

# How **healthcare organizations** can mitigate cybersecurity threats and operational disruption

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

# What we'll discuss today:

- IT challenges in the healthcare industry:
  - Securing confidential electronic health records (EHR's)
  - Privilege assignment and monitoring
  - Detecting and responding to ransomware attacks/insider threats
  - Achieving compliance with HIPAA
- How you can tackle these challenges

# 75%

of healthcare organizations  
have experienced cyberattacks  
globally

## High profile cyberattacks:

- Czech Republic hospital
- Brno University Hospital
- US Department of Health and Human Services (HHS)
- World Health Organisation (WHO)



**68%**  
of breaches  
take months  
or longer  
to discover

# Fortifying your Electronic Health Records (EHR)

- Track the who, what, when, and where behind every successful and failed attempt to access a file across your Windows Server, NetApp, and EMC environments.
- Detect USB devices plugged into domain controllers, servers, or workstations, and receive alerts when files are copied to them.
- Identify where the data in your organization is traveling, and set boundaries on how far it can go.
- **Establish a Zero Trust policy:** Monitor file creation, deletion, modification, and permission changes made by healthcare staff to ensure that permissions are granted on a need-only basis.

# Zero-trust policy based AD management

As organizations grow, networks, additional resources, and administrative tasks also grow at a faster pace. It becomes difficult for the IT department to manage the entire Active Directory in a timely, error-free and efficient manner.

The fact that the IT admins have to follow a long list of best practices to ensure zero trust policy only makes things worse.

# A2. Is AD delegation the solution?

Delegate administrative tasks to non administrative users through an established workflow for completely secure delegation.

- OU Based Delegation
- Group Based Delegation
- Office 365 delegation
- G Suite delegation

# AD security delegation

Security administration tasks are critical making delegation risky. How do you securely delegate the following tasks?

- Reset the user password
- Unlock the user accounts
- Add or remove members from groups
- Move users to a different OU within the domain
- Move computers to a different OU within the domain
- Add/remove workstations in the domain
- Create user accounts
- Create, delete, and modify attributes of the user accounts



# Are you auditing your technicians?

## **Delegation questions that keep admins up at night**

Is my environment safe with admin level privileges delegated to technicians?

How am I going to audit all my technician actions?

# Is Active Directory automation really the key?

Automate AD management task without taking the control out of humans.

How automation and workflows can help you comply with HIPAA?

## **HIPAA clause 164-308:**

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

# A bird's eye view on AD and GPO changes

- Have a complete visibility on who made what change, when, and where.
- Monitor and log changes made to all Active Directory objects, including users, computers, GPOs, passwords, and more.
- Keep tabs on administrative group membership changes, and get instant alerts on critical membership changes.
- Get a consolidated audit trail of changes made to users, computers, and Group Policy Objects (GPOs) within a given time frame.

# Privilege access management

- Assign only the required level of access to a patient's health information to doctors, nurses, health insurance executives, and others who are directly responsible for that patient.
- Identify and get alerts on telltale signs of privilege abuse, such as unusually large volumes of file modifications and attempts to access critical files.

# Track privilege abuse

**Unusual Volume of User Management Activity** \*

(From Feb 17,2019 06:02:50 AM to Mar 19,2019 06:02:50 AM)

Period Last 30 Days Hours All [Business Hours]

Domain admanagerplus.com

[Export As](#) [Add to](#) [More](#)

**Unusual Volume of User Management Activity**

| User      | Count |
|-----------|-------|
| admanager | 2     |

**Unusual Volume of User Management Activity**

| User      | Count |
|-----------|-------|
| admanager | 2     |

| DOMAIN NAME       | HOUR OF ACTIVITY | TIME GENERATED          | MEAN COUNT | THRESHOLD COUNT | ACTIVITY TYPE                                    | MESSAGE   | ANALYZER                |
|-------------------|------------------|-------------------------|------------|-----------------|--|---|-------------------------|
| admanagerplus.com | 12-1 PM          | Feb 26,2019 12:49:02 PM | 10         | 10              | Unusual Activity -User Management Activity Count | 10+ number of User Activity was done by admanager within 12-1 PM. Usual average is 0, Threshold calculated is 10. Anomaly category:Unusual Activity -User Management Activity Count | <a href="#">Details</a> |

# Apart from privilege misuse...

What if a malicious actor is up to something else?

## **What will help:**

- Employee activity monitoring
- File permission monitoring

# 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

# UBA: Find the needle in the hay stack.

## **User Behavior Analytics:**

- Machine Learning based anomaly detection
- Detect anomalous behavior based on irregularities in behavior patterns such as logon/logoff time, number of logon attempts
- Identify indicators of common threats such as account compromise and data exfiltration



# User behavior analytics (UBA)

Creates a baseline of normal behavior specific to each user and alerts about deviations from this norm.

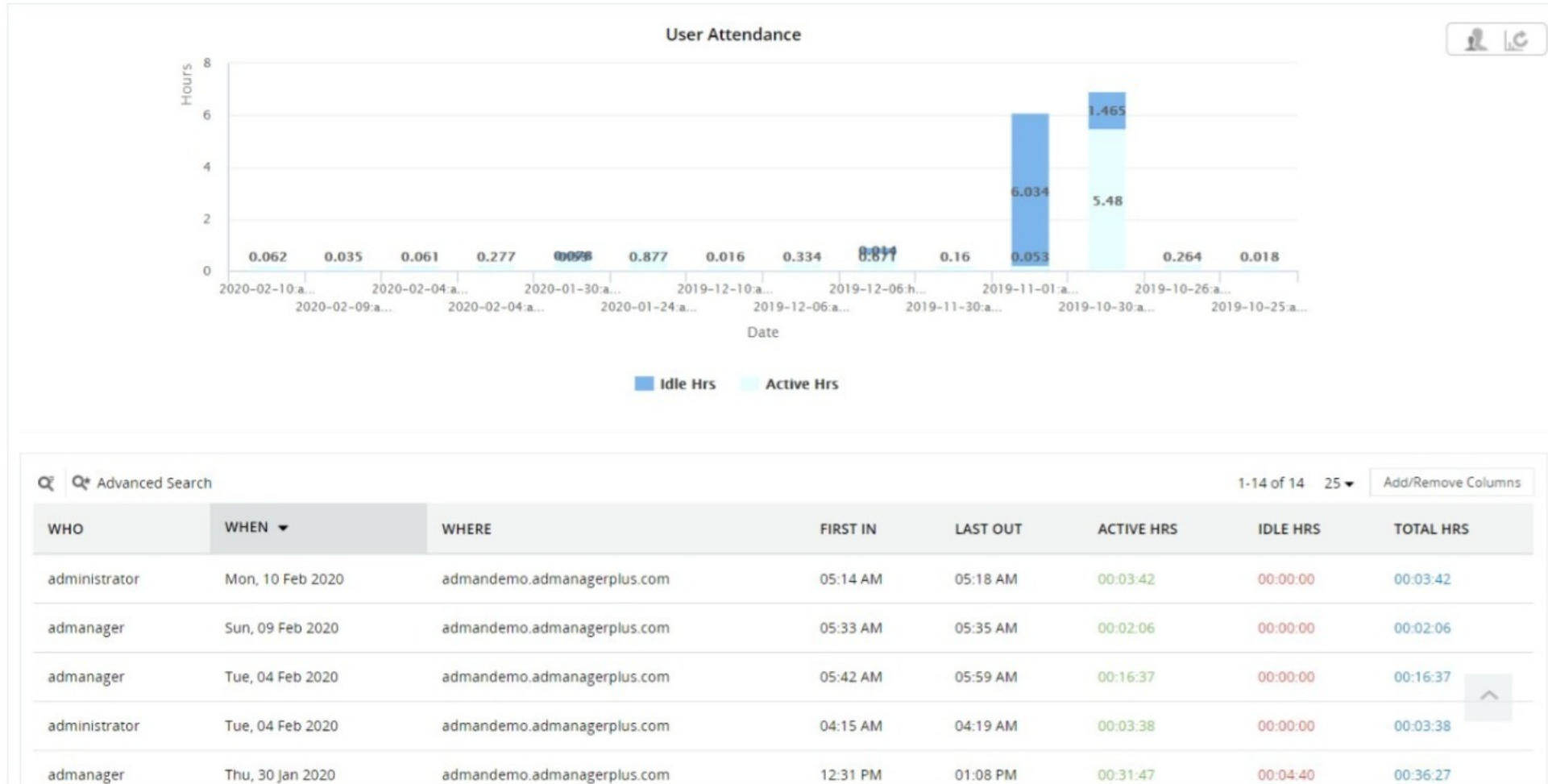
## Type of alerts

- Unusual Count:** If a user's activity or file activity count exceeds
  - + a dynamic threshold.
- Unusual Time:** Any activity occurs after the calculated normal
  - + activity hours.
- New resource access:** If a new resource was accessed. E.g., a
  - + new user access on a computer, new remote to a server from a client, or a new process ran on a server.

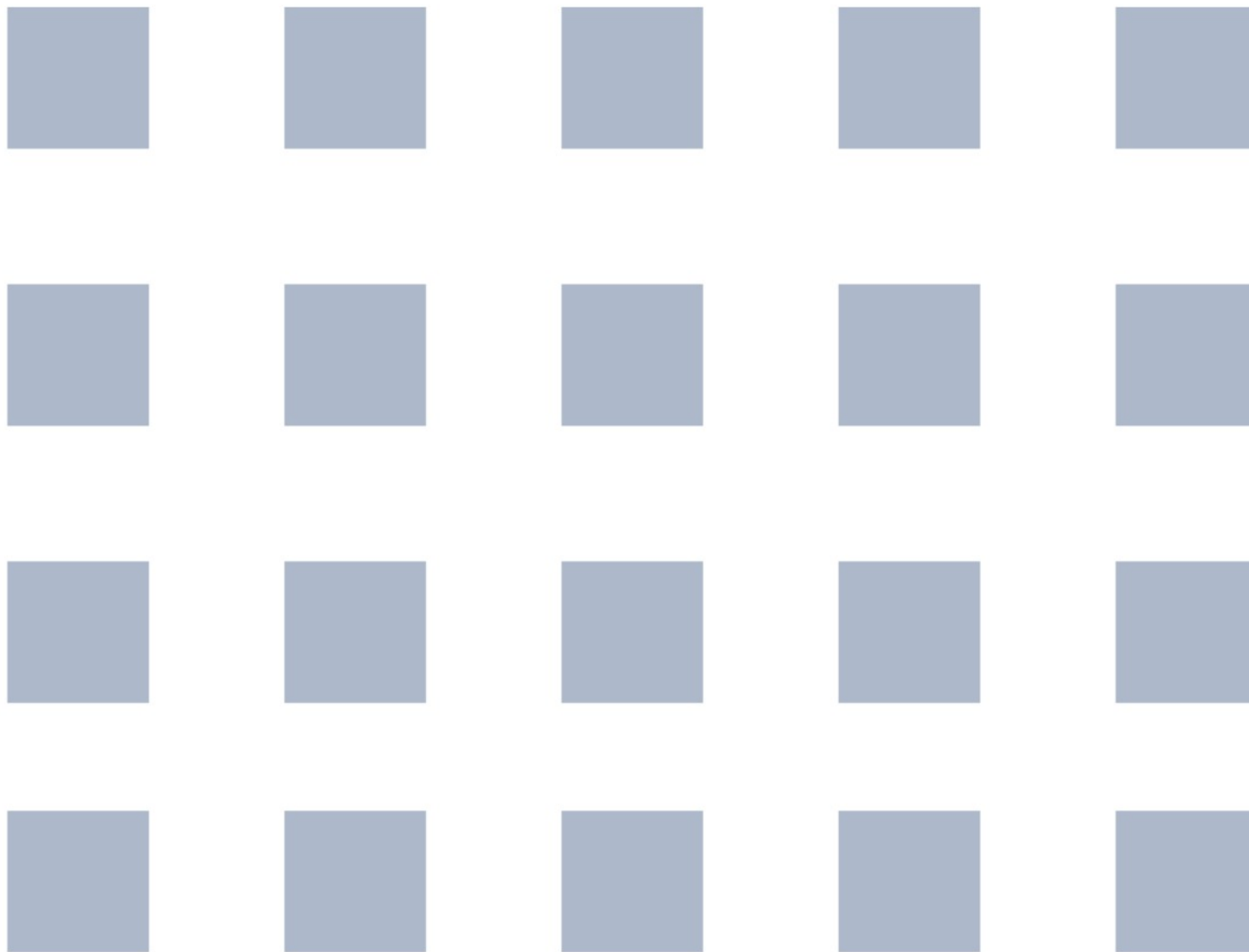
# Why user logon activity should be monitored

1. Brute force attacks
2. Attackers snoop in during non- business hours
3. Remote desktop activity
4. Island hopping – Lateral movement gives them access to more than just a single endpoint.

# Logon tracking report

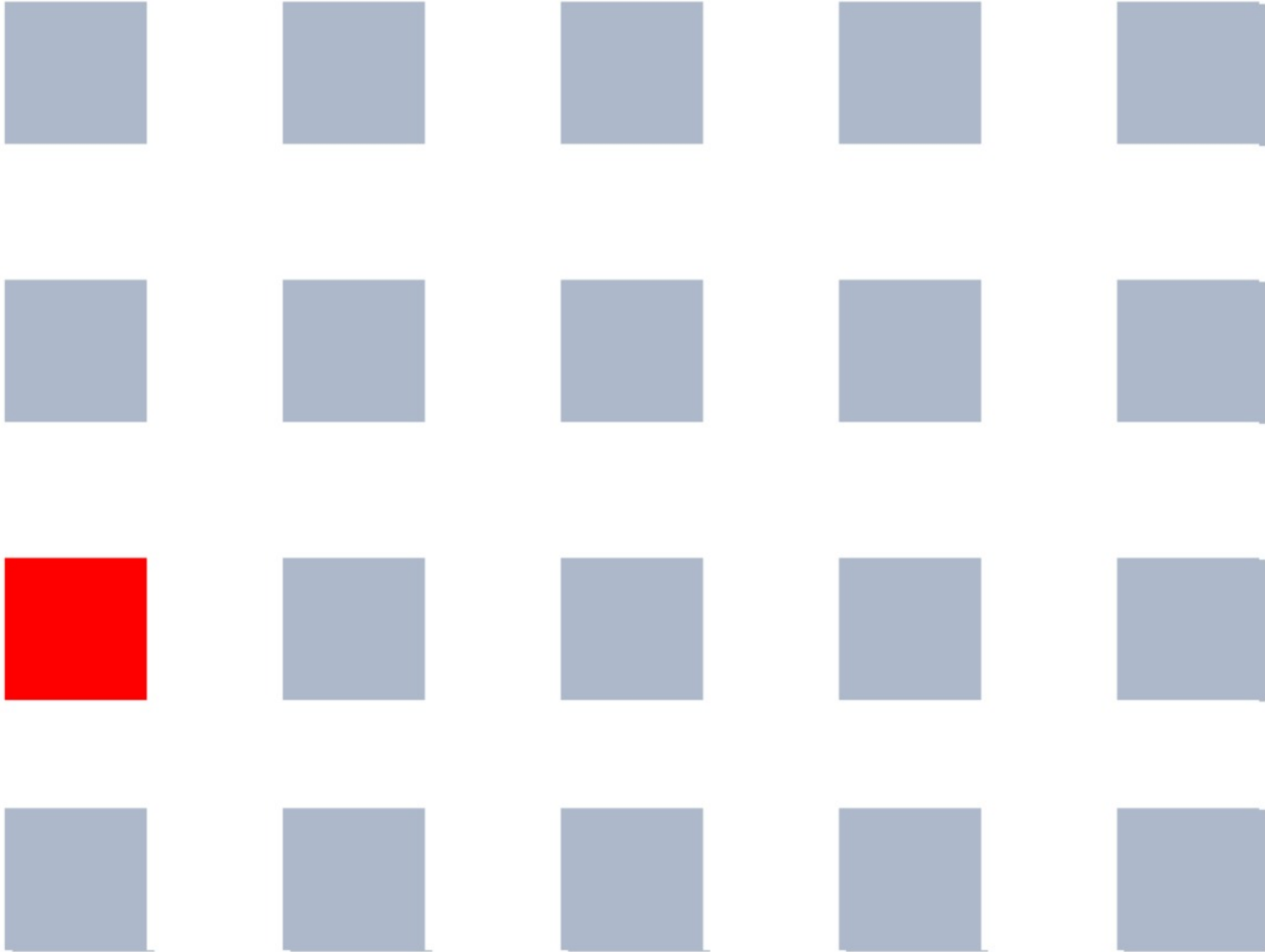


# How does an attacker move laterally?

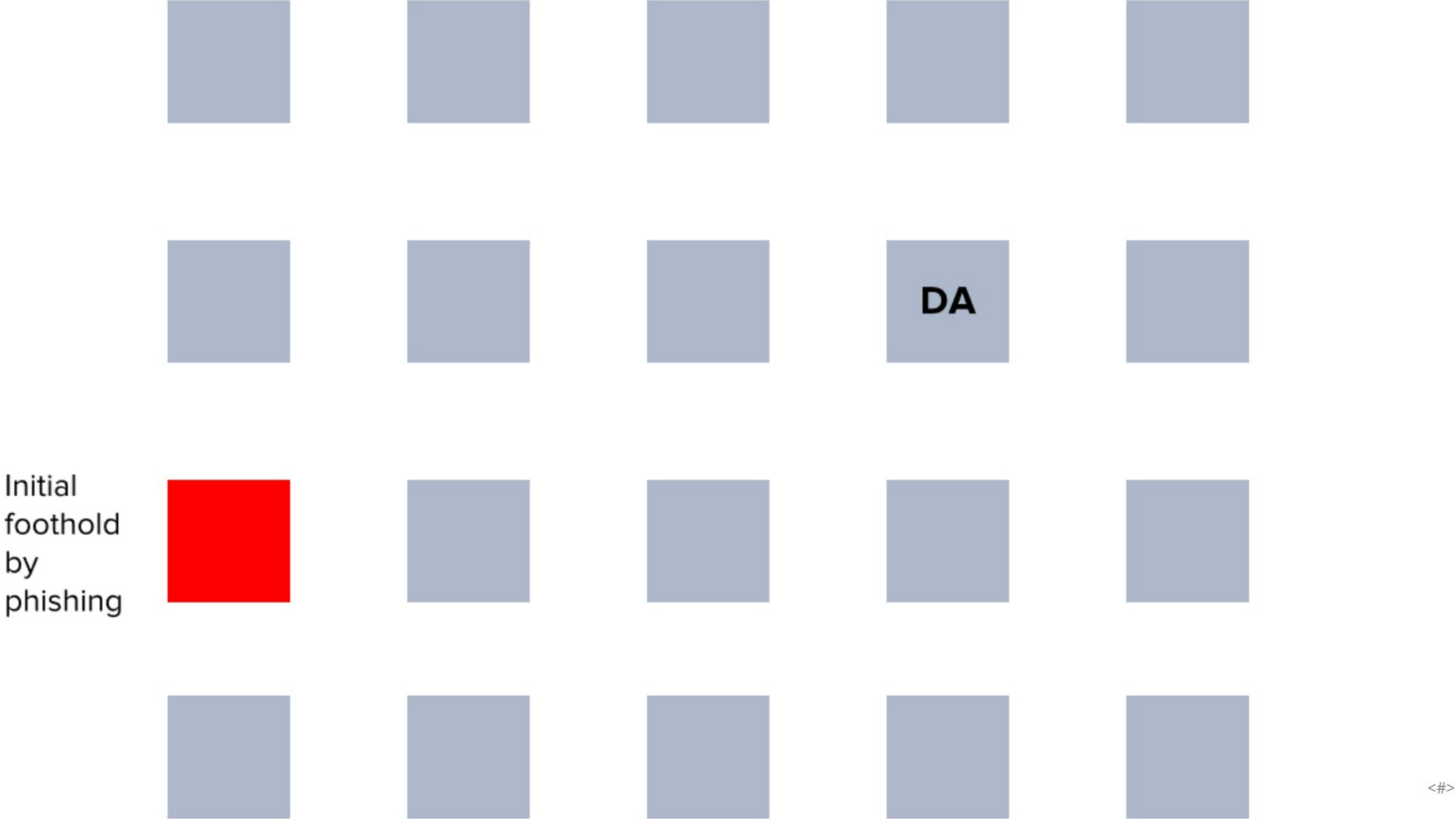


# How does an attacker move laterally?

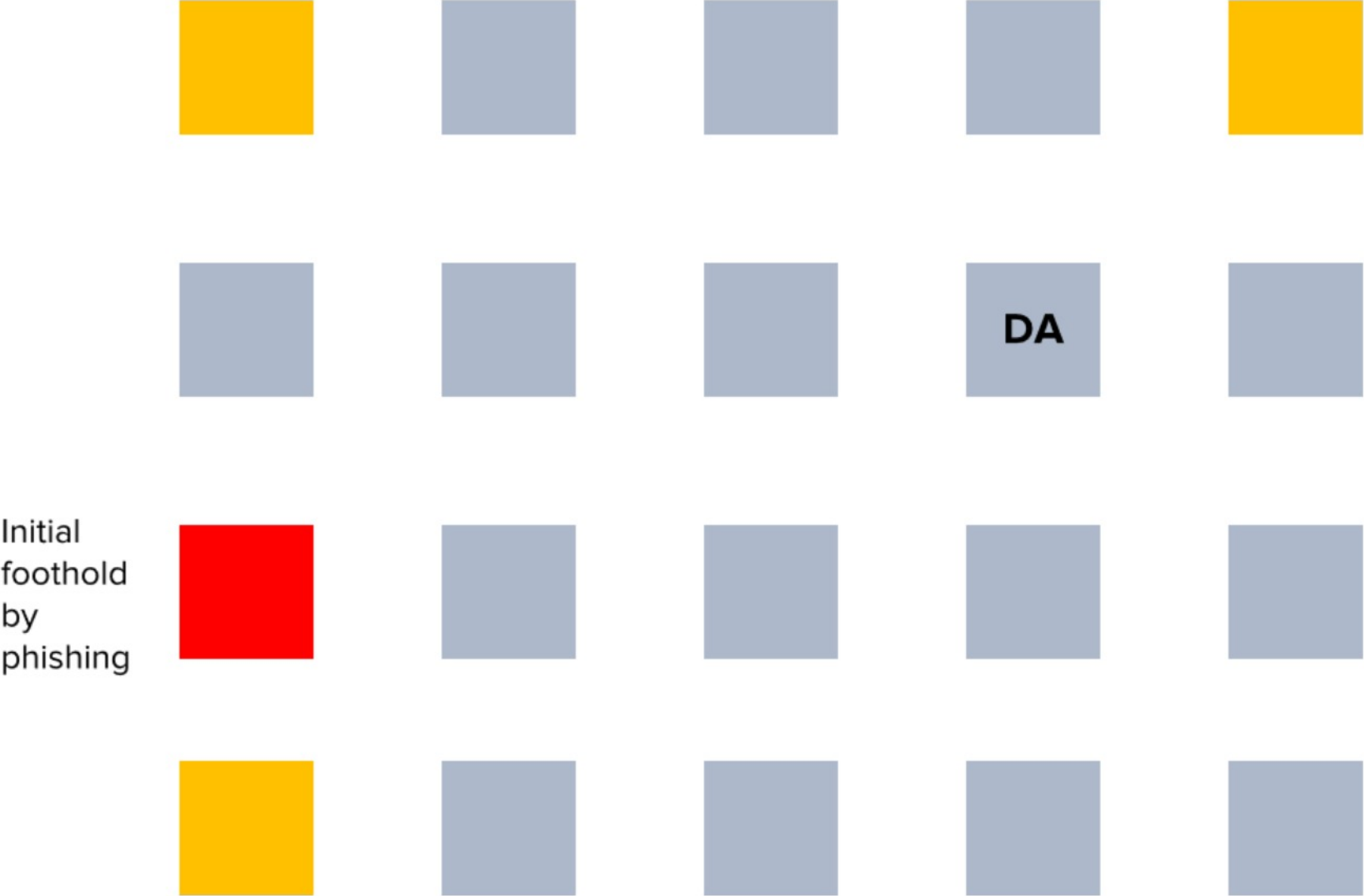
Initial  
foothold  
by  
phishing



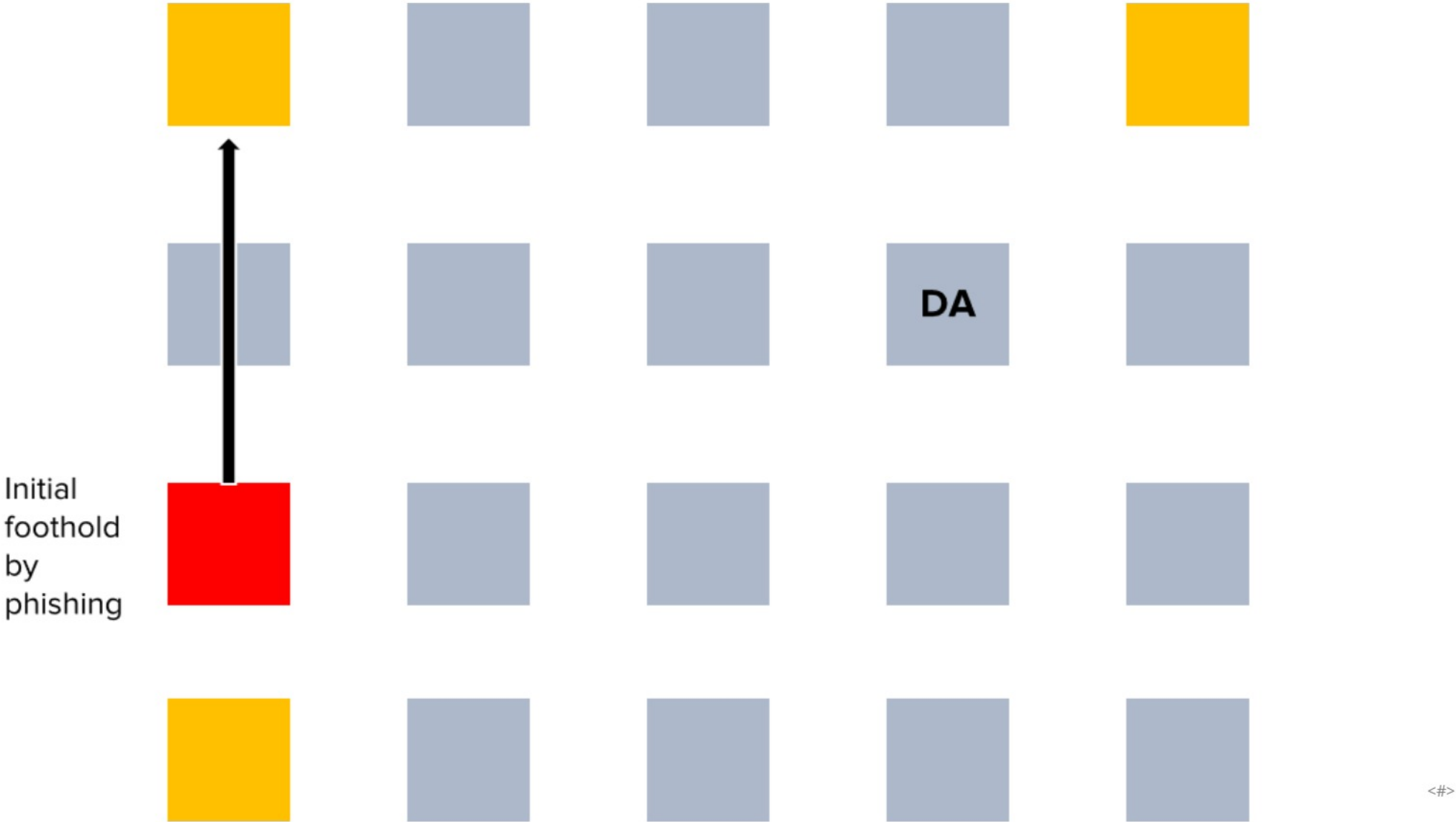
# How does an attacker move laterally?



# How does an attacker move laterally?

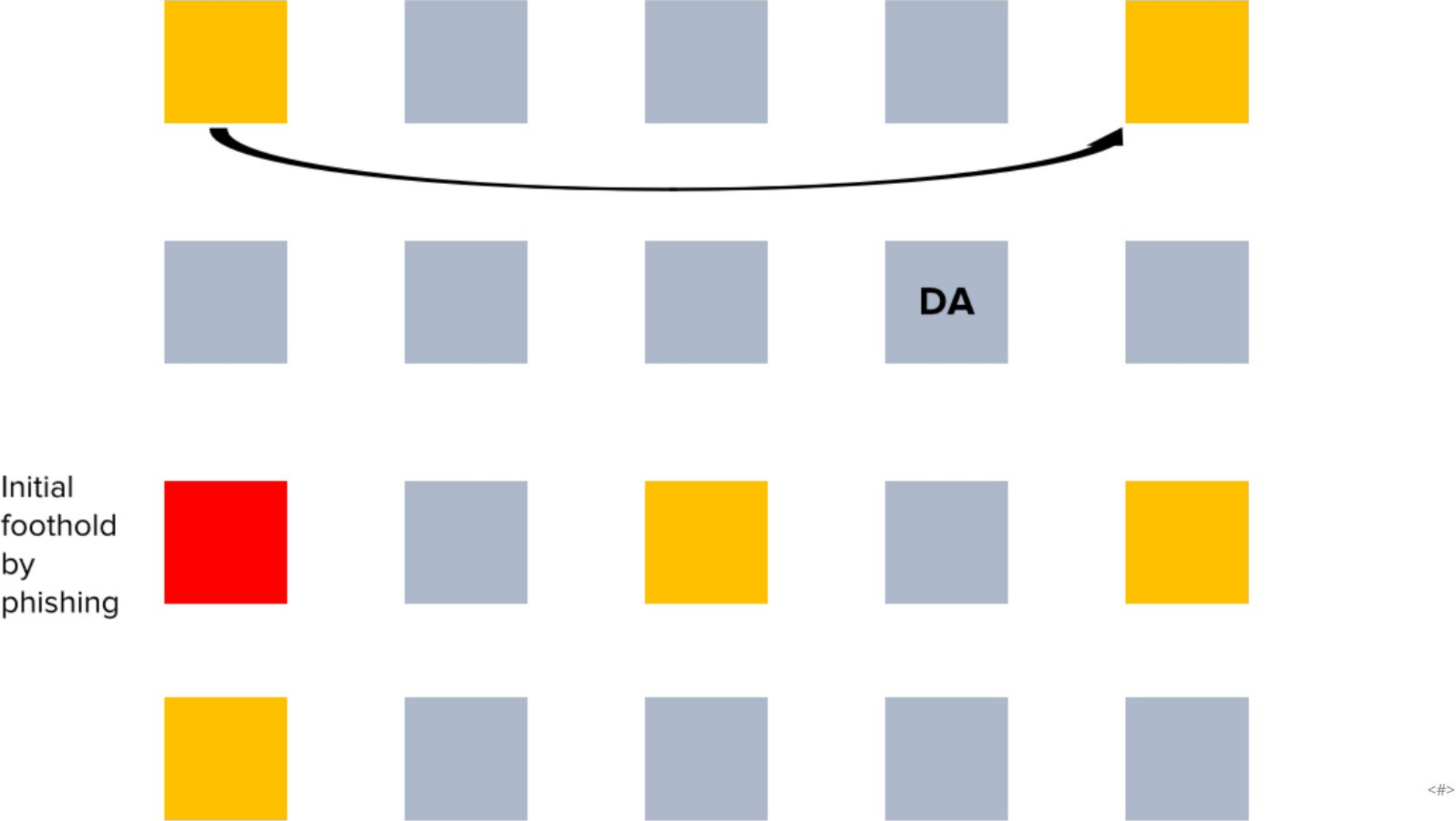


# How does an attacker move laterally?

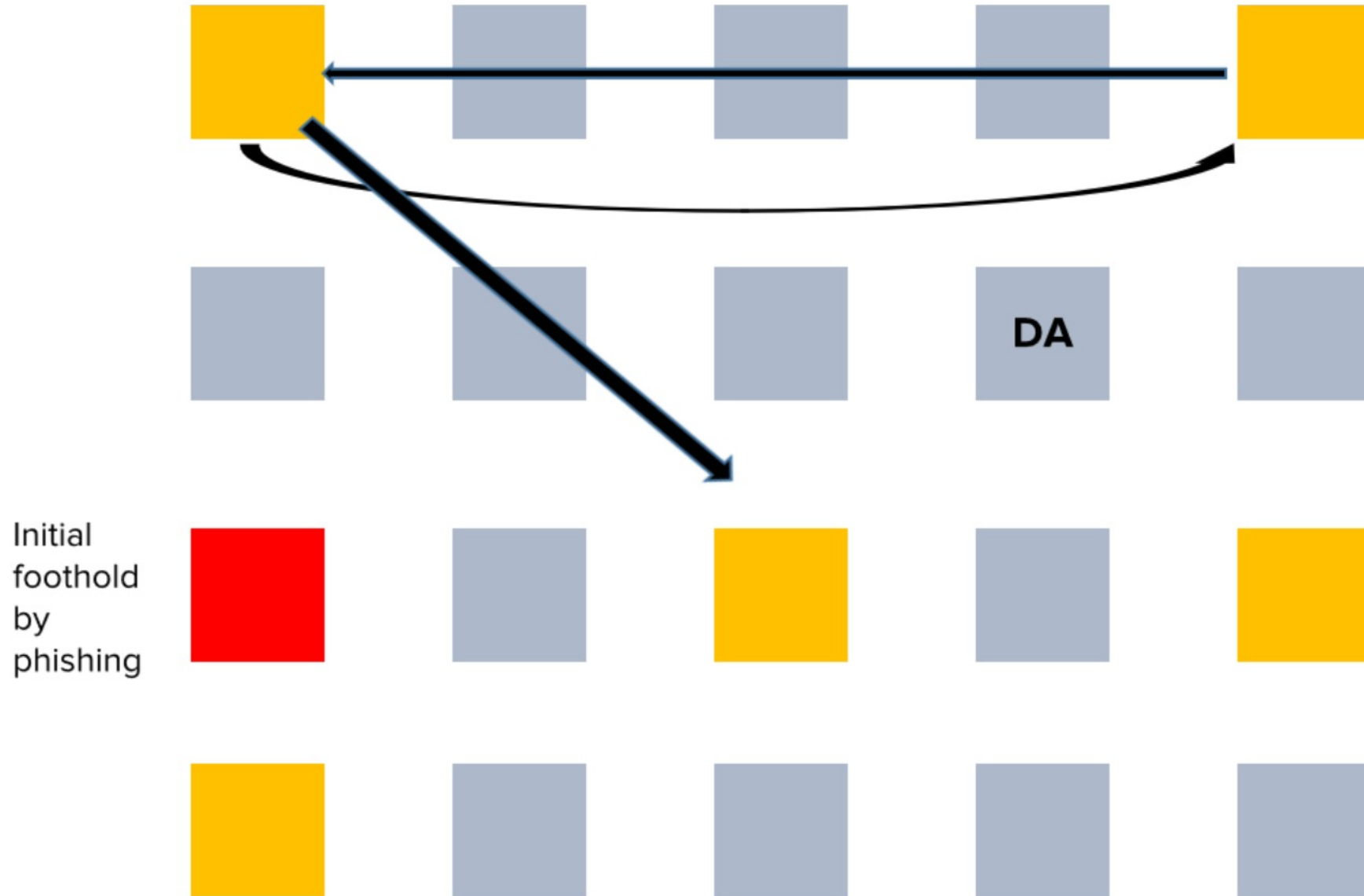




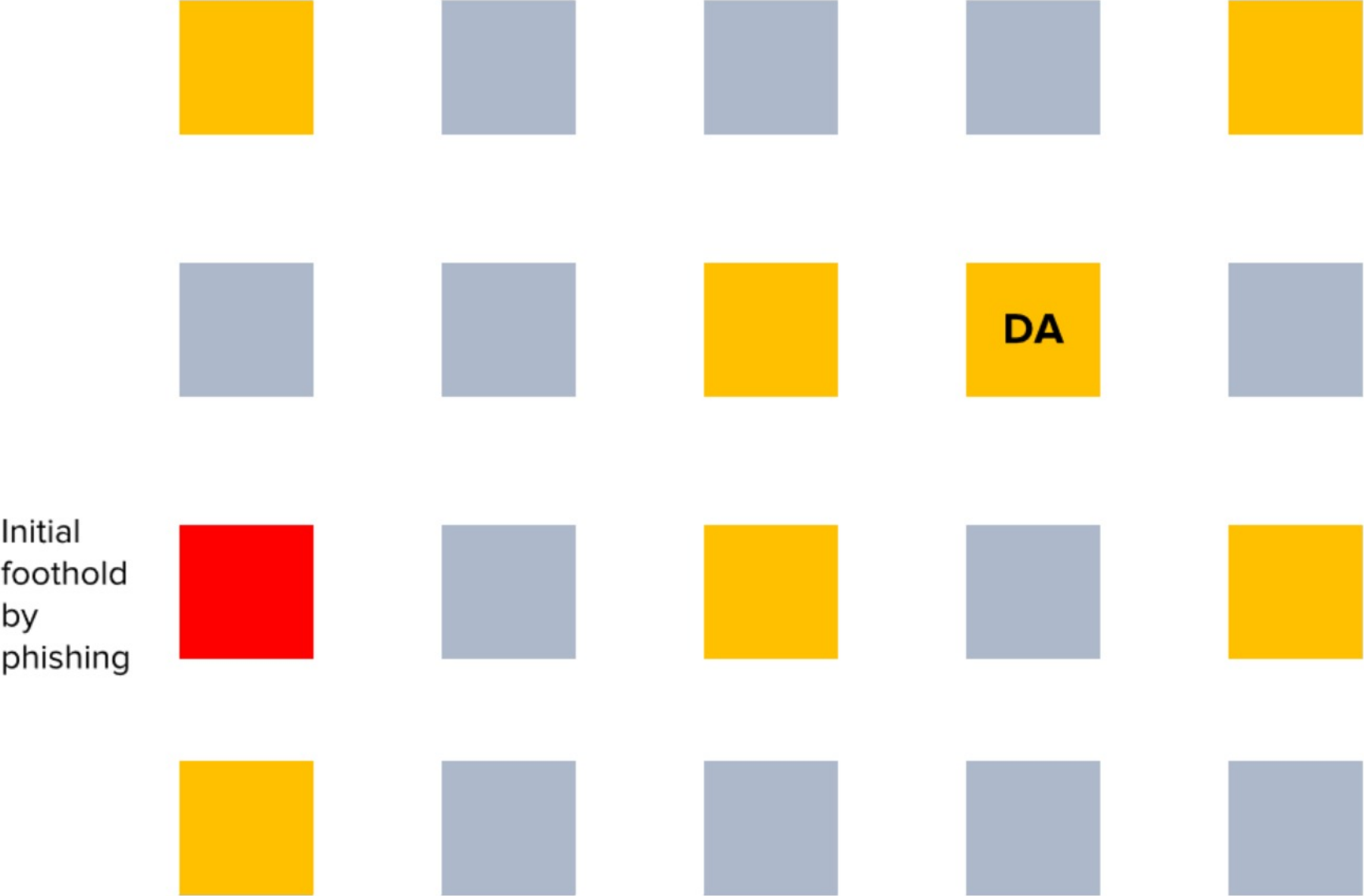
# How does an attacker move laterally?



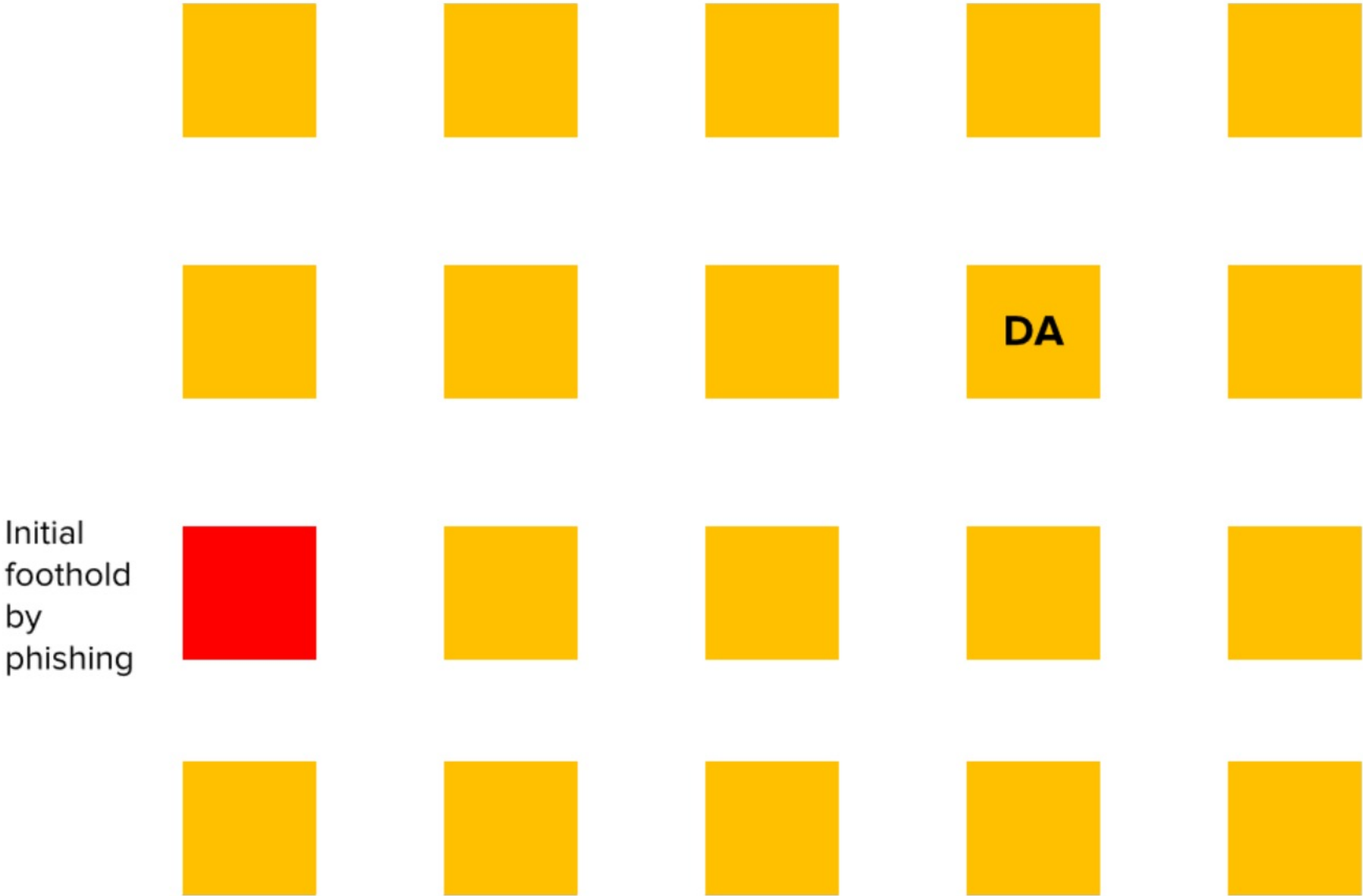
# How does an attacker move laterally?



# How does an attacker move laterally?



# How does an attacker move laterally?



# Detect lateral movements

**First Time Host Accessed by User** ⚡  
(From Sep 20, 2018 06:02:07 AM to Mar 19, 2019 06:02:07 AM)

Domain: admanagerplus.com

Period: Last 6 Months | Hours: All [Business Hours]

Export As | Add to | More

### First Time Host Accessed by User

COUNT

| User      | Count |
|-----------|-------|
| admanager | 3     |

Advanced Search

| URCE SSED TIME  | ACTIVITY TYPE                     | MESSAGE  |
|-----------------|-----------------------------------|--|
| 5,2019 02:01:51 | First Time -Host accessed by User | host:192.168.102.161 was accessed by user:admanager for the first time. Anomaly category:First Time -Host accessed by User |

1-3 of 3 | 25 | Add/Remove Columns


# Get user level granularity

The screenshot displays the Log360 UEBA interface, specifically the 'User Identity Mapping' section. The top navigation bar includes 'Home', 'Reports', 'Settings', and 'Support'. The left sidebar lists various settings categories, with 'User Identity Mapping' selected. The main content area shows a table of user profiles with the following columns: Actions, Name, Domain Name, Email, Anomalies, Unrelated Events, and Configure. The table contains 12 rows of user data.

| Actions                  | Name       | Domain Name   | Email          | Anomalies | Unrelated Events | Configure |
|--------------------------|------------|---------------|----------------|-----------|------------------|-----------|
| <input type="checkbox"/> | Alex       | msc.com       | alex@mail.com  | 20        | 02               | Configure |
| <input type="checkbox"/> | Edwin      | zoho.com      | edwin@mail.com | 10        | 04               | Configure |
| <input type="checkbox"/> | John Peter | csze.zohoc.om | john@mail.com  | 14        | 05               | Configure |
| <input type="checkbox"/> | Johnson    | msc.com       | edwin@mail.com | 15        | 03               | Configure |
| <input type="checkbox"/> | Alex Edwin | zoho.com      | peter@mail.com | -         | 02               | Configure |
| <input type="checkbox"/> | Peterson   | csze.zohoc.om | john@mail.com  | 2         | 03               | Configure |
| <input type="checkbox"/> | Alex       | msc.com       | alex@mail.com  | 20        | 01               | Configure |
| <input type="checkbox"/> | Edwin      | zoho.com      | edwin@mail.com | 10        | -                | Configure |
| <input type="checkbox"/> | John Peter | csze.zohoc.om | john@mail.com  | 14        | -                | Configure |
| <input type="checkbox"/> | Johnson    | msc.com       | edwin@mail.com | 15        | 08               | Configure |
| <input type="checkbox"/> | Alex Edwin | zoho.com      | peter@mail.com | -         | 02               | Configure |
| <input type="checkbox"/> | Peterson   | csze.zohoc.om | john@mail.com  | 2         | 03               | Configure |

# Context to breadcrumbs

### User Details



**John Peter**  
johnson\_peter@microsoft.com

Anomaly Count **20**

- [AD Info](#)
- [Verified Identifiers](#)
- [Last Session](#)

#### Latest Events

- 11:00 PM - Windows Logon
- 10:50 PM - File Copy
- 10:48 PM - Firewall Rule Added
- 10:45 PM - File System Updated
- 10:23 PM - Windows Corrupted
- 10:03 PM - Network Breach

Windows **75** | Unix | Firewall | File Server **02** | Network Devices **02**

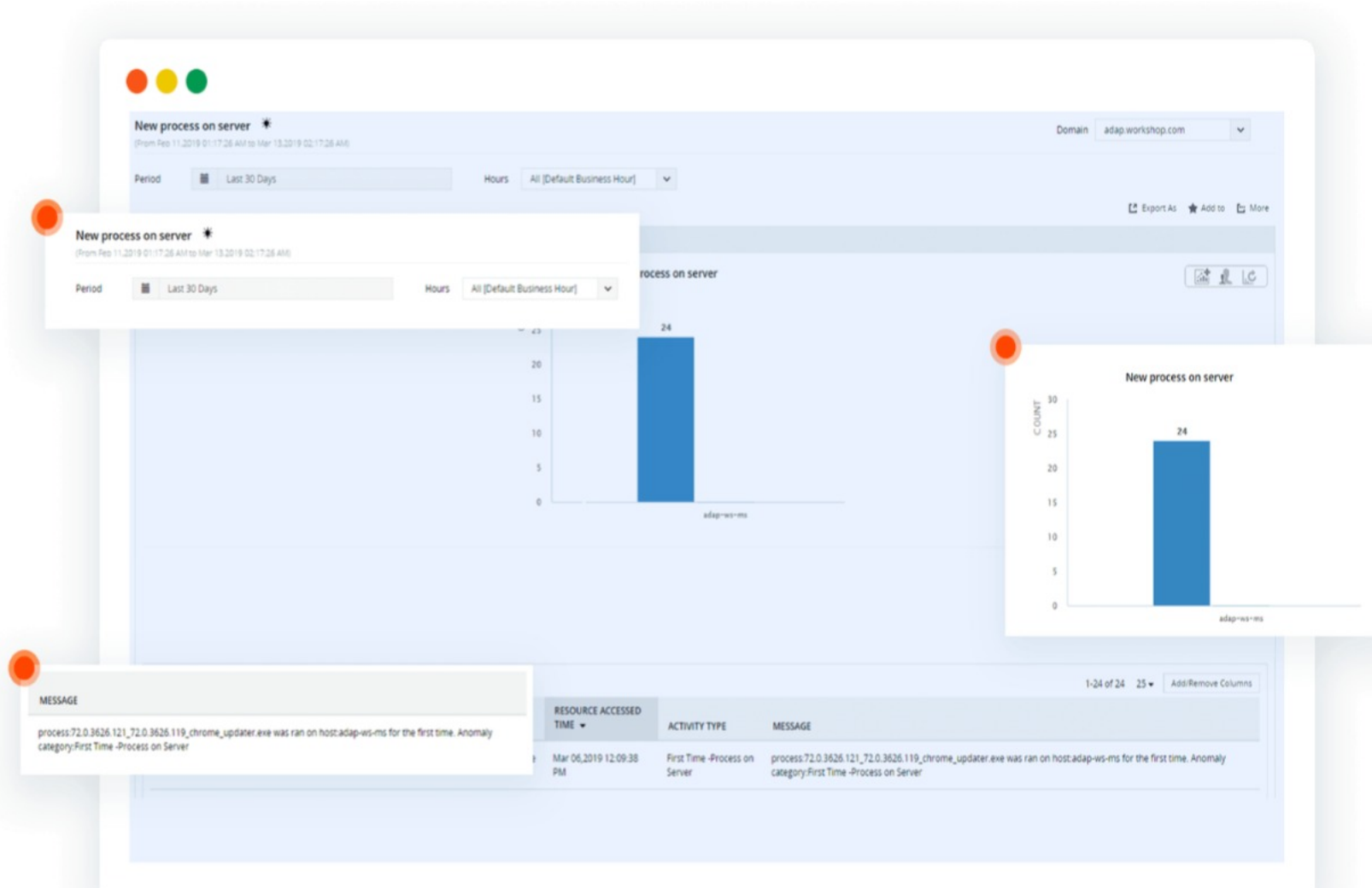
### Identifiers [+ Add Ident](#)

- Verified : ( (username=abc & devicename=device123) & (targetuser=user1) )
- Not Verified : ( (username=edwinalex & devicename=Alex123) & (targetuser=alexedwin-2190) )

### Windows Un-Mapped Identifiers ▾

| Time                  | Anomalies Details     | Correlation Details                      | Feedback   |
|-----------------------|-----------------------|--|--|
| 25 Jun 2018 06:38 PM  | Johnson@mydomain.com  | Identifier : alex@mail.com               | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| 07 Sep 2017, 14:50:05 | Johny@mydomain.com    | Identifier : edwin@mail.com              | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| 25 Jun 2018 06:38 PM  | Peterson@mydomain.com | Identifier : john@mail.com               | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| 07 Sep 2017, 14:50:05 | Peterson@mydomain.com | Identifier : Host - 192.168.1.1, Mess... | <input checked="" type="checkbox"/> <input type="checkbox"/> |

# Thwart malware attacks







## Logon activity

4624 (Successful logon)

4625 (Failed logon)



## Group membership changes

4728 (Member added to securityenabled global group)

4732 (Member added to securityenabled local group)

4756 (Member added to securityenabled universal group)



## Account lockouts

4740 (A user account was locked out)



## Object and file access

4663 (An attempt was made to access an object)



## Event log clearance

1102 (The audit log was cleared)

**Key AD  
events to  
audit in  
your  
network**

# Tips and tricks to prevent insider threats

- + Process and correlate logs across your network
- + Establish a dynamic, user-based activity baseline
- + Identify anomalies and alert admins
- + Monitor privilege escalations
- + Automate incident response

# Automating incident response

- + Cut down on response time with real-time notifications via email or SMS.
- + Reduce alert fatigue by defining triggers based on volume, time, user, and other criteria.
- + Execute automated scripts to perform a predetermined response to an alert.



**45%**  
of  
ransomware  
attacks target  
the healthcare  
industry

# What you should do

- Shut down infected systems immediately.
- Disable all shared drives that hold critical information.
- Disconnect and isolate infected systems from the network.

# If something does happen...

Recovery point is crucial, i.e. **Backup is crucial**

## **Things to consider while backing up:**

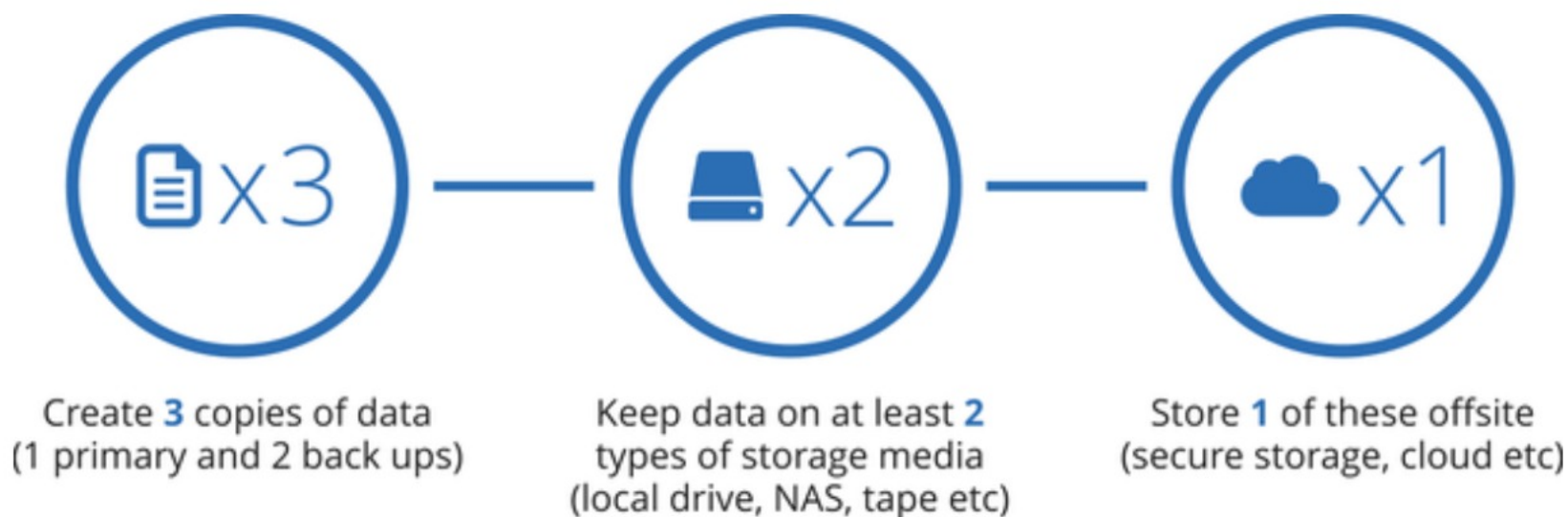
**Incremental backup:** Incrementally back up each change made to an objects' attributes as a separate version.

**Backup retention:** Define a retention period for your backups, and automatically discard the oldest full backup and its associated incremental backups when the limit is reached.

**AD roll back:** Roll back AD to a previous backup point, and undo all changes made to objects after that point in time.

# 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.

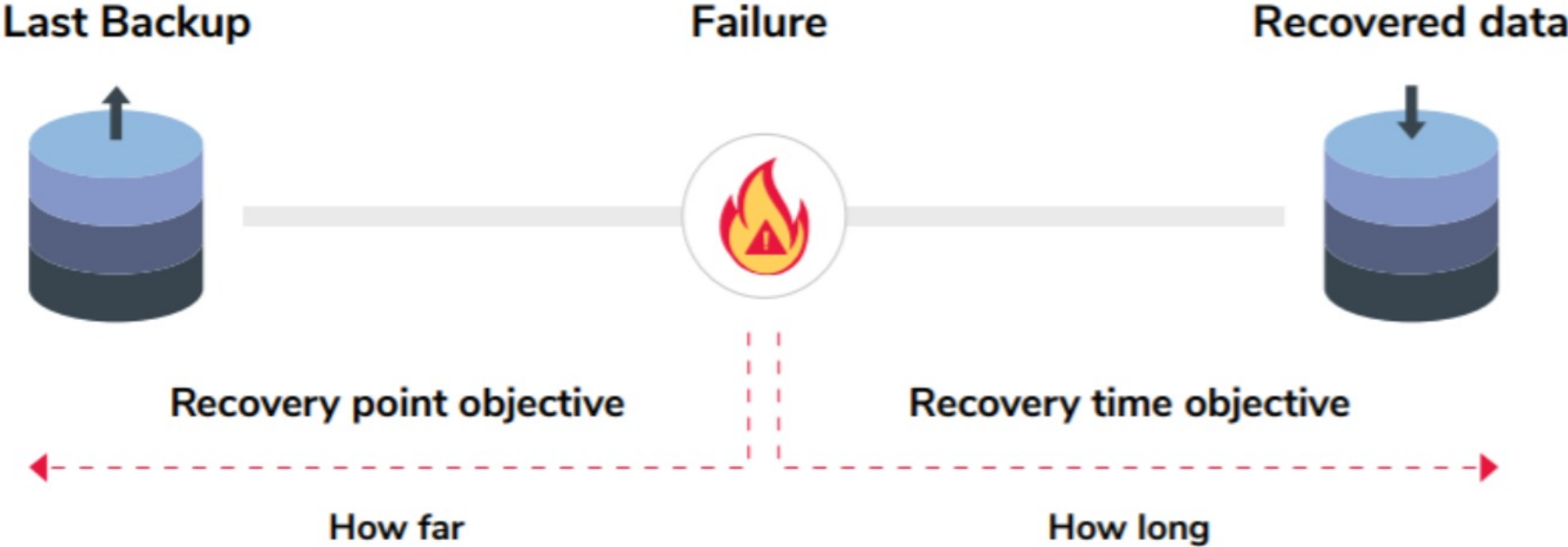


# RTO and RPO

- Recovery time objective is the maximum amount of time business operations can be down after an outage. For critical systems and data, it is advisable to have a low RTO.
- Recovery point objective is the amount of data that an organization can afford to lose in the event of a disaster. The RPO is essential to determine the minimum backup frequency required by the organization.



# How RPO and RTO's are related



**If you've come so far, congratulations!  
You're already partly compliant with  
HIPAA regulations!**

# Key HIPAA Requirements

- ❑ **Sec 164.308 (a) (1) (ii) (D):** Object access
- ❑ **Sec 164.308 (a) (5) (ii) (C) & Sec 164.308 (a) (6) (ii):** Logon & logoff monitoring
- ❑ **Sec 164.308 (a) (7) (i):** System events
- ❑ **Sec 164.308 (a) (3) (ii) (A) & Sec (a) (4) (ii) (B):** Account logon

# What you should monitor

## Object access:

- Track access to the given object (file or folder) that has confidential information.
- Identify the type of operation performed on the object (read, write, delete, or modify).
- Single out the user who accessed or performed operations on the object.
- Know whether the operation or access was successful.

# What you should monitor

- **Logon & logoff monitoring:**
  - Successful logon and logoffs
  - Unsuccessful user logons
  - Terminal service sessions
- **System events:**
  - Local system processes such as the system startup, shutdown, or changes to the system time or audit log.
  - Review records of information system activity such as audit logs regularly.
- **Account logon:**
  - Successful/unsuccessful account validation

# What HIPAA says about password management

- × Enforce fine-grained password policies, and implement password requirements such as minimum password length, password complexity, and password expiration.
- × Prevent users from setting passwords that are dictionary words, using phrases that are blacklisted, or following easy-to-crack patterns.
- × Administer granular password policies for OUs and groups, and implement a stringent password policy for privileged users who have access to PHI.
- × Enforce MFA and use different sets of authentication techniques for different users based on domain, OU, and group memberships.

# Password Policy Strengthener



## Password Policy Enforcer

Ensure end users choose strong passwords by enforcing custom strong password policies.

Select the Policy :

### Enforce Custom Password Policy

Minimum password length

Maximum password length

Number of special characters to include

Must contain both upper and lowercase letters.

Number of numeric characters to include

Password must begin with a letter.

Must contain at least one unicode character. [?](#)

Disallow palindrome passwords.

Disallow use of a character more than 2 times consecutively.

Disallow use of 5 consecutive characters from username.

Disallow use of 5 consecutive characters from old password. [?](#)

Disallow the use of dictionary words. [Choose Dictionary](#) [?](#)

Disallow the use of these patterns. [Modify Patterns](#)

Number of old passwords to be restricted during password reset

Override all complexity rules if password length is at least . [?](#)

Password must satisfy at least  of the above complexity requirements. [?](#)

Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent. [Learn more](#)

Show this policy requirement in Reset and Change Password pages. [Customize View](#)

';--have i been pwned?

**Why is a 60-year old practice still alive?**

There is **no alternative** that can completely replace the password...yet.



\*\*\*\*\*



# Why passwords work better

- ❑ They can be encrypted
- ❑ They're cost efficient
- ❑ They don't require additional hardware
- ❑ If passwords are stolen, they can be modified
- ❑ Most importantly, **they are backwards compatible**

# Multi-factor authentication

Even if hackers obtain passwords, they cannot impersonate the user in second layer of authentication

The screenshot shows a web interface for configuring multi-factor authentication. At the top, there is a header "Multi-factor Authentication" with a help icon and a dropdown menu "How to make users enroll?". Below this is a "Choose the Policy" section with a dropdown menu showing "csez.zohocorpin.com". The main content area is divided into three tabs: "Configuration", "Authenticator Settings", and "Advanced". The "Authenticator Settings" tab is active, displaying a list of authentication methods, each with a gear icon and a right-pointing arrow:

- Security Question & Answer
- Email Verification
- SMS Verification
- Google Authenticator
- Microsoft Authenticator
- Yubikey Authenticator
- Duo Security
- RSA SecurID
- RADIUS Authentication
- Push Notification Authentication
- Fingerprint Authentication
- QR Code Based Authentication

At the bottom of the page, there is a blue footer bar containing several links and contact information:

Get Quote | Extend Trial | Need Features | Report an Issue | Toll free : +1-844-245-1104 | Direct Phone : +1-408-916-9890



SSPCHILD\administrator

Password



[Reset Password / Unlock Account](#)

[Sign-in options](#)

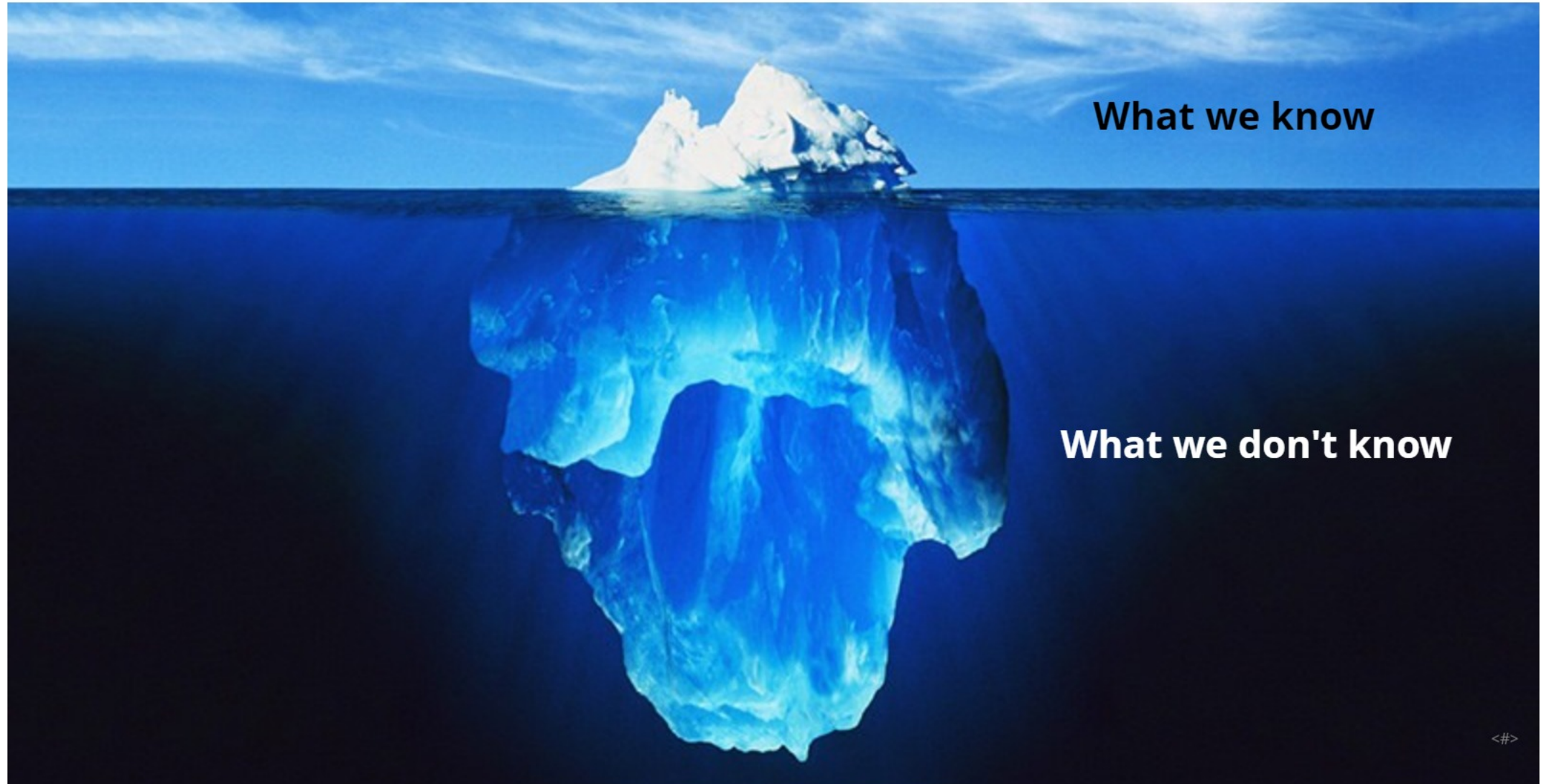


# Adaptive Authentication & Policy Enforcement solutions: What to look for?

Grant or block access attempts by identity or device and based on contextual factors such as user location, network address ranges, biometrics, device security and more.

1. Access to real-time threat data to identify potential security hazards
2. Analytics of the user's context, including their device, location, and network connection
3. Ability to have users enter extra authentication factors to prove their identities in risky scenarios
4. Configuration policies that allow admins to set up authentication procedures that are more secure than entering passwords

# Uncertain dynamic reality check



**Thank you.**  
**Write to me**

[jay@manageengine.com](mailto:jay@manageengine.com)

**ManageEngine**   
[www.manageengine.com](http://www.manageengine.com)