tenable

Securing the Cloud: Putting Identity at the Center

Cloud Security Without Identity Isn’t Cloud Security at all

Alex Feigenson
Global Technical Director
August 25th, 2025

99%

Of the organizations that suffered cloud-related breaches **cited identities and permissions risk as the cause**.

- Tenable 2024 Cloud Security Outlook

tenable

Old Threats, Old Defenses

Securing your Infrastructure, Last Millenium style

tenable

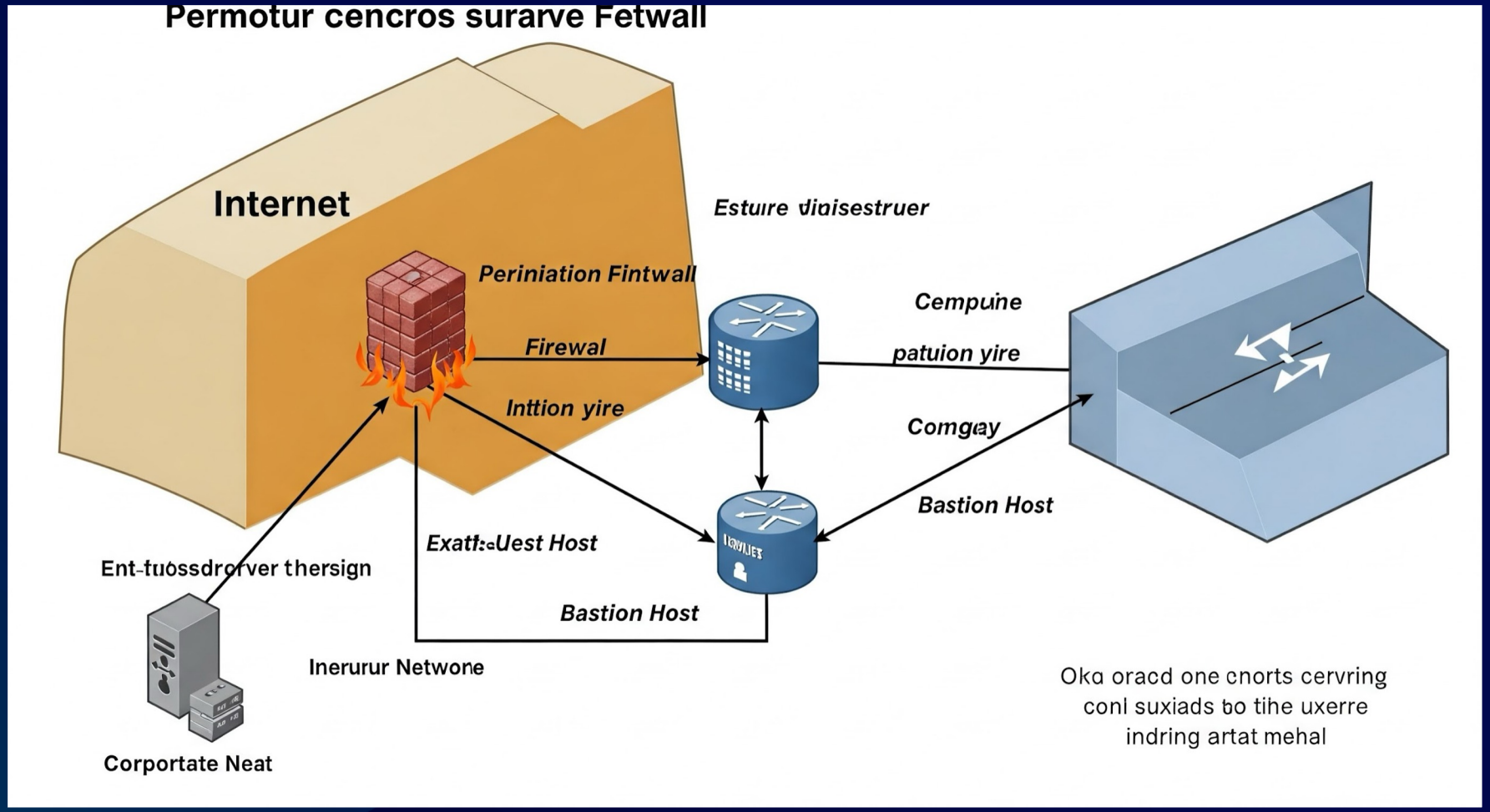
New Threats, New Defenses

Gunpowder and Cannons

Bastion Fort
(built ~1600 AD)

tenable

State of the Art Security (Before the Cloud)



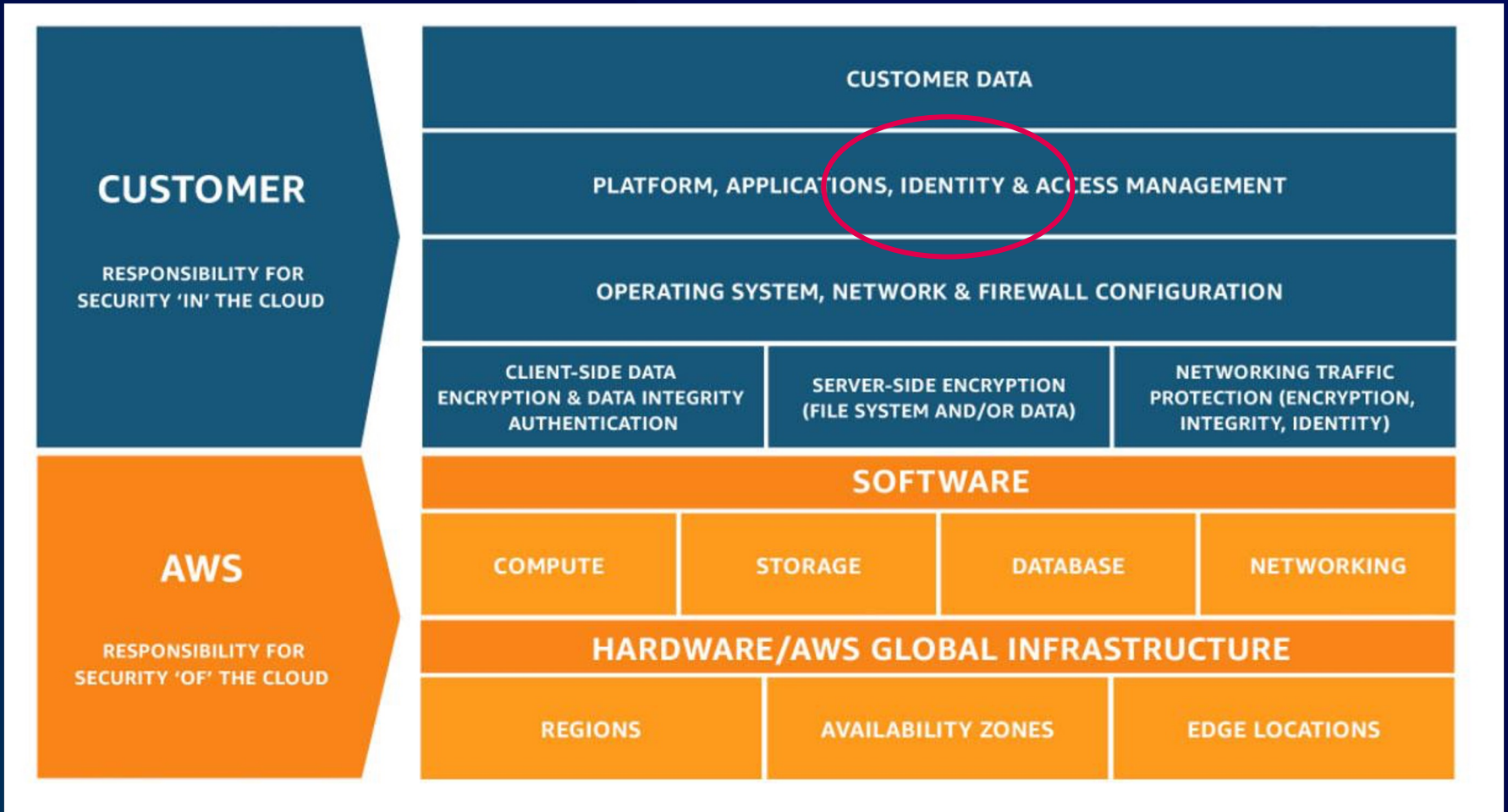
tenable

So what has changed?

Old World	Cloud
Everything is yours to manage	Shared responsibility model
3-5 year server purchases (CapEx)	-as-a-Service model (OpEx)
Hand-crafted, artisanal, custom systems	Lots of cookie cutters
Months to get a new system	Minutes to get a new system
Many different vendor APIs	One API (per Cloud Service Provider)
Networking is the perimeter	Identity is the [new] perimeter

In short, EVERYTHING.

Amazon Web Services Shared Responsibility Model



tenable

AWS IAM Concepts

who (identity) has *what access* (role) for *which resource*

Created by Julian Wiegmann - November 2022 V1

Notes:
Terminology used is official AWS terminology.
For IAM concept details see official AWS documentation
This is not an exhaustive list of security tips/risks around IAM!
Nor covers all Identity features/services in AWS

Can use AWS Organizations service control policy (SCP) to limit the permissions of root user

SCP

Organization
Optional

AWS Organizations helps you centrally govern your environment as you scale your workloads in AWS

Manage & Use

SCP - Service Control Policy

Organization policy to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization.

Contains & Manage

Security credentials are account-specific

AWS Account

AWS account is a container for your AWS resources.
You create / manage your AWS resources in an AWS account, & provides administrative capabilities for access and billing

Full Control over
Root can close account

Contains

Manage

Resources (Service)
EC2, S3 etc.

Can use

Access control lists (ACLs)

Cannot be used to control access for a principal within the same account.

Authorization 2
Similar to resource-based policies, although they do not use the JSON format. Amazon S3, AWS WAF, and Amazon VPC key services that support ACLs.

Signed (authenticated) or unsigned (anonymous) you can configure and not just read. Full control & write to a storage bucket for example are possible. depends on service

Do not use for day2day tasks

Don't create long-term access keys for your root user. If malicious user gains access to your root user access keys = game over

Root User
Email & Password

Cannot use

Manages

AWS IAM
Not a regional service

Contains

IAM Resources

Root is also a Principal

Roles are both a Principals & Resources

Policies are attached to Principlas

Manage

Person or application
Principals include federated users and assumed roles

Principals
Sometimes called Identities

Type

Type

Type

Authentication happens here
IAM Entities / Identities (User or Role)

Group
User Groups

Contains

Use Groups to assign permissions not individual users

User
Account ID / alias
user name

Doesn't have to represent an actual person; you can create an IAM user in order to generate an access key for an application that runs in your corporate network and needs AWS access

Requires Policy

AssumeRole

Role
A role is intended to be assumable by anyone who needs it

Cross Account and Cross Service is possible and Confused Deputy Problem

You can allow Roles to assume other Roles. Role Chaining

Humans can authenticate with these keys

API based access using access keys

AKIA
Access Keys
Access key ID + Secret Access Key

Key known to the creator of the key and consumer (if used by 3rd party). Do not expire

Max two access keys per user (for rotation)

Humans can authenticate with these keys

ASIA
Access Keys
Access key ID + Secret Access Key + expire time

These temporary credentials are called via AWS STS (right?) AssumeRole

Often abused with IMDS v1 SSRF. E.g. vuln webapp can call role creds and attacker can use

Special Type of Policies

Permission Policy
What can role do

Trust Policy
Principal
(who can assume role!)

You can specify ANY user or even whole other AWS accounts to access resources here!

Not Policies managed in Policies but under Roles but "same"

Subtypes

AWS Service Role
For AWS services to use to do their function

EC2 Service Role
For apps running on EC2

AWS Service Linked Role
predefined by the service include all the permissions

Federation
Oauth, SAML 2.0
(external IDP)

Policies that are attached to a single user, group, or role

Attached here for Roles

Unless Inline

Types

AWS Managed
~998 Policies Exist

Careful with "FullAccess" Policies

AWS managed policies don't grant least privilege permissions. (this is what AWS says in their documentation. Take note other CSPs

Customer Managed
You define

Have their own ARN e.g. arn:aws:iam::aws:policy/IAMReadOnlyAccess

Authorization

Policies
(Permission Policy)
All JSON policy

Type

Not the same

Resource Based Policy
For Services/Resources

Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship.

Some service. You can specify ANY user or even whole other AWS accounts to access /edit/ use resources here! This is not a Role!

You specify who has access to the resource and what actions they can perform on the resource

Type

Not recommended by AWS for Users

Are always of type

Control what actions the identity can perform, on which resources, and under what conditions

Identity Based Policies
Attached to an Identity

Type

Inline Policies

Policies that are embedded directly into a single user, group, or role OR Resource

Type

Managed Policies

You can specify who has access to the resource and what actions they can perform on it

Support

Permission Boundaries

A policy that sets the maximum permissions an IAM entities can have

For Users or Roles. NOT Groups!

IAM JSON Policy

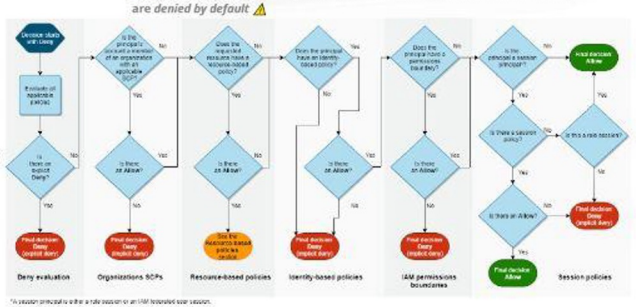
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteInstanceProfile",
        "iam:UpdateAssumeRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListRoleTags",
        "iam:PutRolePermissionsBoundary",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:DeletePolicy",
        "iam:AttachRolePolicy",
        "iam:ListInstanceProfilesTags",
        "iam:DetachRolePolicy",
        "iam:CreatePolicyVersion",
        "iam:SetDefaultPolicyVersion"
      ],
      "Resource": [
        "arn:aws:iam::959321979655:group/*",
        "arn:aws:iam::959321979655:user/*",
        "arn:aws:iam::959321979655:instance-profile/myserver_*",
        "arn:aws:iam::959321979655:policy/*",
        "arn:aws:iam::959321979655:role/*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "210.75.1.1"
        },
        "DateLessThan": {
          "aws:CurrentTime": "2025-06-30T23:59:59Z"
        }
      }
    }
  ]
}
```

Used throughout AWS IAM policies.
Over ~13 000 permissions (actions) exist for the services. Action is allow statement but NotAction (deny) also exist. This can be combined with 'Effect' Deny. E.g. Deny IAM* except Multifactor was done.
Scope can be defined on resources.
Wildcards are possible throughout.
Conditions can use Boolean expressions.
Can include things like "must MFA before allow"

If a single permissions policy includes a denied action, AWS denies the entire request and stops evaluating. This is called an *explicit deny*. Because requests are *denied by default*

Policy evaluation logic

This is key



The New Perimeter Is Exploited in Almost Every Breach

EXTERNAL ATTACK SURFACE

LATERAL MOVEMENT

DESIRED OUTCOME

Exploit Identity

Exploit Asset

Gain initial privileges

Repeat Process

Elevate & take action

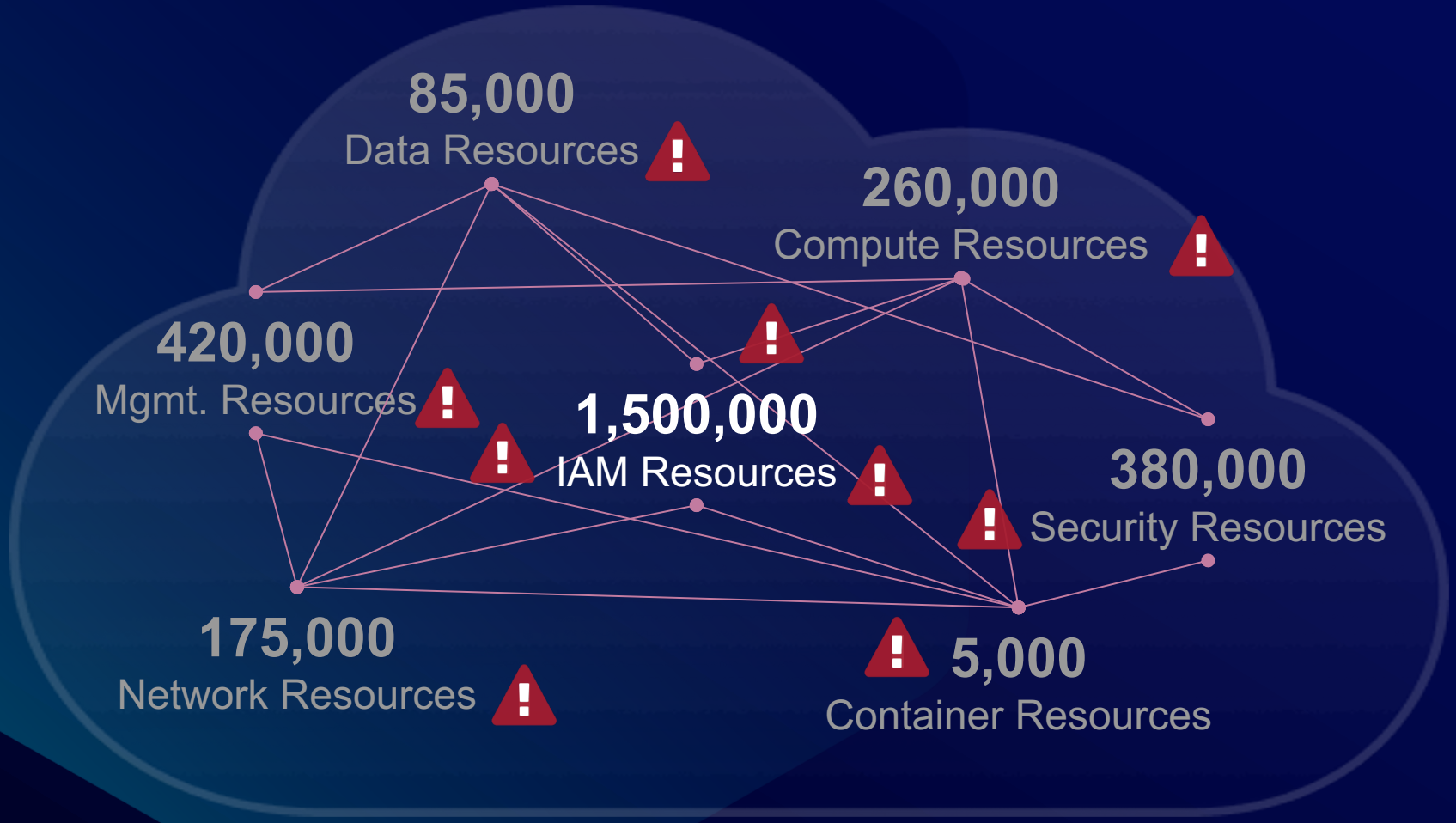
Exfiltrate Data

Extort Ransom

Disrupt Operations

tenable

Securing Identities, Entitlements, Permissions Is Difficult



Fortune 250 Company

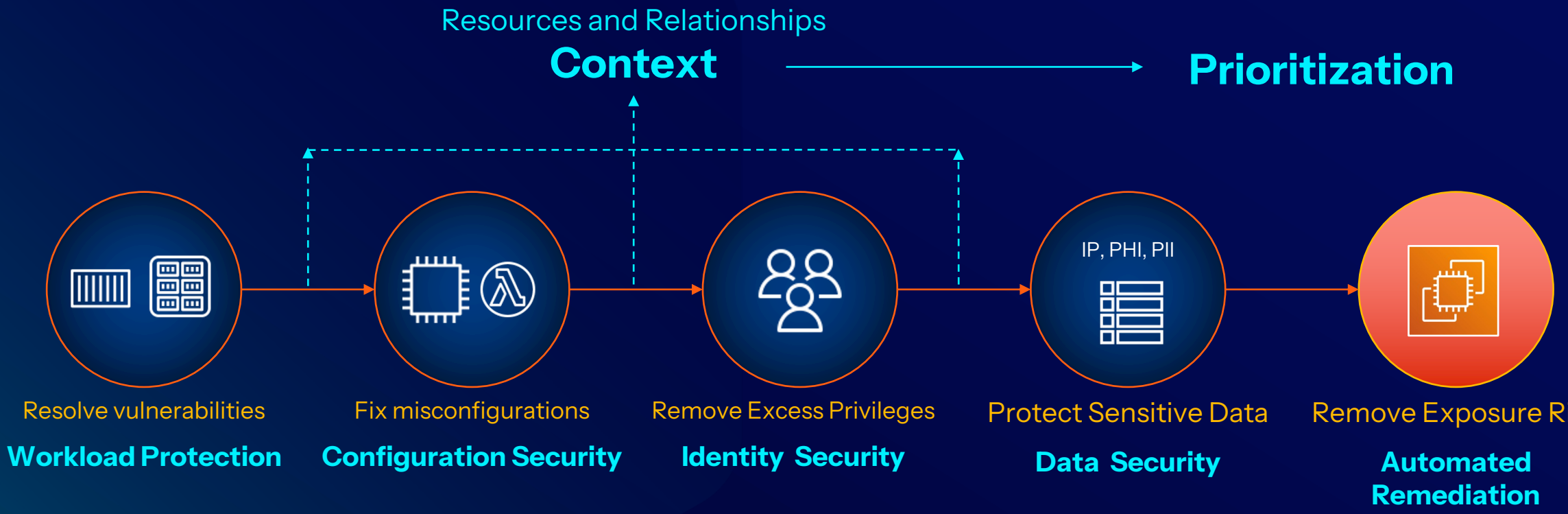
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "FirstStatement",
      "Effect": "Allow",
      "Action": ["iam:ChangePassword"],
      "Resource": "*"
    },
    {
      "Sid": "SecondStatement",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Sid": "ThirdStatement",
      "Effect": "Allow",
      "Action": [
        "s3:List*",
        "s3:Get*"
      ],
      "Resource": [
        "arn:aws:s3:::confidential-data",
        "arn:aws:s3:::confidential-data/*"
      ],
      "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
    }
  ]
}
```

Policy example:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

tenable

How Tenable Cloud Security provides answers

From Visibility, Context, and Prioritization to Remediation



[Tenable Cloud Security] is clear, intuitive, provides valuable context and analysis, and is an extremely powerful tool towards analyzing and addressing security risk in an organization's cloud environment."

tenable

Tenable Cloud Security

Use Cases

➔Expose, prioritize & resolve misconfigurations

➔Assess and meet compliance standards

➔Deep, accurate, accessible visibility

➔Protect sensitive data

➔Streamline security operations

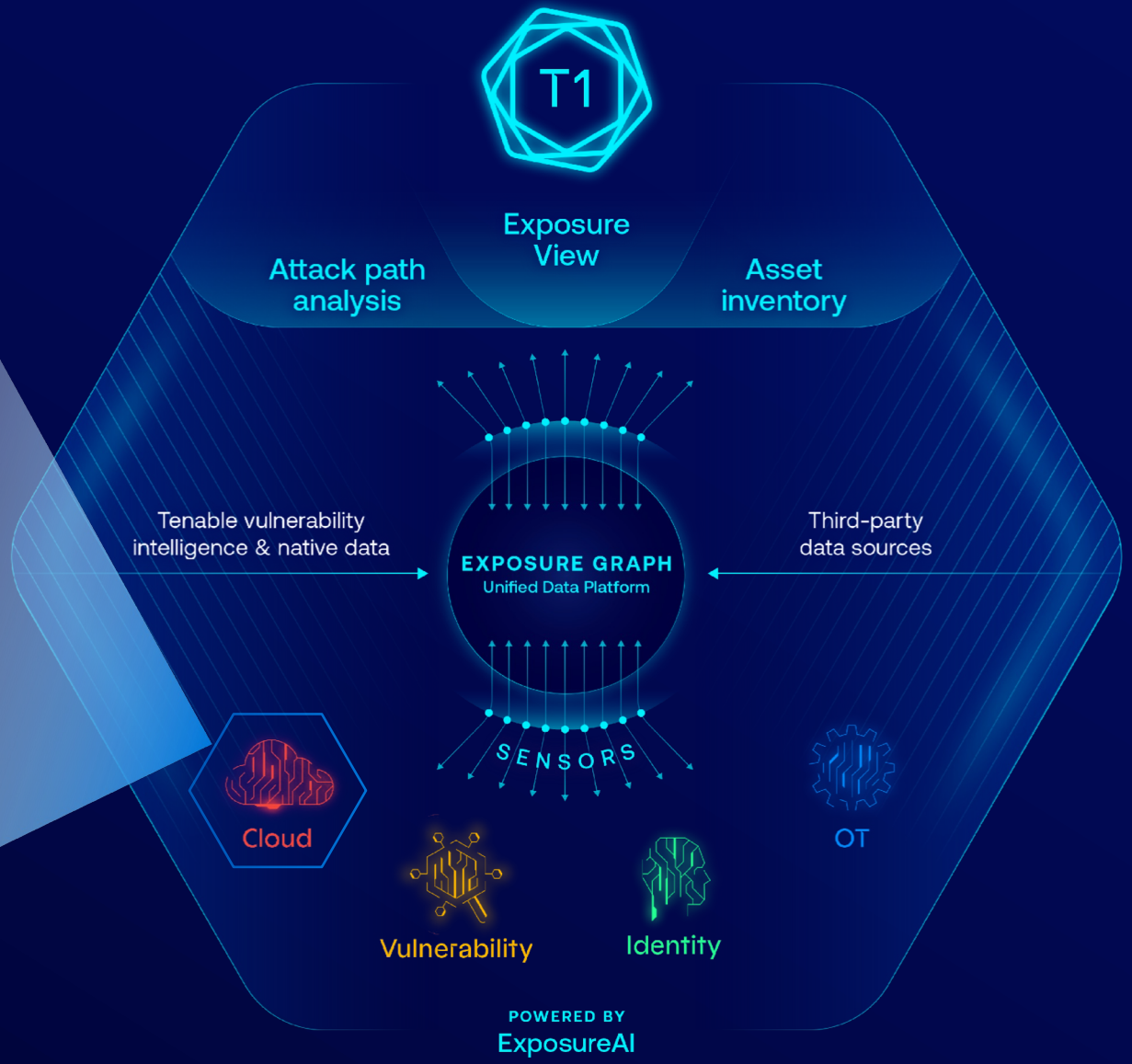
➔Achieve least privilege for cloud identities

➔Minimize exposure to vulnerabilities and malware

TENABLE CLOUD SECURITY WITH TENABLE ONE

Exposure Management Enterprise Wide

Public cloud, hybrid, on premises and OT environments



tenable

Tenable One

The world's leading AI-powered exposure management platform

UNIFY VISION

See all your assets & risks across the attack surface

UNIFY INSIGHT

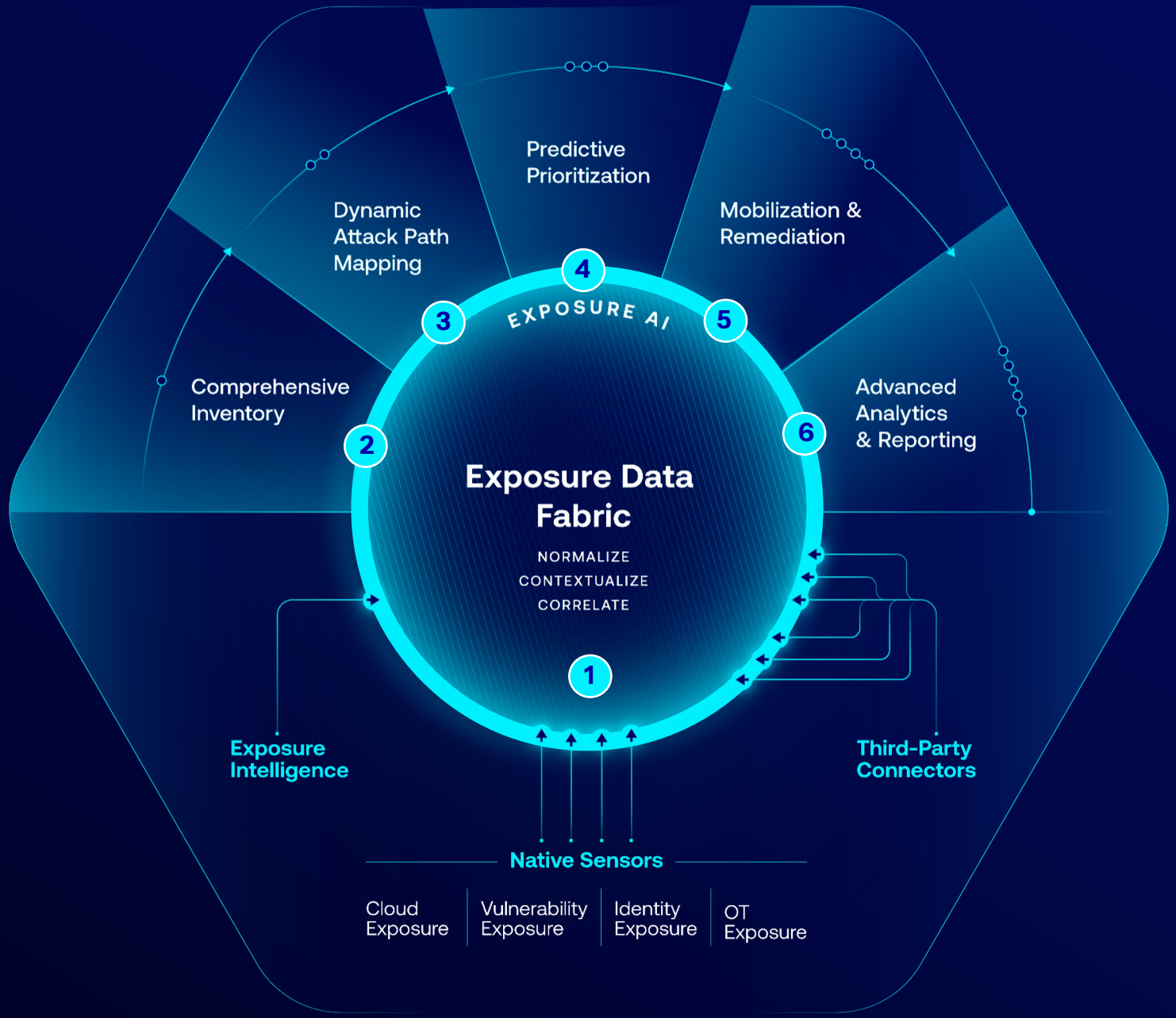
Gain critical context to prioritize true exposure

UNIFY ACTION

Mobilize response across teams to eradicate risk

3rd Party Data | IT / Private | Unseen / Ext. Facing | Web Apps | Multi-Cloud | OT / IoT | On Prem Identity | Cloud Identity

tenable



Tenable One

delivers comprehensive exposure management

tenable