CYBERARK®

ATTACK + DEFEND

Cloud & DevOps

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

LEGAL DISCLAIMER

These materials are for educational and research purposes only. All tools provided are open source and CyberArk is not associated with any tools provided. The content is not meant to encourage or promote any illegal activities. Therefore, do not attempt to violate the law with anything contained here. If this is your intention, then **LEAVE NOW**!

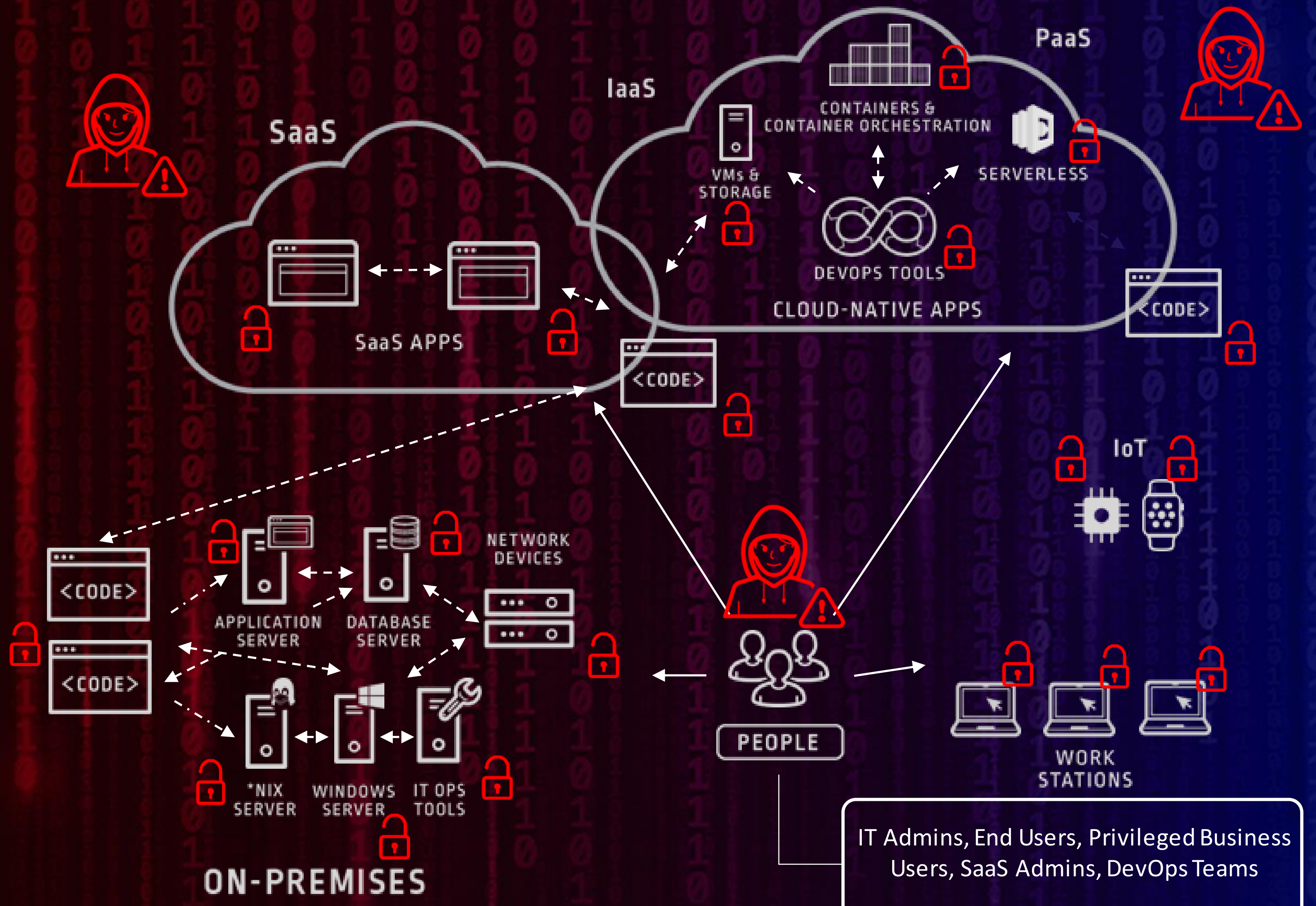
Neither the authors of this material, CyberArk, or anyone else affiliated with the content in any way, is going to accept responsibility for your actions. We promote hacking, but do not promote CRIME! We are documenting the ways criminals steal and perform their nefarious acts, so you can defend yourself and your organization.

Please note that the use of any information or tools within this material is at your own risk. The authors and CyberArk shall not be held responsible for any damages or losses resulting from the use of this material. By using this material, you agree to these terms and conditions.

“To know your Enemy, you must become your Enemy.”

– Sun Tzu

THE NEW NORM : MORE RISK



IT Admins, End Users, Privileged Business Users, SaaS Admins, DevOps Teams

More Infrastructure

More Applications

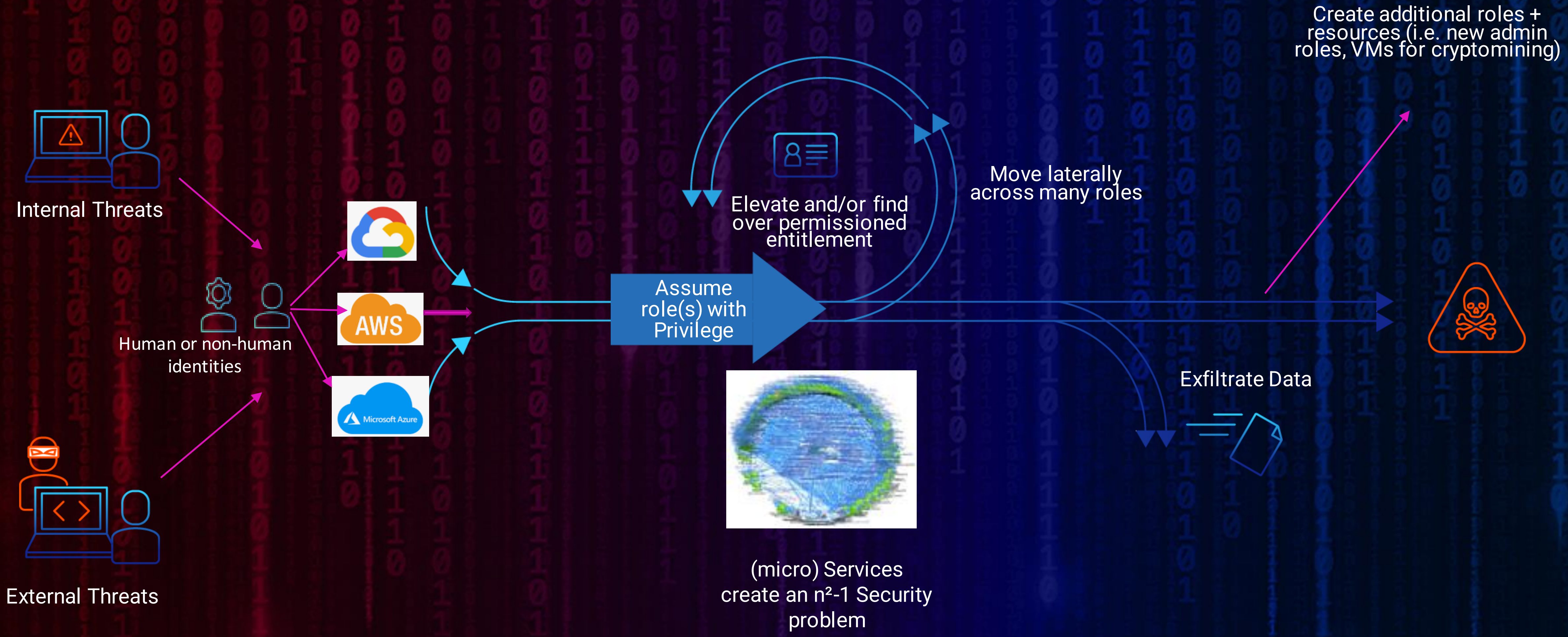
More Privileged Actors

More Automation

More Privileged Security Risk!

New attack paths.
Same attacker mindset.

More cloud & DevOps services = more identities with more entitlements to defend



Internal Threats

Human or non-human identities

External Threats

Assume role(s) with Privilege

Elevate and/or find over permissioned entitlement

Move laterally across many roles

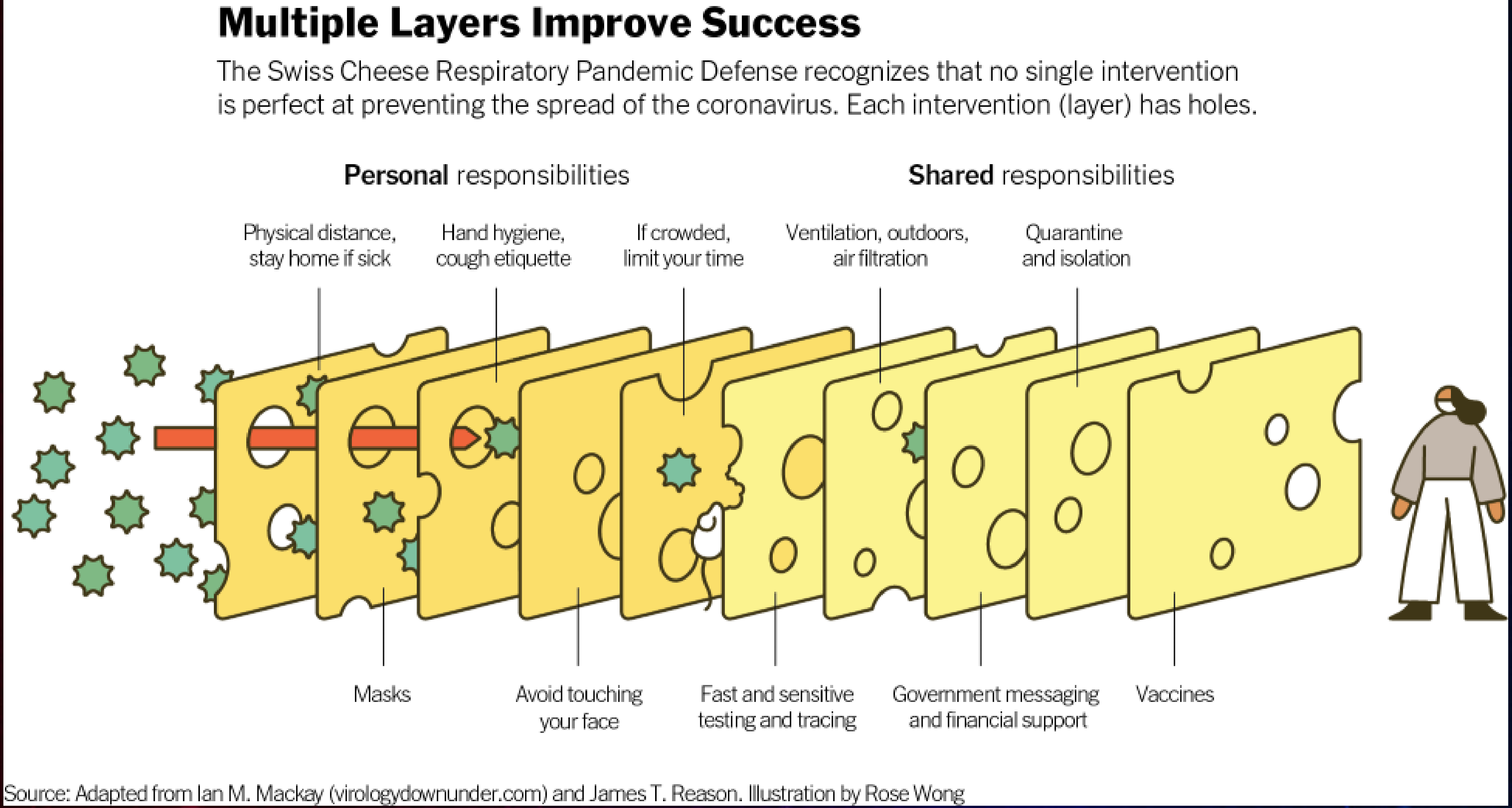
Create additional roles + resources (i.e. new admin roles, VMs for cryptomining)

Exfiltrate Data

(micro) Services create an n²-1 Security problem

Defense in Depth

(The Swiss Cheese Theory)



Multiple Layers Improve Success

The Swiss Cheese Respiratory Pandemic Defense recognizes that no single intervention is perfect at preventing the spread of the coronavirus. Each intervention (layer) has holes.

Personal responsibilities
Shared responsibilities
Physical distance, stay home if sick
Hand hygiene, cough etiquette
If crowded, limit your time
Ventilation, outdoors, air filtration
Quarantine and isolation
Masks
Avoid touching your face
Fast and sensitive testing and tracing
Government messaging and financial support
Vaccines

Source: Adapted from Ian M. Mackay (virologydownunder.com) and James T. Reason. Illustration by Rose Wong

COMMON RISKS AND MISCONFIGURATIONS

Insecure Human Access to Cloud Resources

Insecure Machine Access to Cloud Resources

Sustained Access

Hard-Coded Credentials

Multiple Secret Repositories

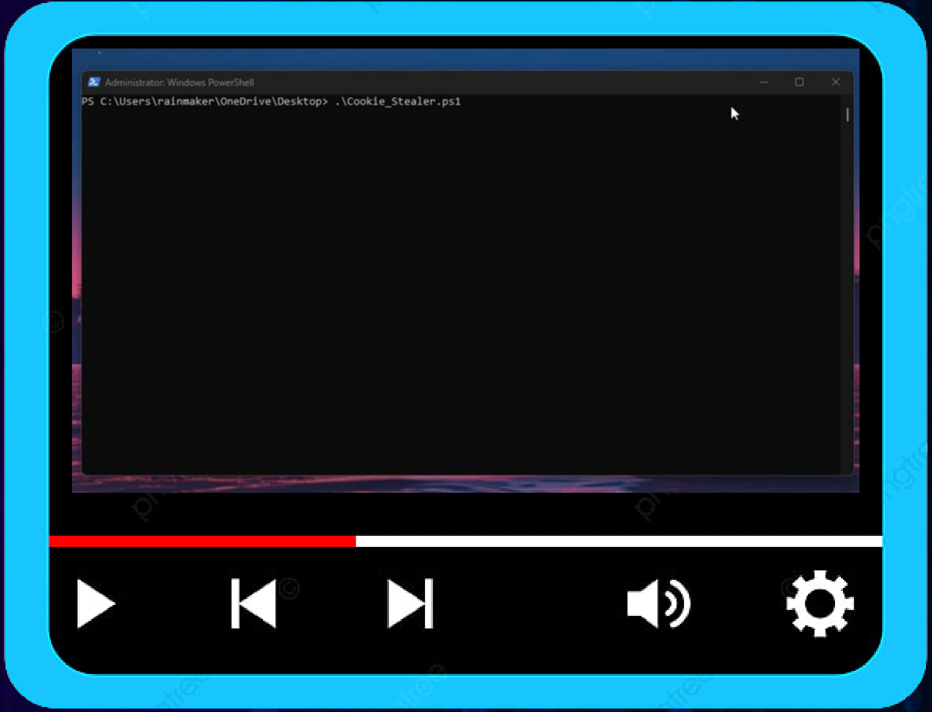
Human Access

😈Attacker Capabilities😈

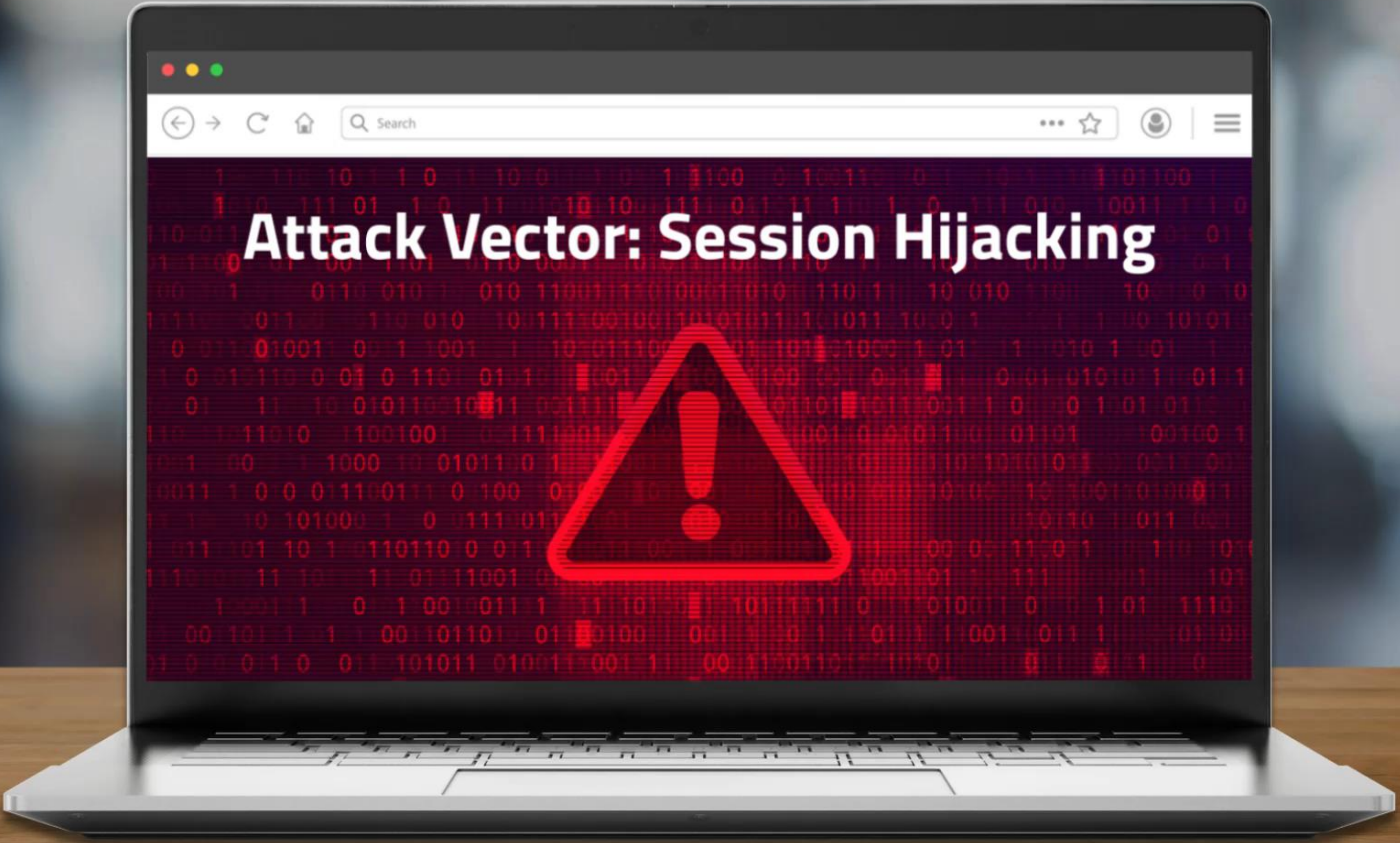
- Data exfiltration
- Data manipulation & sabotage
- Ransomware attacks
- Backdoors, identity, & access theft
- And more!

Attack: Crypto-Mining

- Overprovisioned user is compromised
- Cookies stolen/session hijacked
- Deploys crypto-mining VM's with overprovisioned EC2 access



```
PS C:\Users\rainmaker\OneDrive\Desktop> .\Cookie_Stealer.ps1
```



Attack Vector: Session Hijacking

Cookieless Browsing

Password Replacement

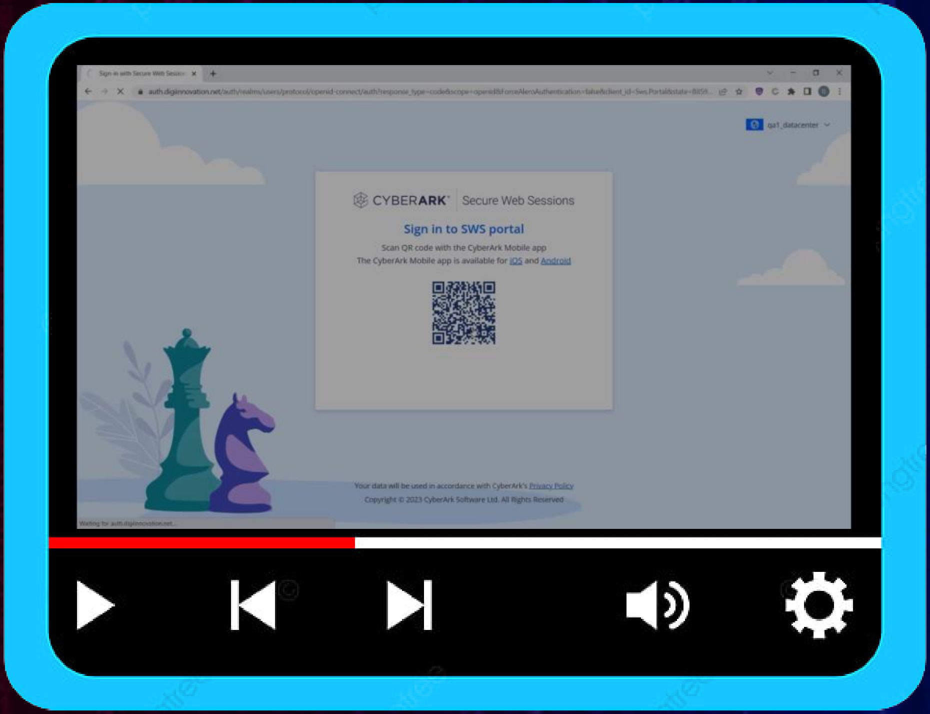
Quick Access Bar

Extensibility

SaaS Apps, PAM Targets, On Prem, Web Based

Secure Browser

Administrator View



Sign-in with Secure Web Sessio

auth.diginnovation.net/auth/realms/users/protocol/openid-connect/auth?response_type=code&scope=openid&forceAleroAuthentication=false&client_id=Sws.Portal&state=8X59...

qa1_datacenter

CYBERARK | Secure Web Sessions

Sign in to SWS portal

Scan QR code with the CyberArk Mobile app
The CyberArk Mobile app is available for iOS and Android

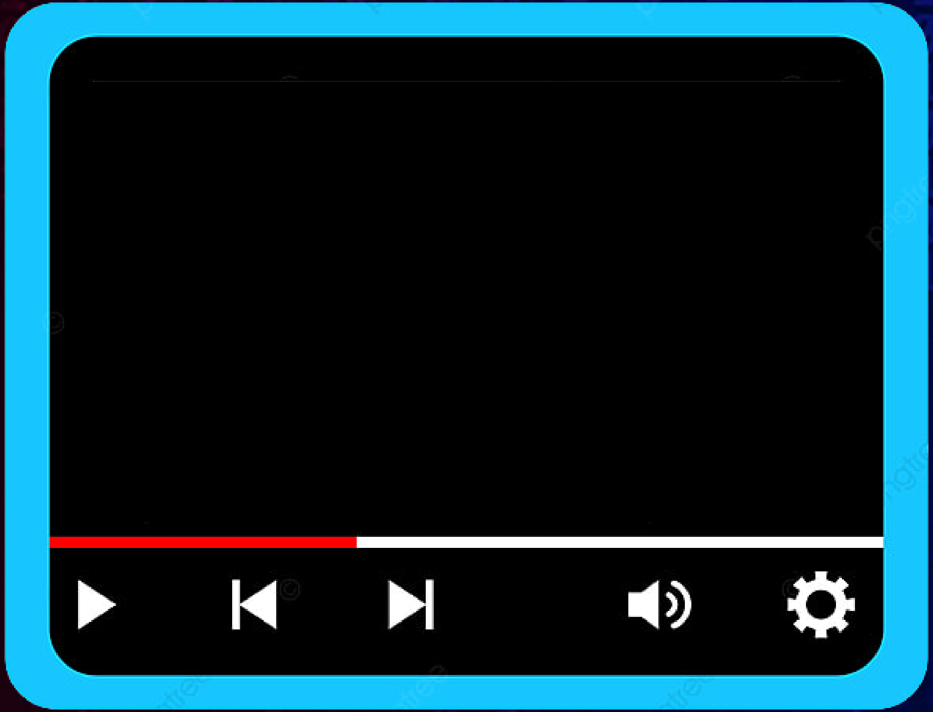
Your data will be used in accordance with CyberArk's Privacy Policy
Copyright © 2023 CyberArk Software Ltd. All Rights Reserved

Secure Browser

User Experience

Attack FAILURE

Unable to harvest browser secrets.



CYBERARK®

ATTACK + DEFEND

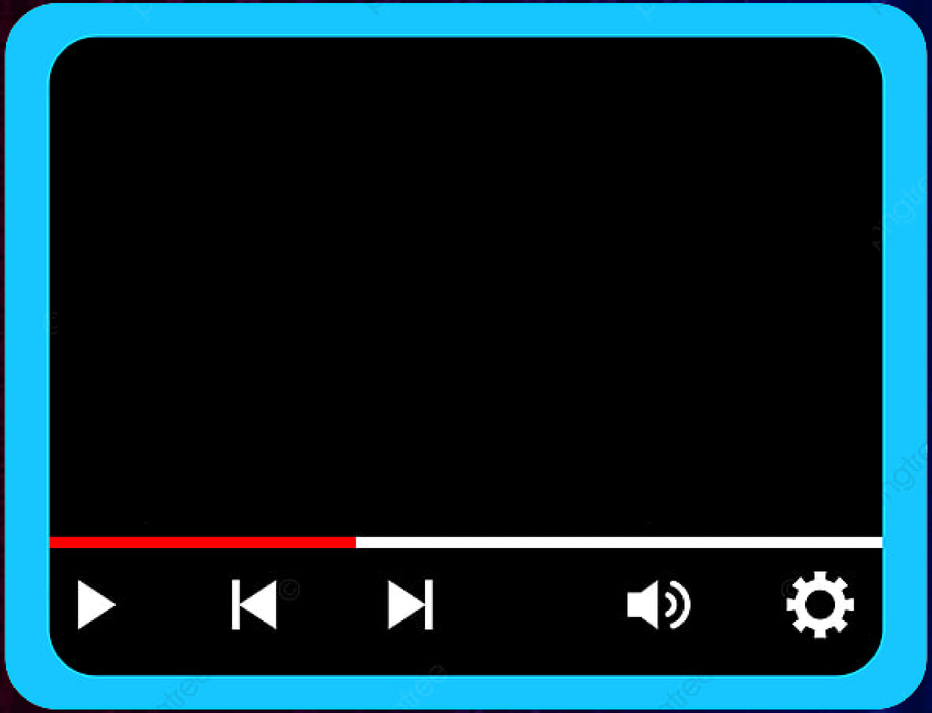
Cloud & DevOps

Secure Cloud Access

(Interactive Access)

Defense

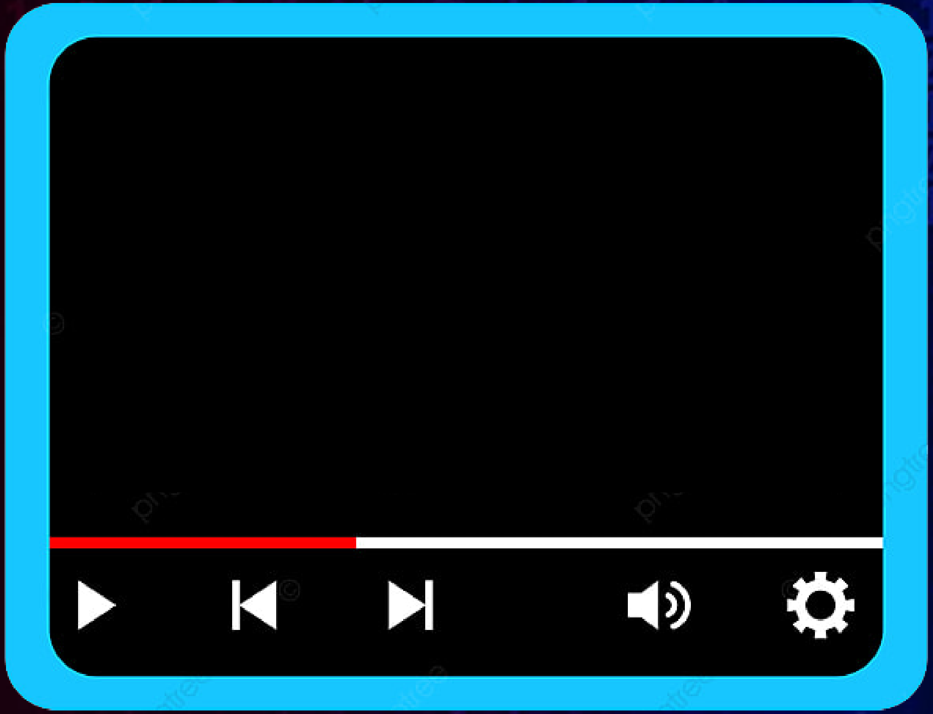
SCA Logon & Action Block



Attack Failure

No Accounts to steal

Must logon with AD + MFA



Programmatic Access

😈Attacker Capabilities😈

- Unauthorized Access to Cloud Resources
- Data Exfiltration & Theft
- Resource Abuse & Cost Inflation
- Malware Propagation
- Infrastructure Disruption
- And more!

Attack: S3 Data Exfil

- User is compromised
- Attacker steals & clones AWS secrets
- Attacker logs on, lists s3 buckets, & exfils data
- Attacker lists permissions

```
PS C:\users\Victim\.aws>
```

CYBERARK®

ATTACK + DEFEND

Cloud & DevOps

Secure Cloud Access

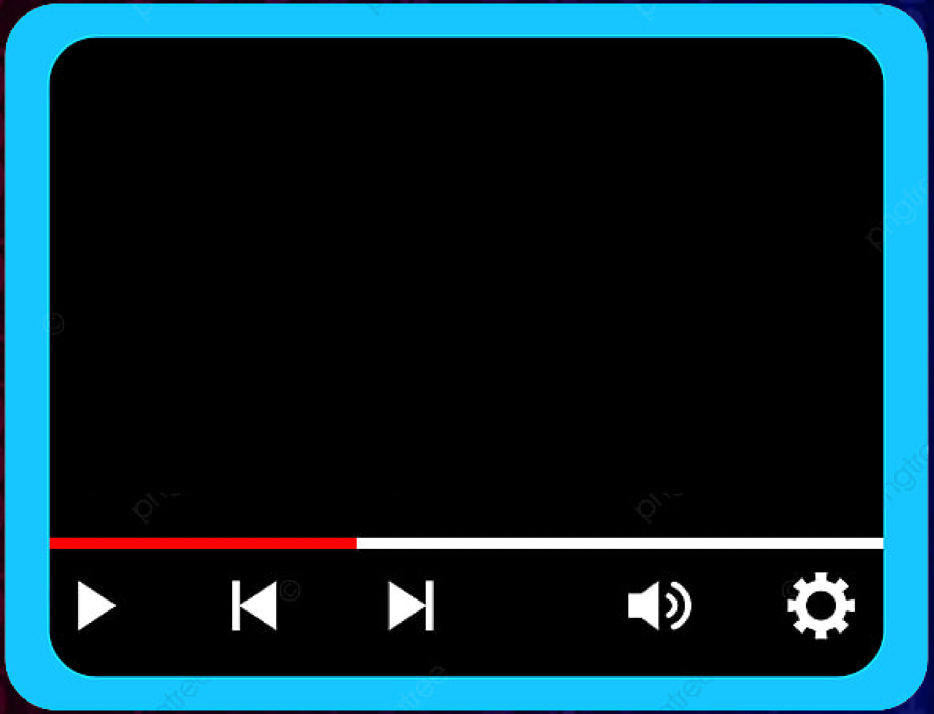
(Programmatic Access)

Defense: On Demand CLI

- Initial IAM & S3 (no EC2) access
- Request EC2 access via SCA
- Imports CLI Token
- Demonstrates EC2 access

Attack Failure

Token expired!



Secure Cloud Access

Secure access to multicloud environments, reduce risk, and maintain native user experience.

Sign up for a FREE trial today!

Consistent

Apply multicloud access policies from one platform

Native

Drive utilization with native access

Pragmatic

Reduce risk by implementing Least Privilege with on-demand elevation

CYBERARK®

https://www.cyberark.com/products/secure-cloud-access/

ATTACK + DEFEND

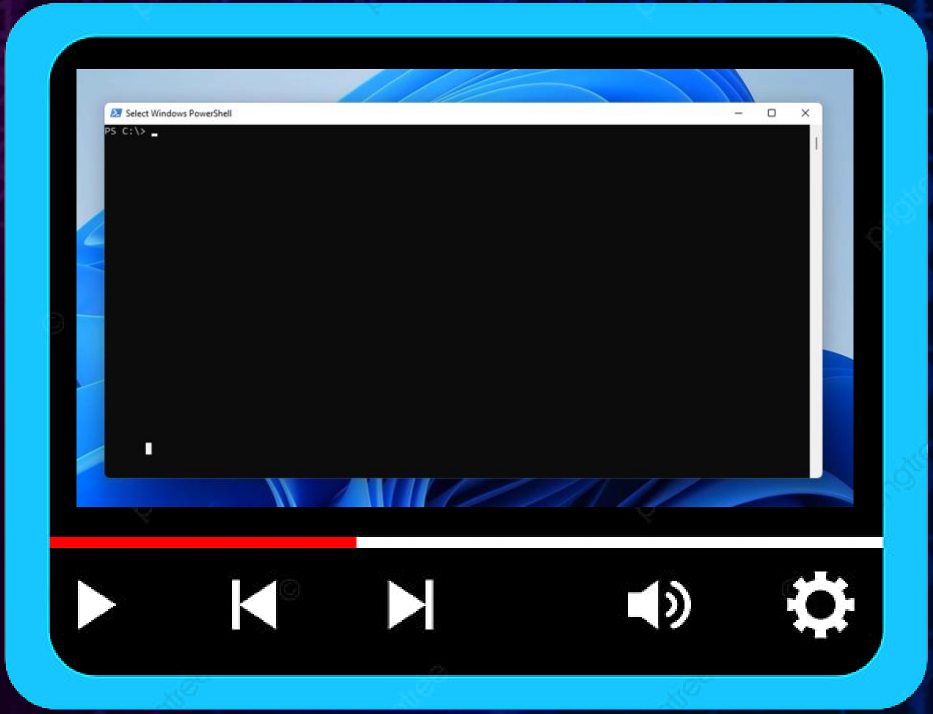
Sustained Privilege

😈Attacker Capabilities😈

- Lateral movement & privilege escalation
- Insider threats and data theft
- Complex identity management
- Inadequate access control
- Difficulty in monitoring/auditing

Attack: Local Account Abuse

- Passwords found in C:\SuperSecretFiles\Passwords.txt
- Threat actor logs on via RDP using stolen credentials
  - Listed as Local Admin



```
PS C:\> _
```

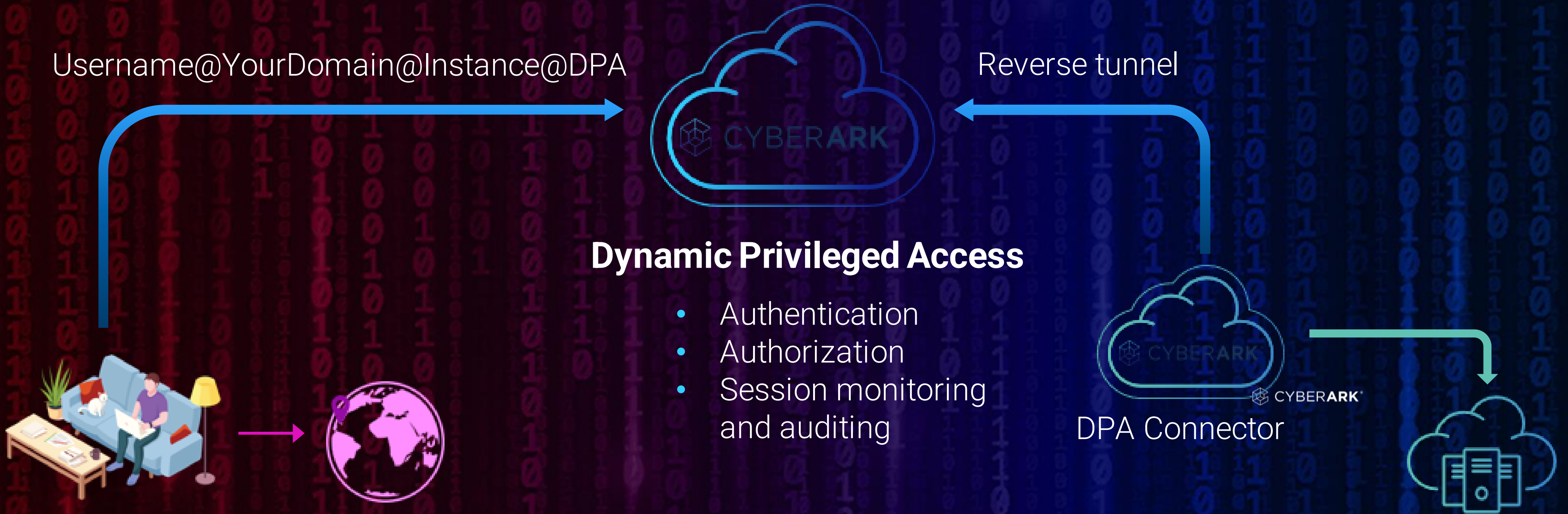
Dynamic Privileged Access

Dynamic Privileged Access

- Just-in-Time Access
- Elevated Privileges
- Session Isolation
- Approval Workflow
- Granular Access Controls

- Audit & Accountability
- Session Management
- No need for credential rotation!

Dynamic Privileged Access in Action



Username@YourDomain@Instance@DPA

Reverse tunnel

Dynamic Privileged Access

- Authentication
- Authorization
- Session monitoring and auditing

DPA Connector

End User

- VPN-less
- SSO
- MFA

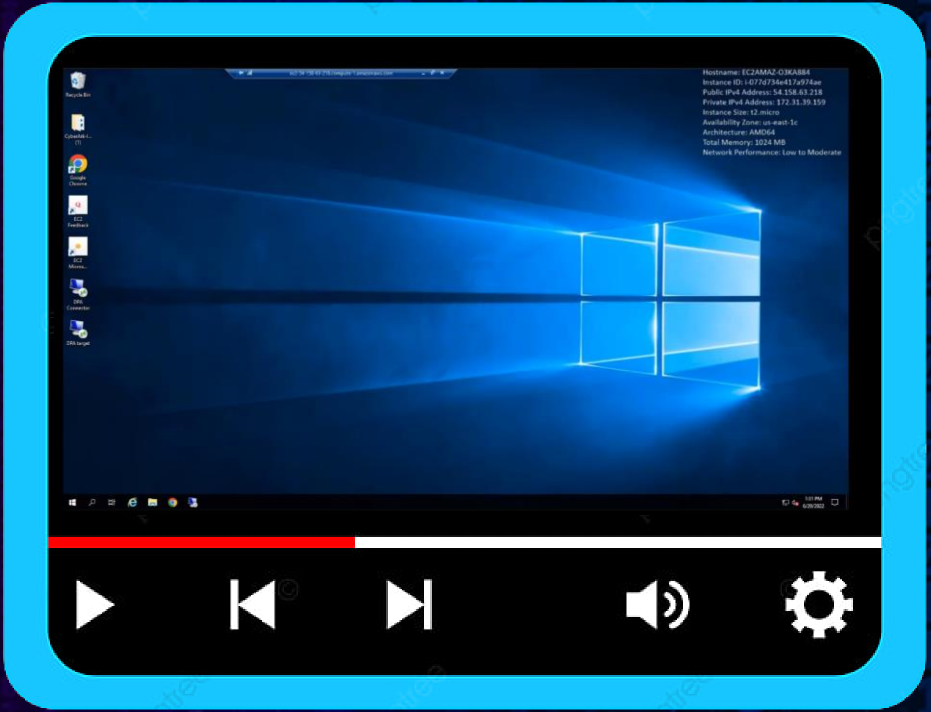
Linux/Windows

Target Environment

- Agentless
- Ephemeral access

Defense: Ephemeral Access

- Initial Access through RDP
- User authenticates to DPA
- Account immediately created
- Account expires and deleted



```
Hostname: EC2AMAZ-O3KA884
Instance ID: i-077d734e417a974ae
Public IPv4 Address: 54.158.63.218
Private IPv4 Address: 172.31.39.159
Instance Size: t2.micro
Availability Zone: us-east-1c
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate
```

DPA Outcomes

Drive Measurable Cyber-Risk Reduction:

- Remove standing access and provide JIT Access to Cloud VMs and Windows Servers
- Ephemeral sessions prevent lateral movement and malware spread
- Access is verified via MFA while supporting the native user experience

Enable Operational Efficiencies:

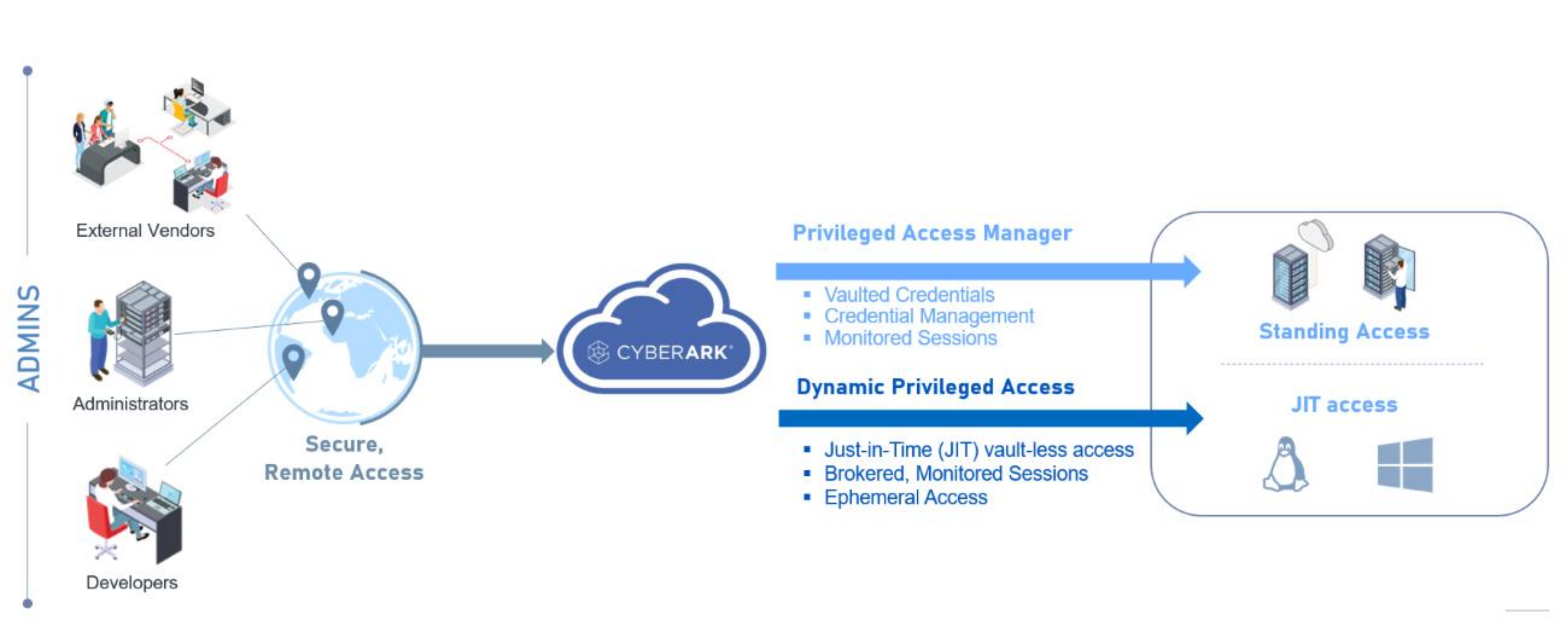
- Empower Privileged Users to natively connect with their preferred client
- Zero downtime, no patches, and no upgrades with cloud born solution
- Agentless SaaS solution to reduce resources used for PSM

Secure Digital Transformation:

- Enable access for the remote workforce without the need for VPN
- Accelerate Zero Trust initiatives by extending PAM coverage across hybrid + multi-cloud environments
- Secure dynamically scaling environments

Dynamic Provisioning Access

Provision Just-in-Time (JIT) privileges access.
Reduce risk in hybrid and multi-cloud infrastructure.



Privileged Access Manager

- Vaulted Credentials
- Credential Management
- Monitored Sessions

Dynamic Privileged Access

- Just-in-Time (JIT) vault-less access
- Brokered, Monitored Sessions
- Ephemeral Access

Request a Demo

https://www.cyberark.com/products/dynamic-privileged-access/

Hard-coded Credentials

Hard-Coded Credentials

If hard-coded passwords are used, it is almost certain that malicious users will gain access to the account in question.

- Read application data
- Gain privileges
- Assume identity
- Execute unauthorized code
- And more!

https://cwe.mitre.org/data/definitions/798.html

Attack: API Key Harvesting

- Steals session cookie
- Recon finds vulnerable webapp
- Enumerates folders
- Traverses misconfigured logs directory
- Finds API keys to abuse

Defense: Conjur

- API keys replaced with Conjur
- Pulls the API key from vault
- No keys in logs to steal

Secrets Management Made Simple with Conjur

A seamless open-source interface to securely authenticate, control and audit non-human access across tools, applications, containers and cloud environments via robust secrets management.

- Manage secrets across tools, apps, and clouds
- Isolate secrets from applications
- Consistently control access for non-human identities
- Secure and authenticate containers natively

https://www.conjur.org/

CYBERARK®

ATTACK + DEFEND

Unchanging Credentials

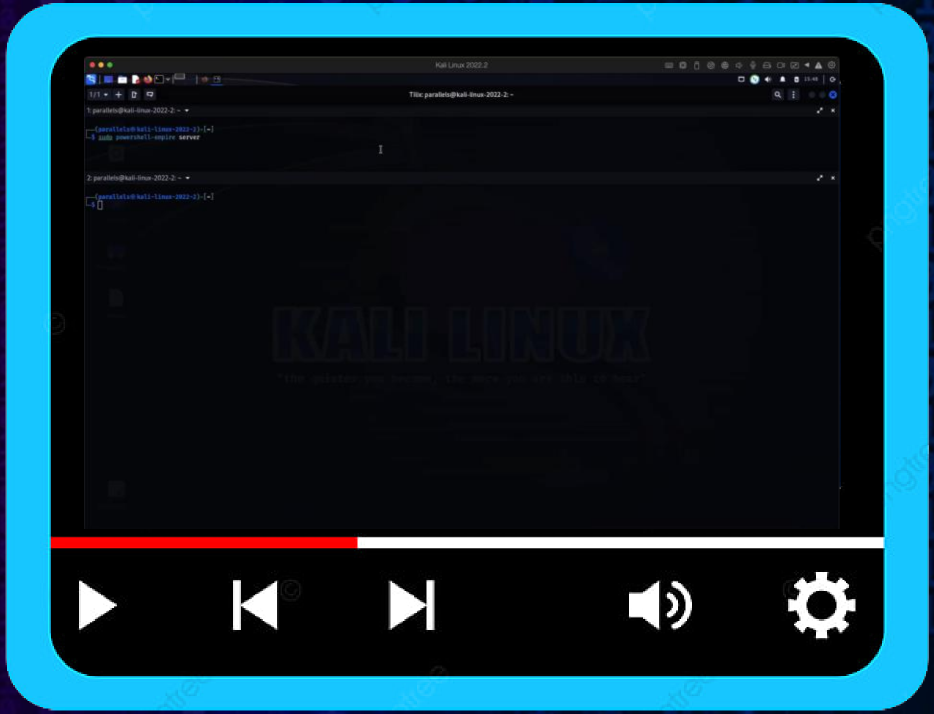
Unchanging Credentials

If static credentials are compromised,
attackers gain prolonged access.

- Developers need a way to securely access and use credentials.
- Bridging the gap beyond on-prem credentials is challenging.
- Often leads to static credentials allowing prolonged access.

Attack: Access AWS Secrets

- User is compromised
- Attacker steals CLI token
- Attacker accesses credentials through AWS Secrets Manager



Kali Linux 2022.2
Tilix: parallels@kali-linux-2022-2: ~
1: parallels@kali-linux-2022-2: ~
2: parallels@kali-linux-2022-2: ~

```
┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ sudo powershell-empire server
```

```
┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ 
```

Secrets Hub

Centralized secrets management and rotation for project teams using AWS Secrets Manager

Request a Demo

Centrally Manage and Rotate

Enables security to establish centralized control and enforce unified policies over all secrets.

Unchanged Developer Experience

Giving developers the same native experience using AWS Secrets Manager.

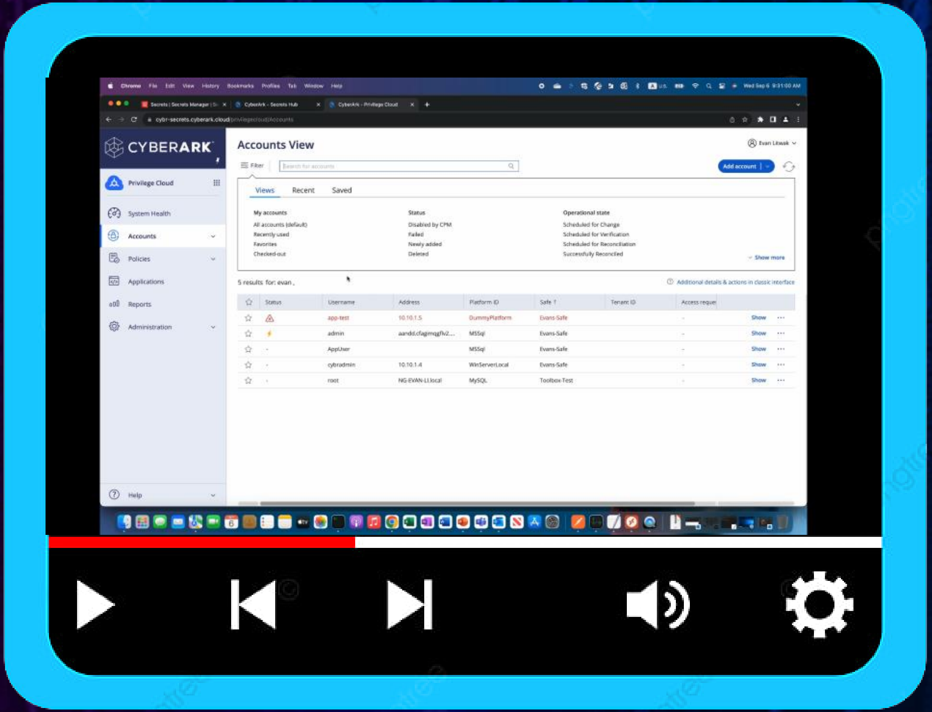
Reduce Vault Sprawl

Simplifying operations by centralizing secrets management across projects which uses AWS Secrets Manager.

https://www.cyberark.com/products/secrets-hub/

Defense: Secrets Hub Synchronization

- Priv Cloud securely stores the creds
- Synchronizes to AWS Secrets Hub
- Provides synchronized credential rotation
- Ease of use for developers



Accounts View

Views Recent Saved

My accounts	Status	Operational state
All accounts (default)	Disabled by CPM	Scheduled for Change
Recently used	Failed	Scheduled for Verification
Favorites	Newly added	Scheduled for Reconciliation
Checked-out	Deleted	Successfully Reconciled

Show more

5 results for: evan ,

Additional details & actions in classic interface

☆	Status	Username	Address	Platform ID	Safe ↑	Tenant ID	Access reque		
☆	⚠	app-test	10.10.1.5	DummyPlatform	Evans-Safe		-	Show	···
☆	⚡	admin	aandd.cfagmqgfv2....	MSSql	Evans-Safe		-	Show	···
☆	-	AppUser		MSSql	Evans-Safe		-	Show	···
☆	-	cybradmin	10.10.1.4	WinServerLocal	Evans-Safe		-	Show	···
☆	-	root	NG-EVAN-LI.local	MySQL	Toolbox-Test		-	Show	···

CYBERARK®

ATTACK + DEFEND

Cloud & DevOps

Insecure Human Access

Secure Cloud Access

CYBERARK®

ATTACK + DEFEND

Cloud & DevOps

Insecure Machine Access

Secure Cloud Access

CYBERARK

ATTACK +
DEFEND

Cloud & DevOps

Sustained Access

Dynamic Privilege Access

CYBERARK®

ATTACK + DEFEND

Cloud & DevOps

Secrets in Code

Conjur

CYBERARK®

ATTACK +
DEFEND

Cloud & DevOps

Multiple Secrets Repositories

Secrets Hub

CYBERARK®

ATTACK + DEFEND

THANK YOU