Identity Blind Spots

How they quietly expand your attack surface

Olav Helland
Co-founder & Cloud Architect

bsure.

What we'll cover

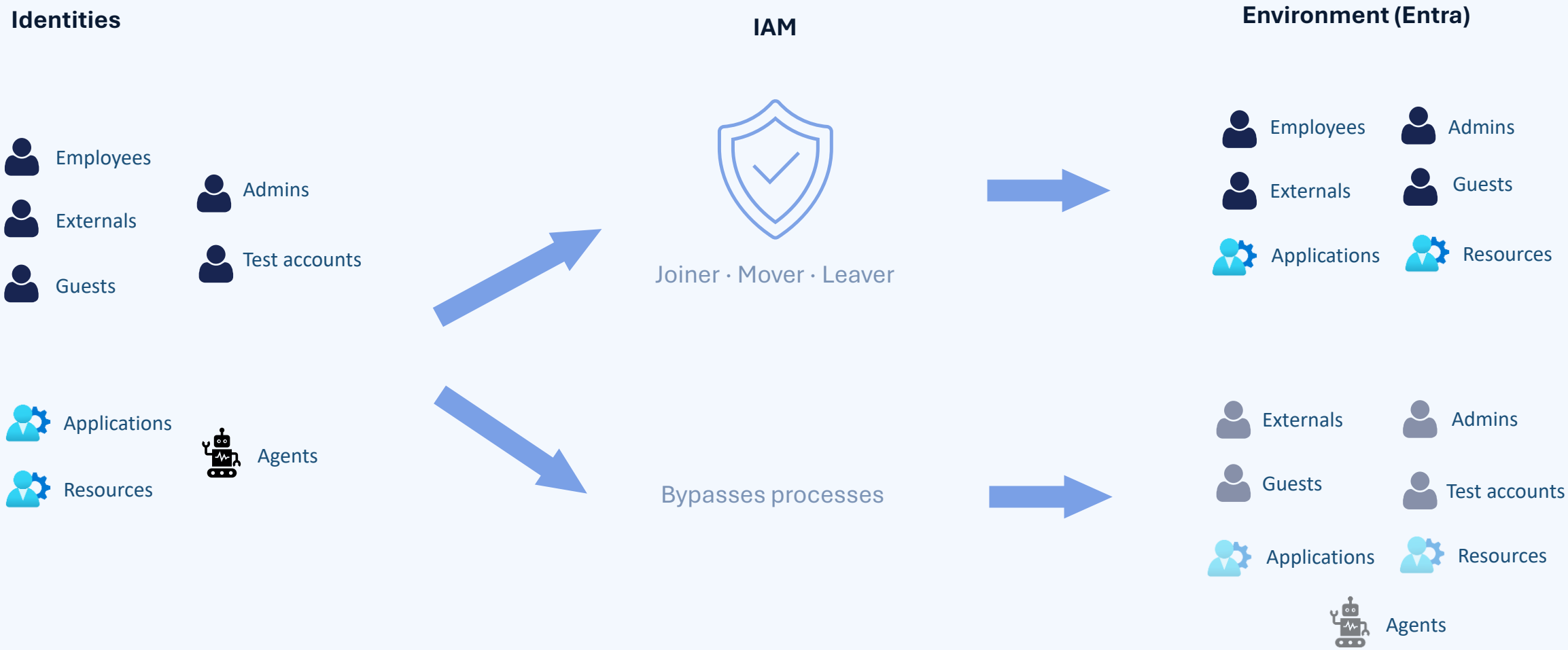
1 How identity blind spots emerge

2 Four common blind spots

3 What this looks like in a real environment

How identity blind spots emerge

Not all identities follow the same path



Blind spot #1

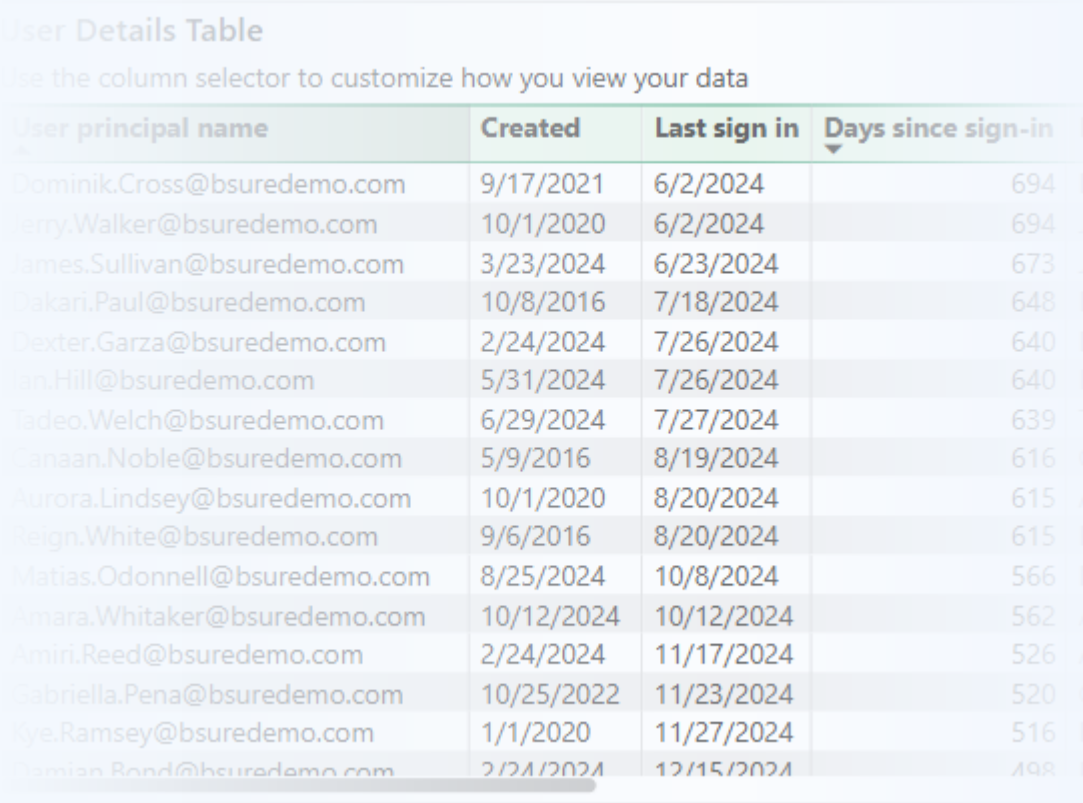
Inactive / orphaned accounts

Inactive identities that still have access

- No recent sign-in
- Still enabled
- Still has access

➡ **20-40%**

of identities in a typical tenant are inactive



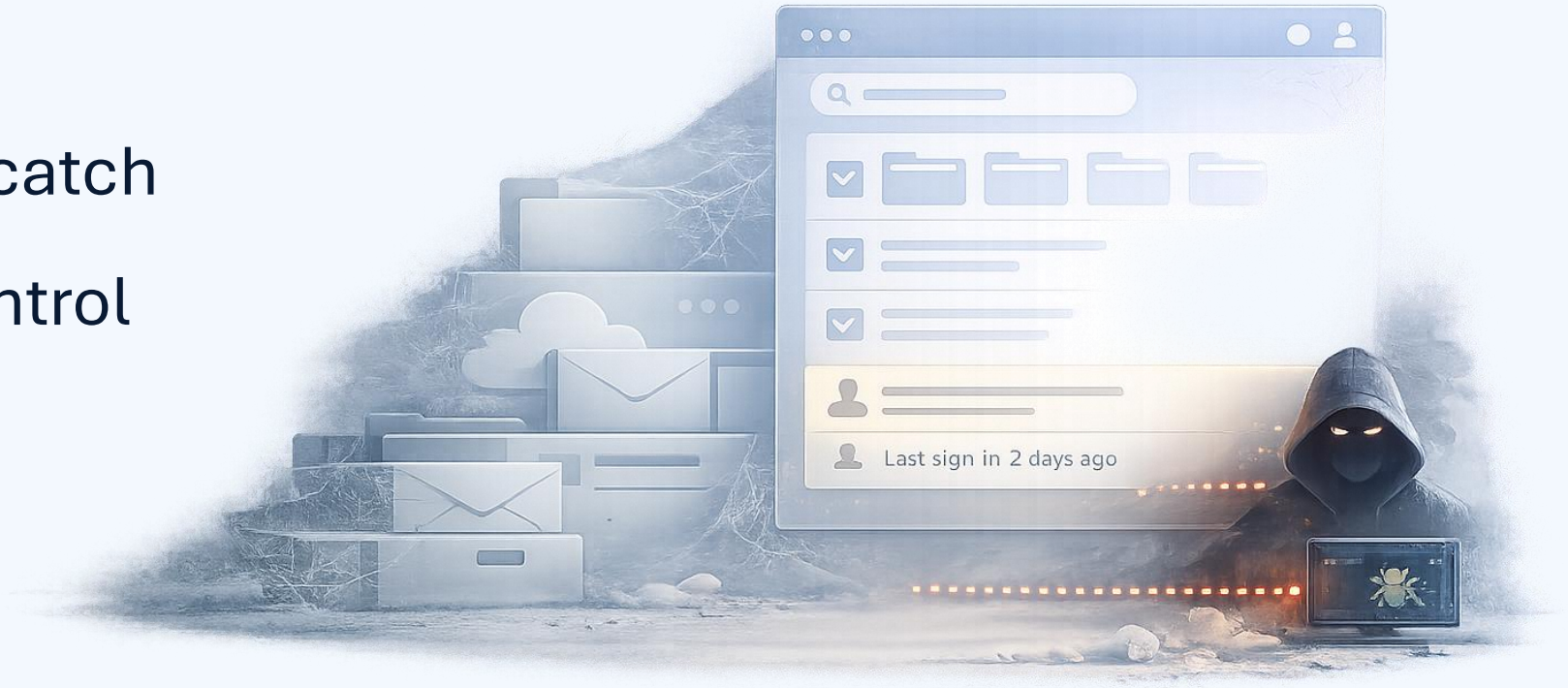
User Details Table

Use the column selector to customize how you view your data

User principal name	Created	Last sign in	Days since sign-in
Dominik.Cross@bsuredemo.com	9/17/2021	6/2/2024	694
erry.Walker@bsuredemo.com	10/1/2020	6/2/2024	694
ames.Sullivan@bsuredemo.com	3/23/2024	6/23/2024	673
akari.Paul@bsuredemo.com	10/8/2016	7/18/2024	648
Dexter.Garza@bsuredemo.com	2/24/2024	7/26/2024	640
an.Hill@bsuredemo.com	5/31/2024	7/26/2024	640
adeo.Welch@bsuredemo.com	6/29/2024	7/27/2024	639
anaan.Noble@bsuredemo.com	5/9/2016	8/19/2024	616
Aurora.Lindsey@bsuredemo.com	10/1/2020	8/20/2024	615
eign.White@bsuredemo.com	9/6/2016	8/20/2024	615
Matias.Odonnell@bsuredemo.com	8/25/2024	10/8/2024	566
mara.Whitaker@bsuredemo.com	10/12/2024	10/12/2024	562
Amiri.Reed@bsuredemo.com	2/24/2024	11/17/2024	526
abriella.Pena@bsuredemo.com	10/25/2022	11/23/2024	520
ye.Ramsey@bsuredemo.com	1/1/2020	11/27/2024	516
Damian.Bond@bsuredemo.com	2/24/2024	12/15/2024	498

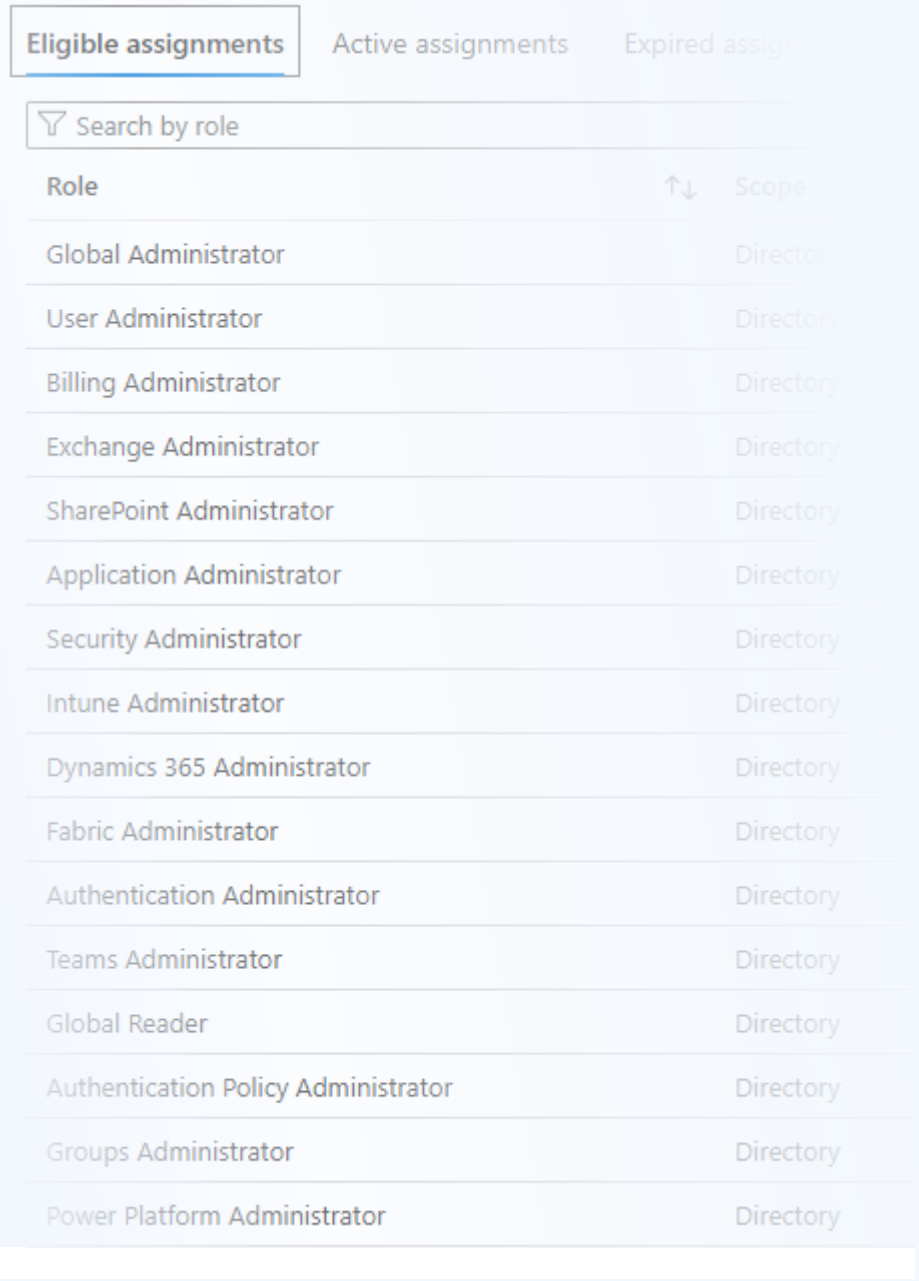
Why this matters

- No owner. Still has access
- Risk you don’t see
- Misuse you don’t catch
- Cost you don’t control



Blind spot #2

Excessive privileged access



What we see in Entra

- Permanent admin roles
- Global Admin used daily
- Roles assigned “just in case”
- Admin roles on «normal» user accounts
- Orphaned and inactive admin accounts

Why this matters

- **One compromised admin account is enough**

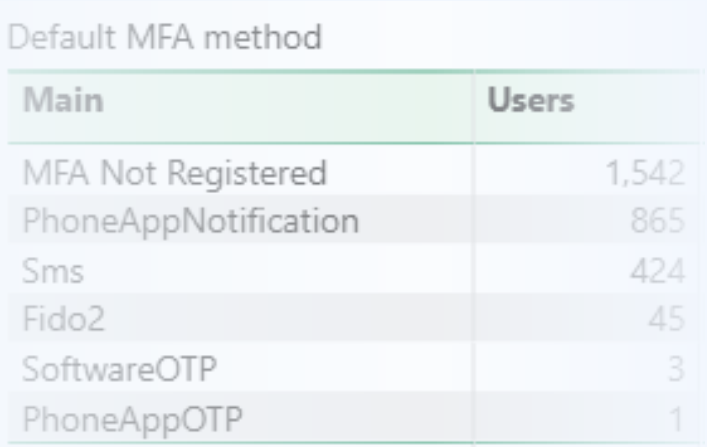
- Activity looks legitimate
- No clear signal of misuse
- Immediate full tenant impact

Blind spot #3

Incomplete MFA enforcement

What we see in Entra

- Conditional Access gaps and exclusions
- Users not registered for MFA
- Security info registration not controlled
- Weak MFA for privileged users



Default MFA method

Main	Users
MFA Not Registered	1,542
PhoneAppNotification	865
Sms	424
Fido2	45
SoftwareOTP	3
PhoneAppOTP	1

How MFA gaps get used

- No MFA challenge
  - A policy gap let’s sign-in through
- MFA prompt approved
  - Phishable MFA gets accepted
- Session becomes trusted
  - Access continues without challenge
- Impact expands
  - Privileged access increases blast radius

Blind spot #4

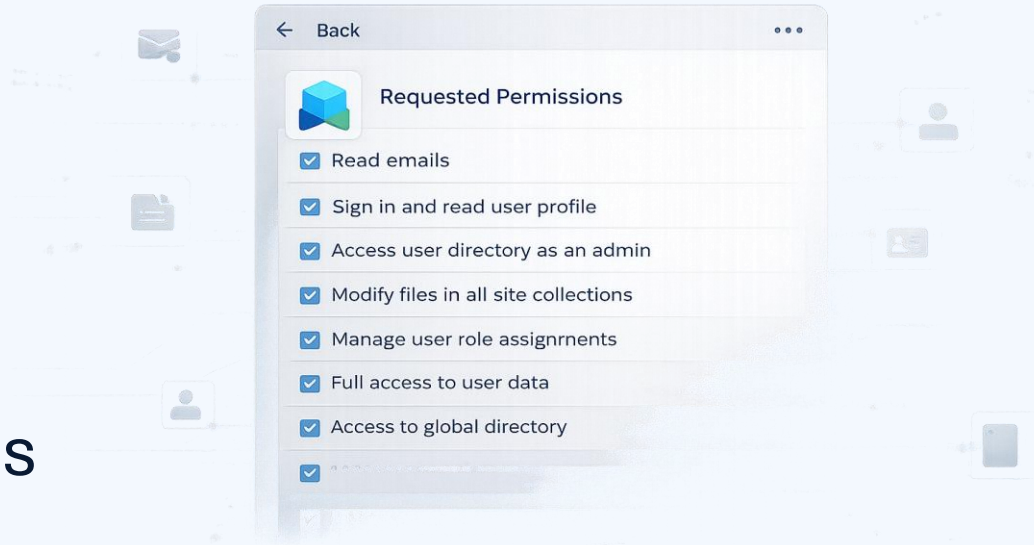
Over-privileged apps and agents

Common patterns we see

- Apps and agents with broad Graph permissions
- Unused and orphaned
- Secrets instead of certificates
- No clear ownership

How app access gets used

- Consent phishing
- Apps become a path to privilege
- Secrets added or reused
- Over-privileged apps expand blast radius

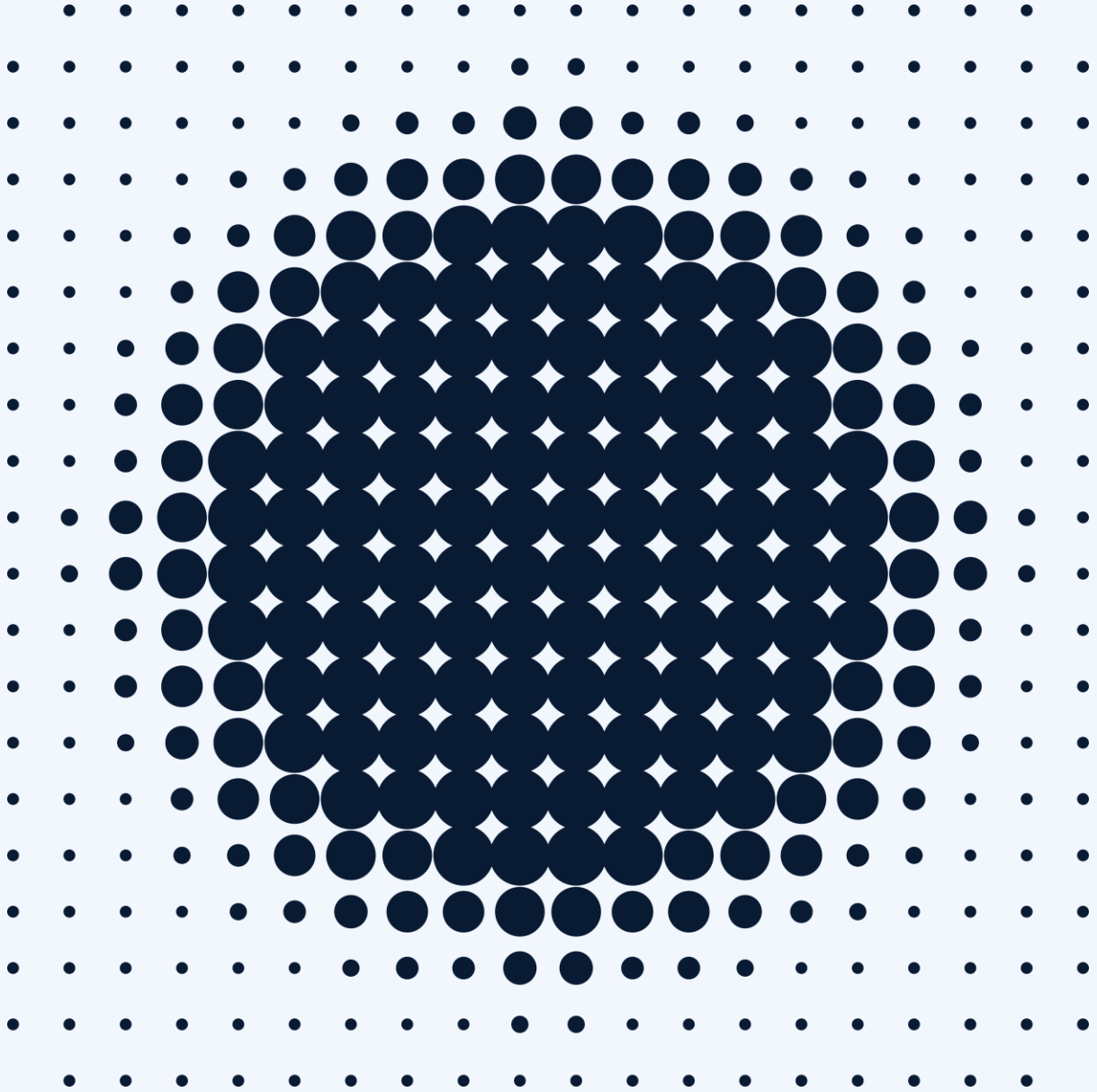


Summary

Expands your attack surface

Nothing looks wrong. Together, it becomes risk.

- Orphaned and inactive identitites
- Excessive admin roles
- Gaps in MFA enforcement
- Apps and agents without ownership



Demo

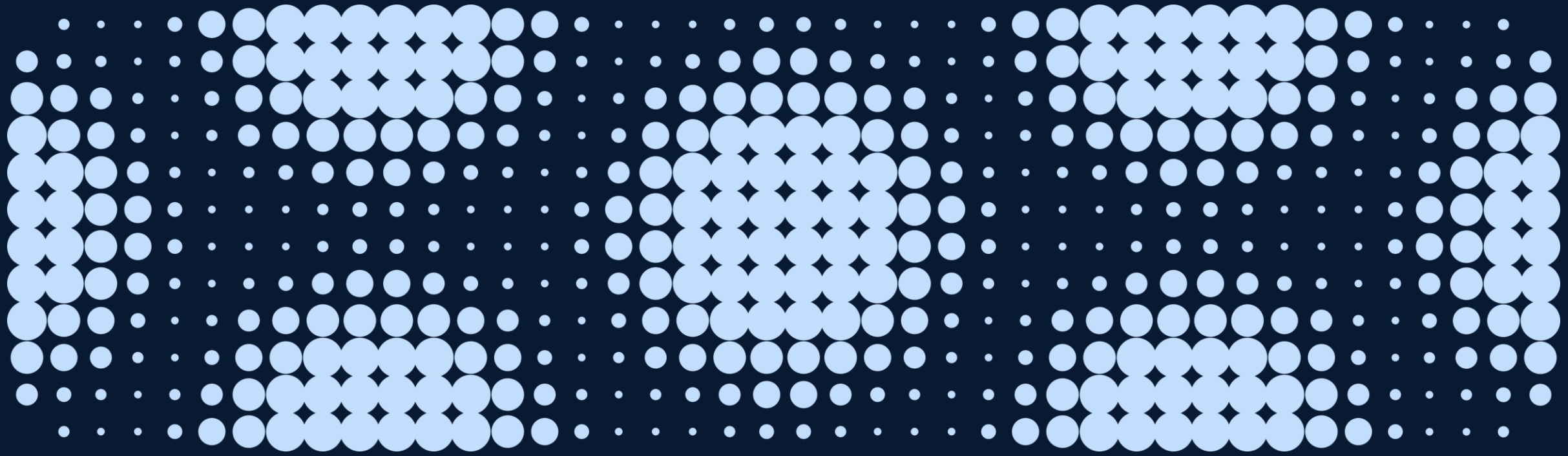
PART 2 OF THIS WEBINAR SERIES

How to distribute identity governance across the organization

DATE
13 MAY

TIME
15:00 CEST

Gunnar Weld
Co-founder & CTPO



Questions?

bsure.

support@bsure.io +47 64 80 82 22 bsure.io

Follow us