Microsoft

Real World Lessons

from 18 months of Cloud Infrastructure Entitlement Management (CIEM) implementations in the Enterprise

Bailey Bercik /in/baileybercik
Mark Morowczynski /in/markmorow
Product Managers – Microsoft

Agenda

What is CIEM?

What we find

Getting to least privilege

Go-Do's

CIEM: Cloud Infrastructure Entitlement Management

"The challenge of managing privileges in IaaS is worsening, with thousands of services added in recent years by cloud providers. Security and risk management leaders must combine traditional IAM approaches with CIEM to achieve efficient **identity-first security** management results."

- Gartner

Cloud infrastructure entitlement management (CIEM) offerings are:

- Specialized identity-centric SaaS solutions focused on managing cloud access risk via administration-time controls for the governance of entitlements in **hybrid and multicloud** IaaS.
- Typically use analytics, machine learning (ML) and other methods to **detect anomalies** in account entitlements, like **accumulation of privileges**, **dormant and unnecessary entitlements**.
- CIEM ideally provides remediation and enforcement of **least privilege** approaches.

- Gartner

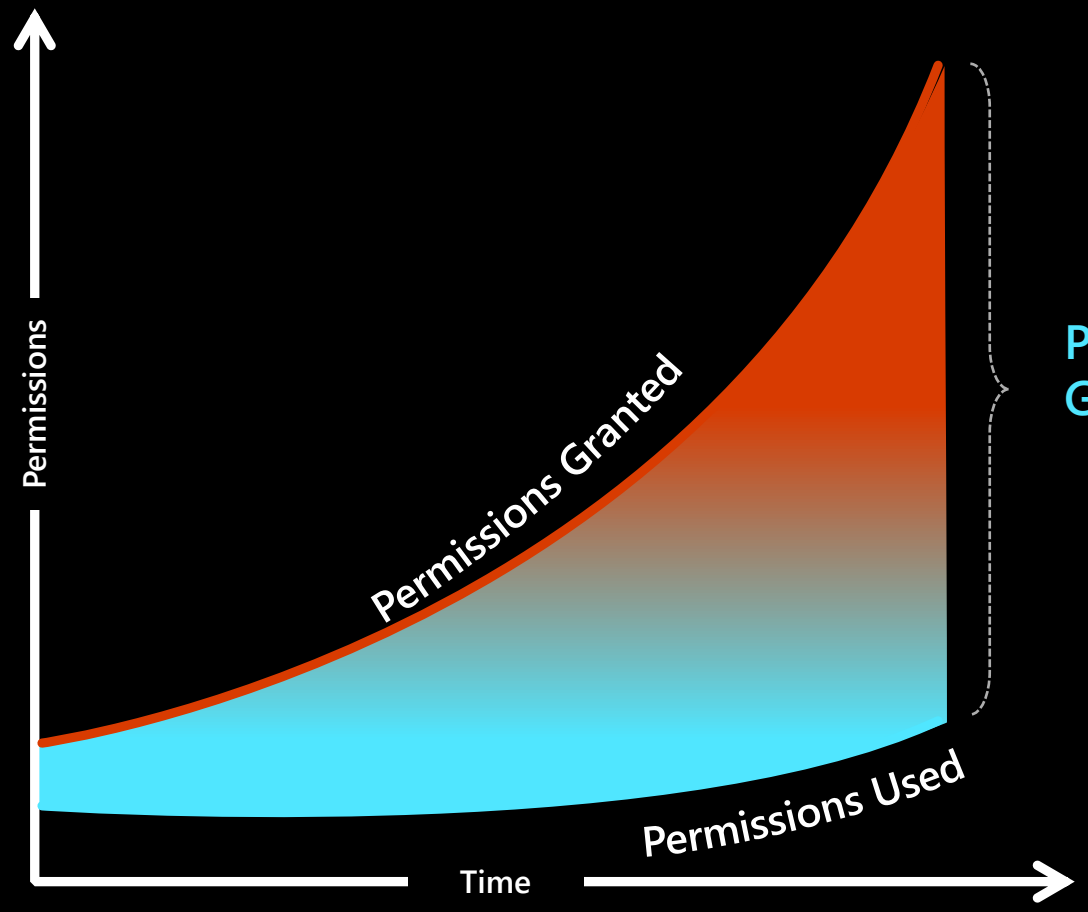
(Multi-)cloud adoption brings new permission challenges

Exponential growth of identities, machines, functions, and scripts operating in the cloud infrastructure

>90% of identities are using **<5% of permissions** granted

>50% of permissions are high-risk and can cause catastrophic damage

Unmanaged permissions are expanding the attack surface



Permissions Gap

Lack of comprehensive visibility into identities, permissions and resources

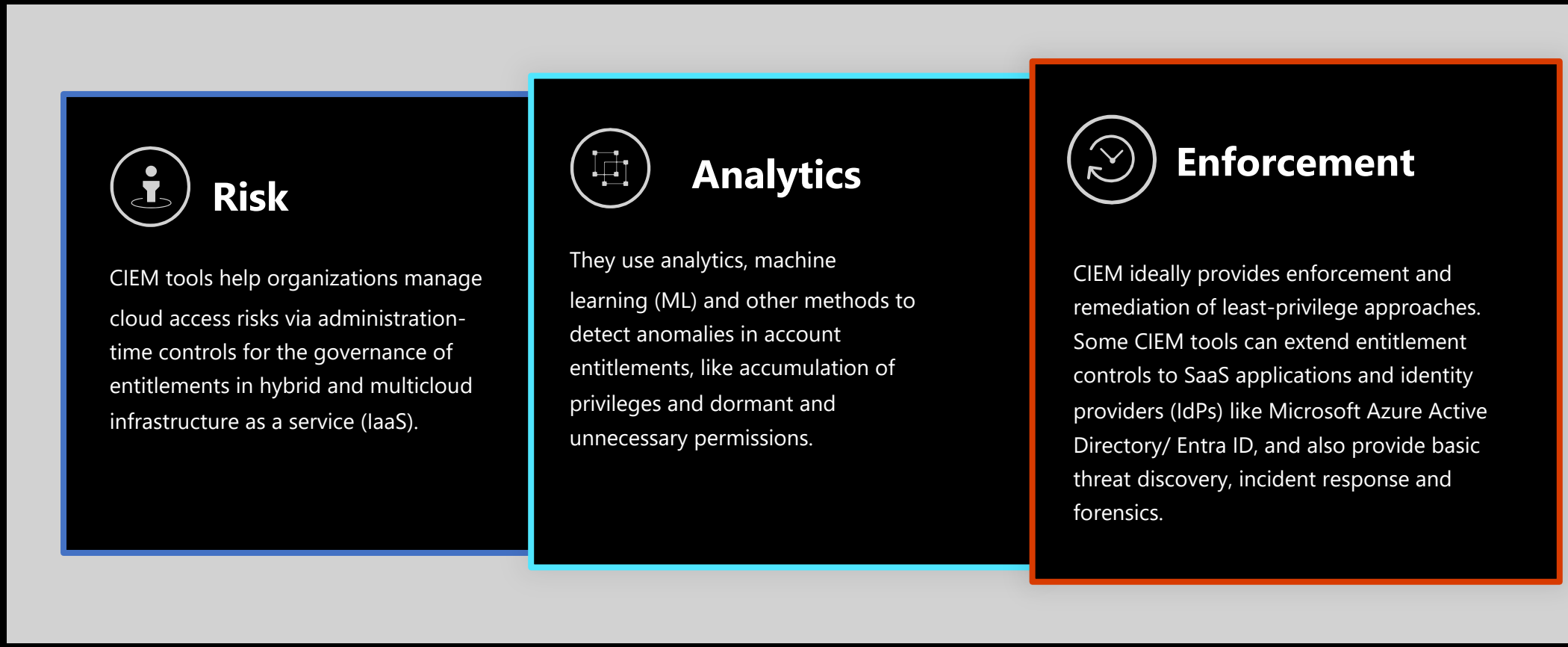
Increased complexity for IAM and security teams to manage permissions across multicloud environments

Increased risk of breach from accidental or malicious permission mis-use

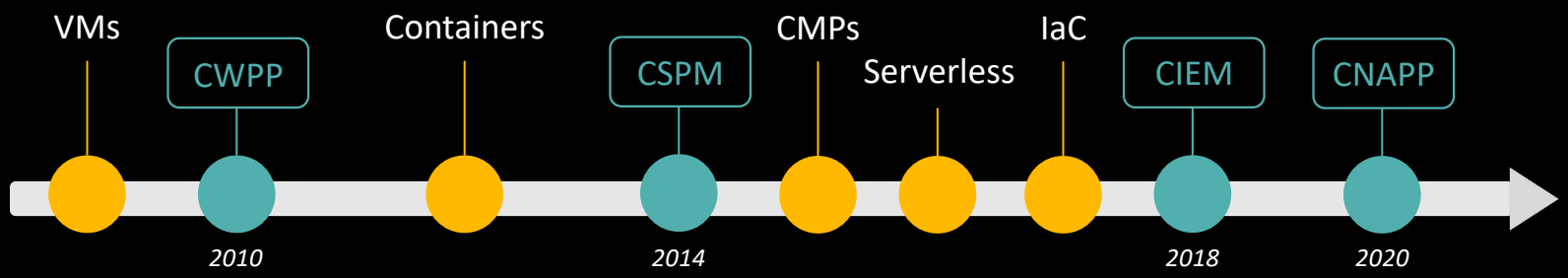
What are the *common* challenges?

- Permissions granted based on broad job roles and responsibilities
  - Common to grant broadest permissions that could ever be needed by a role or team
  - Not based on what tasks each person will **actually perform**
- IAM admins manually grant permissions which are not time-bound
  - Permission requirements **change over time** – not enough admins in the world to keep up with the pace of change in most enterprises. Users will naturally accrue more and incorrect permissions as time goes on
  - Compromised account can be used to wreak havoc, especially if attacker can phish an MFA credential
- Permission clean-up is done manually on an as-needed basis
  - Access review processes are manual, time-consuming, and usually **all or nothing**
  - Hard to gain deep enough insights into actual usage to do real **least privilege** right-sizing
  - Hard to operationalize if processes are too manual – permission right-sizing not performed frequently enough

How does a CIEM help?

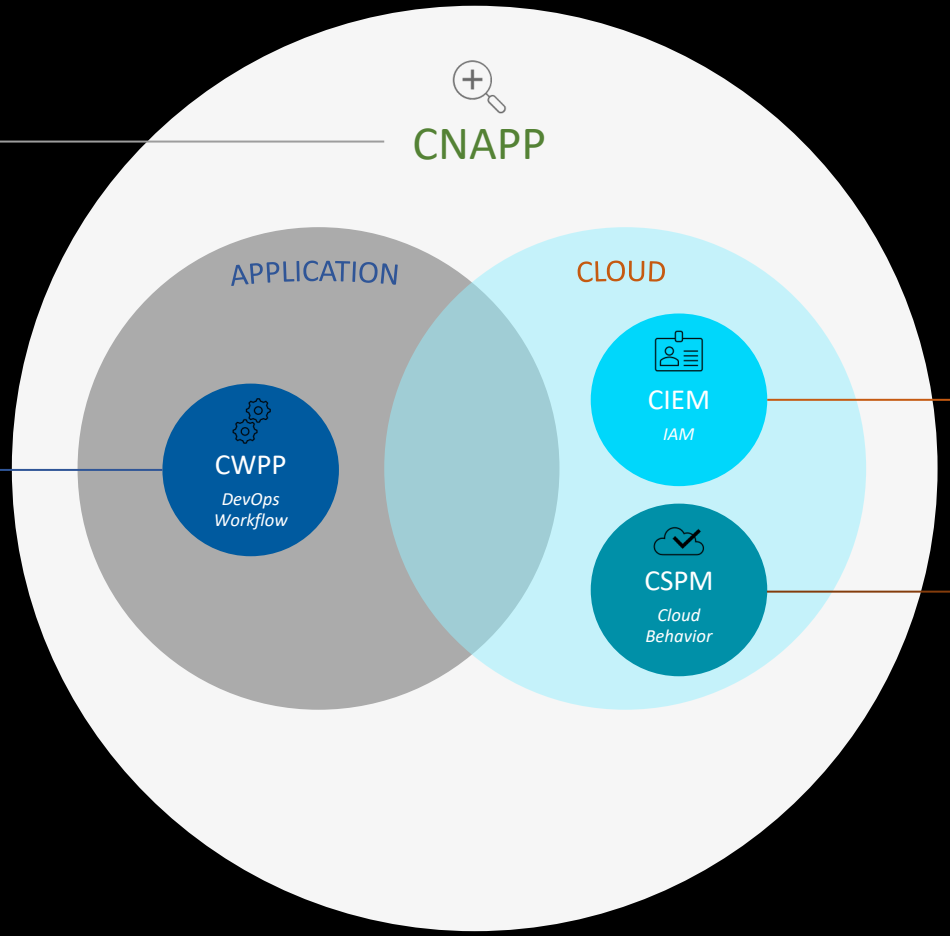


How does a CIEM solution fit in with your other tech?



Cloud Native Application Protection Platforms
Provides a holistic view of cloud security risks by scanning workloads and configurations in development and protecting them at runtime. Secures applications by identifying, assessing, prioritizing, and adapting to risk in cloud-native applications, infrastructures, and configurations.

Cloud Workload Protection Platform
Endpoint protection solutions tailored to server workloads wherever they are running today (VMs, public cloud IaaS, PaaS, etc.).



Cloud Infrastructure Entitlement Management
Manages identities and access privileges in multi-cloud environments, applying the principle of least privilege access to cloud infrastructure and services while identifying anomalies in account entitlements.

Cloud Security Posture Management
Leverages native API integrations with IaaS cloud service providers to discover and assess risks of cloud assets and configuration.

Agenda

What is a CIEM?

What we find

Getting to least privilege

Go-Do's

Common CIEM Stakeholders

- Identity team
- Cloud Infrastructure team: Architects and Operations team for Azure, AWS, and GCP environments
- InfoSec team: Architects and Operations
- Security Assurance / Audit team
- Target resource technical owners (e.g. administrators/developers)
- Incident Response team (you'll see in a minute)

What We're Told Before We Start

- We don’t have exposed ports
- We don’t have any exposed storage
- We use tool (Azure ARM/AWS CloudFormation/Terraform) so it will be consistent
- We **will** have overprivileged **users**

What We Find

- We have exposed ports
- We have exposed storage
- We have inconsistency despite using (Azure ARM/AWS CloudFormation/Terraform)
- We have overprivileged **users, groups and apps**
  - Some are even Global Admin/root/Super Admin
  - This is why we have the incident response team listed
    - The IR process now starts!

After the Incident Response: Quick Wins

- Clean up Inactive
  - Users
  - Groups
  - Apps/Functional Accounts
- Open Ports & No Resources - Network Security Groups, Security Groups or GCP VPC
- Users with MFA not enabled
- Unused IAM Access Keys
- IAM Access keys greater then 90 days

Immediate Alerting and Monitoring Needs

- Focus on what you're trying to take action on right **NOW**
- Catch any new 'super accounts'
- First time using high set of permissions
- 'Failures' can be strong SOC signal, Crown jewel monitoring
  - Ex: KeyVault access failed. **Why?**

Agenda

What is a CIEM?
What we find
Getting to least privilege
Go-Do's

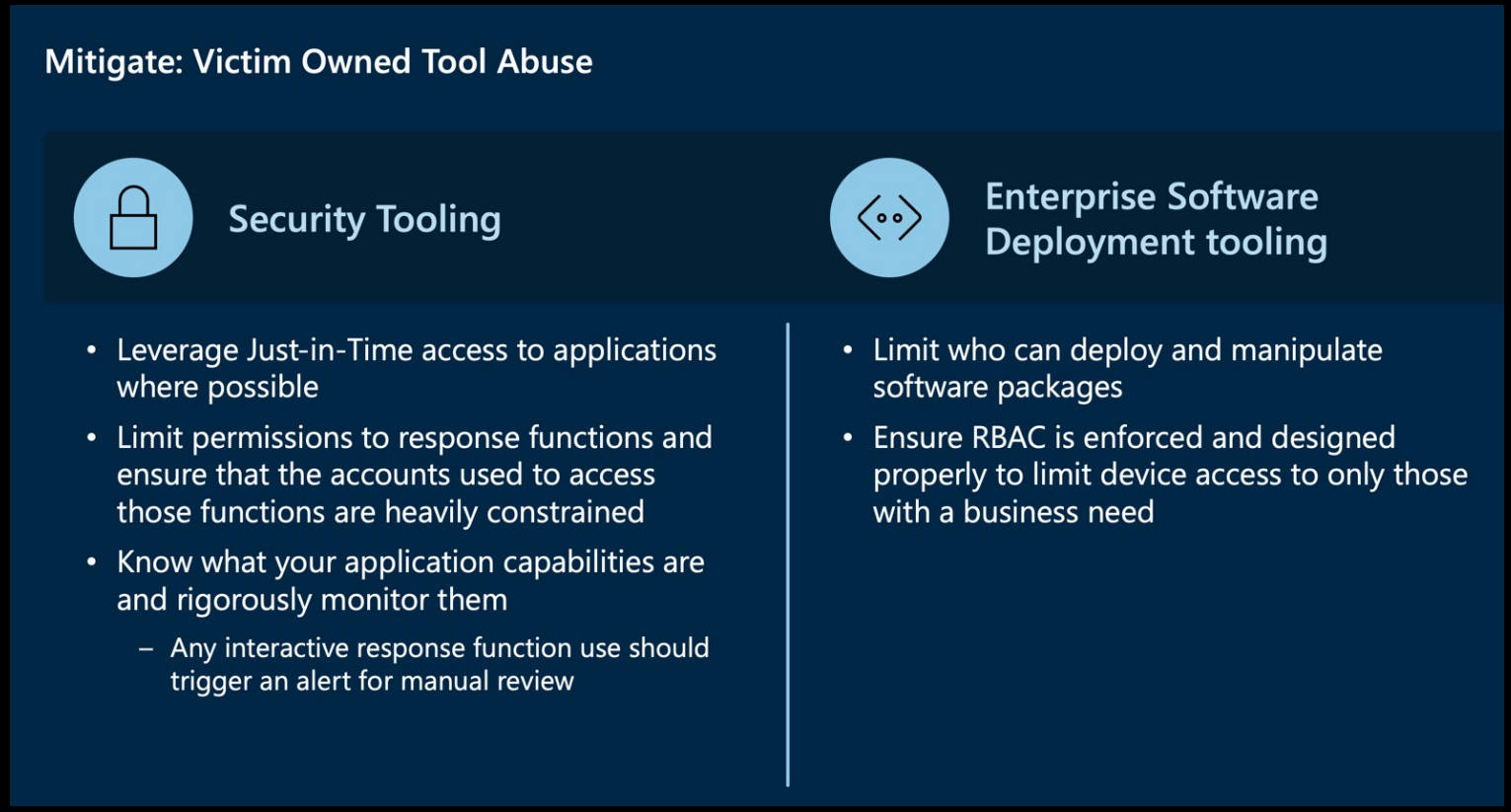
The Road to Least Privilege (Plan)

- Find the right stakeholders & be aware of seasonal access
- Start with non-human accounts
  - Repeatable access patterns/least likely to change
  - Super workload identities (serverless functions, apps, etc)
  - Access to crown jewel resources
- Human accounts with high privilege move to JIT/JEA
  - Not ‘taking away’ permissions, just no standing access...
  - Monitor usage, eventually ‘take away’ entirely
- How did we get here? Policy improvements (Owner access is given to ‘their stuff’)
- Show improvement to leadership, repeat/keep going.
  - This is going to take a while. Any improvement is good!

Upcoming Blog Post: Octo Tempest

Talk last week at Bluehat about threat actor Octo Tempest (formerly Storm-0875)

Watch Blog: aka.ms/SansSecuritySummit/OctoTempest



Framework & Process (Day 0 –30)

- Define owners and inventory of the problem space
  - Typical owners: infosec
  - Understand the scope and risk

- Determine process/permissions for NEW resources
  - Typical owners: infosec & cloud infrastructure
  - Don’t add to the current problem

- Determine permission creep reduction strategy
  - Typical owners: infosec
  - Goals and risk reduction

Monitoring & Tracking (Day 30-60)

- Reporting for key stakeholders
  - Typical owner: infosec
  - Where we are as an org, next to remediate, risk that will be reduced

- Any changes in past permission behavior
  - Typical owner: infosec & cloud infrastructure
  - Confirm new permissions will meet requirements, no breaking changes

- Additional security monitoring
  - Typical owner: SOC
  - Additional insights and alerts to consume

Remediate & Operationalize (Day 60-90)

- Remediate & right size permissions
  - Typical owner: infosec & cloud engineering
  - Drive down permission creep to target levels

- Implement permissions on demand
  - Typical owner: infosec & cloud engineering
  - Process to onboard users, request/approval flow process for roles/templates

- Operationalize
  - Typical owner: infosec & cloud engineering
  - Regular cadence to review and report permissions, update processes (repeat)

Agenda

What is a CIEM?
What we find
Getting to least privilege
Go-Do's

Go-Do's

- You probably have gaps in your CSPM coverage, find & remediate
- Do you have an organization CNAPP strategy?
  - Read the cloud permissions risk report (aka.ms/StateOfCloudPermissions2023)
- Who are the key stakeholders, start to socialize this problem space
- Look to run a trial/POC, understand the scope & risk
- Start with non-human identities
  - Repeatable access patterns
- Think about new policy/process, mindset change
- Get this full deck at aka.ms/SANSDeck2023