RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

SESSION ID: MASH-M03

Telling Fairy Tales to the Board: **Turn Attack Graphs into Business Stories**

#RSAC

Andy Ellis

Advisory CISO, Orca Security
Author, 1% Leadership
@csoandy

Oren Sade

Chief of Staff,
Orca Security

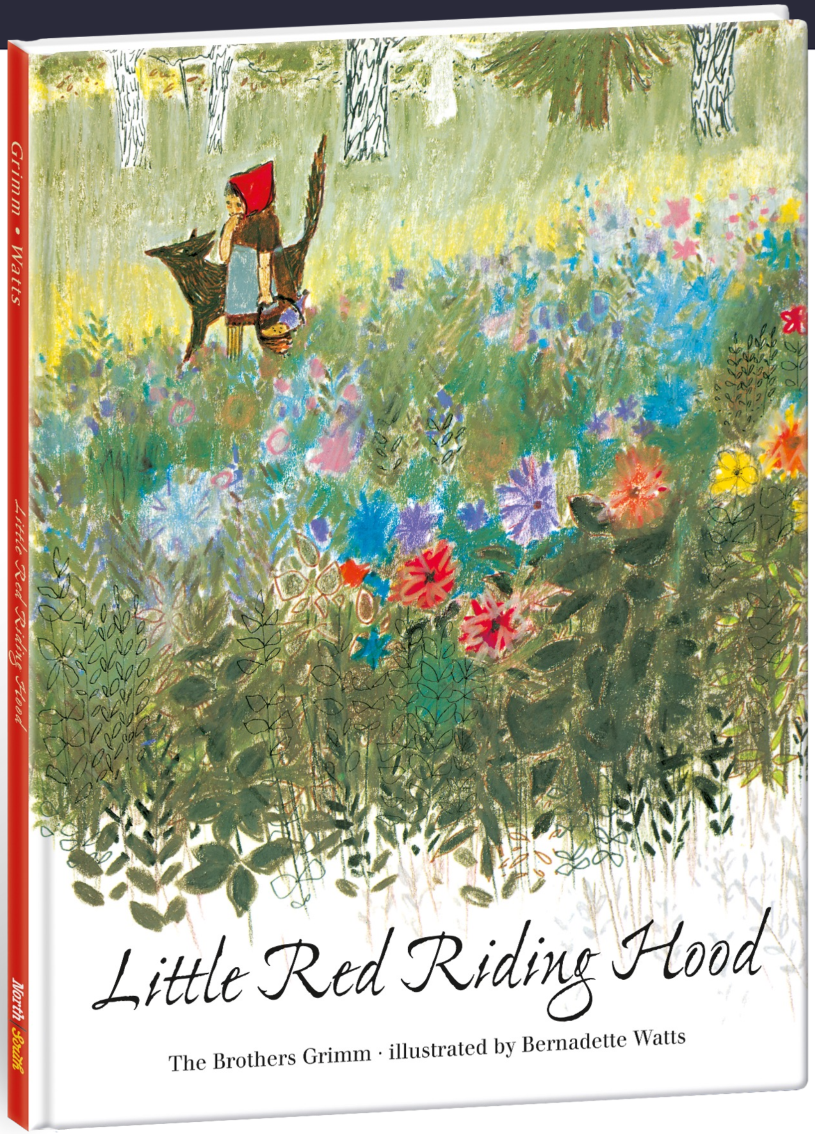
Stronger Together

Disclaimer

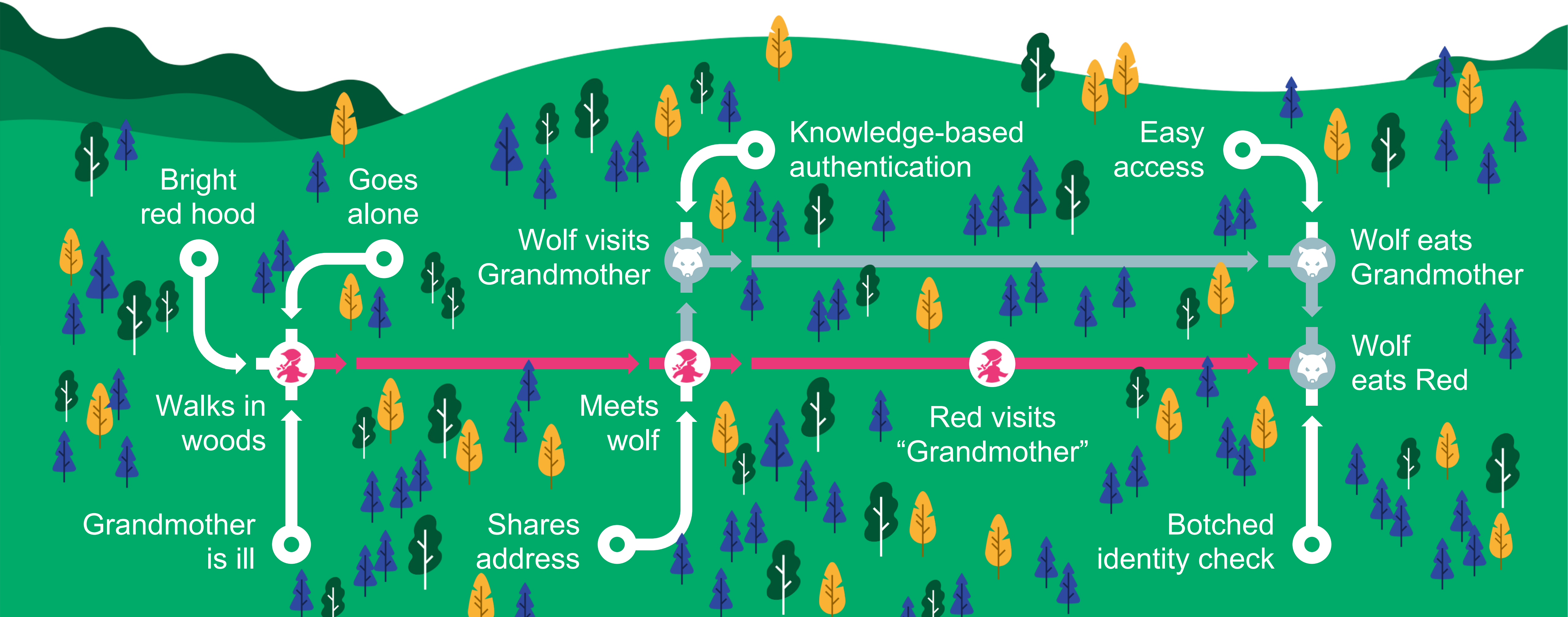
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

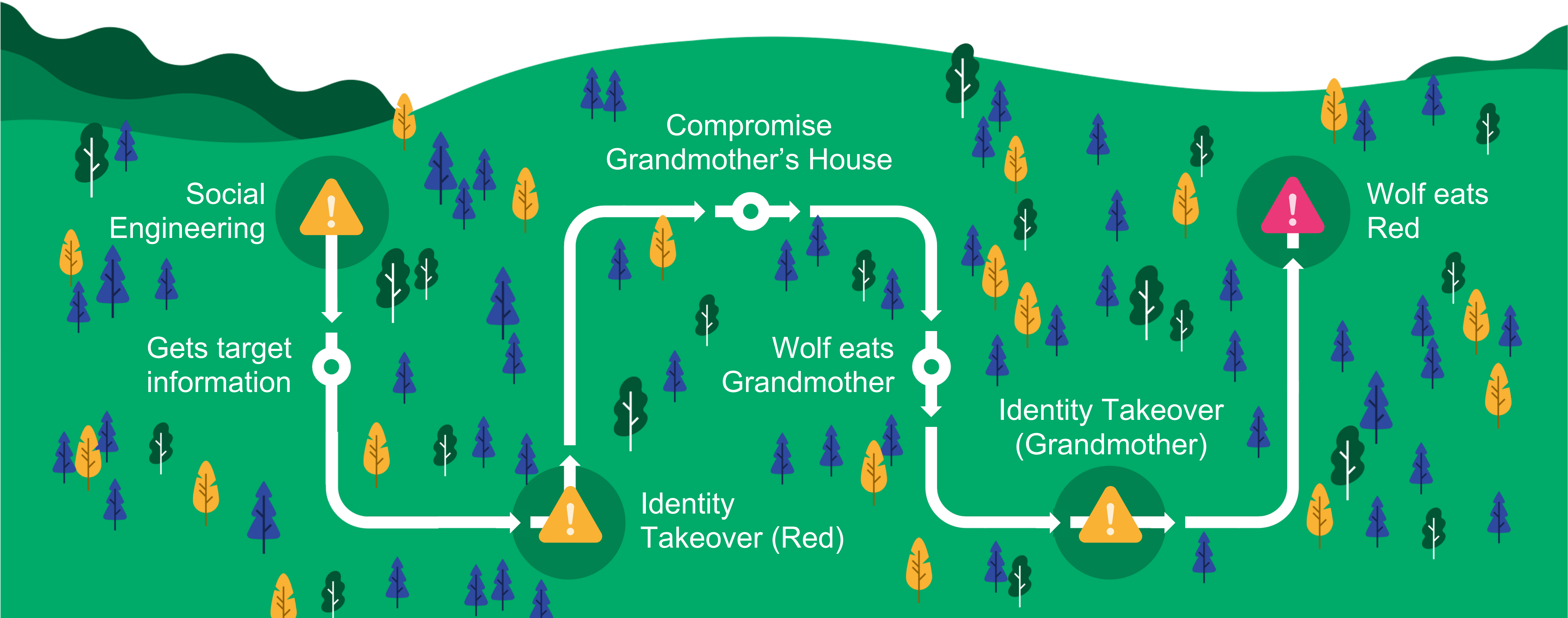
A Reading from the Book of Red



An Attack Forest



An Attack Path



Lessons from a fairy tale

Red Riding Hood Awareness Initiative

Unacceptable Loss	Hazards	Initiative
Little Red gets eaten	Knowledge-Based authentication vulnerable to social engineering Lack of adversary awareness	Teach Red to question strangers more, and to trust her instincts that someone is lying to her. Put a lock on Grandmother’s door.

See also: **Multi-Factor Authentication Initiative**

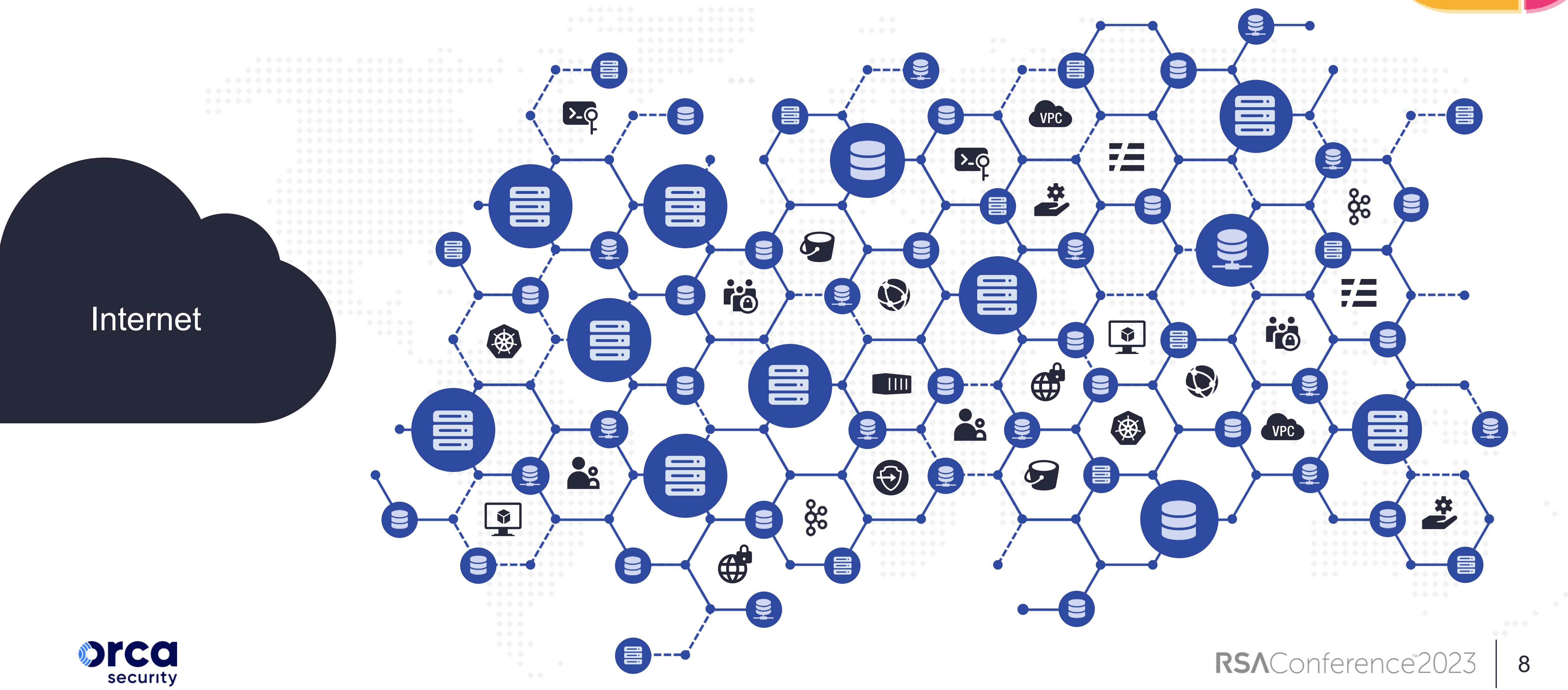
RSAConference™2023

Stronger Together

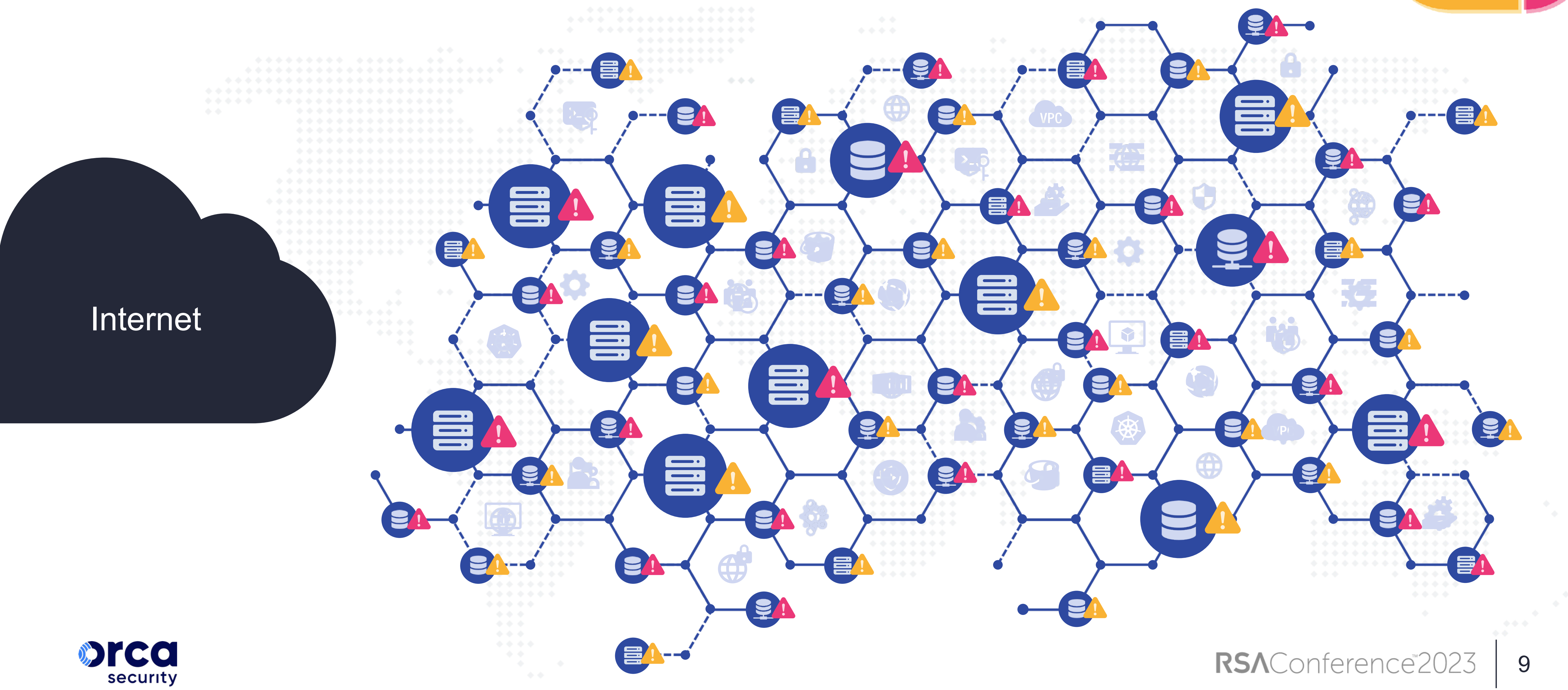
What about your cloud forest?

#RSAC

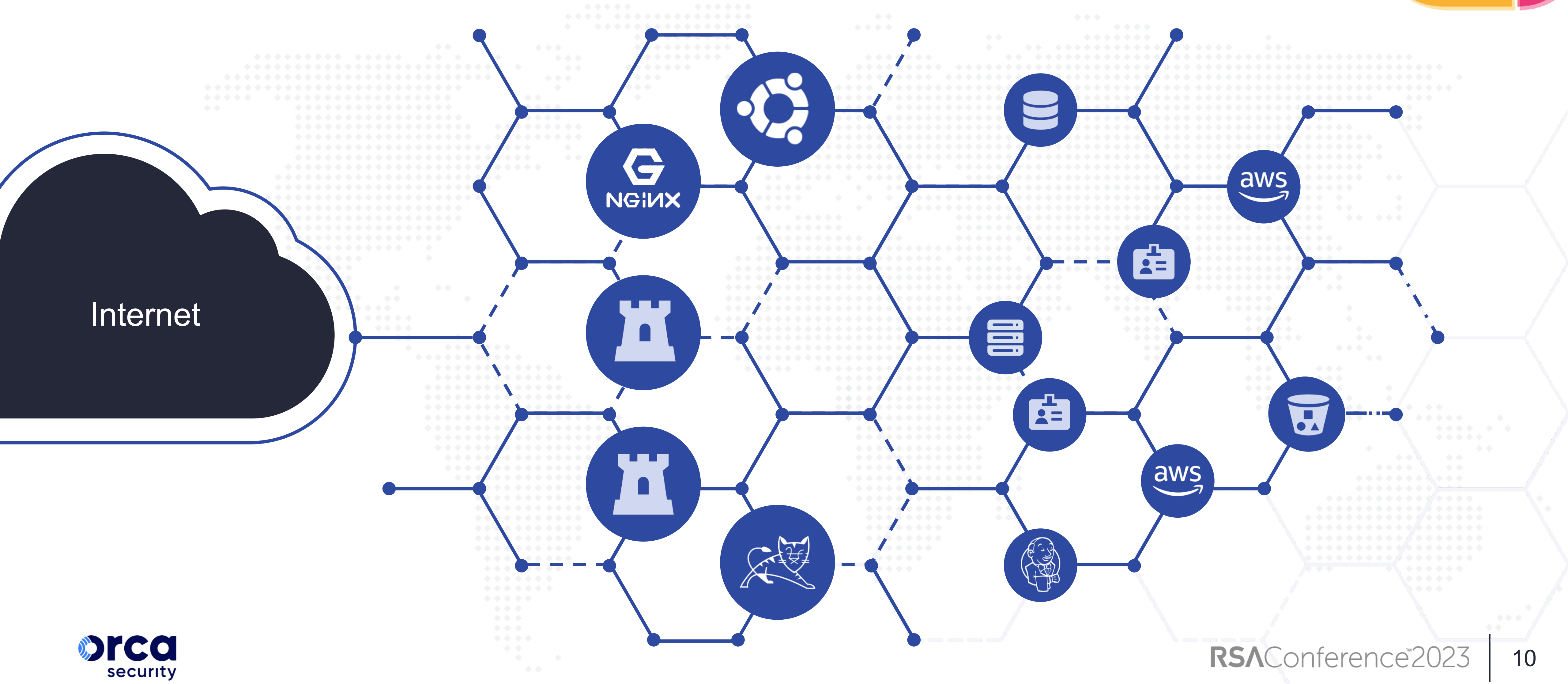
A typical cloud environment



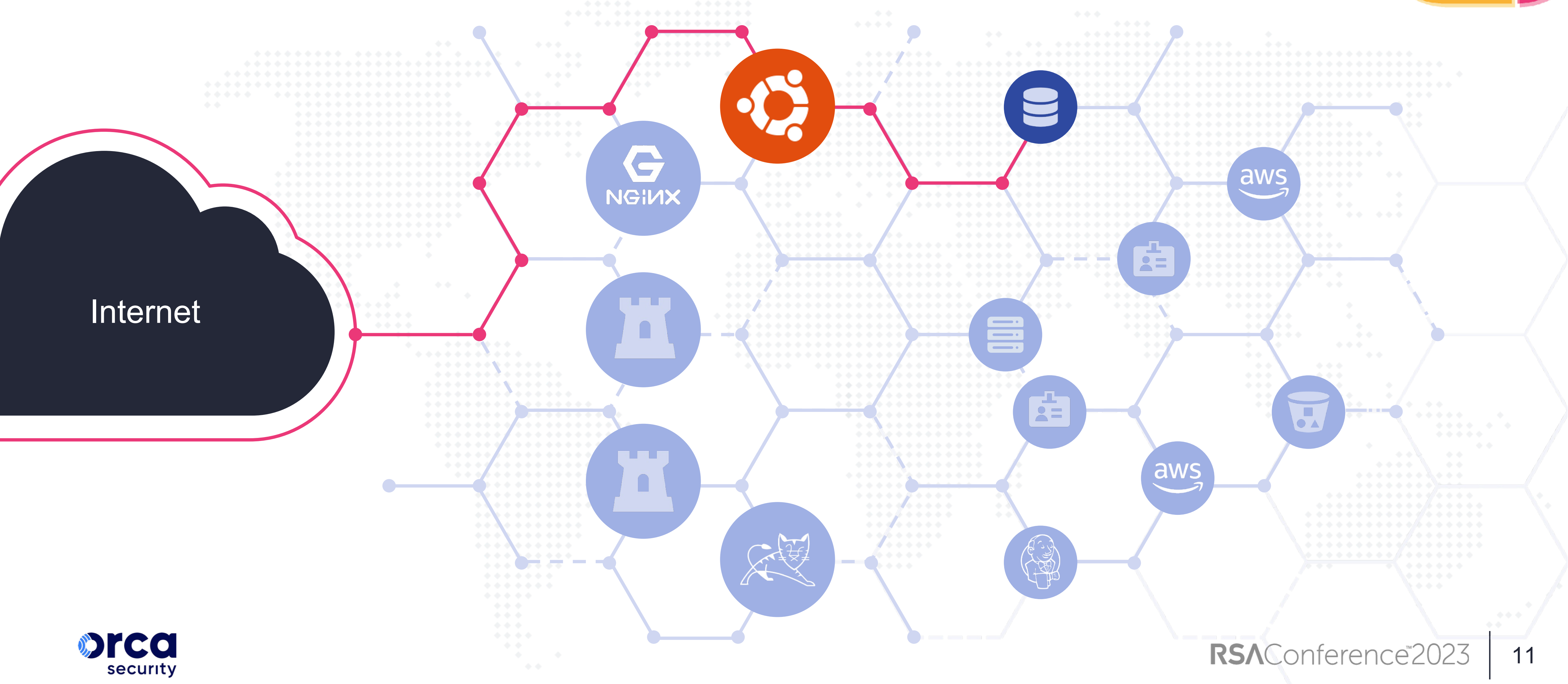
A typical cloud environment



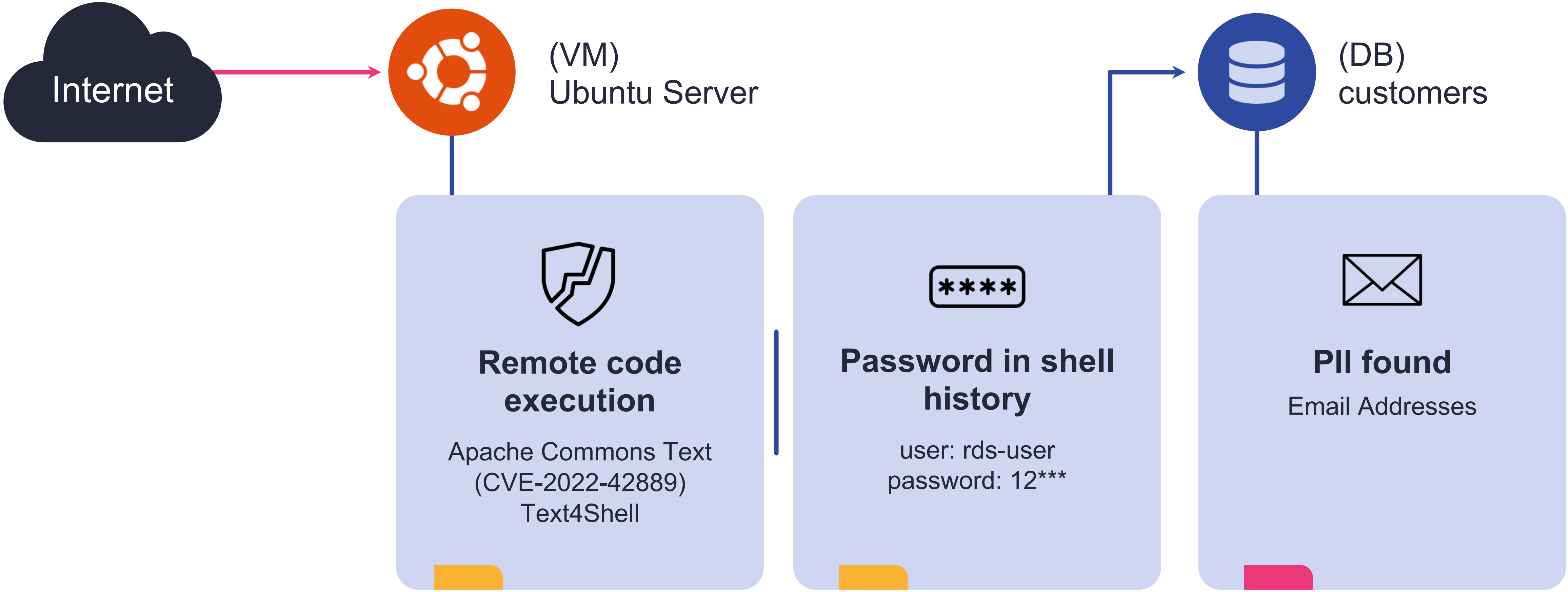
A cloud environment (for this talk)



Unpatched Machine (full view)



Unpatched Machine (attack path view)



Internet

(VM)
Ubuntu Server

(DB)
customers

Remote code execution

Apache Commons Text
(CVE-2022-42889)
Text4Shell

Password in shell history

user: rds-user
password: 12***

PII found

Email Addresses

Unpatched Machine (management view)

Software Vulnerability Management Initiative

Unacceptable Loss

Customer data breach

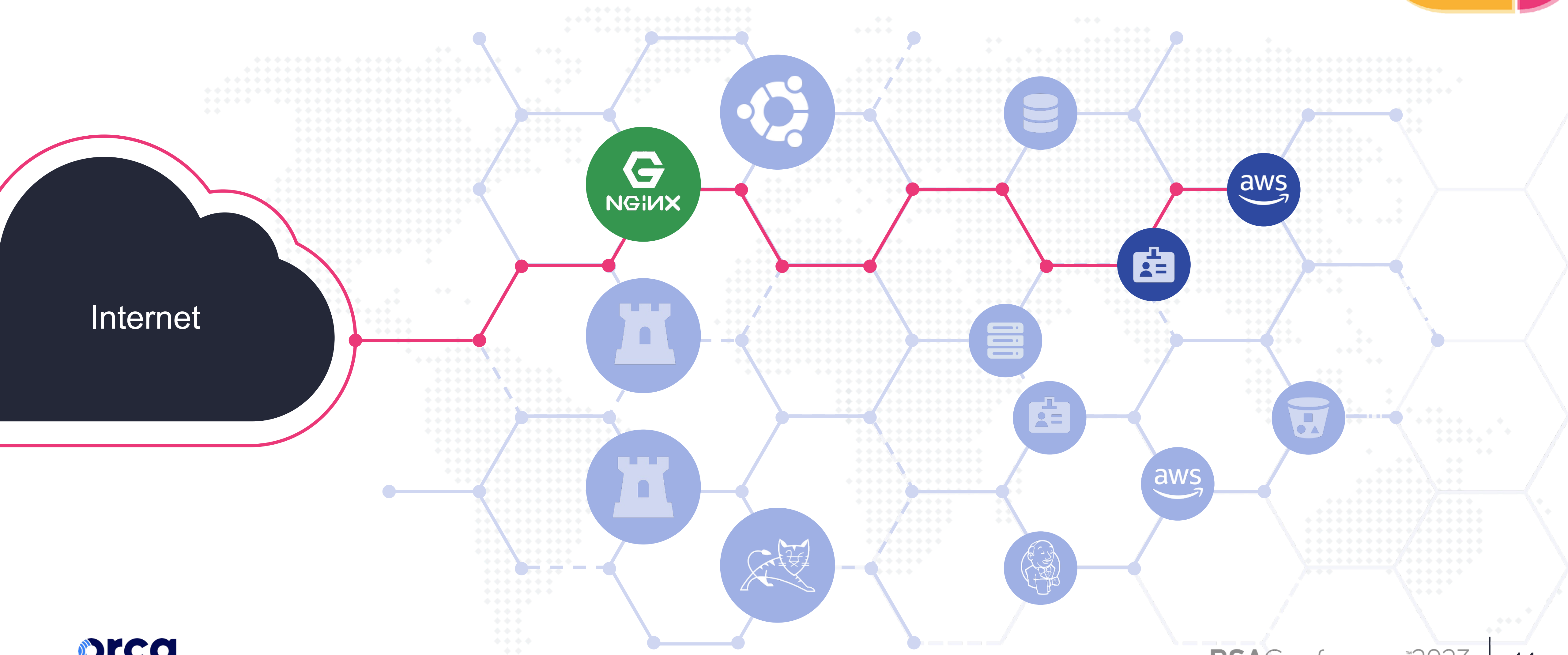
Hazards

78% of all attack paths start with known exploitable vulnerabilities in our environment

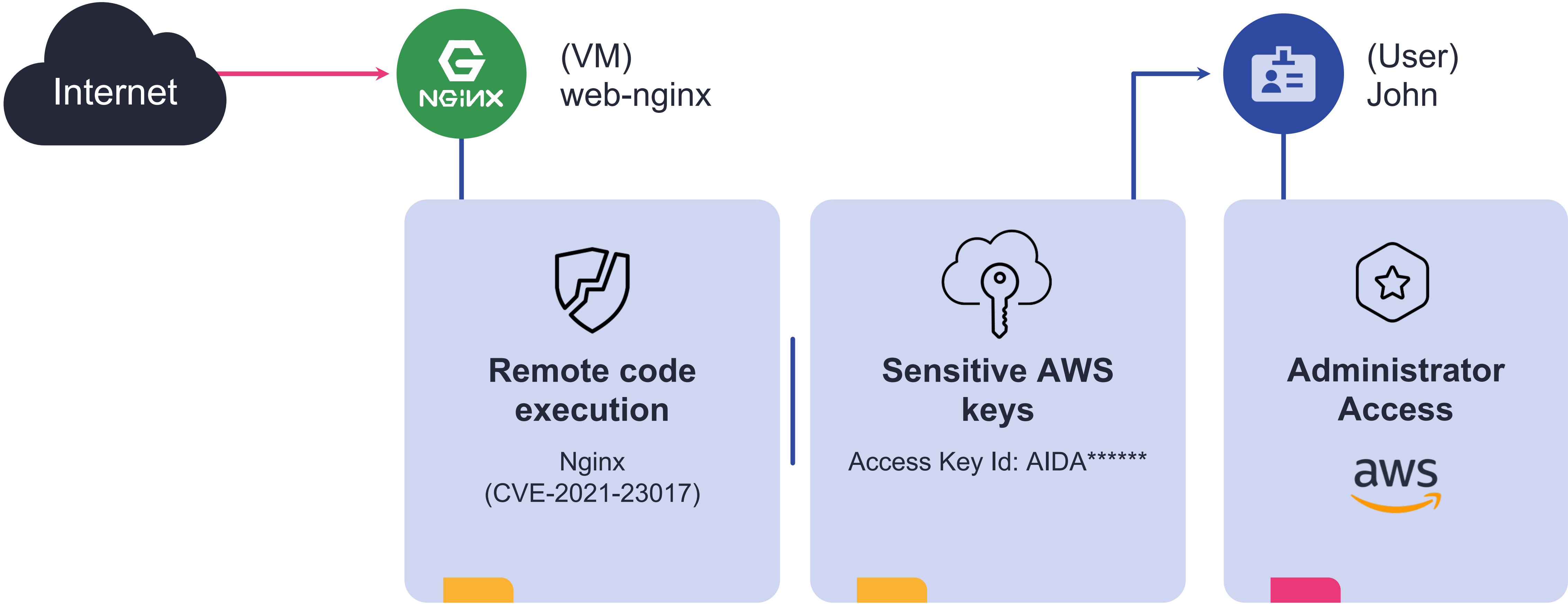
Initiative

Improve and monitor patch management to reduce open windows that give attackers a toe in the door

Administrator role accessible (full view)



Administrator role accessible (attack path view)



Internet

(VM)
web-nginx

(User)
John

Remote code execution

Nginx
(CVE-2021-23017)

Sensitive AWS keys

Access Key Id: AIDA******

Administrator Access

Administrator role accessible (management view)

Cloud Identity Entitlements Management Initiative

Unacceptable Loss

Loss of control of all cloud assets

Hazards

Highly privileged accounts in widespread use

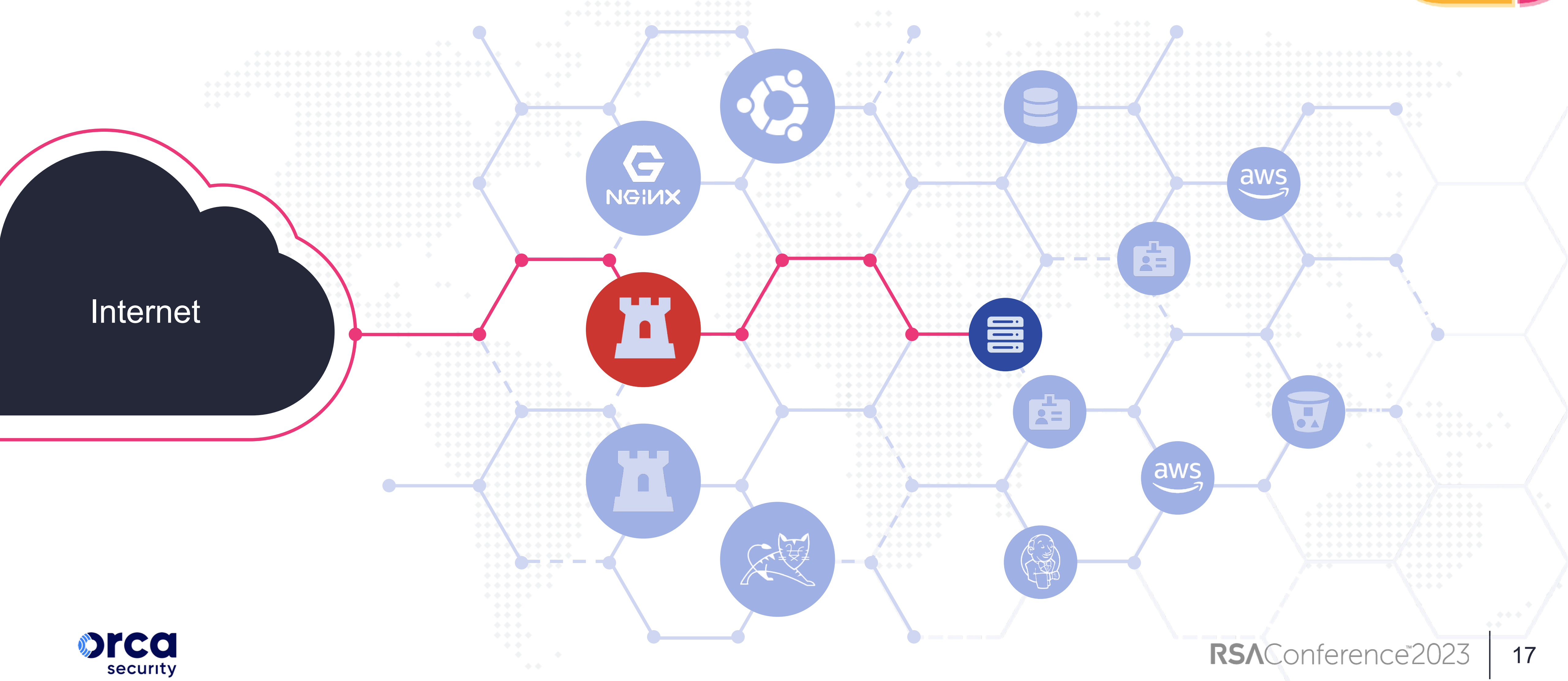
Keys stored insecurely on disk

Initiative

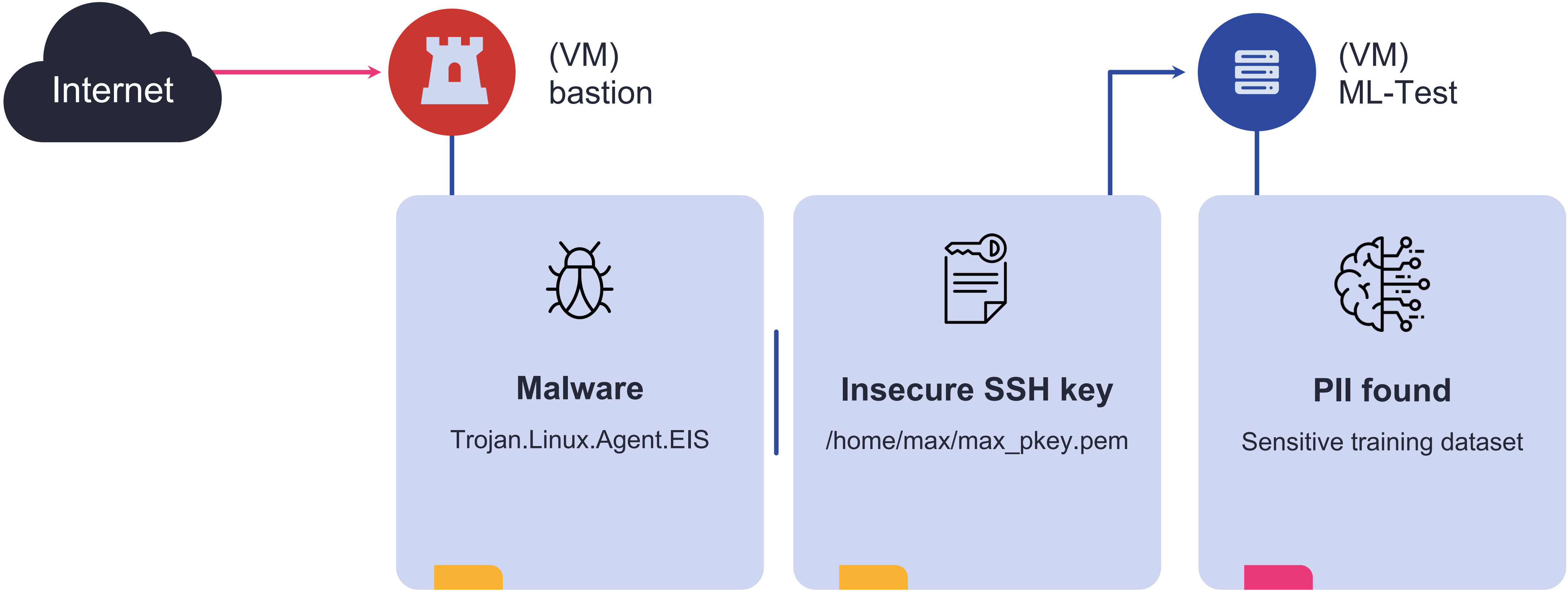
Identity management initiative to restrict access to necessary users and applications

Clean up key storage

Compromised bastion server (full view)



Compromised bastion server (attack path view)



Malware

Trojan.Linux.Agent.EIS

Insecure SSH key

/home/max/max_pkey.pem

PII found

Sensitive training dataset

Compromised bastion server (management view)

Malware Cleanup *Incident*

Unacceptable Loss

Loss of sensitive data

Hazards

Malware has access to assets in the cloud

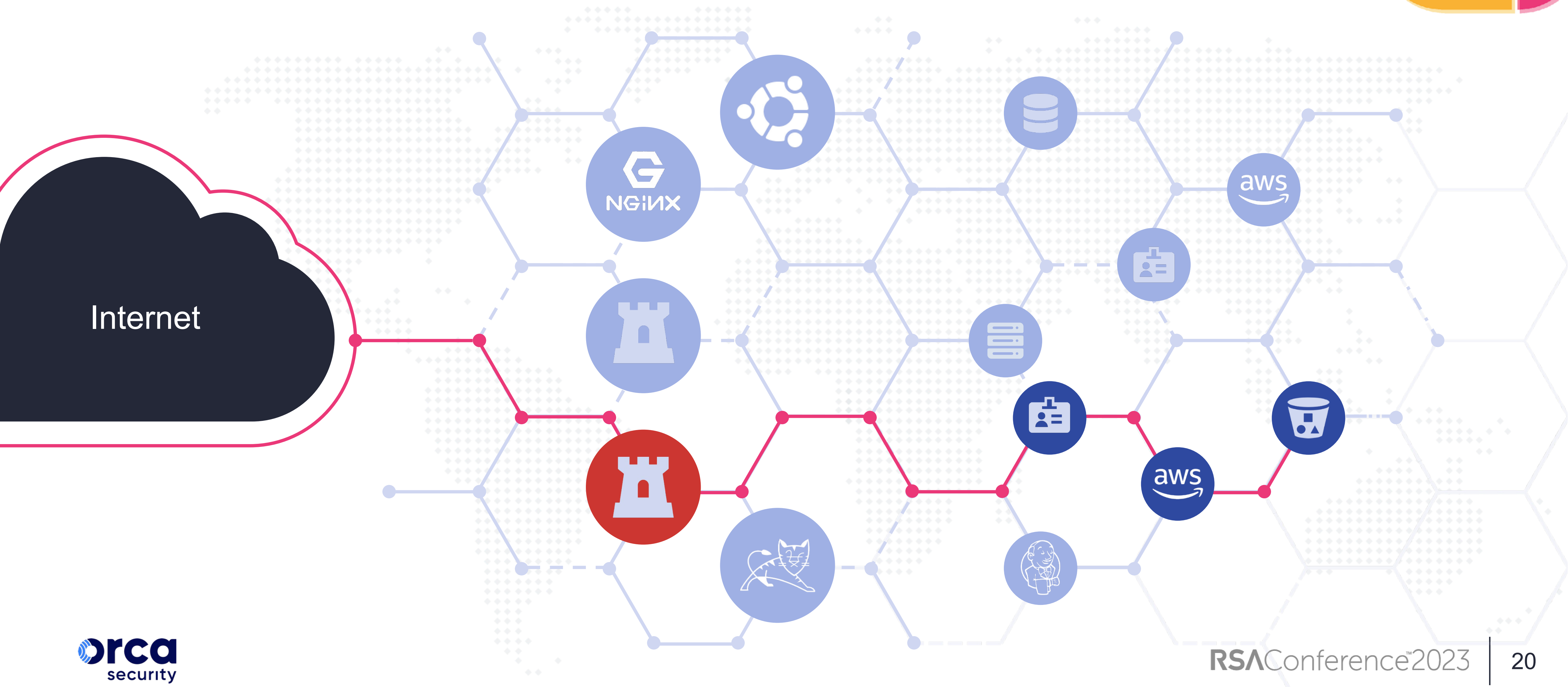
Malware remained undetected for extended periods of time

Initiative

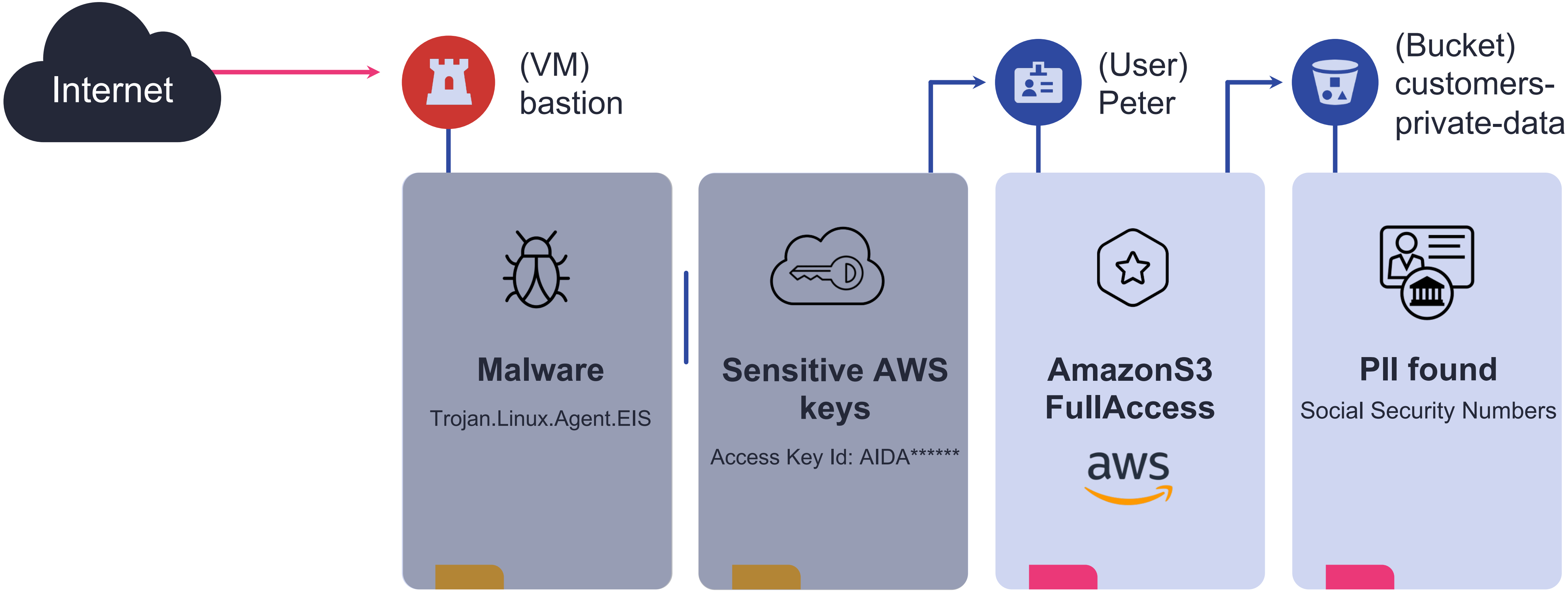
Remove existing malware by redeploying systems

Build operational processes to respond to malware more quickly.

Compromised bastion, *plus* PII (full view)



Compromised bastion, *plus* PII (attack path view)



Compromised bastion, *plus* PII (management view)

PII Identification Initiative

Unacceptable Loss	Hazards	Initiative
Customer Data Stolen	PII stored in many cloud datastores	Identify locations of sensitive data in cloud servers. Remove/restrict access to support the principle of least privilege.

See also: **Malware Cleanup *Incident***
Cloud Identity Entitlements Management Initiative

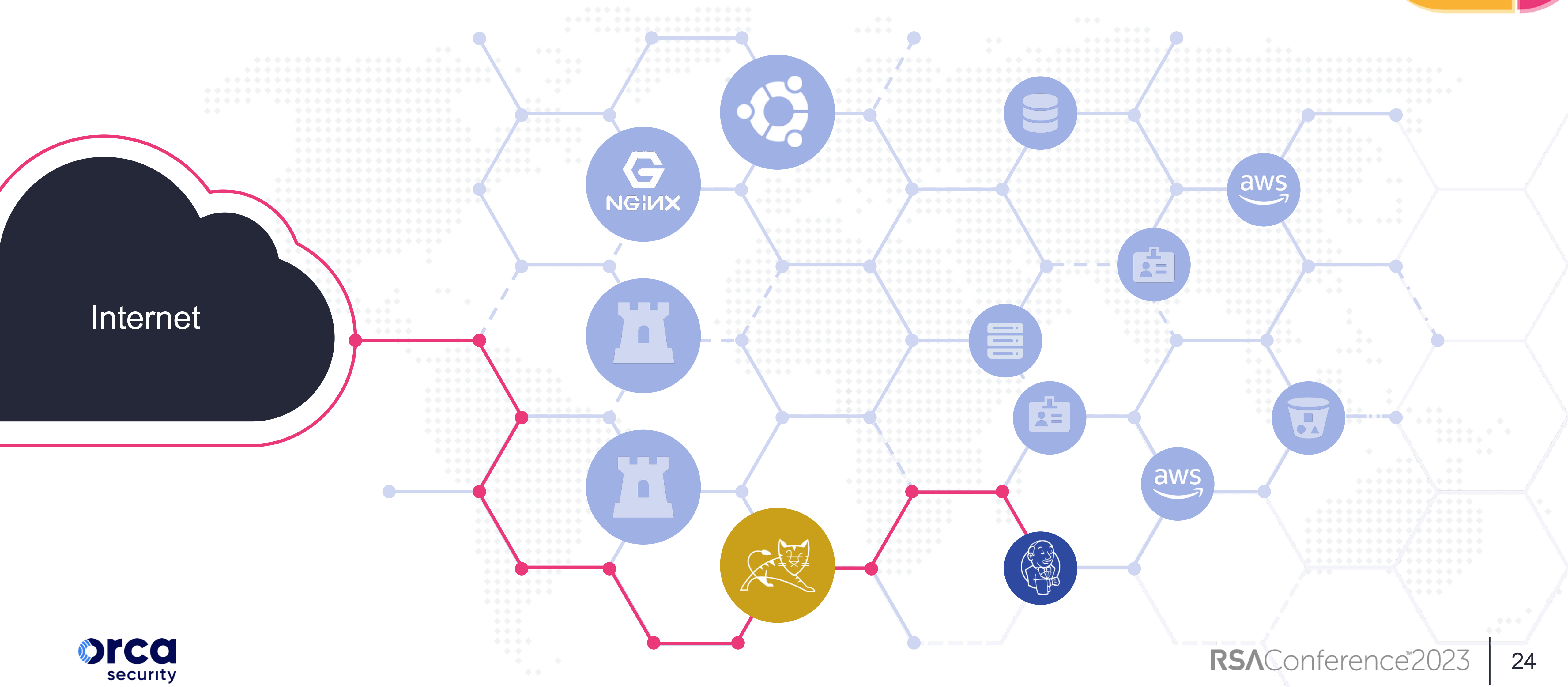
Compromised bastion, *plus* PII (management view)

PII Identification Initiative

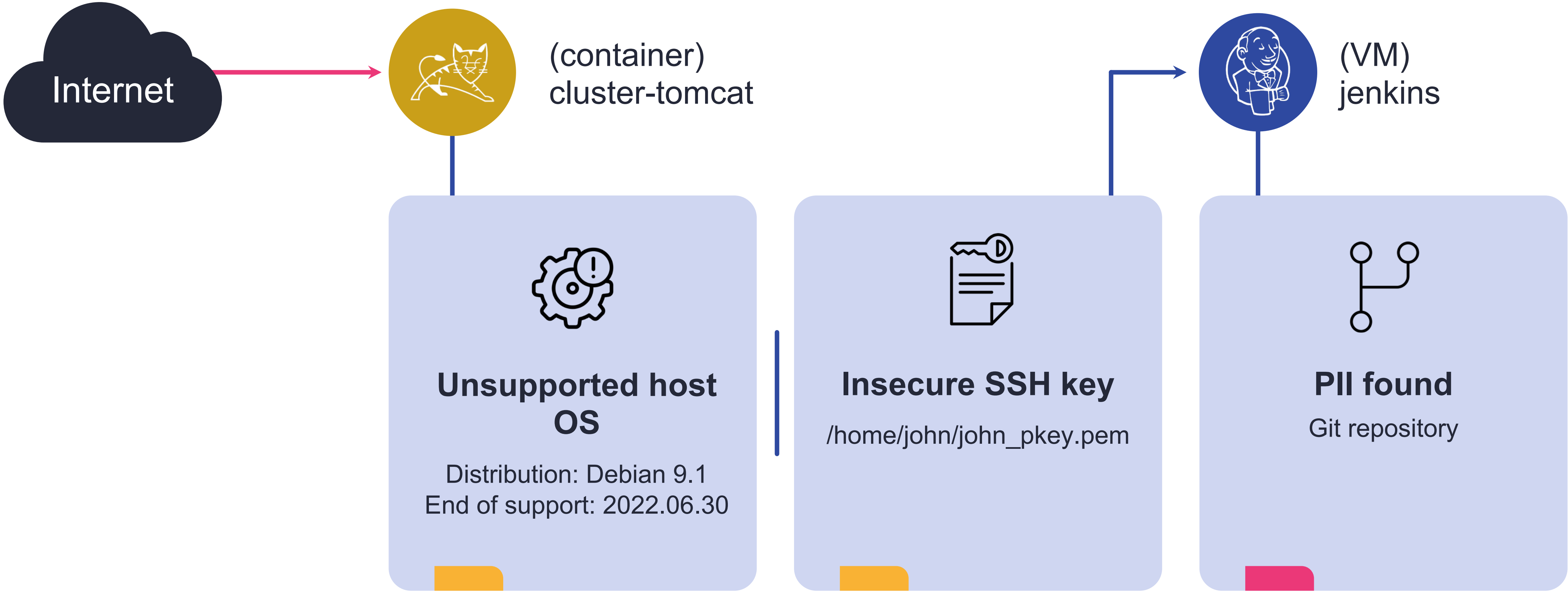
Unacceptable Loss	Hazards	Initiative
Customer Data Stolen	PII stored in many cloud datastores Highly privileged accounts in widespread use	Identify locations of sensitive data in cloud servers. Remove/restrict access to support the principle of least privilege.

See also: **Malware Cleanup *Incident***
Cloud Identity Entitlements Management Initiative

Unsupported Internet-facing OS (full view)



Unsupported Internet-facing OS (attack path view)



Unsupported host OS

Distribution: Debian 9.1
End of support: 2022.06.30

Insecure SSH key

/home/john/john_pkey.pem

PII found

Git repository

Unsupported Internet-facing OS (management view)

System Support Initiative

Unacceptable Loss	Hazards	Initiative
Loss of IP – code repository	Assets without owners become neglected over time Neglected assets are unsupported by vendors	All systems to have designated DevOps owners, to support/maintain systems Tracking systems to identify and escalate failures

See also: **Software Vulnerability Management Initiative**

Going from attack paths to initiatives:

Unpatched machine

Software Vulnerability Management

Administrator role accessible

Cloud Identity Entitlements Management

Compromised bastion server

Malware Cleanup

Compromised bastion + PII

PII Identification

Unsupported host OS

System Support

Apply What You Have Learned Today

Identify your risks

- **Map out** critical attack paths in your environment

Understand your hazards

- Evaluate **common elements** of your attack paths to solve structural problems
- Define appropriate controls to **mitigate** the risk

Elevate the conversation

- Tell **simplified stories** about exemplars of your risk
- Drive **effective projects** with executive buy-in

RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

SESSION ID: MASH-M03

Telling Fairy Tales to the Board: **Turn Attack Graphs into Business Stories**

#RSAC

Andy Ellis

Advisory CISO, Orca Security
Author, 1% Leadership
@csoandy

Oren Sade

Chief of Staff,
Orca Security

Find us later in the show

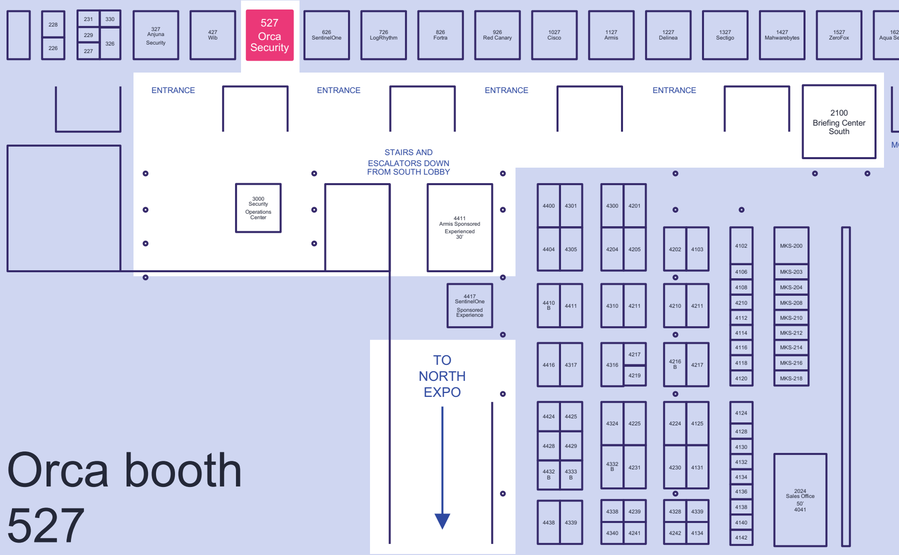
#RSAC

Stronger Together

Cocktail reception

tomorrow night at the Terra Gallery

Andy will be signing his book at the RSAC bookstore, today from 12:00 to 12:30



Orca booth 527

RSAConference2023

San Fransisco | April 24-27 | Moscone Center

SOUTH EXPO

Welcome reception tonight
(first 75 in line get a free signed copy of 1% Leadership)