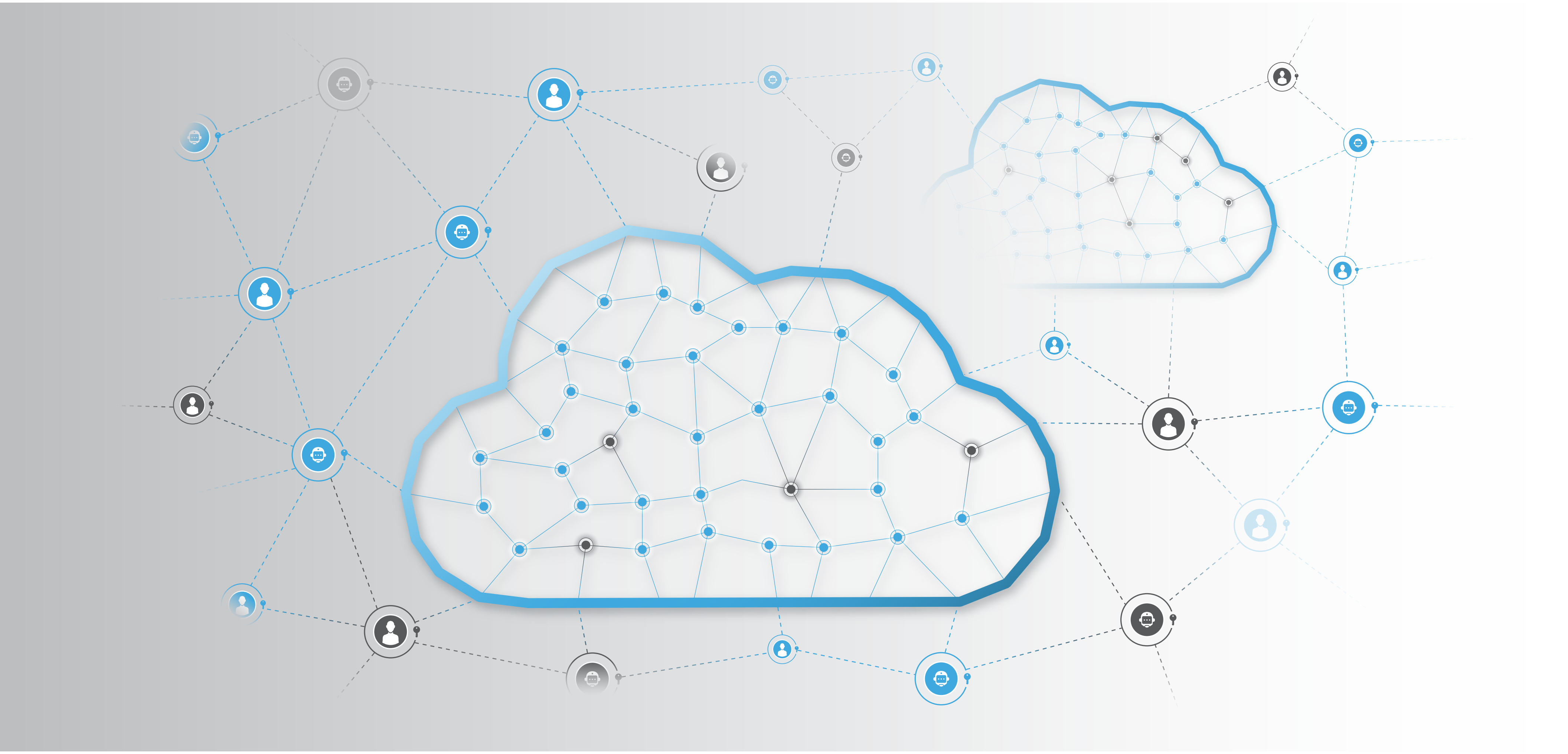
WHAT IS
SHADOW ACCESS?



STACK IDENTITY

WHAT IS SHADOW ACCESS?

The widespread use of cloud services and the increase in data-centric applications has led to the proliferation of data stores containing sensitive information.

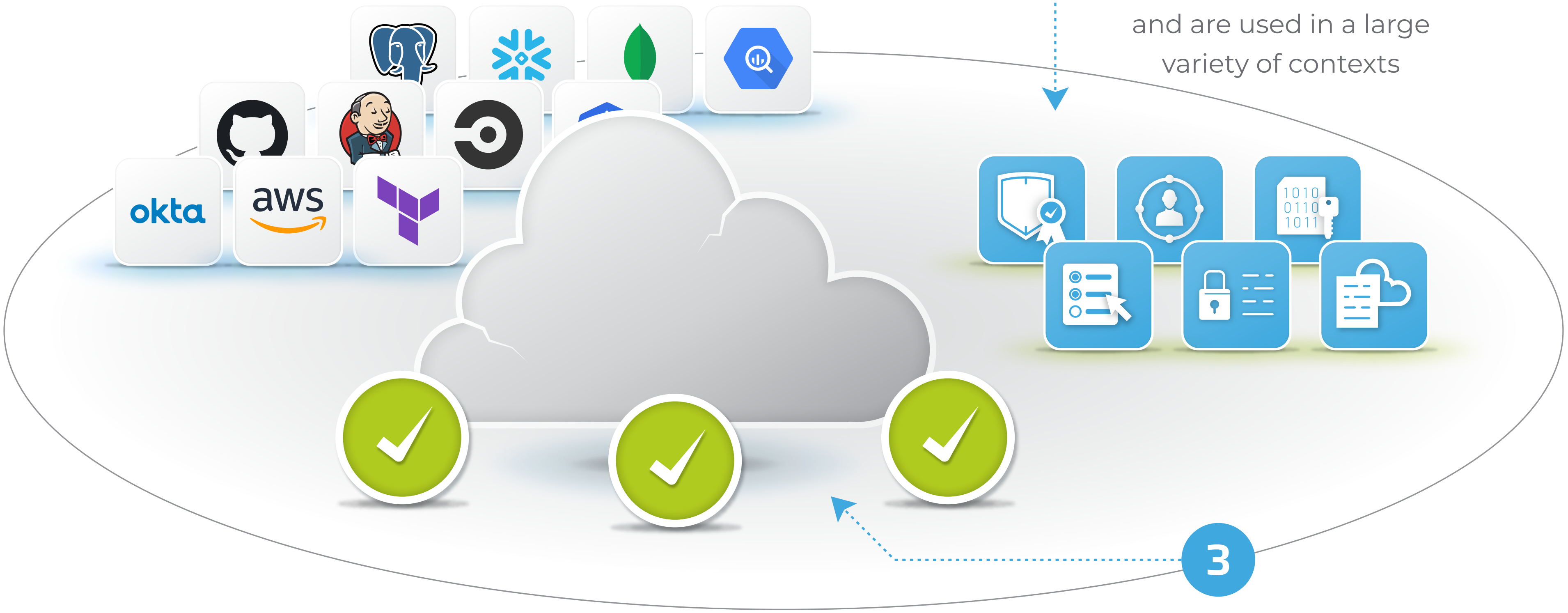
There is high demand for access to this large volume of data. However, this also creates a new problem called **Shadow Access**, which refers to unauthorized, unmonitored, and invisible access to cloud data, applications, and software.

Shadow Access increases the risk of cloud and data breaches and complicates access compliance, audit and governance. In simple terms, shadow access should not exist and should be removed.

WHAT CAUSES SHADOW ACCESS?

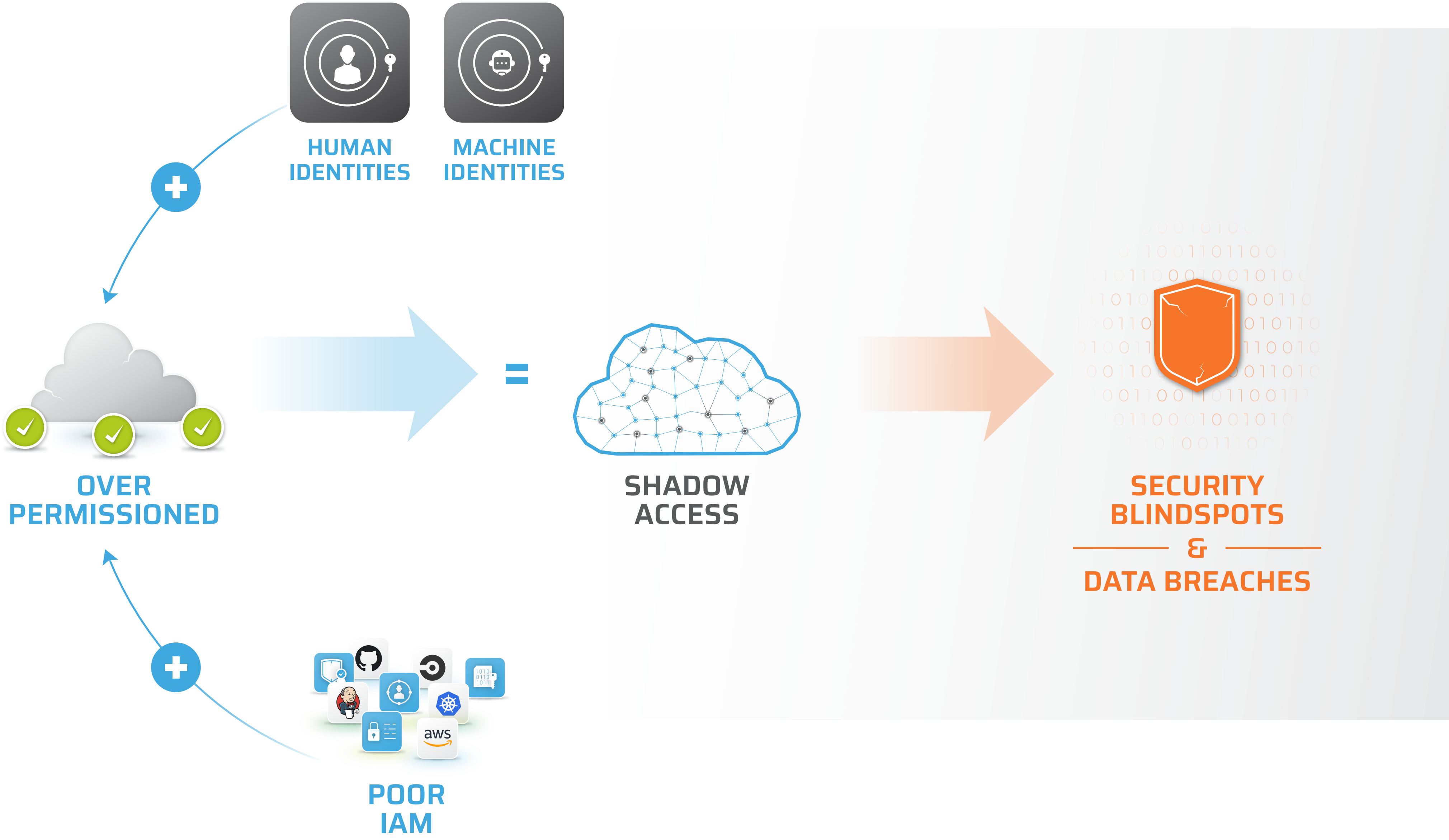
1 Identities are often automatically created, and live across multiple ecosystems

2 Access credentials live across multiple systems and are used in a large variety of contexts



3 Overly permissive policies generate more identities and more access than necessary

CLOUD IDENTITIES AND OVER-PERMISSIONED ACCESS CREATE IAM BLINDSPOTS



HUMAN IDENTITIES

MACHINE IDENTITIES

OVER PERMISSIONED

POOR IAM

=

SHADOW ACCESS

SECURITY BLINDSPOTS

&

DATA BREACHES

HOW DOES SHADOW ACCESS IMPACT DEVOPS AND SECOPS?

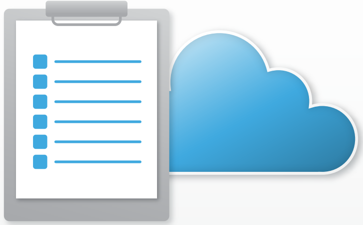
Cloud creates an untenable and continuous risk of data exfiltration caused by thousands of automated, & distributed access controls and entitlements.

This creates shadow access that complicates & inhibits the efficacy of teams involved in cloud architecture, audit & compliance and data security.

CLOUD ARCHITECTURE AND CI/CD

DevOps teams inadvertently create security risks with automated creation of infrastructure and identities.

Simultaneously, SecOps teams need to remove under-utilized identities and over-permissioned access to reduce risk.



AUDIT AND COMPLIANCE

Audit and compliance processes are continuously catching up with the dynamic changes in a cloud native environment.

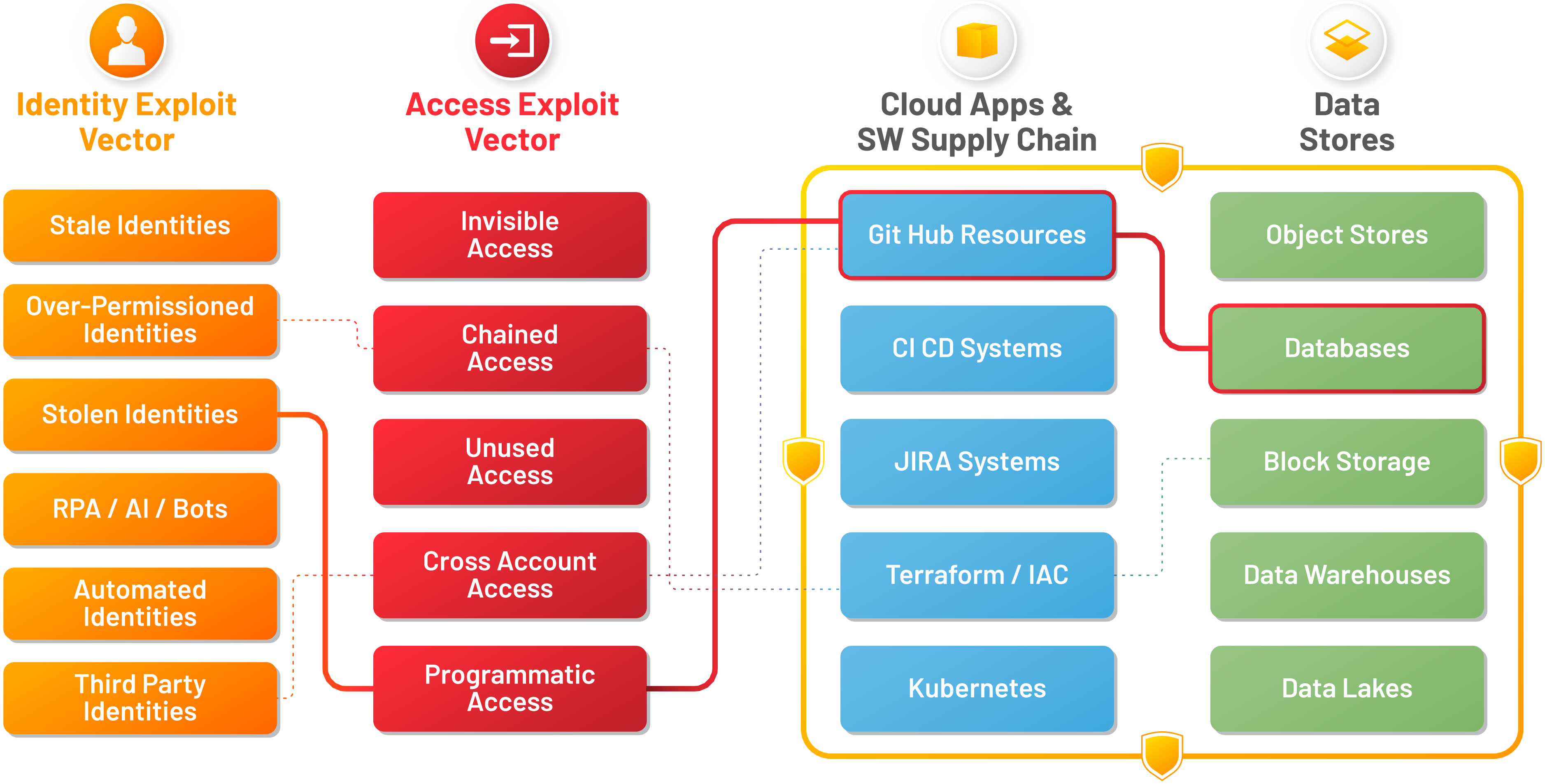
Who has access to what, and who is accessing what can change drastically thirty days after a SOC2 audit.

DATA SECURITY PROCESSES

Data security processes and tools lack big picture visibility as they are fragmented across IAM and governance systems.

Identity and access information is disconnected across Cloud IAM & IDP, IaC and data stores, ticketing systems and spreadsheets.

TOXIC IDENTITY AND ACCESS COMBINATIONS CREATE SHADOW ACCESS



AWS alone has 12,800 API connections with 13,800 permissions to cloud data and services

Source: https://aws.permissions.cloud/ as of April 2023

WHAT ARE DIFFERENT TYPES OF SHADOW ACCESS?

INVISIBLE ACCESS

AWS console did not show effective permissions for an S3 bucket when scanning which led to an S3 bucket being left open

UNWANTED ACCESS

Lambda function replaced by malicious code creating unauthorized external access being left open

EXCESSIVE ACCESS

Policy with full access is given where only access to specific data stores, or cloud services are needed

DORMANT ACCESS

Policy with full access has not been used in 60 days but was still available for assignment to a role

CROSS ACCOUNT ACCESS

Not a customer for 2 years yet still has cross account sharing enabled

DATA RECOVERY ACCESS

Assumed role access to programmatic access to an S3 bucket used for data backup for DR

RISKY ACCESS

Customer critical situation allows developers access to resources but permissions are not revoked after the situation is resolved

TOXIC COMBINATION

Programmatic access to S3 Bucket via application identity along with permissions management permissions

UNUSED DATA

The flip side of Dormant Access, where data has not be used for 60 days, but access is still enabled

RIGHT SIZING

Understanding which policies and permissions are not being used and change them to make sure access is correct

HOW TO ADDRESS THE PROBLEM OF SHADOW ACCESS?

Cloud IAM Operations must be transformed to protect data from shadow access, and close the loop with IAM governance and compliance for the cloud.

TO DO THIS, 3 KEY IAM PROBLEMS MUST BE ADDRESSED

TOO MANY ALERTS AND TOOLS

Companies operate too many IAM tools with too many signals (alerts) and are still unable to prevent cloud breaches and data theft.

1

WHAT'S NEEDED

A single source of truth for “all things access” that informs risk based access controls to secure data and governance of cloud IAM

NO VISIBILITY DUE TO SCATTERED DATA

Current tools lack big picture visibility to IAM data, which is distributed across many tools including Cloud IAM, Cloud IDP, Infrastructure as Code, data stores and HR systems. Governance of access is also scattered across ticketing systems, emails, spreadsheets and screenshots.

2

WHAT'S NEEDED

IAM data must be consolidated to gain the connected context across identities, access, data posture and governance that is needed for Cloud IAM operations.

MANUAL, STATIC PROCESSES

IAM governance and compliance are manual, static and time consuming. Companies rely on spreadsheets, screenshots and email to collect required information on who has access to what data, who is accessing what data and what are the recent changes in access.

3

WHAT'S NEEDED

Automated, accurate and timely reports on access to data to simplify cloud access audit processes, and enable governance to close the loop to control access against data theft across development and production environments.

Learn more about Shadow Access:

WWW.STACKIDENTITY.COM

STACK IDENTITY

Identity-first cloud security