How to Combat Insider Threats in 2021

ManageEngine – RedmondMag CyberSec Series

JAY REDDY
CYBERSEC EVANGELIST

Distributed workforce still the trend in 2021 📡?

- Employees world over are working from home.
- IT admins have to manage remote users, speed up access requests and fulfillment, track remote worker's productivity, access patterns, user behavior, etc...
- Employees need self service capabilities so that work don't get stopped till their password reset/account unlock tickets are resolved.

Do you trust your users ?

- With increase in remote users, own devices, cloud adoption etc. the old method of granting access to requests originating from secure IP addresses is ineffective.
- Granting such implicit trust to any user weakens an organization's security posture by:
  - Not considering compromised devices
  - Ignoring compromised credentials
  - Not accounting the context of access request

1, 1, 2, 4, 8 . . .

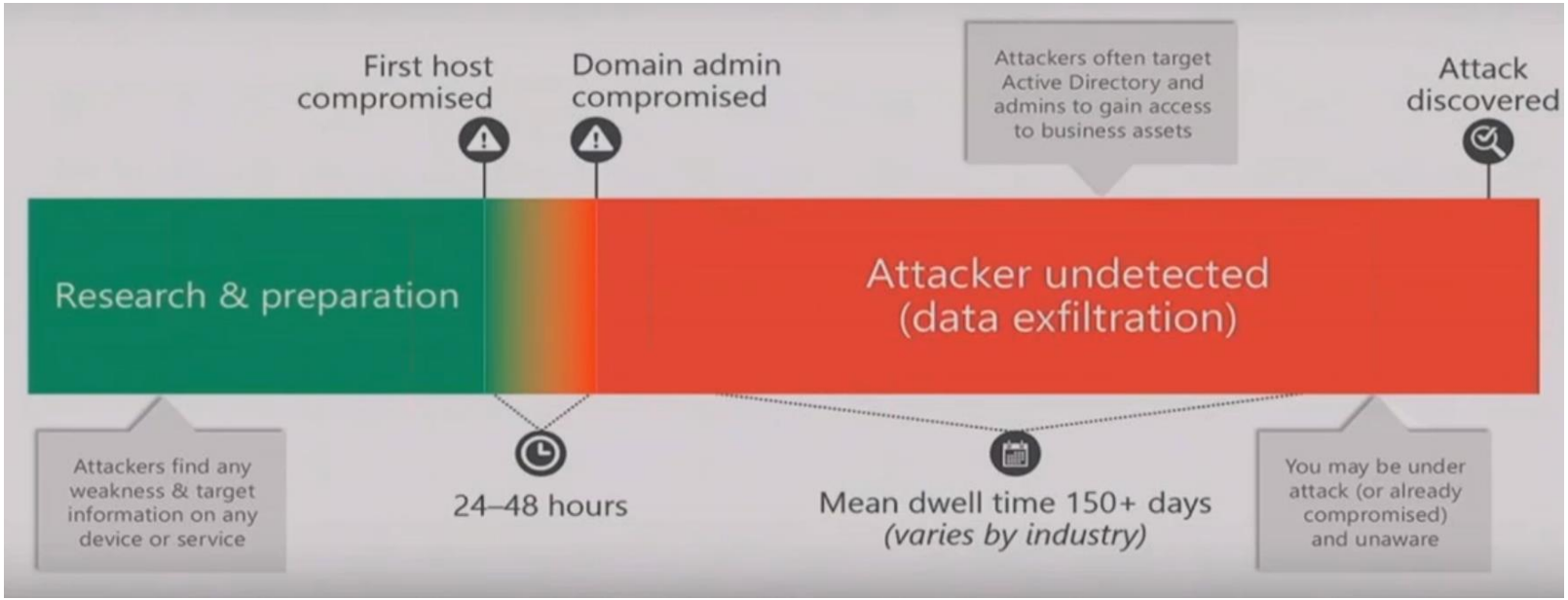
Behavior patterns

Security holes

Puzzles

What do attackers see ?

Attack timeline: According to Microsoft

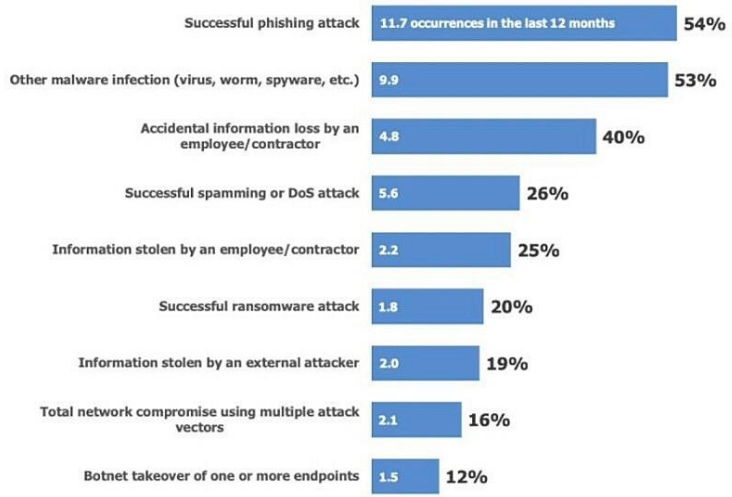


Source: blog.microsoft.com

68%

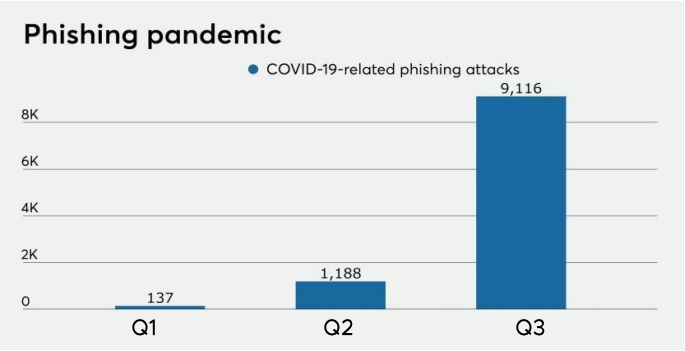
insider breaches
took months
or longer
to discover

Threats in the past few months and their frequency



Source: Osterman Research, Inc.

600% increase in malicious emails amid Covid-19 crisis: UN Official



Source: Barracuda Networks

70%
of breaches were caused by Insiders intentionally or unintentionally

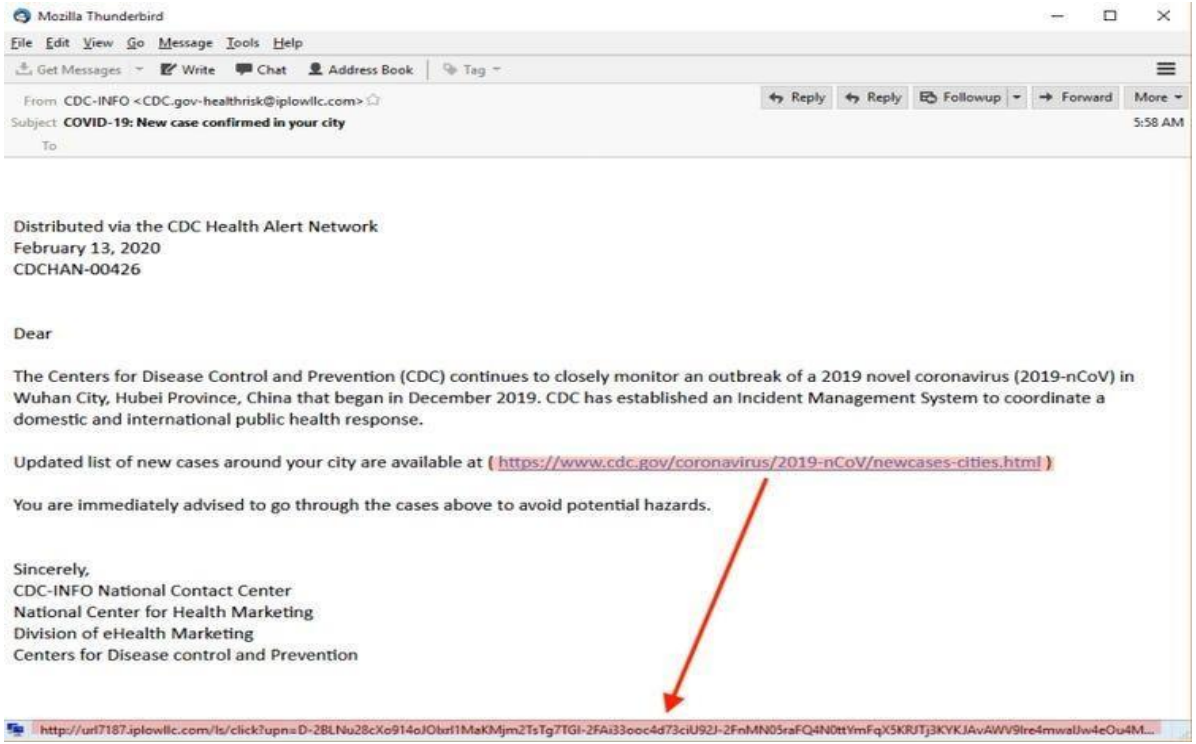
86%
of breaches were financially motivated.

43%
of breaches were attacks on web applications, more than double the results from last year.

27%
of malware incidents can be attributed to ransomware.

Verizon 2020 data breach investigations report

COVID-19 SCAM



Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

Reply | Reply | Followup | Forward | More

From CDC-INFO <CDC.gov-healthrisk@iplowllc.com>

Subject **COVID-19: New case confirmed in your city**

5:58 AM

To

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

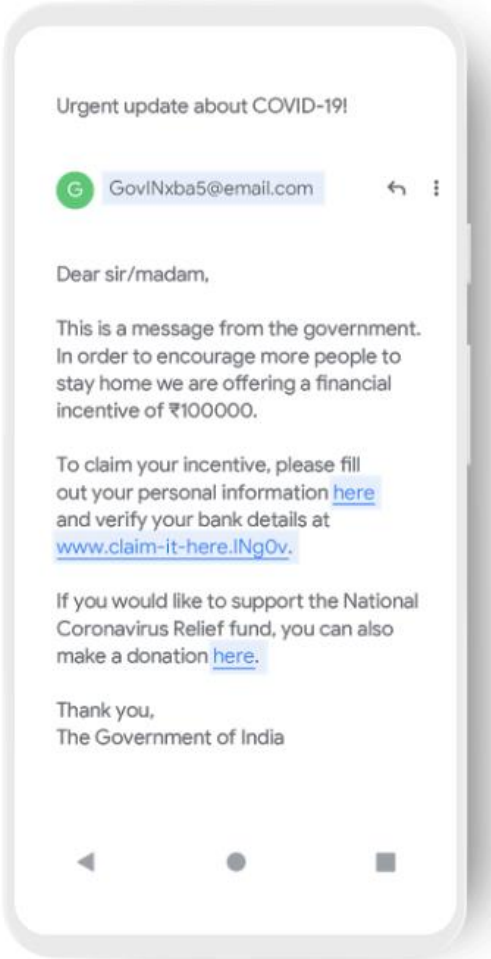
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

http://url7187.iplowllc.com/ls/click?upn=D-2BLNu28cXo914oJObxl1MaKMjmzTsTg7TGI-2FAi33ooc4d73ciU92J-2FnMN05raFQ4N0ttYmFqX5KRJTj3KYKJAvAWV9lre4mwaUw4eOu4M...



Urgent update about COVID-19!

GovINxba5@email.com

Dear sir/madam,

This is a message from the government. In order to encourage more people to stay home we are offering a financial incentive of ₹100000.

To claim your incentive, please fill out your personal information here and verify your bank details at www.claim-it-here.INgOv.

If you would like to support the National Coronavirus Relief fund, you can also make a donation here.

Thank you,
The Government of India

Let’s address the elephant in the room.

1. **Identifying weak spots.**
2. Detecting activity patterns that could lead to a breach.
3. Field notes.
4. Putting together a security strategy that can proactively secure your network
5. Compliance & CyberSec synergy

1. RISK ASSESSMENT: WHAT NEEDS TO BE PROTECTED?

To practice cybersecurity risk management, you can start with these steps:

1. Monitor and valuate assets
2. Identify your network risks
3. Document the impact to your business due to loss or damage of assets
4. Prioritize your mitigation activities accordingly

ASSETS TO MONITOR & VALUATE

- Extensive log monitoring to know exactly **what** happened **where**, **when**, **how**, and **why**.
- Factor in it all.
  - Workstations
  - Domain controllers
  - Databases
  - Cloud platforms
  - Network devices
  - Servers
  - IDS/IPS
  - Anything and everything

IDENTIFYING RISKS IN YOUR NETWORK

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

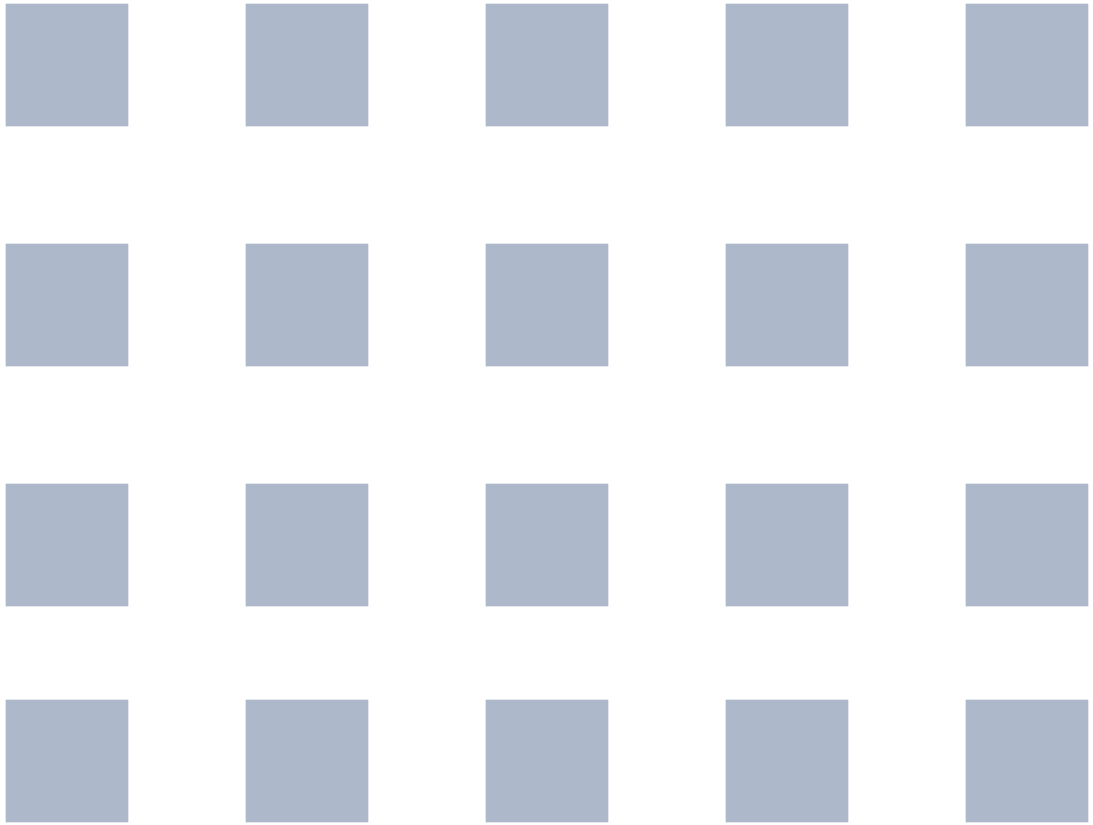
Building an Insider Threat Program for your Organization

1. Identifying weak spots.
2. **Detecting activity patterns that could lead to a breach.**
3. Field notes.
4. Putting together a security strategy that can proactively secure your network
5. Compliance & CyberSec synergy

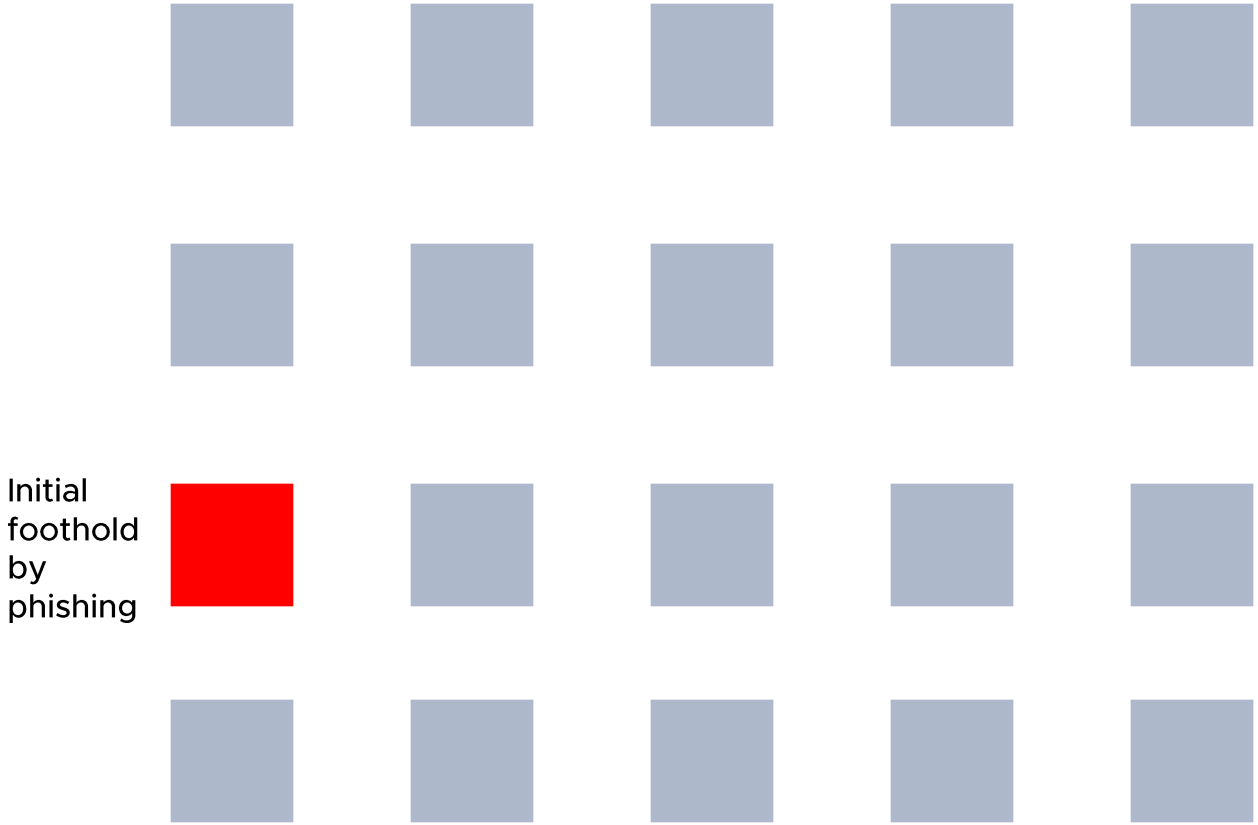
2. DETECTING ACTIVITY PATTERNS THAT COULD LEAD TO A BREACH.

- 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

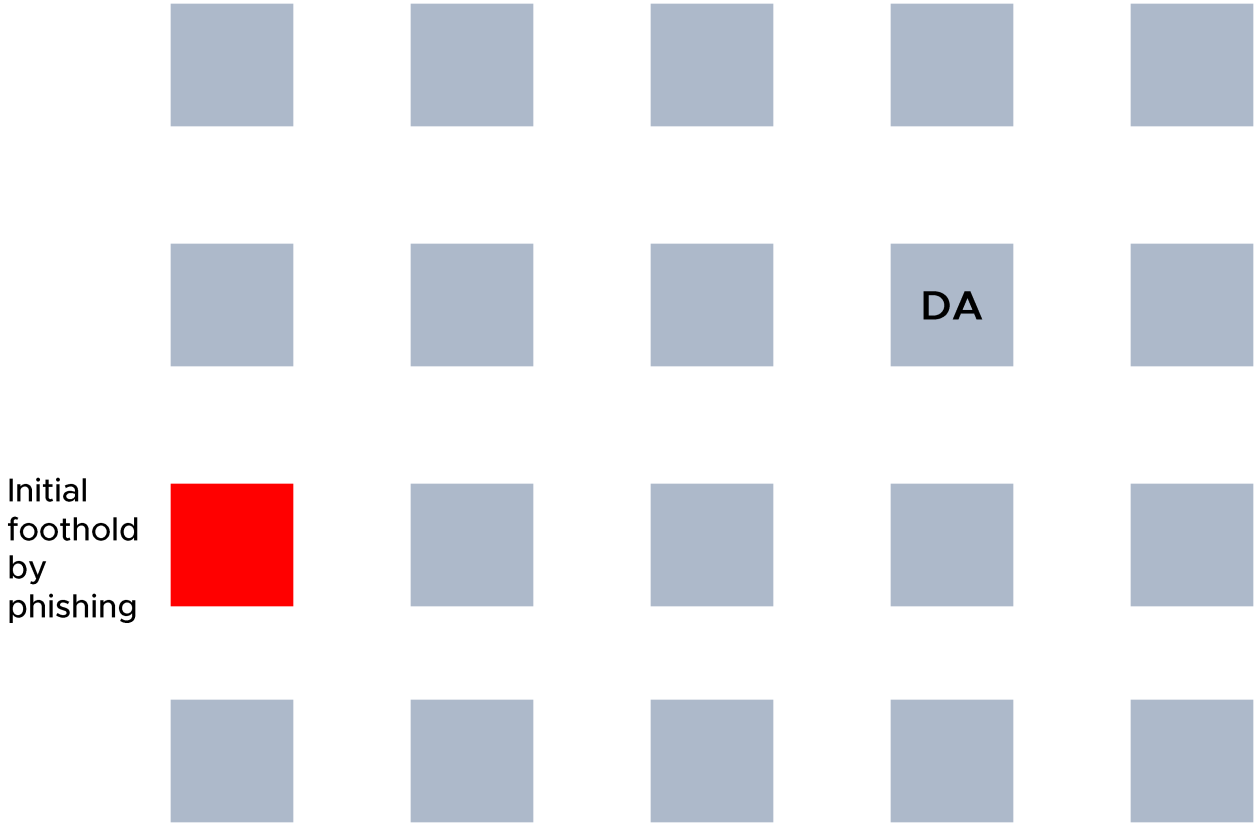
How does an attacker move laterally?



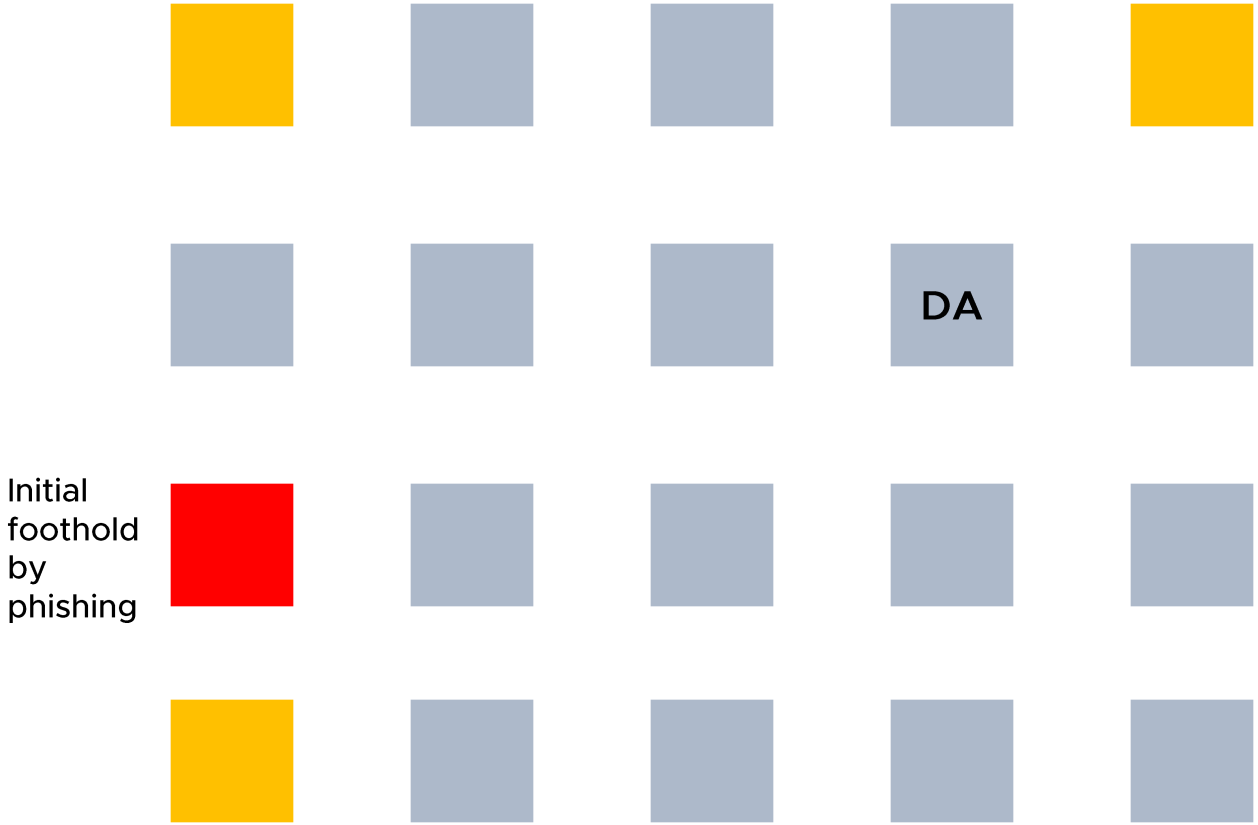
How does an attacker move laterally?



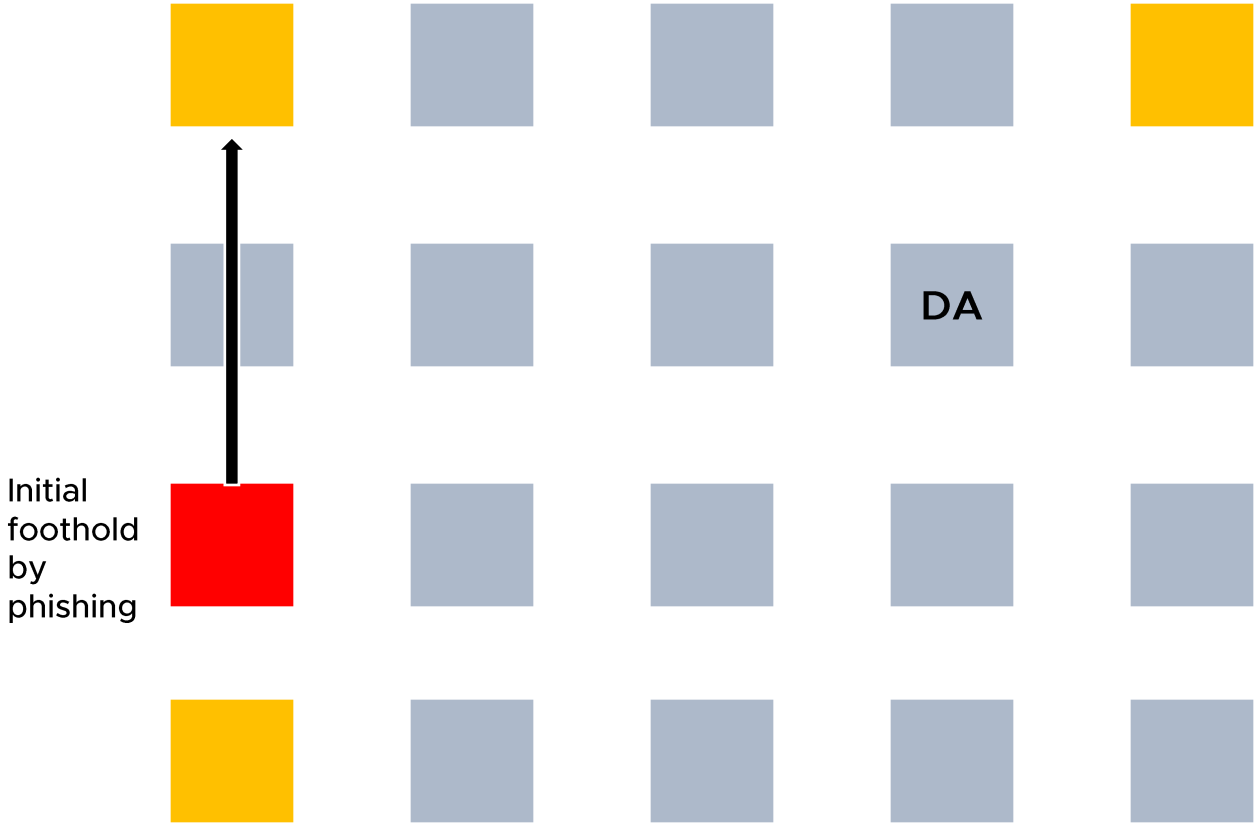
How does an attacker move laterally?



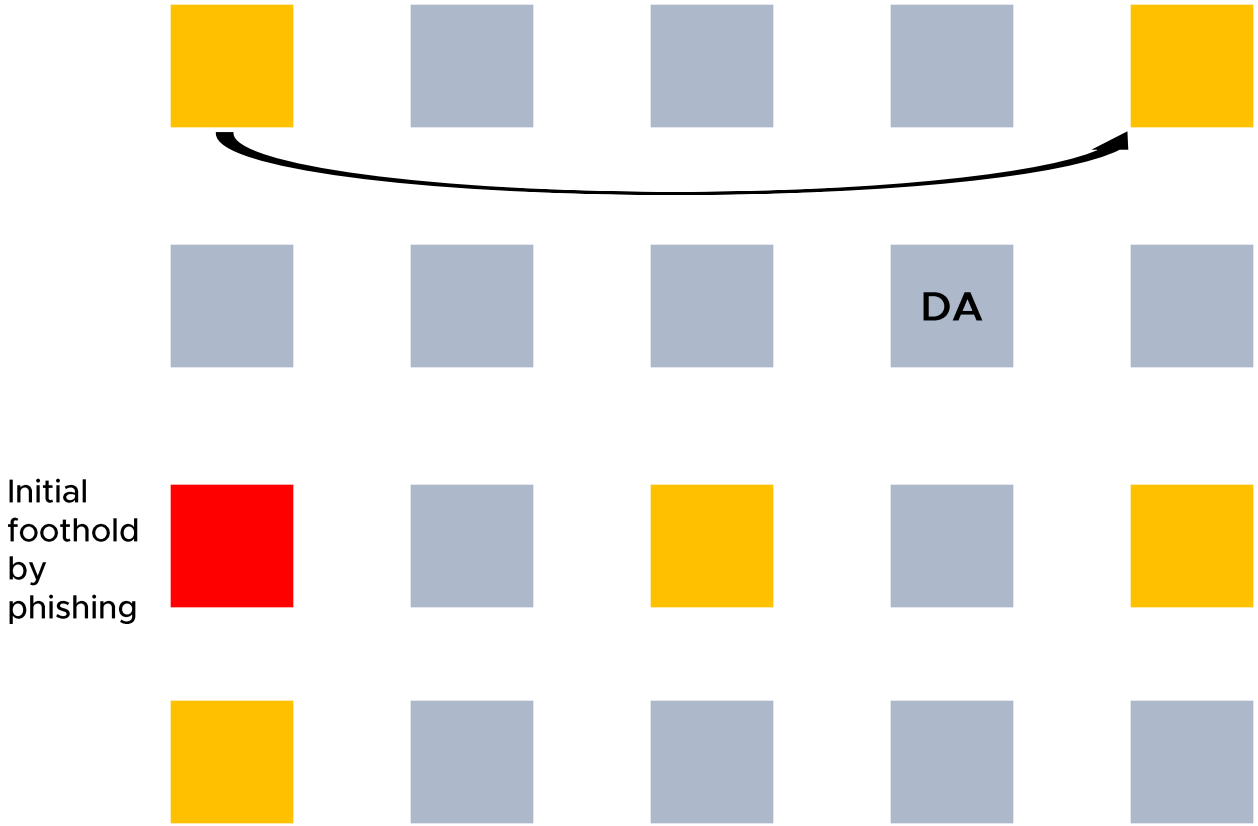
How does an attacker move laterally?



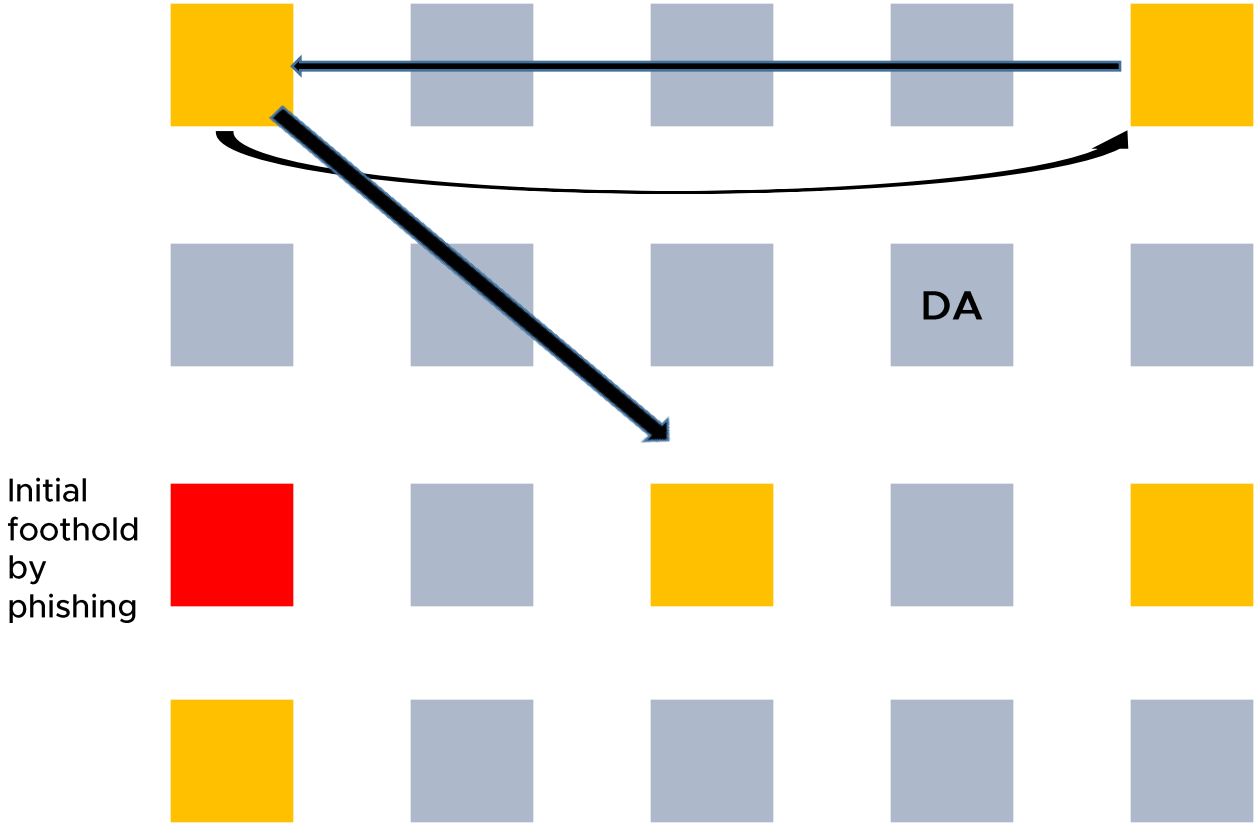
How does an attacker move laterally?



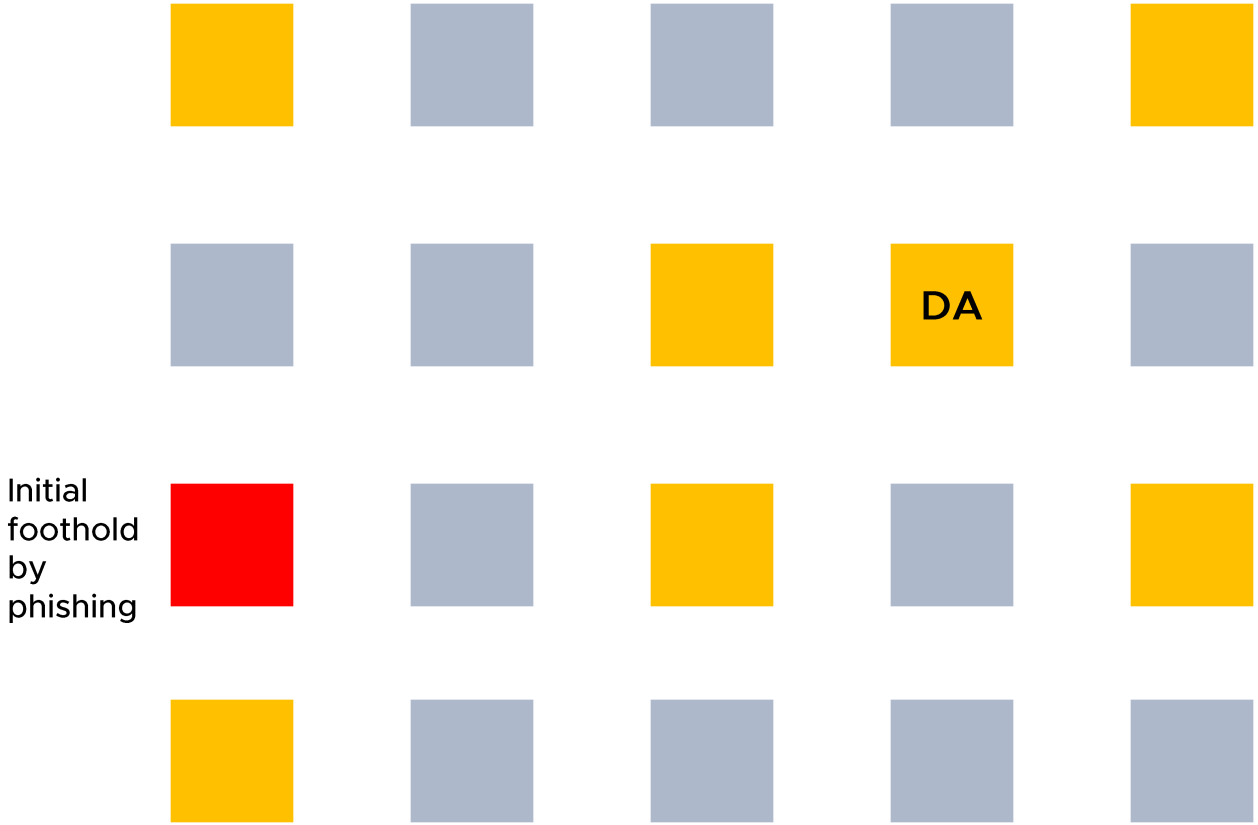
How does an attacker move laterally?



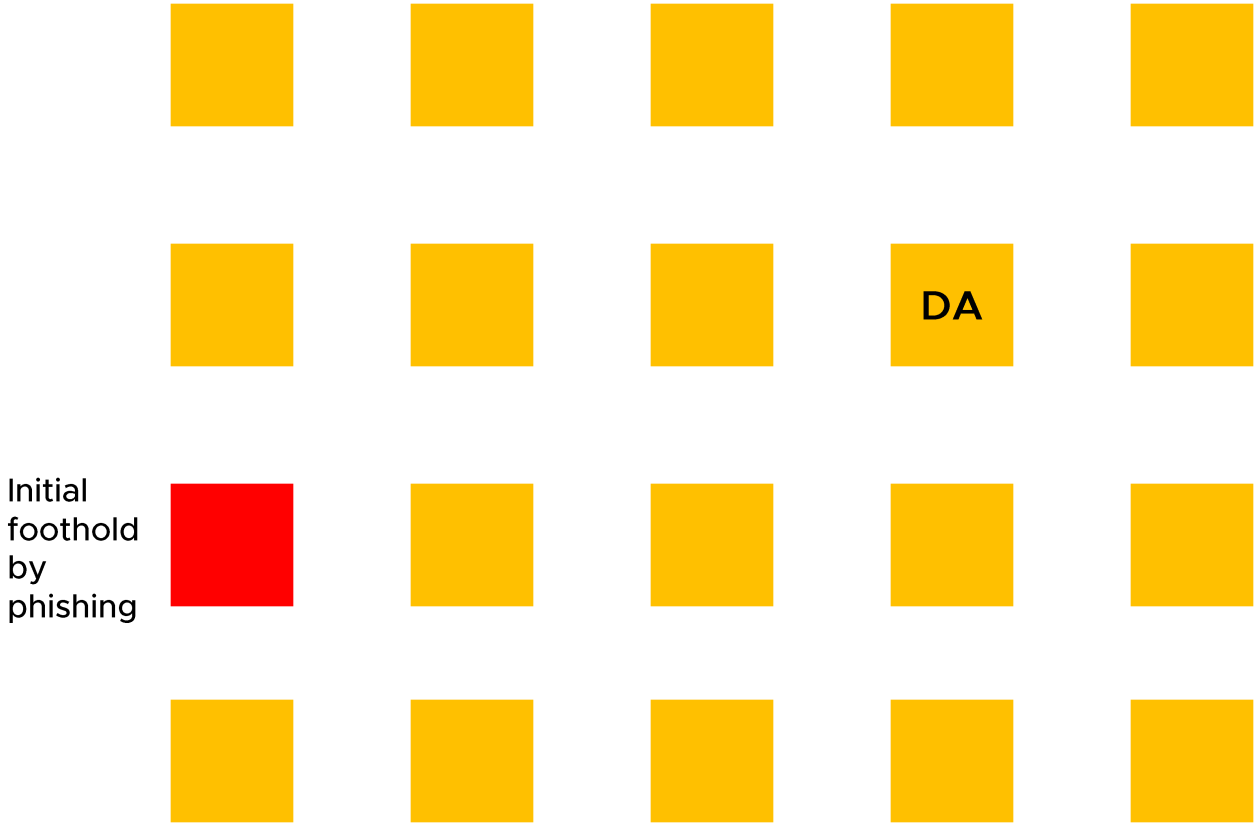
How does an attacker move laterally?



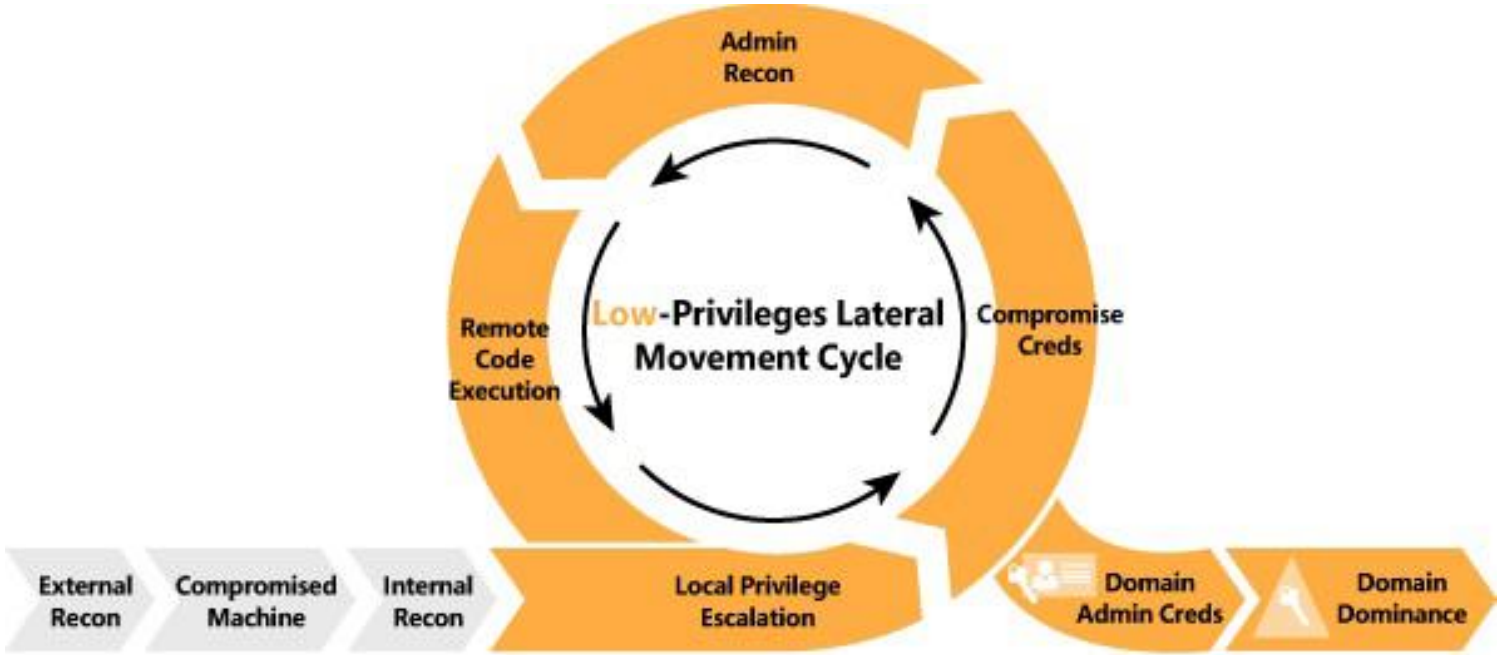
How does an attacker move laterally?



How does an attacker move laterally?



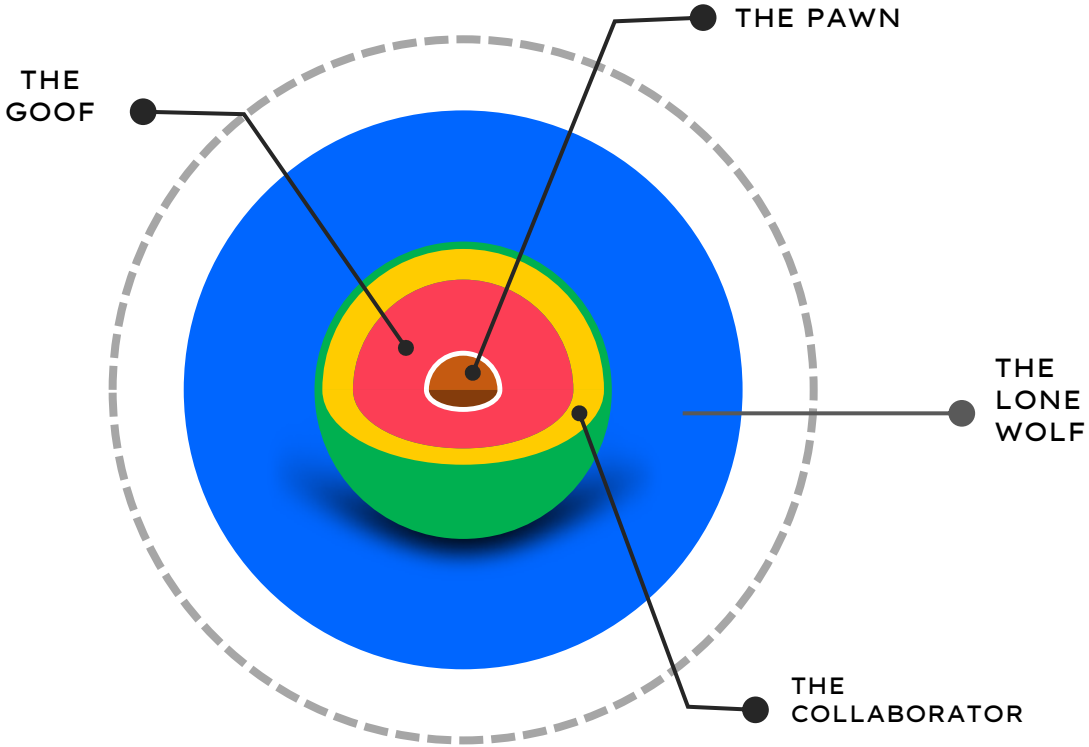
THE CYBER KILL CHAIN



Building an Insider Threat Program for your Organization

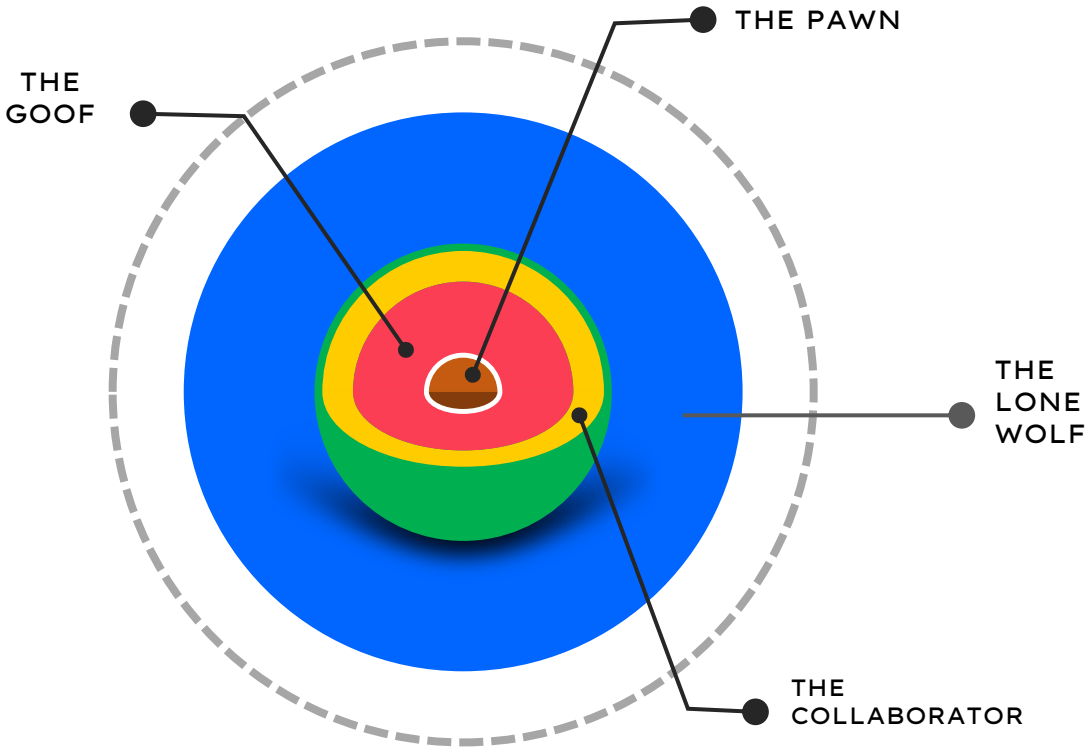
1. Identifying weak spots.
2. Detecting activity patterns that could lead to a breach.
3. **Field notes.**
4. Putting together a security strategy that can proactively secure your network
5. Compliance & CyberSec synergy

WHAT'S WRONG WITH THE CURRENT APPROACH?



Our networks are like M&M, with a hard crunchy outside and a chewy center.

ATTACKS IN 2020: Fewer Speed Bumps for Internal Bad Actors



shopify

Shopify data breach

amazon

Insider trading at Amazon

STRADIS HEALTHCARE

Stradis Healthcare attack

Twitter hack

TESLA

Attempted attack on Tesla

IDENTIFYING RISKS IN YOUR NETWORK

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

Building an Insider Threat Program for your Organization

1. Identifying weak spots.
2. Detecting activity patterns that could lead to a breach.
3. Field notes.
4. **Putting together a security strategy that can proactively secure your network**
5. Compliance & CyberSec synergy

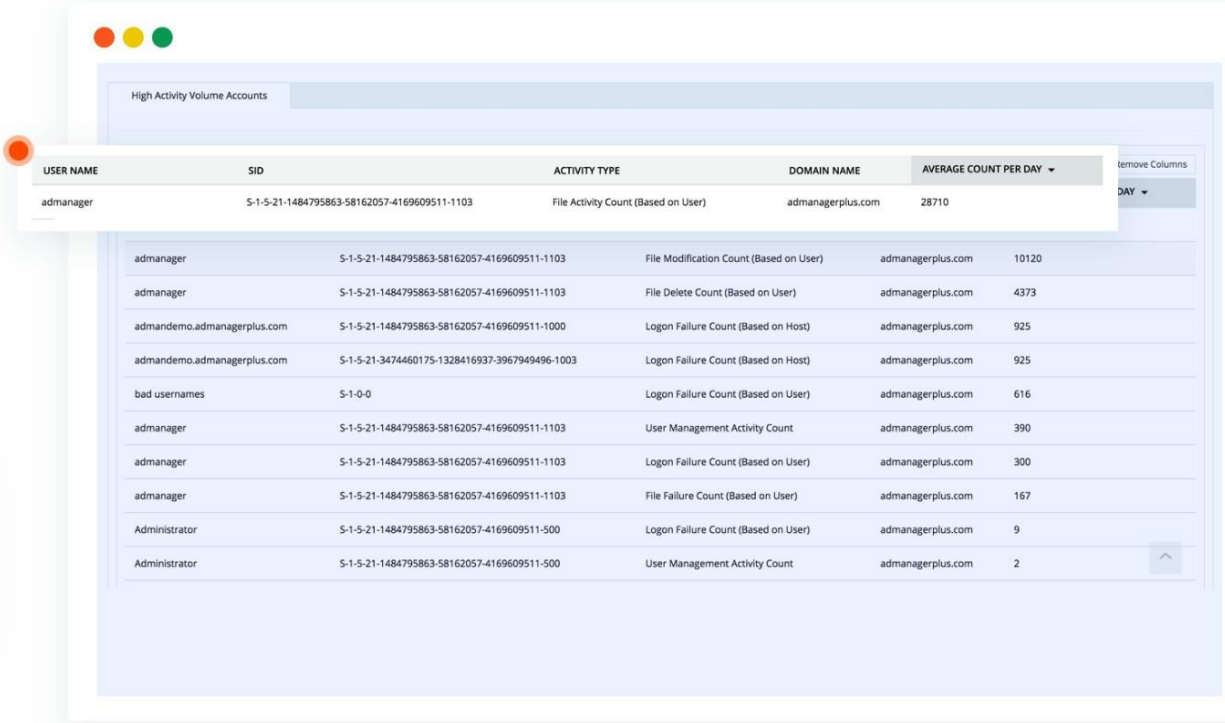
4. User behavior analytics (UBA)

- Applying machine learning to create a baseline of normal behavior specific to each user and alerts about deviations from this norm.

Type of alerts

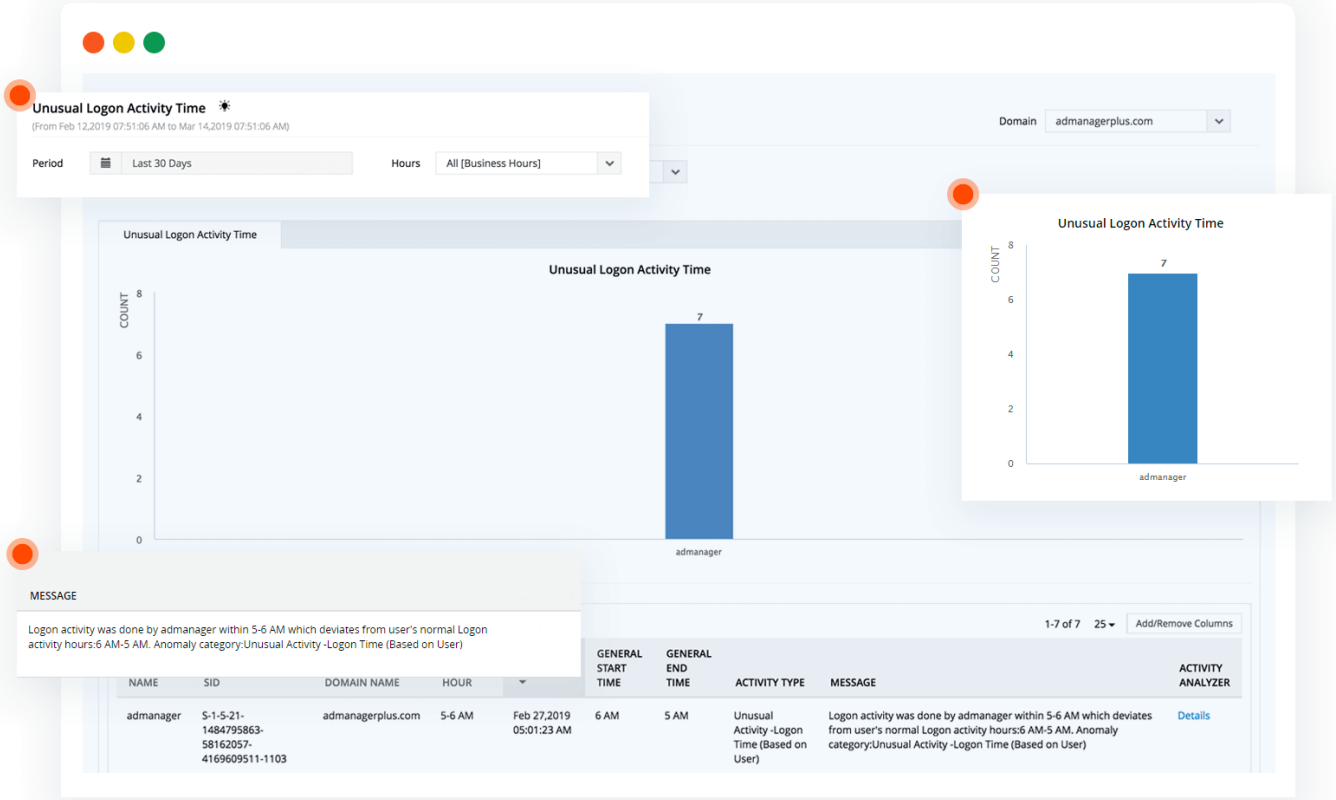
- **Unusual Count:** If a user's activity or file activity count exceeds a dynamic threshold.
- **Unusual Time:** Any activity occurs after the calculated normal activity hours.
- **New resource access:** If a new resource was accessed. E.g., a new user access on a computer, new remote to a server from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

INVESTIGATE ANOMALIES



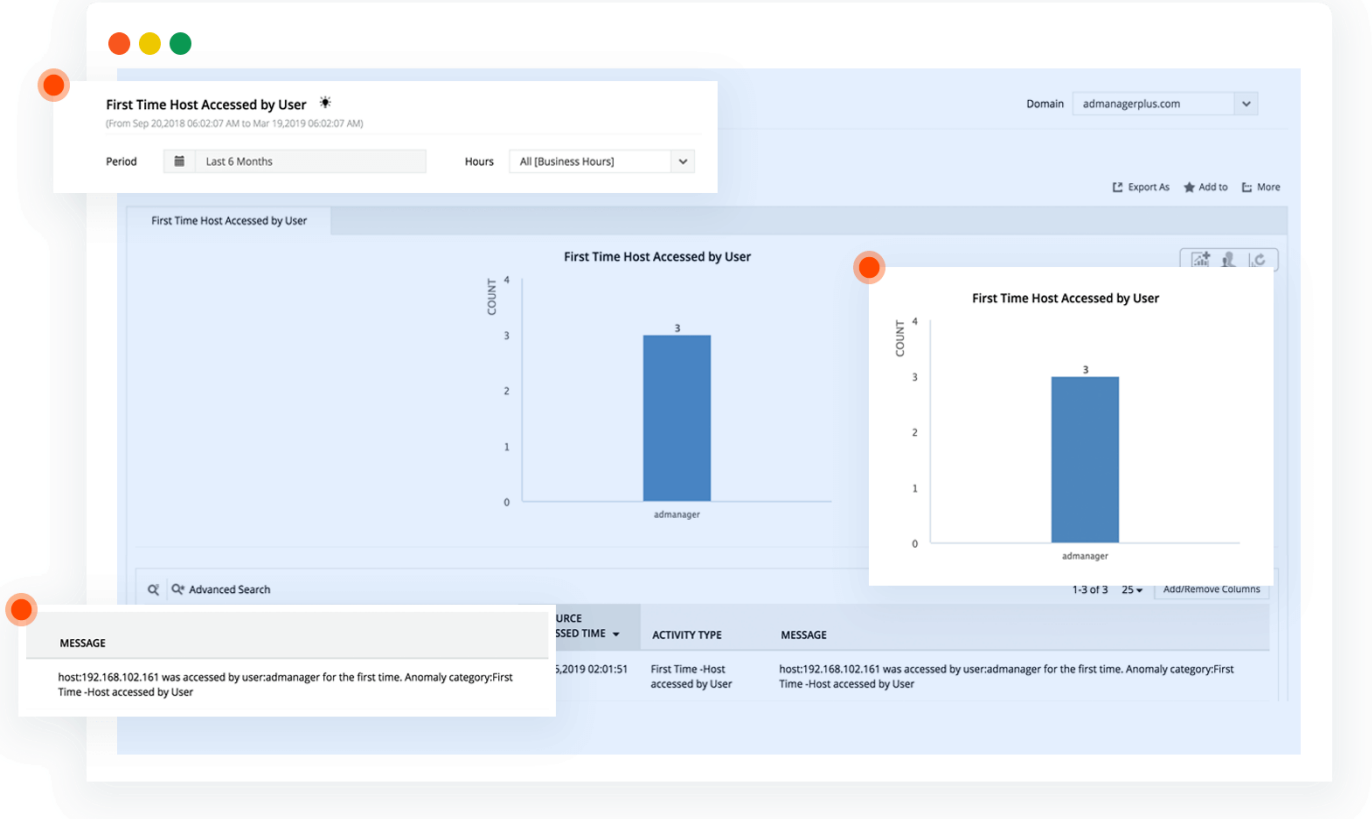
See who did what, when, and where, along with other details surrounding each anomaly.

UNUSUAL LOGON ACTIVITY



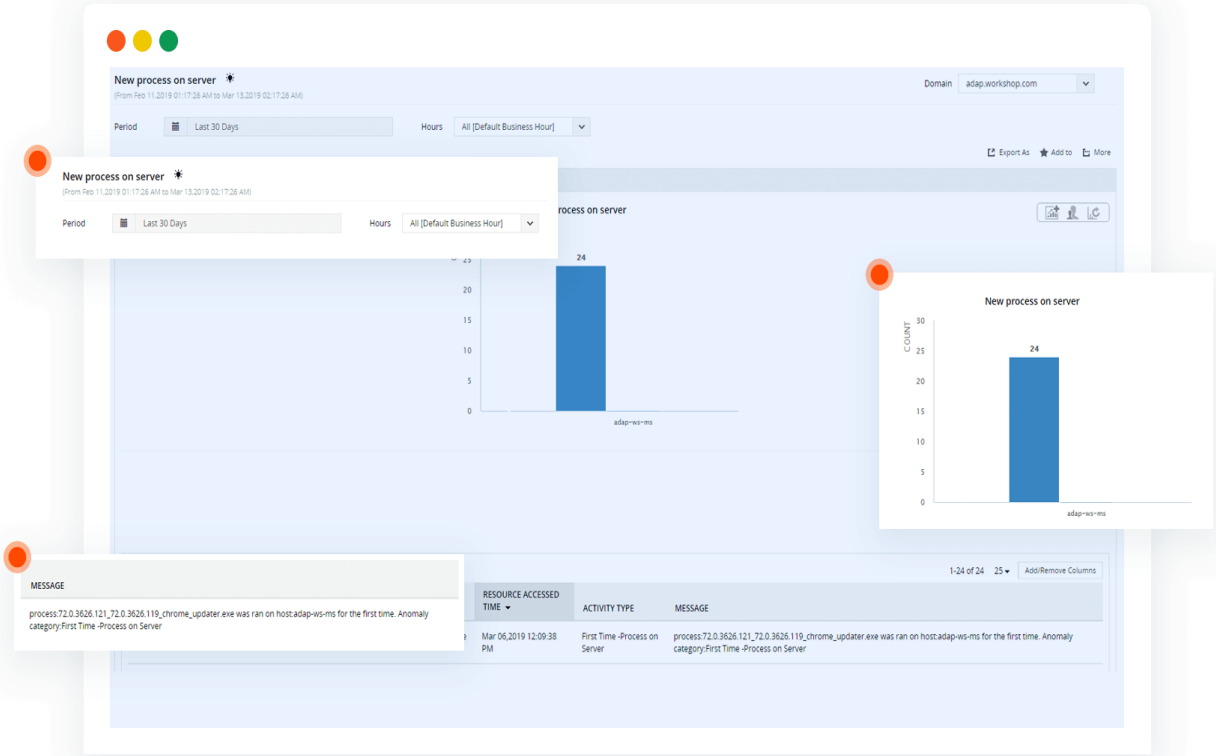
This critical data in the event of an unauthorized entry or regular monitoring is at the utmost ease to view with detailed reporting which helps prevent further wrong doing at the earliest.

DETECT LATERAL MOVEMENTS



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.

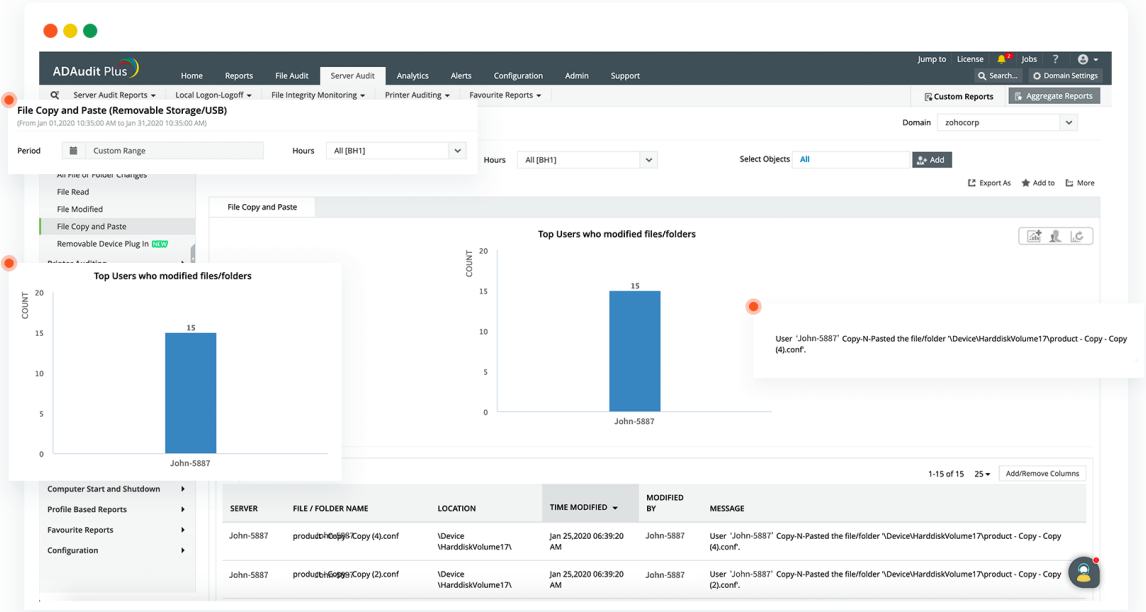
THWART MALWARE ATTACKS



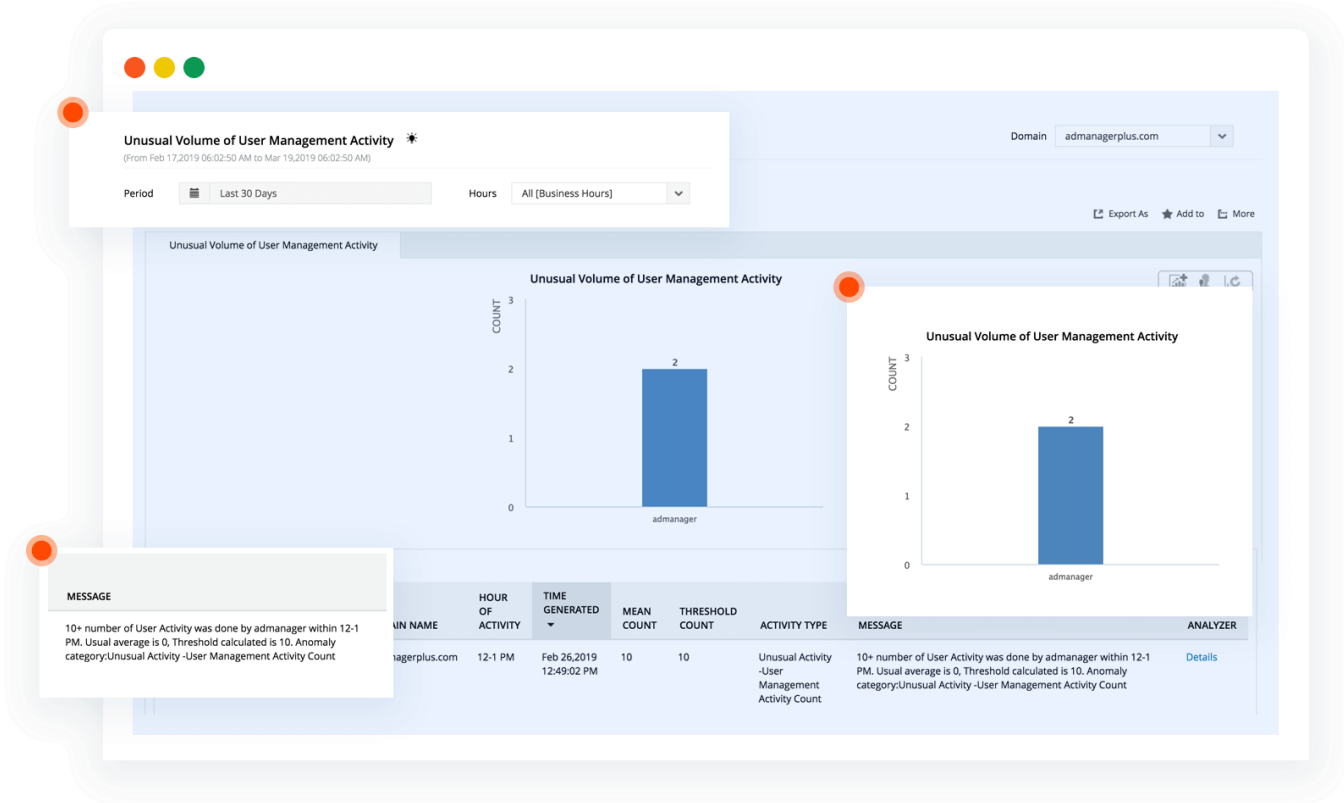
Look for new programs that are installed automatically and monitor modifications done to executable files.

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.

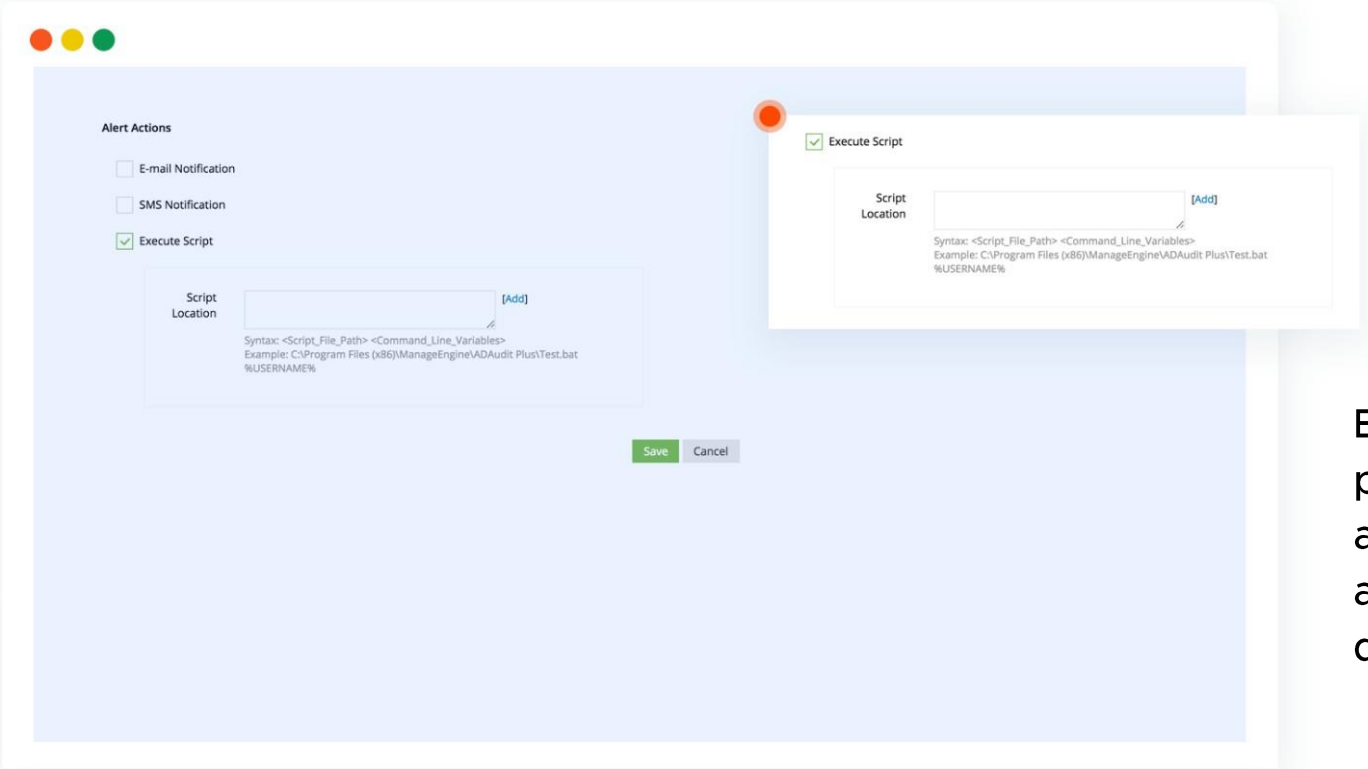


TRACK PRIVILEGE ABUSE



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.

MITIGATE THREATS



Execute a predetermined action whenan anomaly gets detected.

KEY EVENTS TO AUDIT IN YOUR NETWORK

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)

Audit logs that can help you with forensic analysis. Key step in drawing a realistic security posture.

ZERO TRUST APPROARCH

- Tenets
- Fixing the perimeter with stronger password policies
- MFA & adaptive authentication

Dealing with it:

- ❑ Automated incident response
- ❑ 3-2-1 backup and data protection

IDENTIFY | DETECT | EXP. VIEW | **PROTECT** | SYNERGIZE

TENETS OF ZERO TRUST ARCHITECTURE

All data and computing services are considered resources.

All communication is secured regardless of network location.

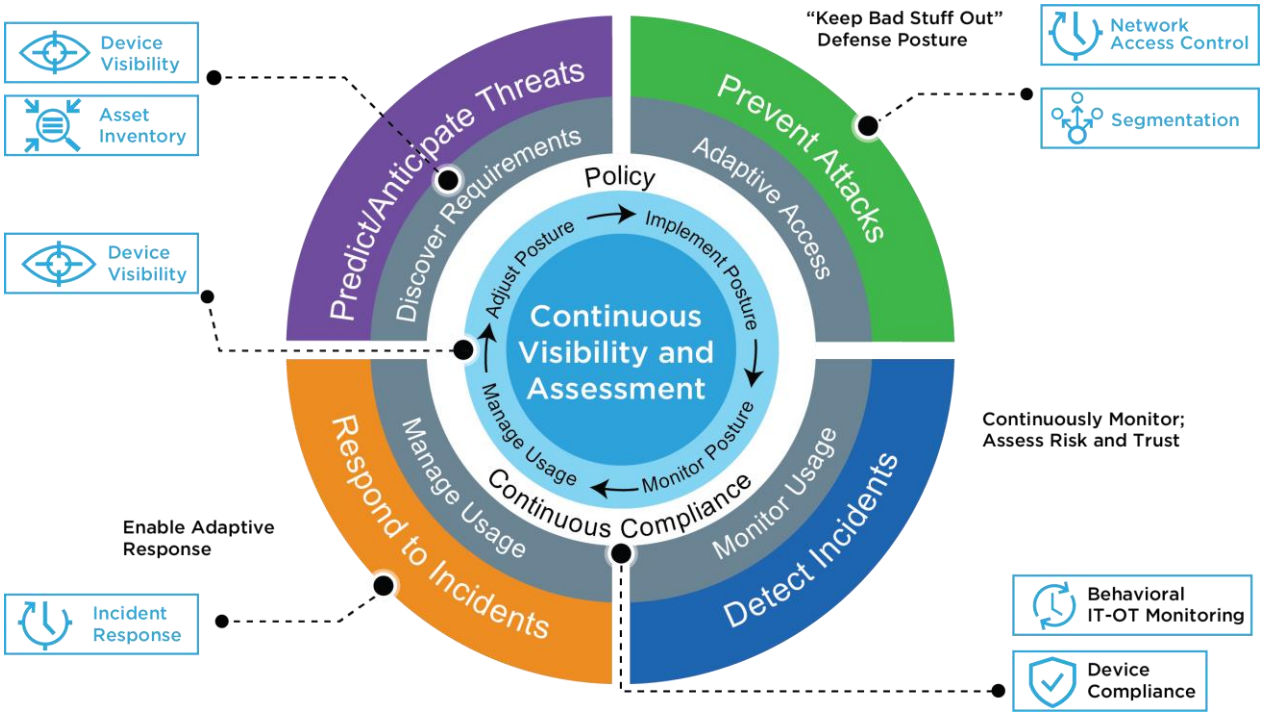
Access to individual enterprise resources is granted on a per-session basis.

Access to resources is determined by dynamic policy.

The enterprise monitors all owned and associated systems to maintain security.

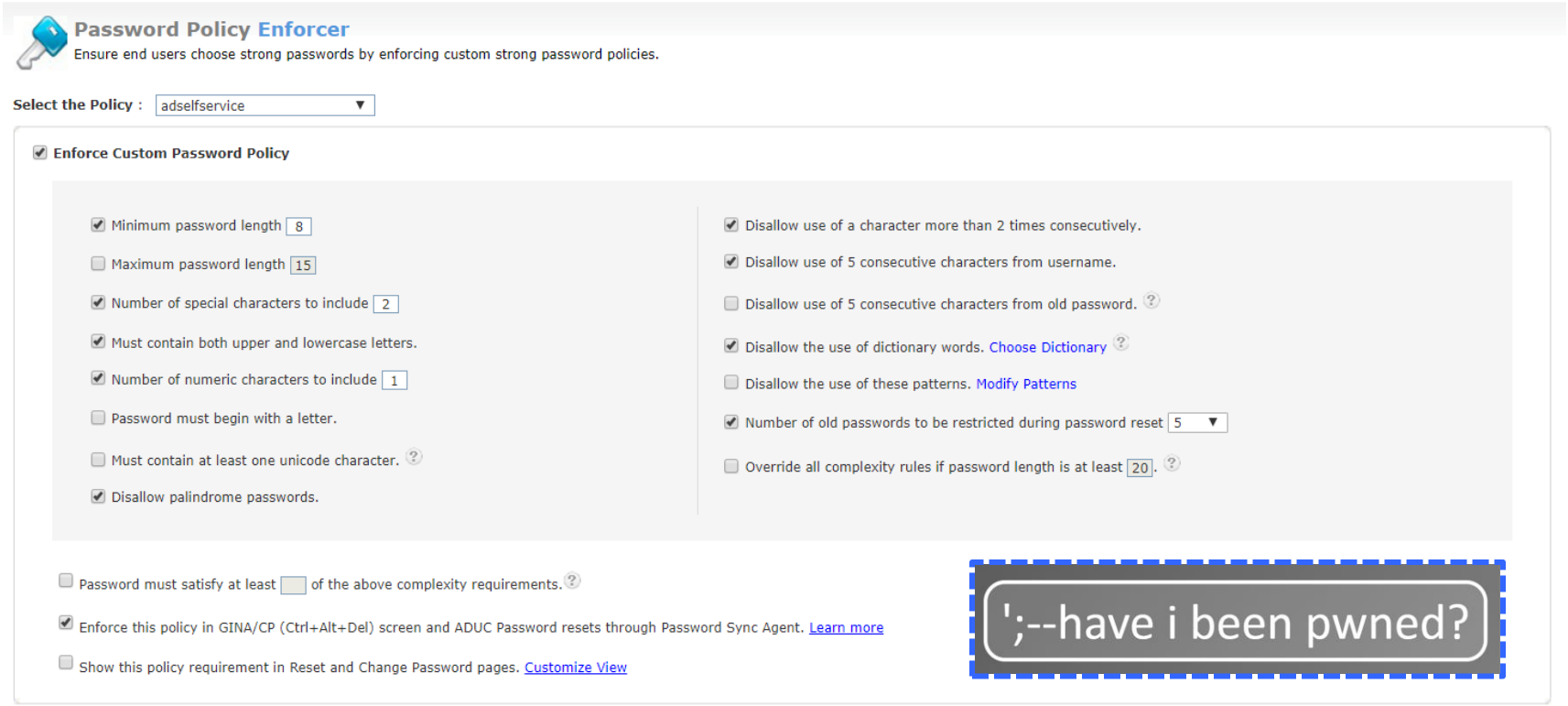
User authentication is strictly enforced before access is allowed.

ZERO TRUST IN ACTION



FIXING THE PERIMETER WITH STRONGER PASSWORD POLICIES

Comprehensive password policies can be applied based on the users' OU or group membership to improve security



MFA & ADAPTIVE AUTHENTICATION

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

AUTOMATE YOUR SOC'S INCIDENT RESPONSE PLAN

Automate responses at every stage of threat mitigation and thereby making your SOC analyst achieve more in less time.

Here is why you shouldn't overlook automation:

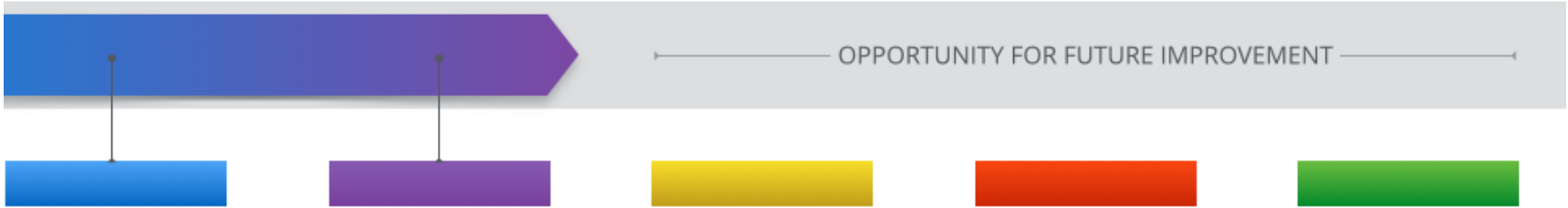
1. Pre-built timelines for rapid investigation
2. Security analytics that shorten the investigation cycles
3. Security orchestration with the ITSM for ensured accountability
4. Automated workflow to decrease meant time to resolution (MTTR)

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.

ROUNDUP: NIST'S CYBERSEC FRAMEWORK



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

jay@manageengine.com

JAY REDDY
SR. TECH EVANGELIST

ManageEngine