
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT011

SPONSORED BY JUPITERONE

Reducing exposure in the cloud

Mauricio Ruiz

Solutions Architect
JupiterOne

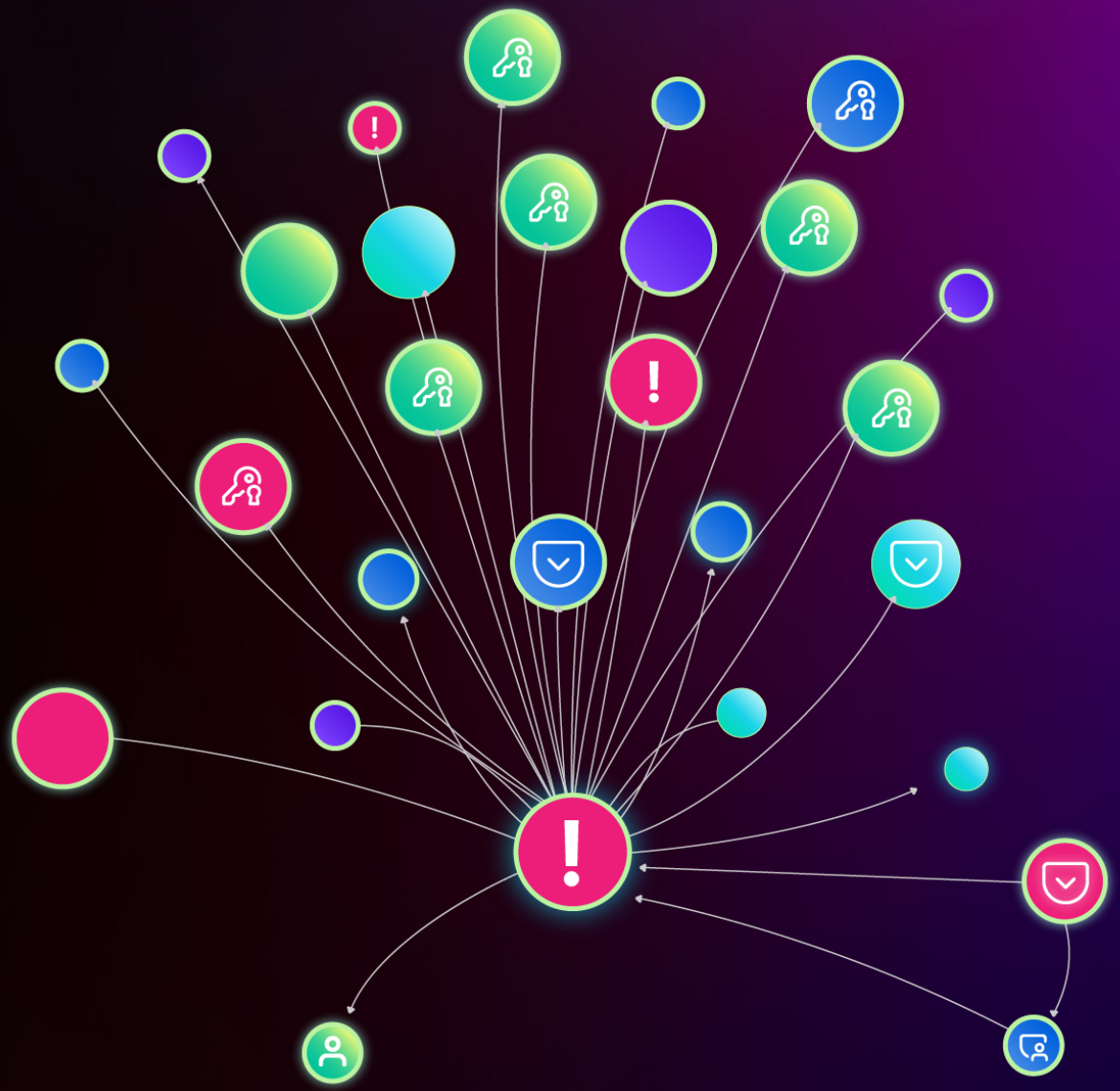
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The modern challenge

In the age of cloud, **assets** are

- More than just IP-based devices
- Software-defined and ephemeral
- Highly complex relationships that connect people, process, and technology

Asset management is not just for security – it is the foundation to everything in cyber governance, compliance, and engineering



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud security trends

Security teams have many assets to secure . . .

27%
companies

are now using more than one public cloud

79%
companies

have experienced at least one cloud data event

165K+
cyber assets

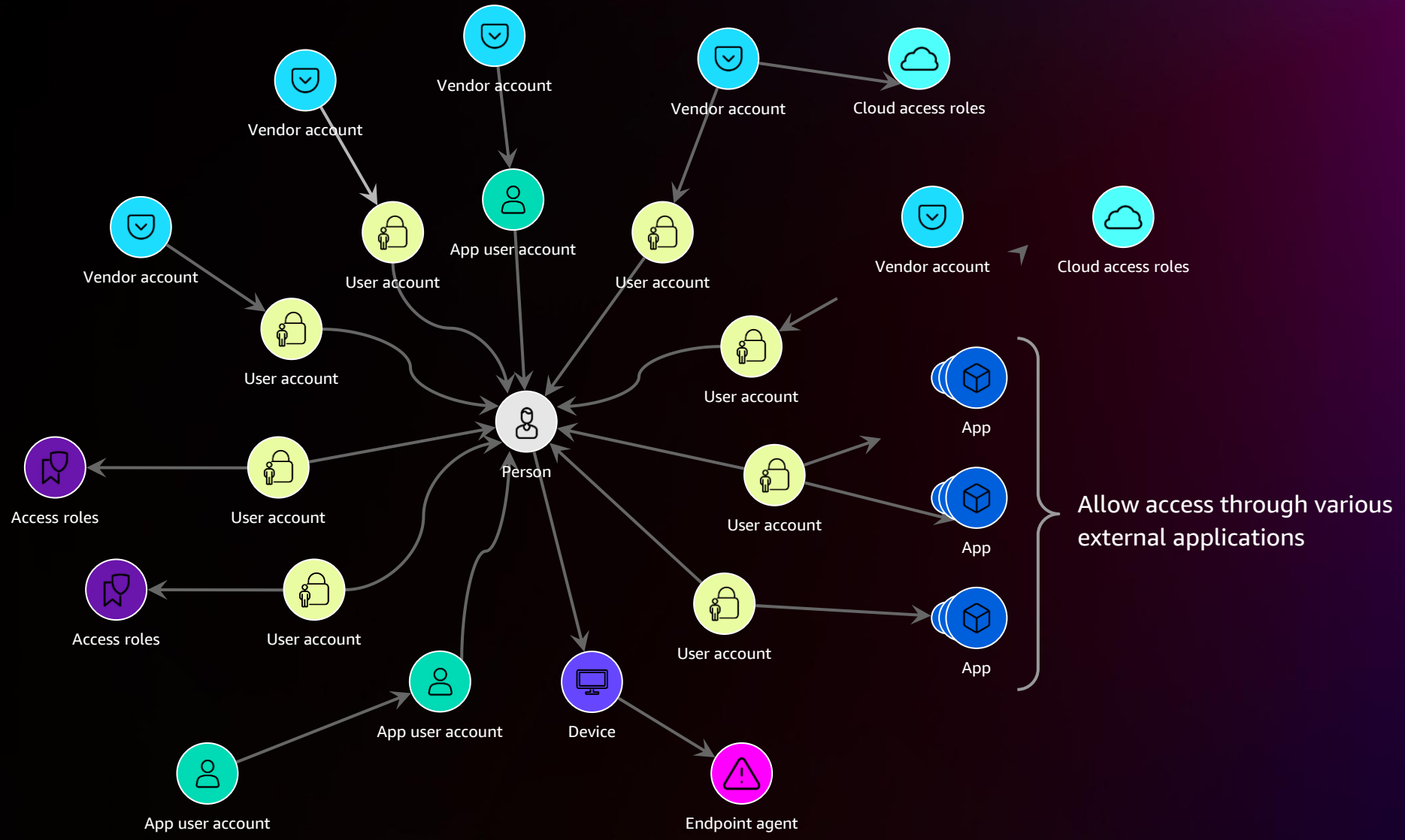
in the average asset ecosystem that the security team is responsible for

130+
security tools

that the average enterprise uses –
A lot of point-solution security tools

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cyber asset visibility: Connecting the dots



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is cyber asset attack surface management (CAASM)?

Enables security teams to solve persistent asset visibility and vulnerability challenges. Enables organizations to see all assets (internal and external) through API integrations with existing tools, query against the consolidated data, identify scope of issues and gaps in security controls, and remediate them.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

180+
existing products and service integrations

JupiterOne



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why graphs matter for security professionals

Just 0.2% of the attack surface is internet-exposed

67% of attack paths are deleted each month

Security teams are racking up some big wins

Recognize “communities“ in your security graph that hold predictable paths for unauthorized users

Increase the tempo of surface and path turnover to maintain security

Lists are not inherently worthless

Lists are ideal, but they must be built and ranked using graphs, especially LRE/GRE correlation metrics

Prune your graphs, but don’t rely on connectivity as a definitive risk measure

Reduce global risk exposure, particularly for critical assets

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What makes JupiterOne different?



Cloud-native agentless API-first platform

Integrates with CSPs, IDPs, dev/workflow, endpoint security, event management, etc. tools



Graph DB

We provide a graphical analysis of how customer assets relate to one another



J1 QL

Almost 600 prebuilt queries that are easy for our customers to use



Monitoring, accurate alerts, and insights

No noise – Create alerts and insights that matter

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ask questions, get answers from your data

Simple ones

- Are my Amazon S3 buckets encrypted?
- Which buckets do not have access logging enabled?
- What are the production instances?
- Are there backups configured for my databases?

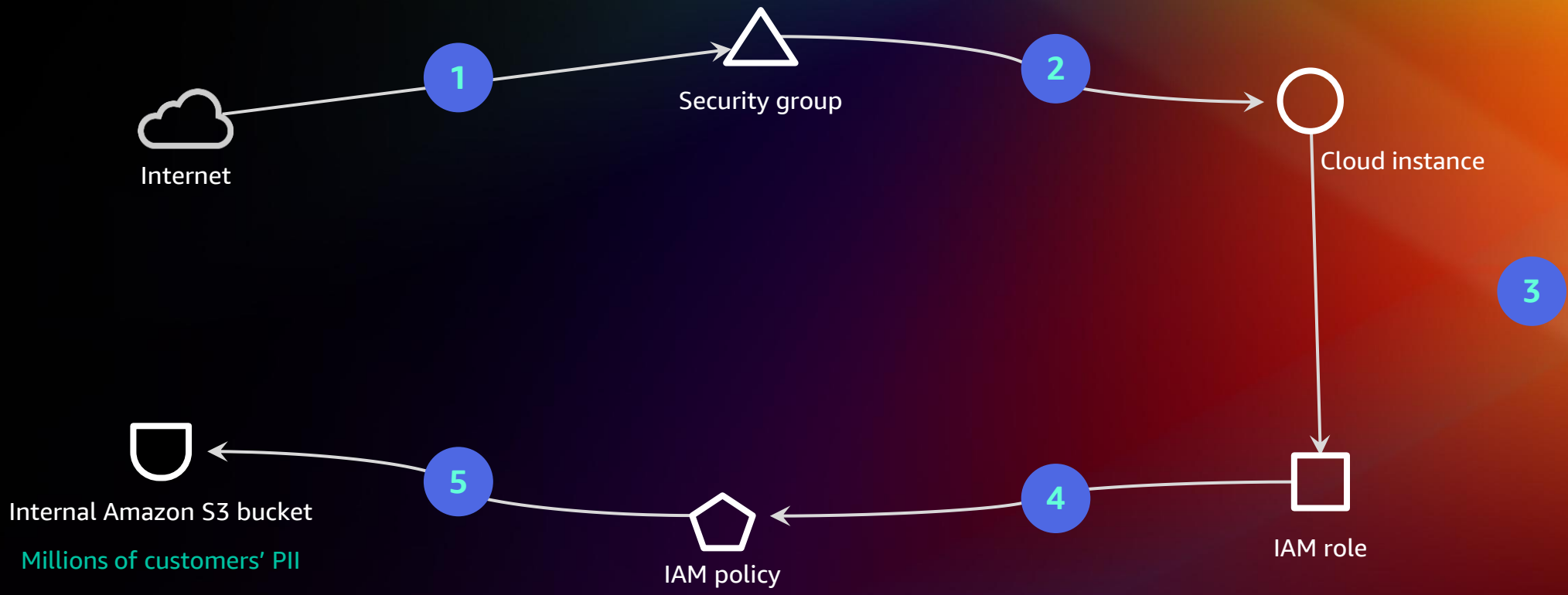
Complex ones

- Are there internet-facing Amazon EC2 instances that are allowed access to non-public Amazon S3 buckets?
- Are there cross-account IAM trust relationships to external/vendor accounts?
- Which PRs/developers introduced new security findings this past week?

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cyber asset attack surface management



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The reason JupiterOne exists



Cyber asset visibility and governance

e.g., inventory of ephemeral devices, cloud workloads, applications, code repos, users, and access



Security operations & engineering

vulnerability management, incident response, appsec



Cloud security posture mgmt.

configuration monitoring, policy-as-code, violation and drift detection



Governance, risk & compliance

audits, evidence collection, metrics, and reporting

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Mauricio Ruiz
mauricio.ruiz@jupiterone.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.