams and ransomware booming amid Covid-19 lockdowns – Europol

INCREASE IN CYBER ATTACKS!

Huge rise in hacking attacks on home workers during lockdown

2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic

Cyber Risks: An Increased Threat During

Cyber criminals are attempting to take advantage of the upheaval caused by the CO

Big increase in cyber-attacks during the Covid-19 pandemic

Cyber crime will cost the global economy $6.1 trillion annually if we are not careful

WHO reports fivefold increase in cyber attacks, urges vigilance

Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic

Cybersecurity companies, and law enforcement report 800% surge.

UK sees a 31% increase in cyber crime amid the pandemic

Cybercrime Skyrockets 300% Since COVID-19

Cybercrime soars in 2020 as hackers take advantage of COVID-19 pandemic; here's how you can protect yourself

Microsoft report reveals increasing sophistication of cyber threats globally

UN reports sharp increase in cybercrime during coronavirus pandemic

Roundup: COVID-19 pandemic delivers extraordinary array of cybersecurity challenges

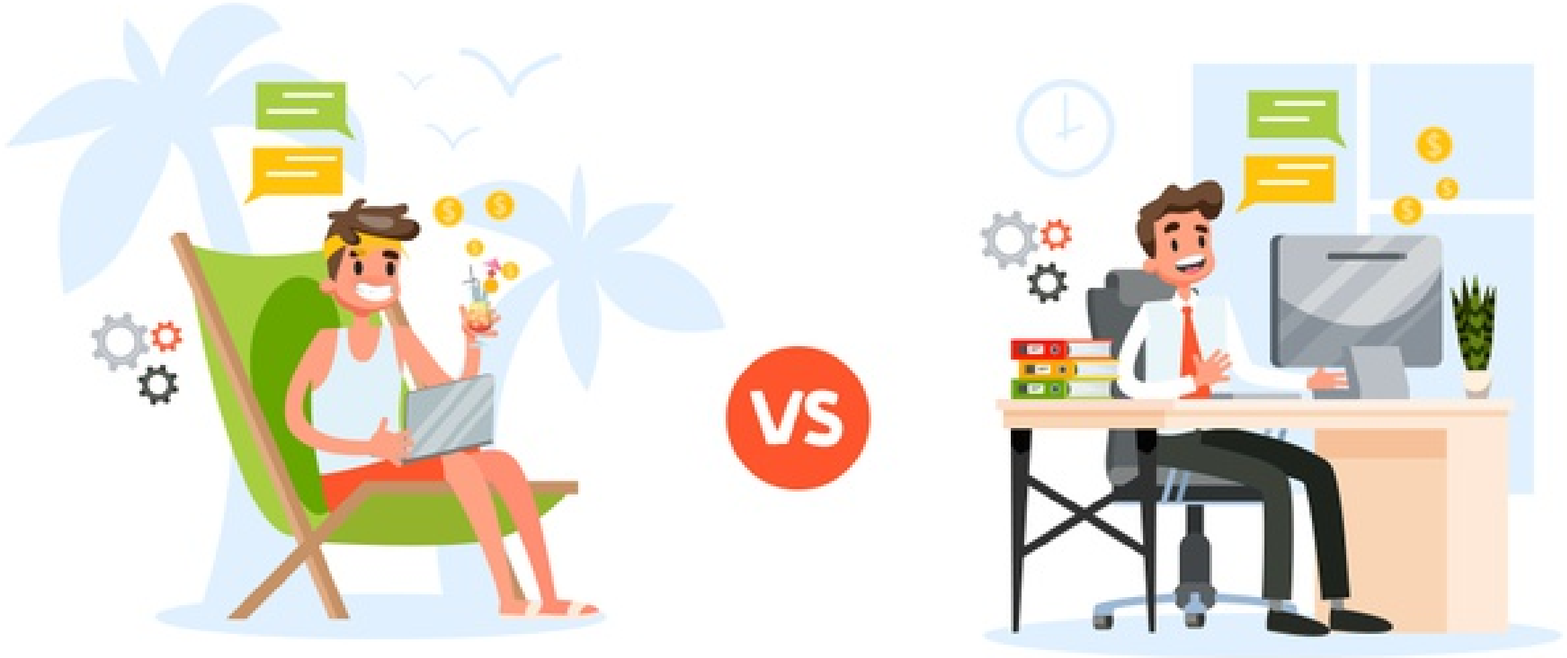
Cybercrime ramps up amid coronavirus chaos, costing companies billions

Online Education Due to Covid-19 is Causing Massive Spike in Cyber Attacks on Schools, Colleges

Report Finds 63% Increase in Cybercrime

WHAT DO I DO?

Office workstations became laptops at the kitchen table, in-person meetings became video chats and wired networks became at-home Wi-Fi connections.

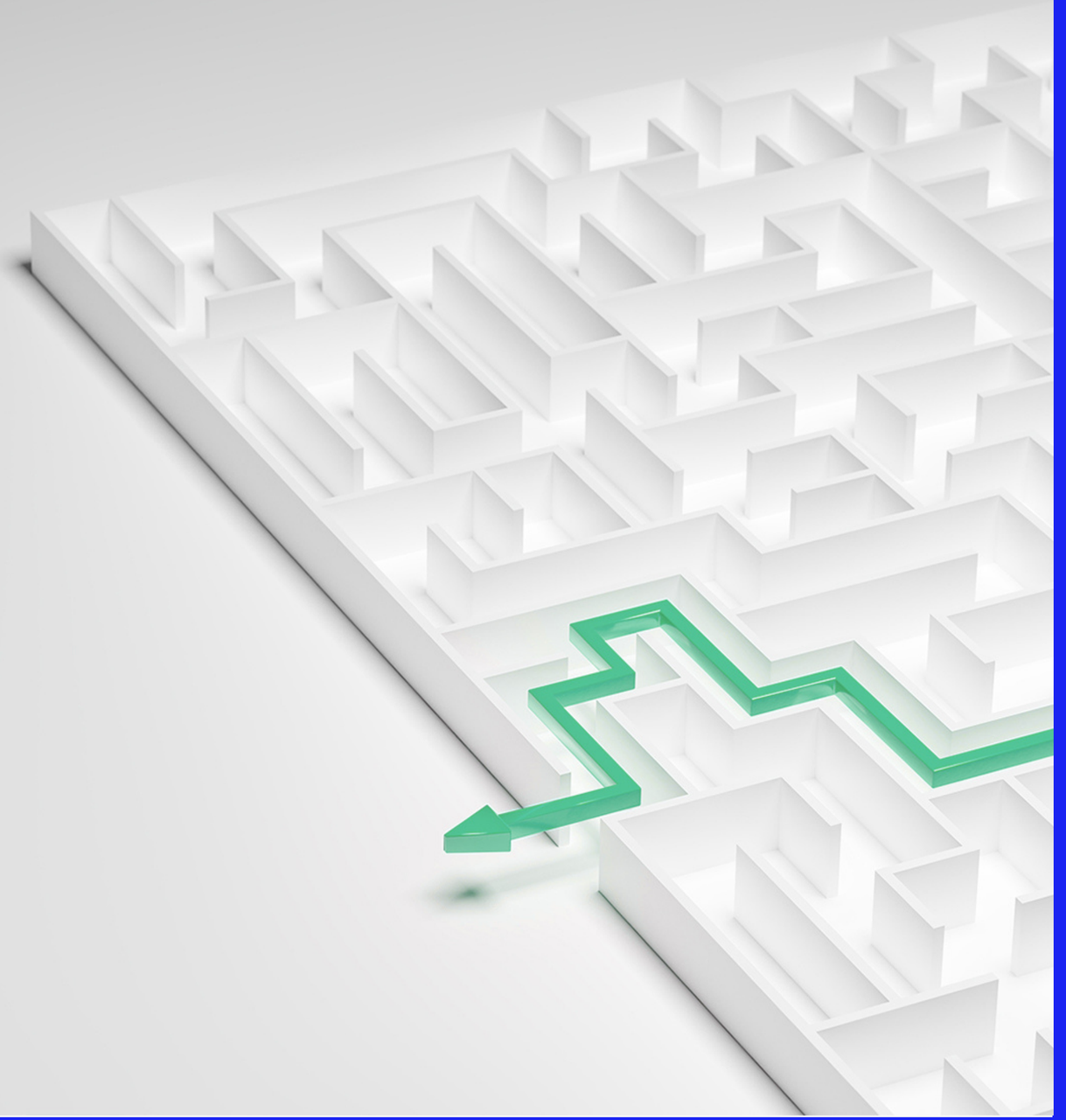


Data is flowing **everywhere!**

The network is no longer a position of advantage.

Identity is now the new perimeter.

Now that organizations are comfortable with the new normal, it's time for IT teams to **re-evaluate** their strategies to discover if and where their old strategies fall short, and prioritize their efforts to **plug any security loopholes** waiting to be exploited by cybercriminals.



5 PREDICTIONS ON IDENTITY AND ACCESS MANAGEMENT TRENDS FOR 2021

Prediction #1 - Accelerating cloud adoptions

Forrester predicts that in 2021 remote work will rise to 300% of pre-covid levels.

It also predicts that the global public cloud infrastructure market will grow 35% to $120 billion in 2021.

What was once a "nice to have" for employees and organizations became "must have" in the midst of the pandemic, and this trend is here to stay.

According to a Gartner survey, 48% of employees will work remotely after the pandemic, compared to 30% pre-pandemic.

Another Gartner survey revealed that 82% of company leaders plan to allow employees to work remotely at least some of the time.

For organizations that have employees both onsite and working remotely, it becomes a huge challenge for IT teams to adapt to managing a new, more complex hybrid workforce.


ManageEngine
AD360
New Employees
User details
Automation module
Create
AD user accounts
Active Directory
User Accounts
with or without licenses
Create Mailboxes
User Accounts
Office 365
Exchange Server
Google Apps

Prediction #2 - Bottlenecks in the employee onboarding process

While industries such as aviation, retail, finance, real estate, and automotive are among the worst affected by the pandemic—resulting in record job losses—other industries such as healthcare are **ramping up** hiring to meet demand.

Also, the vaccine rollout and general optimism about the economy has led to a spike in hiring. Even companies that had to lay off employees due to COVID-19 may need to **fill existing and new positions.**

A seamless onboarding and off-boarding process is critical for both the start and end of a positive employer-employee experience and the safety of sensitive corporate data.

What happens in most cases?

1. The HR manager exports the user details in a CSV file from their human resource management system (HRMS)
2. Shares the file with the IT team via email.
3. The IT admin then creates new user accounts—either individually or in bulk using PowerShell scripts
4. Grants appropriate access to resources based on the role of the employee.

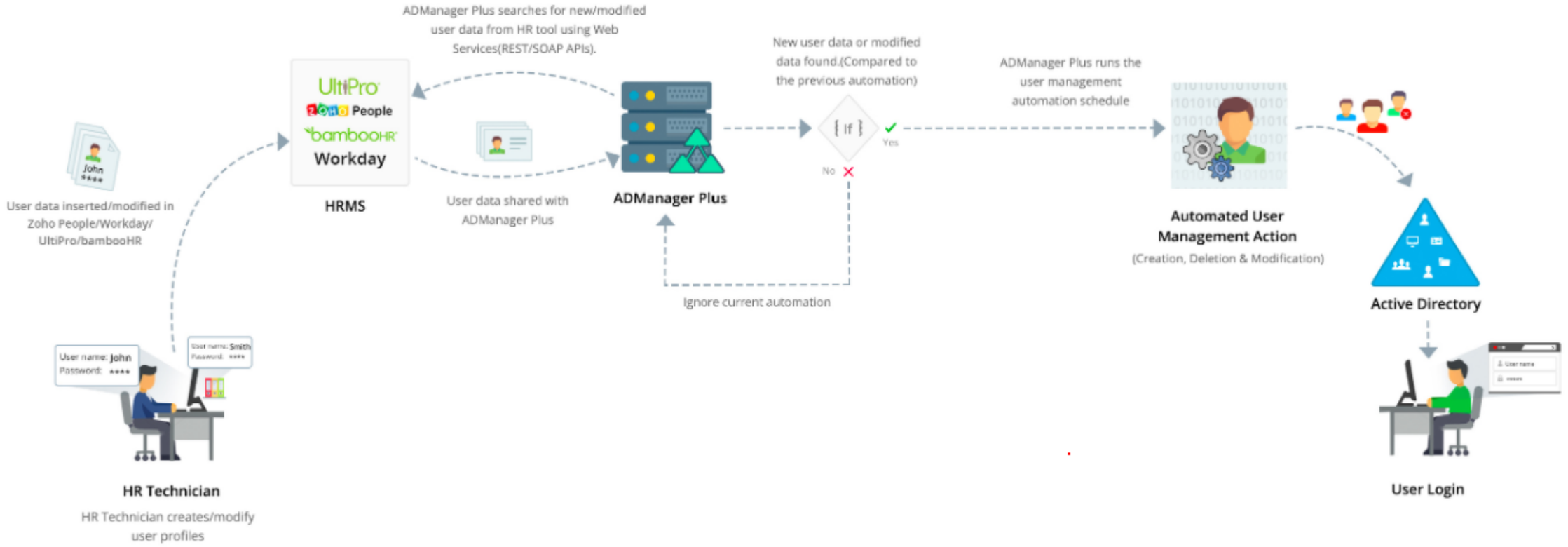
This process creates unnecessary bottlenecks since it is challenging to ensure **real-time collaboration** between the HR department and the IT department. Also, creating user accounts manually is often **tedious**, **time-consuming**, and **error-prone**.

AD360 integration with some of the important IT applications

Seamless employee onboarding using AD360

- AD360's capability to integrate with HRMS applications helps overcome all the common challenges in a typical employee on-boarding process.
- Once the user details are entered in the HRMS application, you can use AD360 to automatically provision accounts in AD, Microsoft 365, Exchange, Skype for Business, and Google Workspace.
- Also, any changes made in the HRMS application thereafter are reflected across all accounts in real time.

Integration with human resource management systems



Integrating with databases used by HR applications

Prediction #3: Legal risk associated with expanded employee data collection

- According to Gartner, even before the pandemic, organizations were increasingly using **nontraditional employee monitoring tools** to keep track of employee activities.

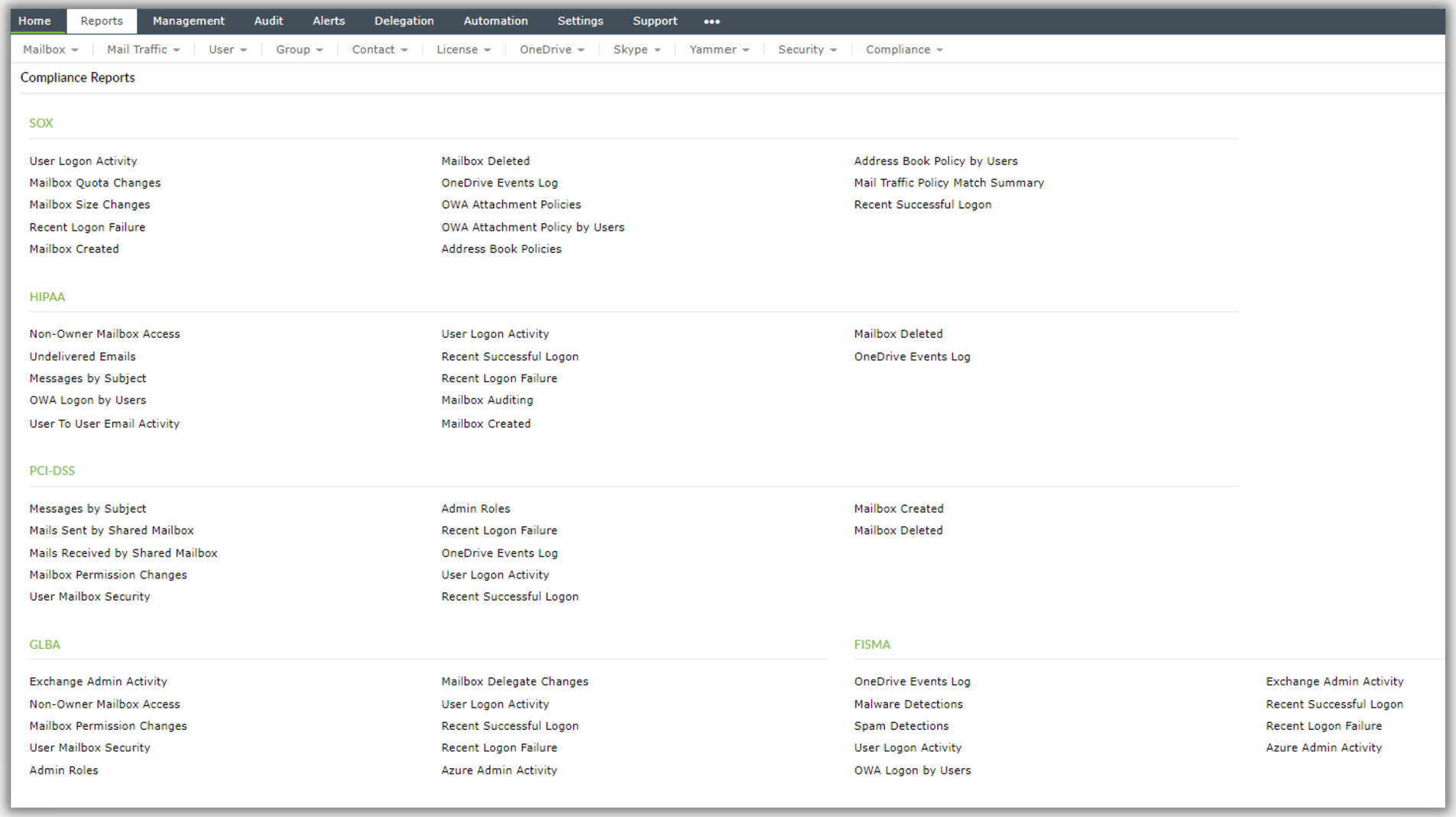
- Gartner's analysis shows that this trend will only accelerate in 2021 given the increased adoption of remote work due to the pandemic. In addition, Forrested believes that regulatory and legal activity regarding employee privacy will **double in 2021.**

To ensure compliance with regulations such as **SOX, HIPAA, PCI DSS, the GLBA, and the GDPR,** organizations must have elaborate records of all the data collected on employees' day-to-day activities.

Much of the data these regulations pertain to involves organizational activities occurring in AD, but most organizations **lack a comprehensive reporting system** for activity in AD.

Unfortunately, using native AD tools is highly laborious and time-consuming.

Compliance reporting with AD360



Prediction #4: Increase in contingent workers

Gartner predicts that organizations will look to increase hiring contingent workers in order to maintain more flexibility in workforce management post-COVID-19.

- Although a contingent worker's tenure is limited, they must be given **appropriate access to company resources** based on their role and job function.

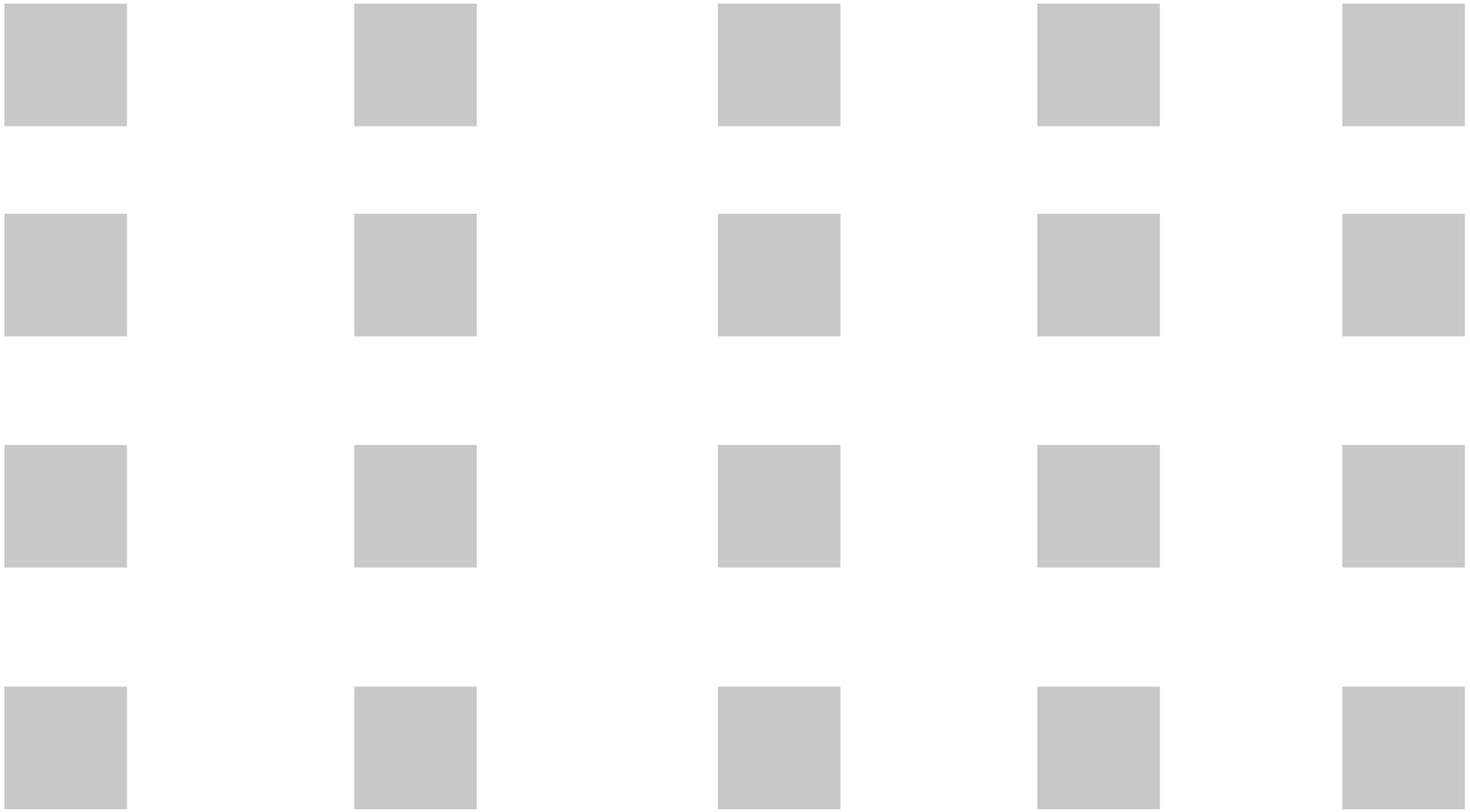
- However, once their job is done and they are no longer part of the organization, all the access pertaining to their user account must be revoked and the account must be **purged permanently.**

- If this action is done manually on an ad hoc basis, there is a risk of **account compromise attacks** if the IT administrator forgets to delete the contingent worker's account.

The risk is higher if the account belongs to a privileged user.

A SINGLE ACCOUNT COMPROMISE CAN POTENTIALLY PARALYZE YOUR ENTIRE NETWORK

HOW DOES AN ATTACKER MOVE LATERALLY?



HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account

HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account

DA

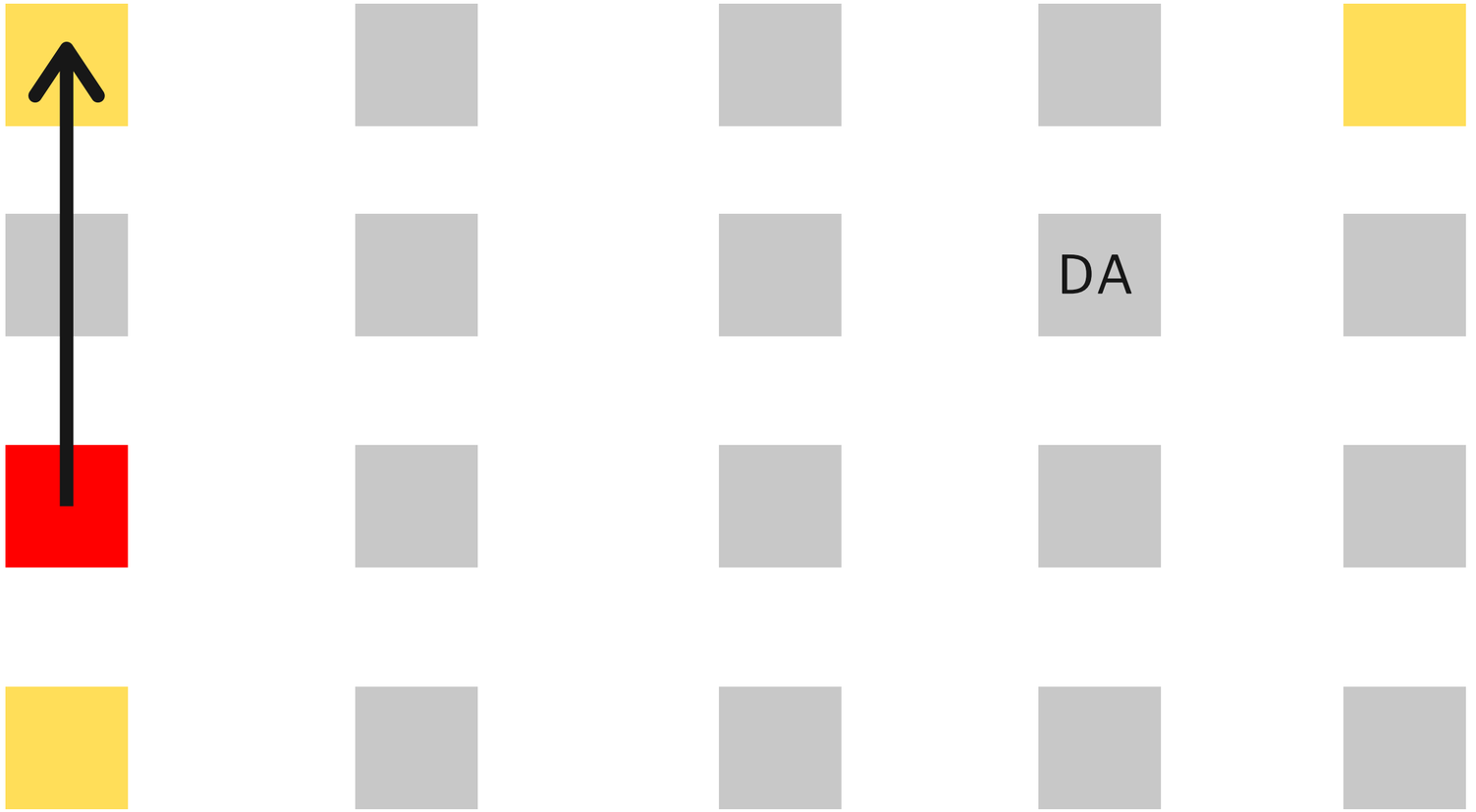
HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account

DA

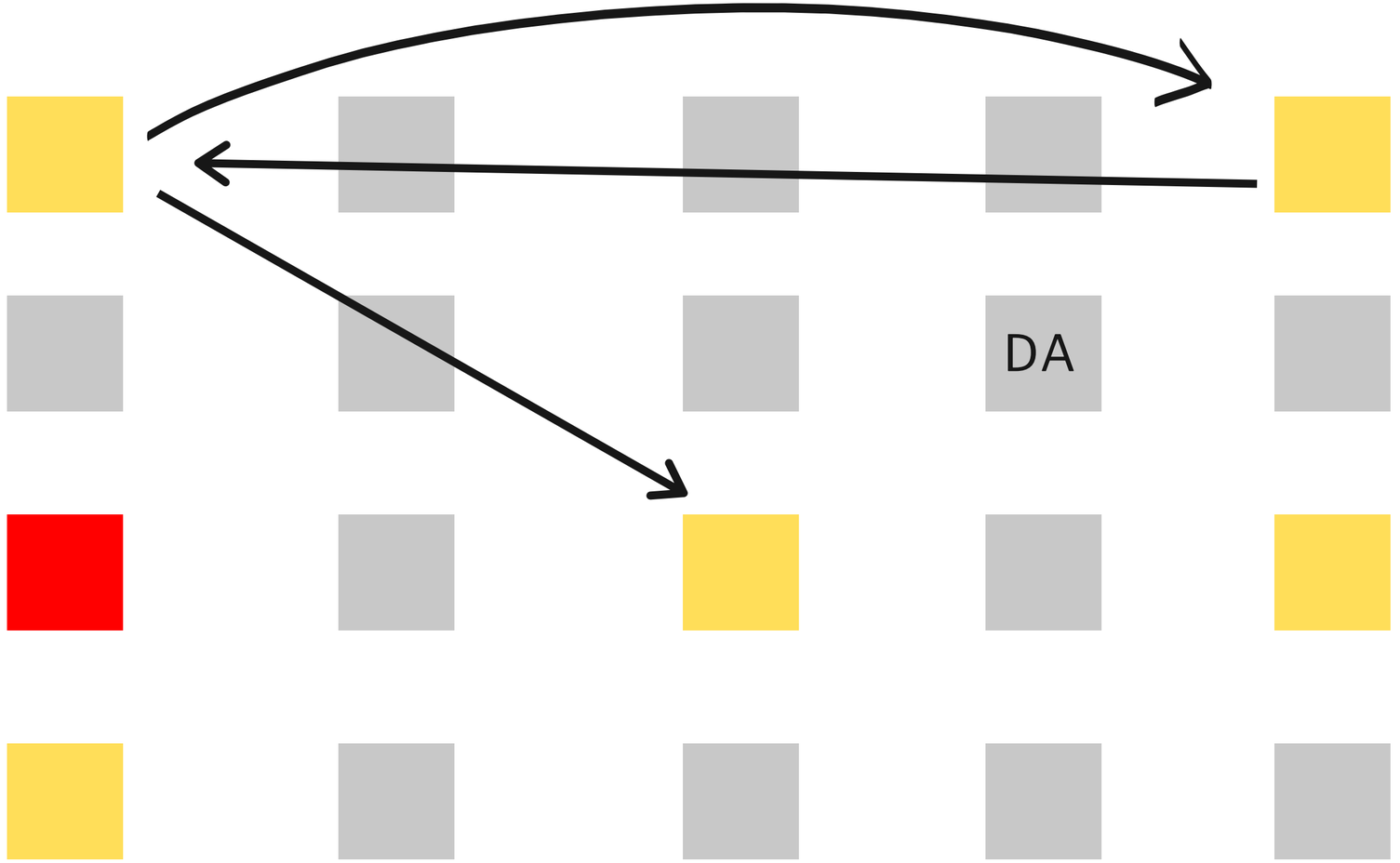
HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account



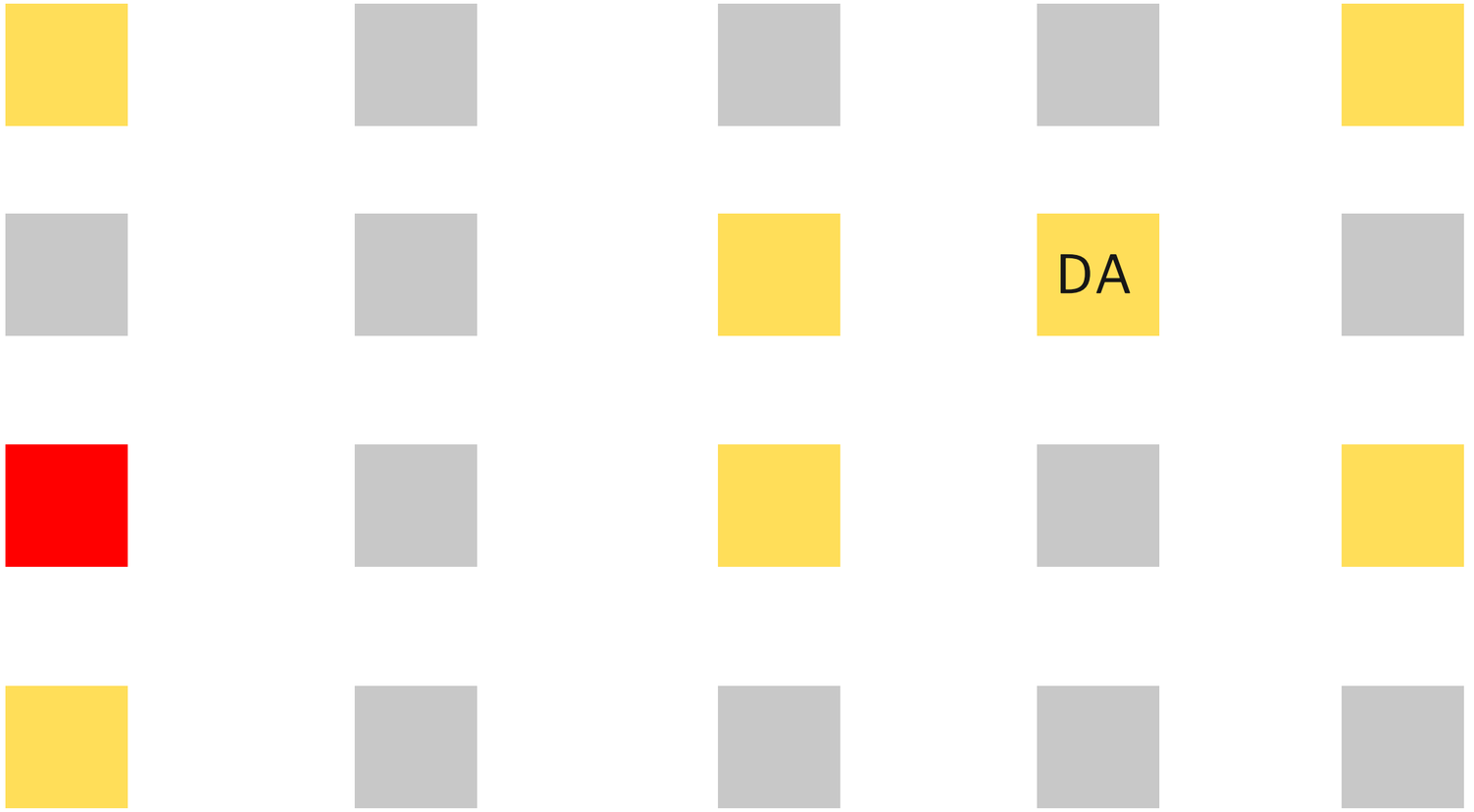
HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account



HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account



HOW DOES AN ATTACKER MOVE LATERALLY?

initial foothold by compromising an inactive account

DA

- This is why it's crucial to identify such inactive accounts and **immediately purge them**. However, the only way to ensure that all inactive accounts are removed immediately is by automating the process.

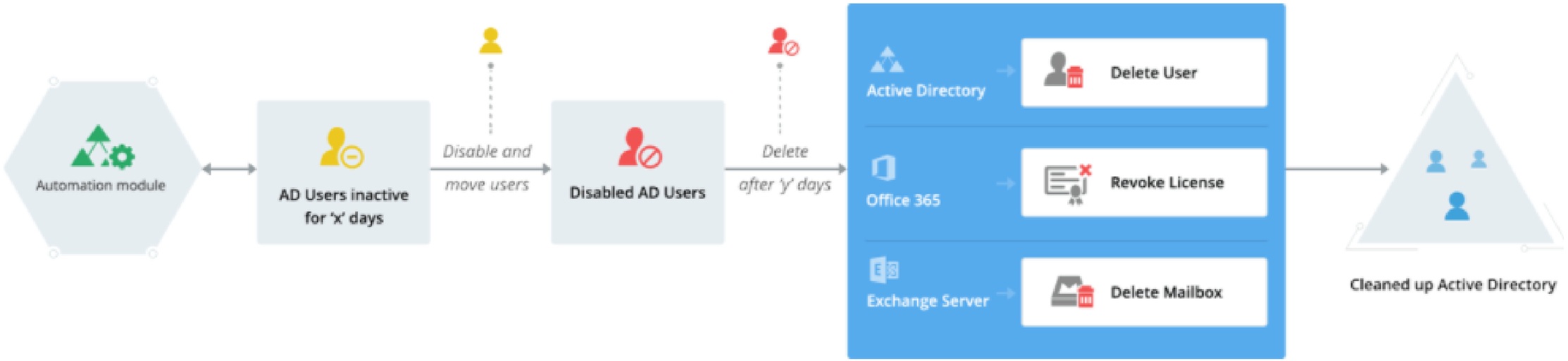
- While native AD has provisions to track down and eliminate inactive user accounts, it **cannot remove them in bulk or automate the process.**

Move, disable or delete dormant or stale user or computer accounts

- AD360 lets you effortlessly report on **all inactive user accounts, disabled user accounts, and expired user accounts**. Right from these reports, you can delete or disable these accounts in bulk instantly.

- If required, you can also move them to a separate organizational unit, **quarantine them for a desired period**, and then delete them eventually. Best of all, you can automate these tasks and specify how often you want this automation to run.

How it works


Automation module
AD Users inactive for 'x' days
Disable and move users
Disabled AD Users
Delete after 'y' days
Active Directory
Delete User
Office 365
Revoke License
Exchange Server
Delete Mailbox
Cleaned up Active Directory

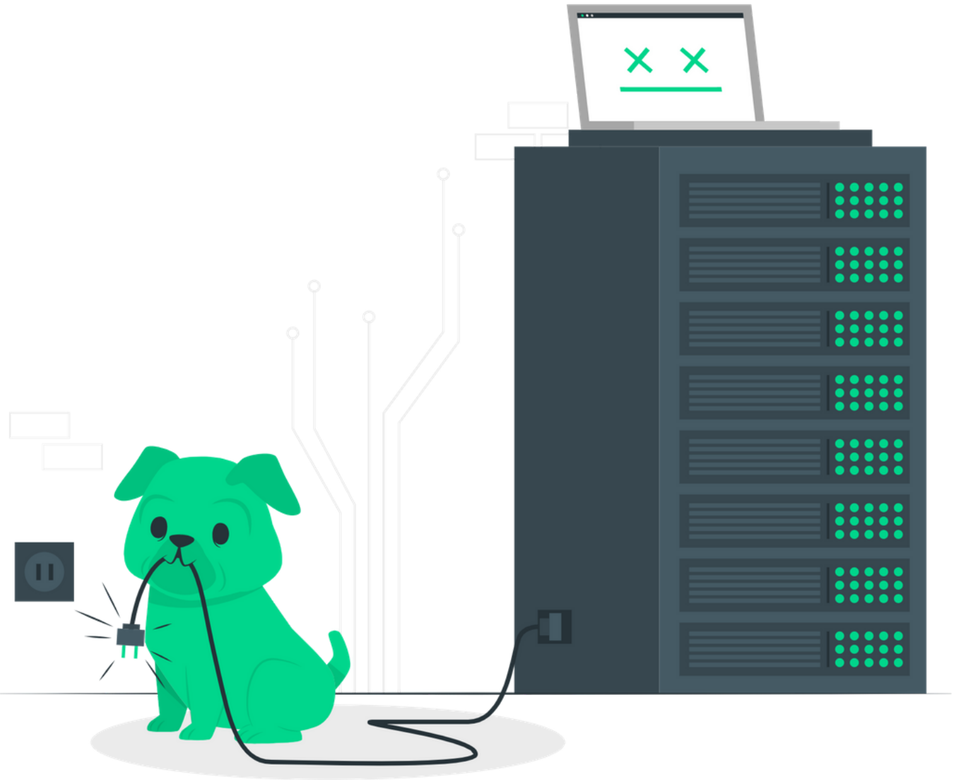
Prediction #5: New working conditions may drive up the risk of human error

Some organizations found themselves already equipped with the right technologies and protocols to sustain a sudden transition to remote work, while some organizations were forced to adopt remote work hastily to maintain business continuity.

However, the scale at which this transition had to occur was certainly not anticipated by IT teams on either side.

Remote work at this scale is somewhat unfamiliar territory for IT teams that are already overburdened, mistakes are bound to happen.

These mistakes could be an unintended modification or deletion that affects a single user, perhaps preventing them from logging in or accessing a file, or it could be an error that brings down the whole domain controller and affects multiple users at once.



THE AD360 ADVANTAGE

01 Effortlessly back up and restore AD objects, Exchange mailboxes, Office 365 mailboxes, SharePoint Online sites, OneDrive for Business folders, etc.

02 Perform item-level or attribute-level restorations, and speed up the backup process by making incremental backups.

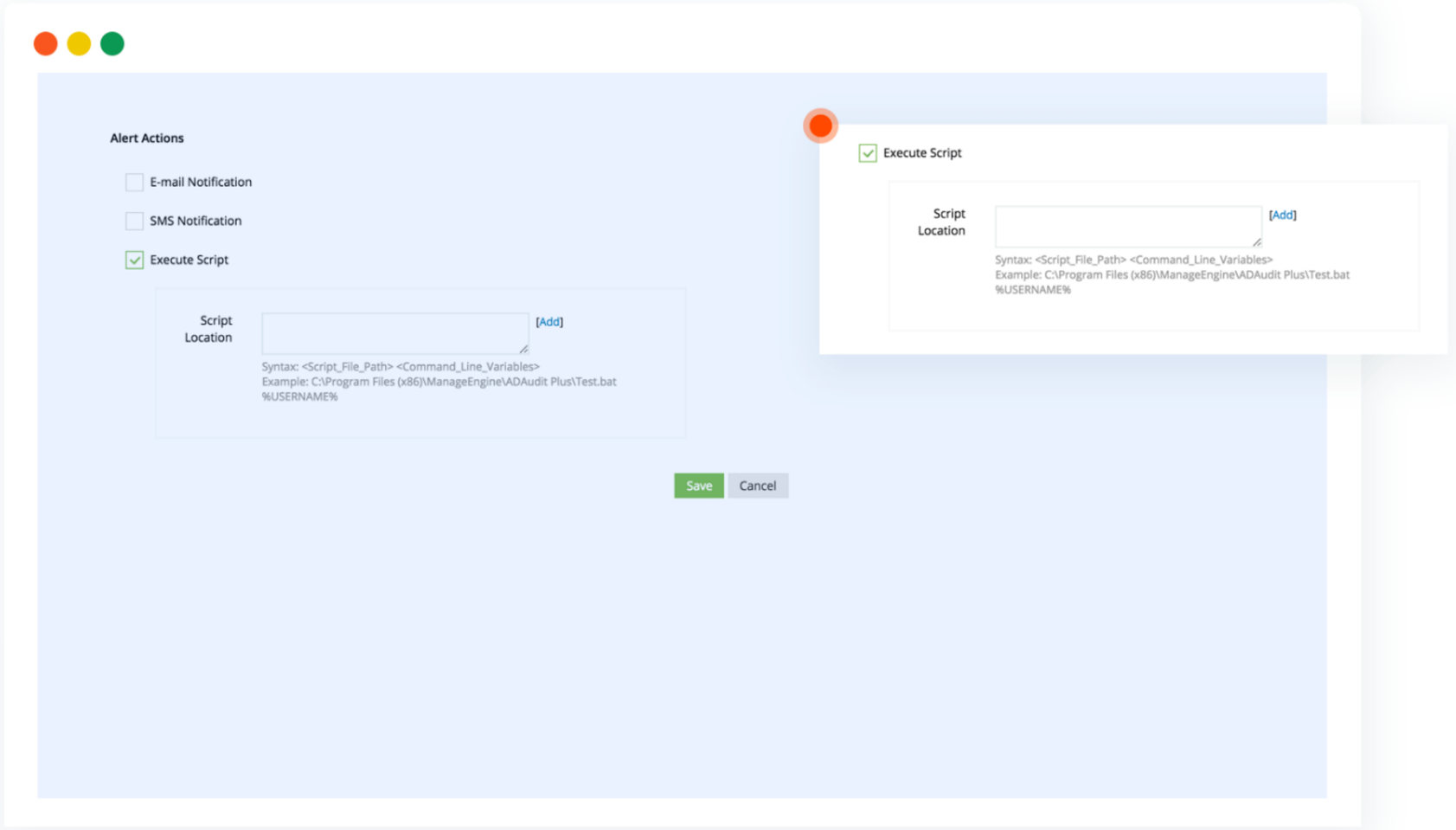
03 Schedule backups to run during non-business hours, and more.

CRUCIAL INSIDER THREAT STATISTICS

- Businesses in the US encounter about **2,500 internal security breaches daily**.
- **More than 34% of businesses** around the globe are affected by insider threats yearly.
- 66% of organizations consider malicious insider attacks or **accidental breaches** more likely than external attacks.
- Over the last two years, the number of insider incidents **has increased by 47%**.
- The cost of insider threats (related to credential theft) for organizations in 2020 is **$2.79 million.**
- Insider threat stats reveal that **more than 70% of attacks** are not reported externally.

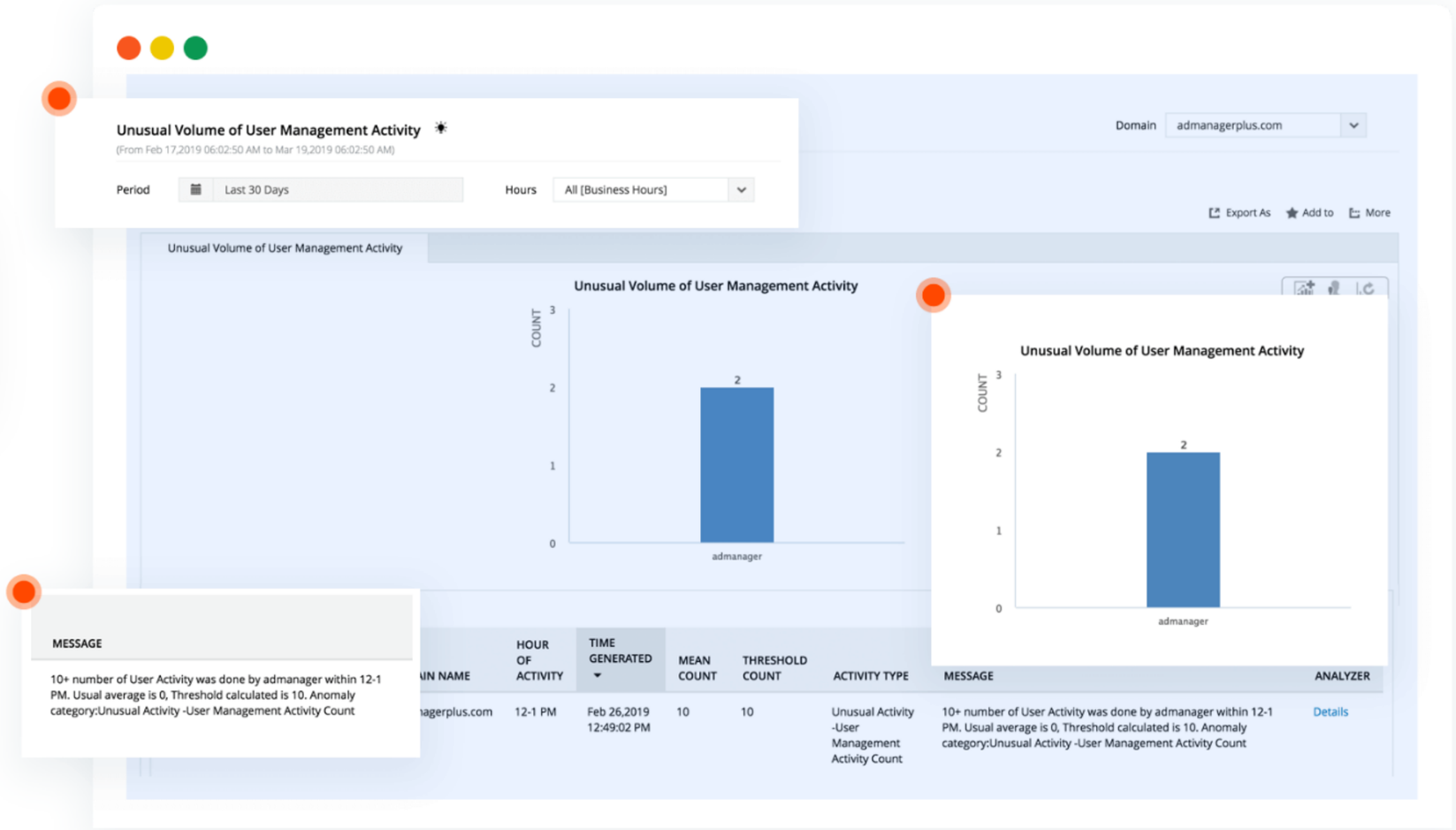
Source: Techjury

MITIGATE THREATS



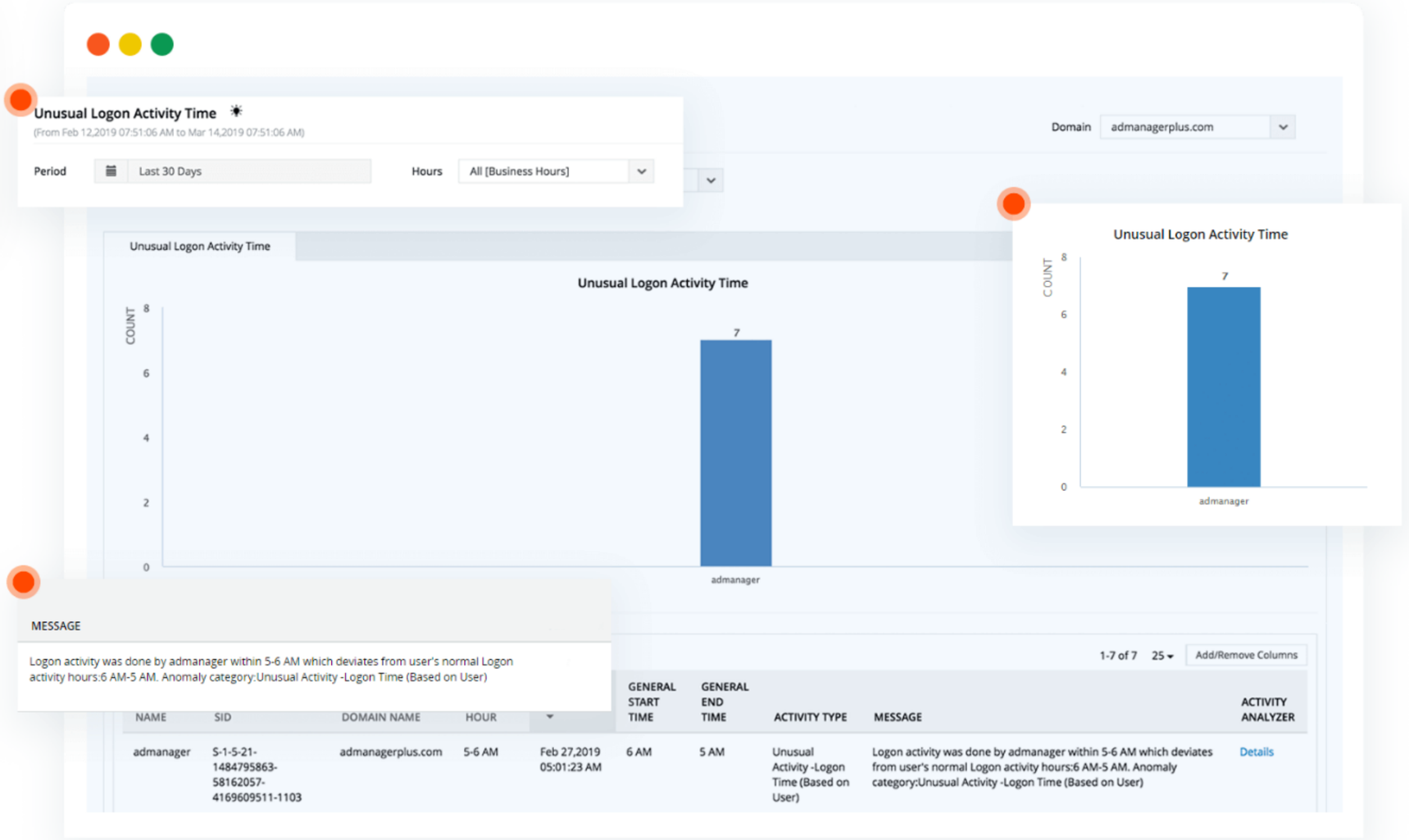
Execute a predetermined action when an anomaly gets detected.

INVESTIGATE ANAMOLIES



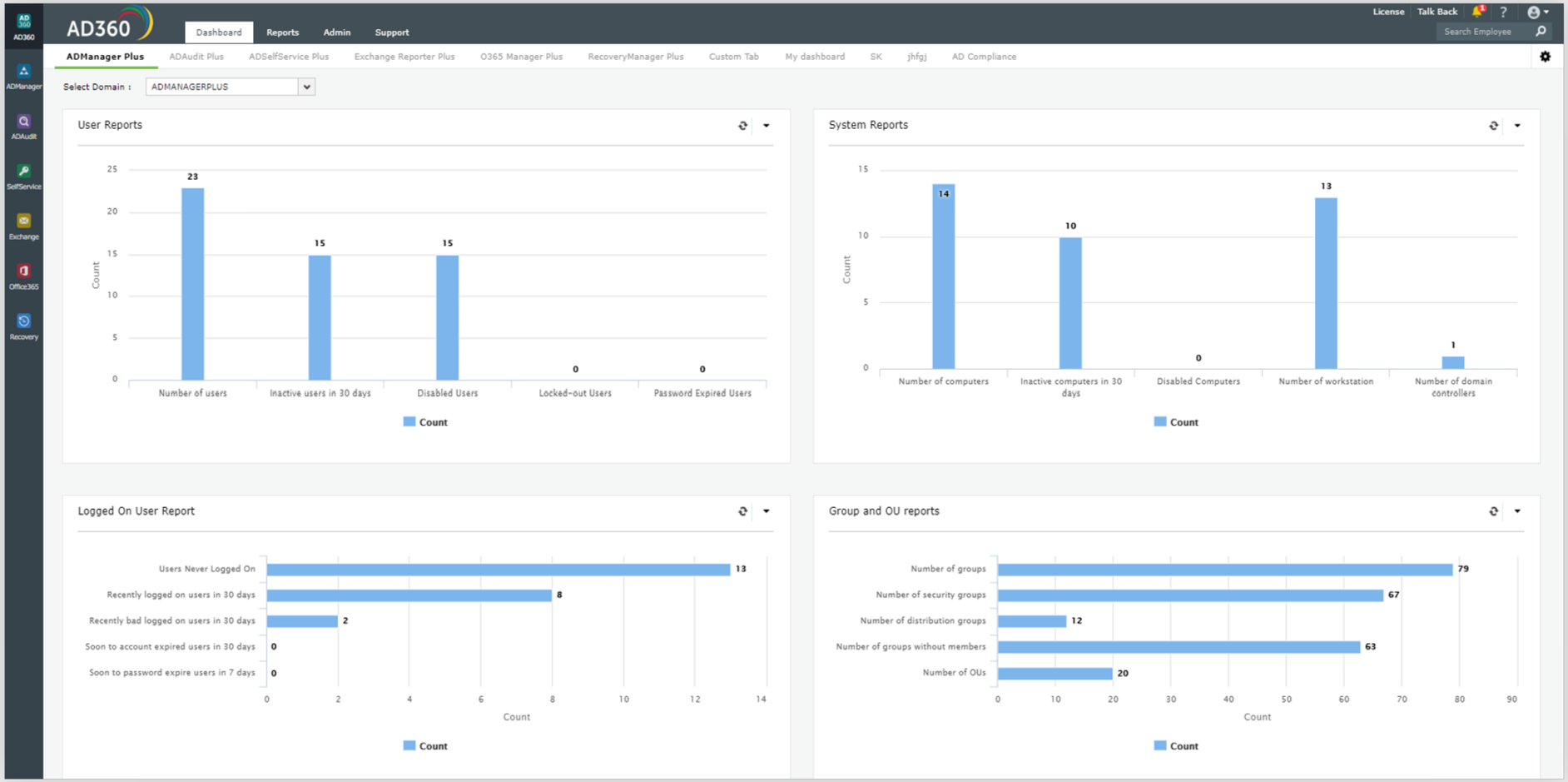
See who did what, when, and where, along with other details surrounding each anomaly.

MALICIOUS LOGINS



Receive notification if a critical server is accessed during unusual hours, or when there's been an unusual number of login failures.

AD360 - AN INTEGRATED IAM SOLUTION



ManageEngine

AD360

ensures that the right people get the right access to the right resources at the right times for the right reasons, enabling the right business outcomes.

THANK YOU

Write to me. Cheers.

jay@manageengine.com

ManageEngine

www.manageengine.com