SailPoint

Identity-aware Infrastructure

Identity at the Center of Security, Compliance & IT Operations

Darran Rolls, CTO & CISO

SailPoint at a Glance

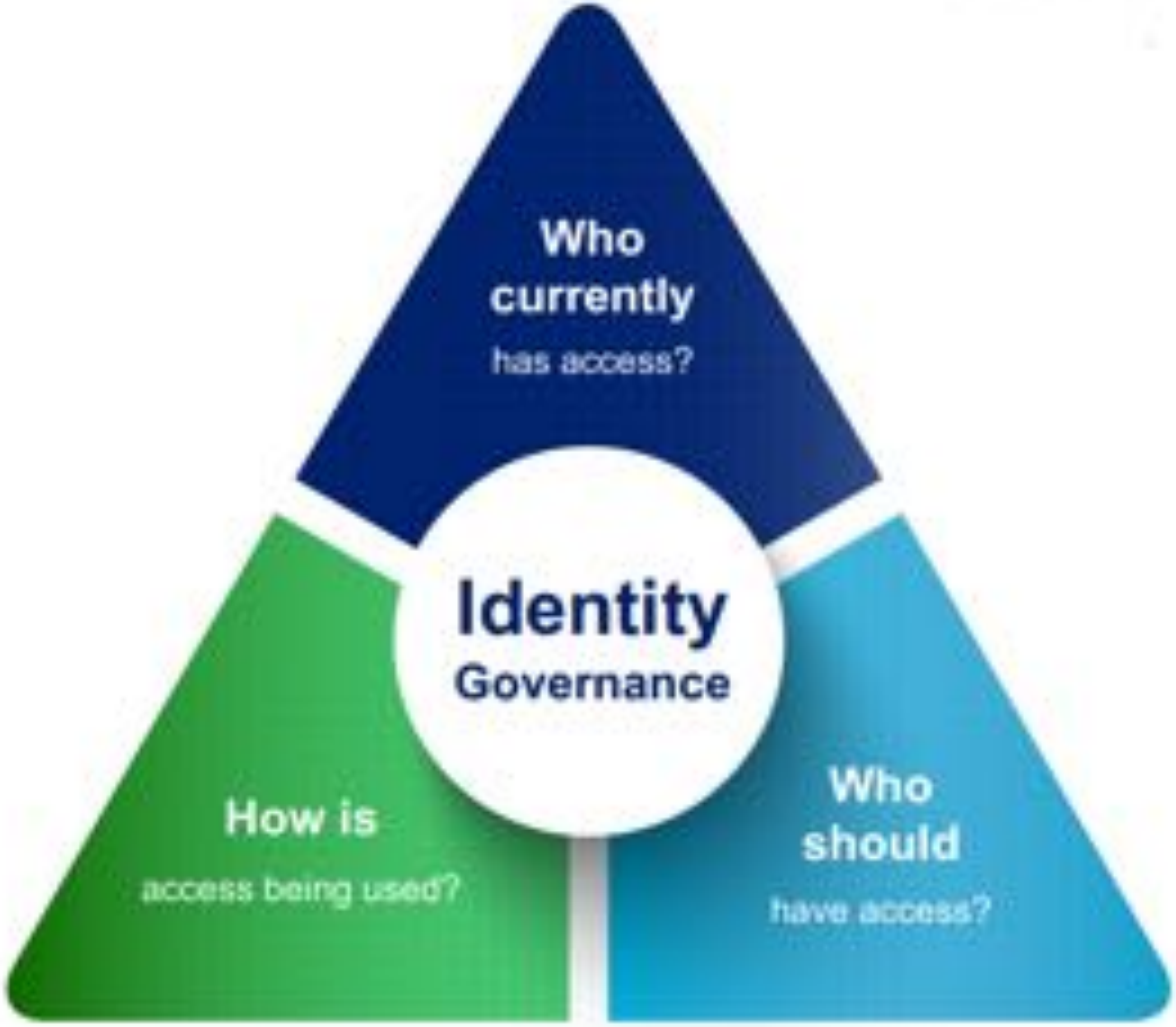
World’s largest, dedicated IAM vendor

- Based in Austin Texas, USA
- Operations in 15 countries
- 300 Partners worldwide
- Customers in every vertical

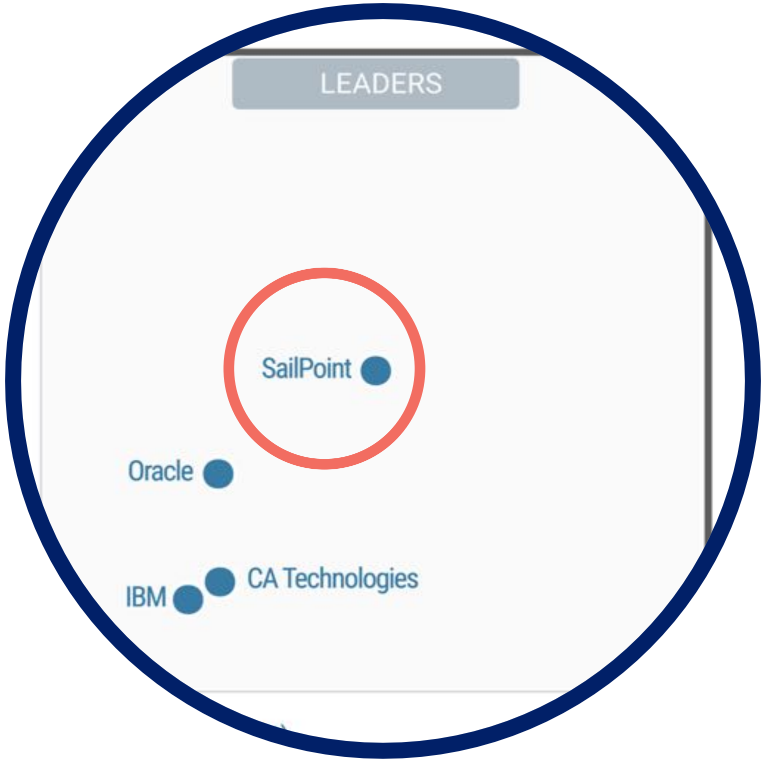
The leader in identity governance

SailPoint secures digital identities

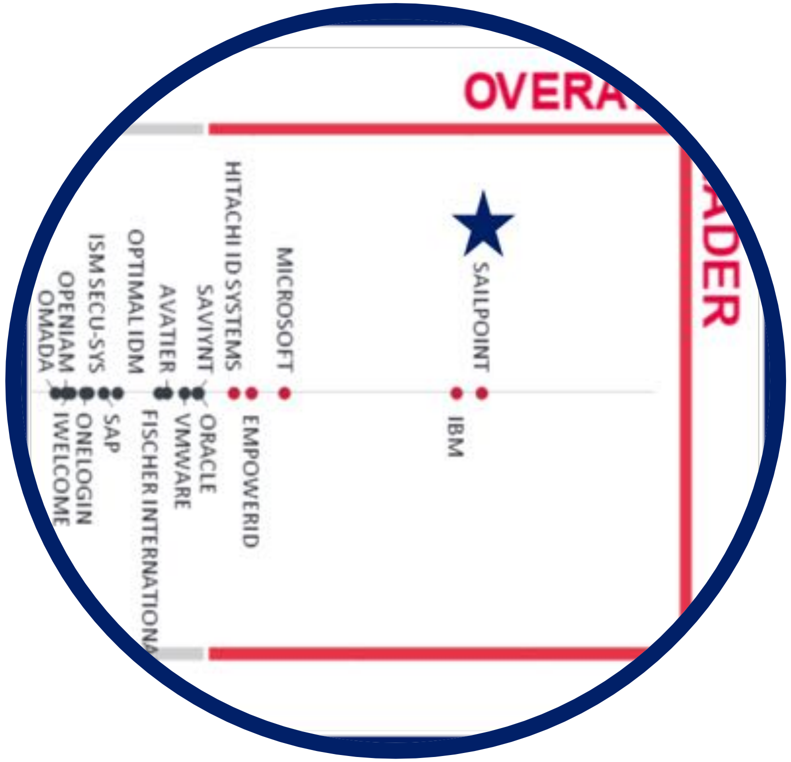
Enabling organizations to answer **three critical questions**



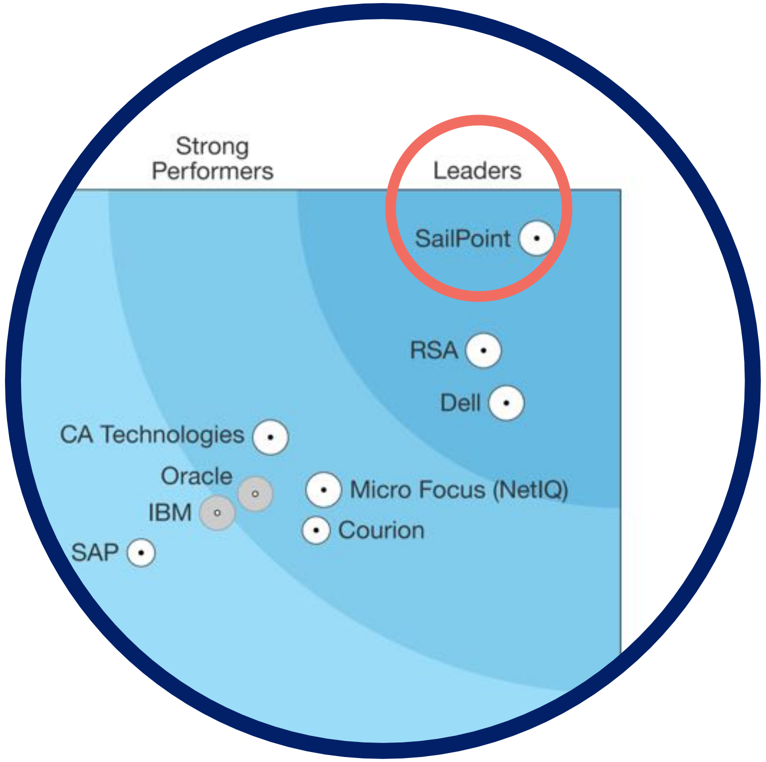
Identity Governance market leadership



Gartner
Magic Quadrant for IGA, 2017



KuppingerCole Report,
Leadership Compass, 2017



Forrester
Wave for IMG, 2016

20 Years of Identity Management Evolution

Evolution #1
Delegate Administration

1998

Tivoli

IBM

Generation #2
Automated Provisioning

2004

waveset

Sun microsystems

Generation #3
Identity Governance

2018

SailPoint

20 Years of Identity Management Evolution

Evolutic
Deleg
Administ

1998

Tivo

IBM

- ✓ Business user focused
- ✓ Full lifecycle
- ✓ Embedded controls
- ✓ Securing & managing all access

Sun microsystems

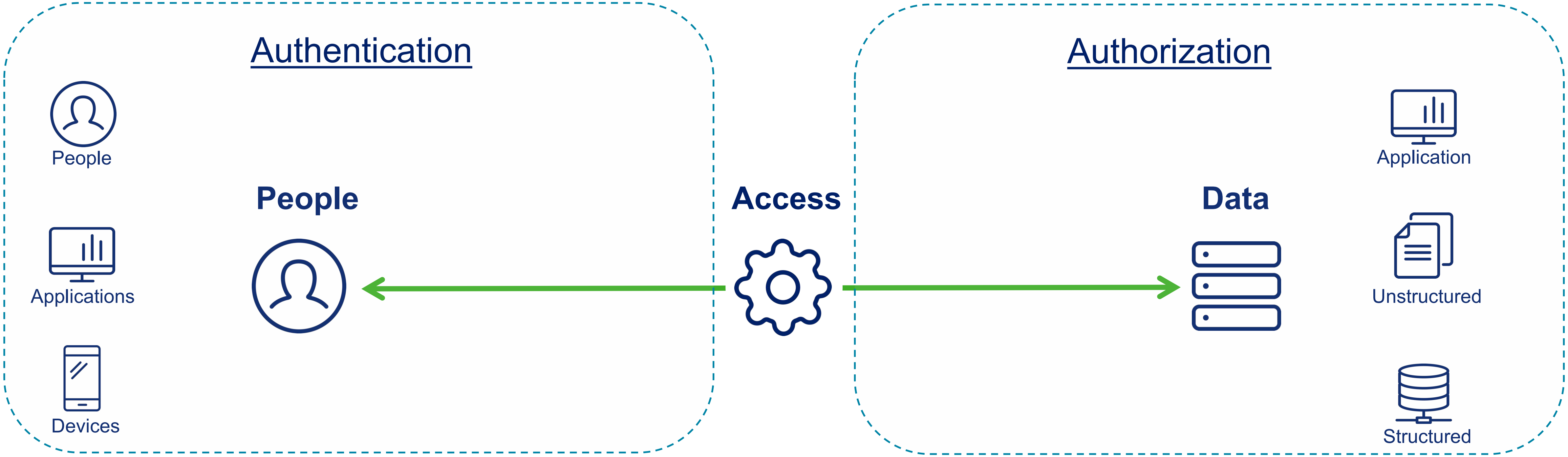
eration #3
Identity
overnance

2018

SailPoint

Securing & Managing Access

Securing & Managing Access



Authentication

People

Applications

Devices

People

Access

Authorization

Data

Application

Unstructured

Structured

PKI Based

Password Based

Web Based

Bio-Metric

SAML Based

OAuth Based

Application Specific

Group Based

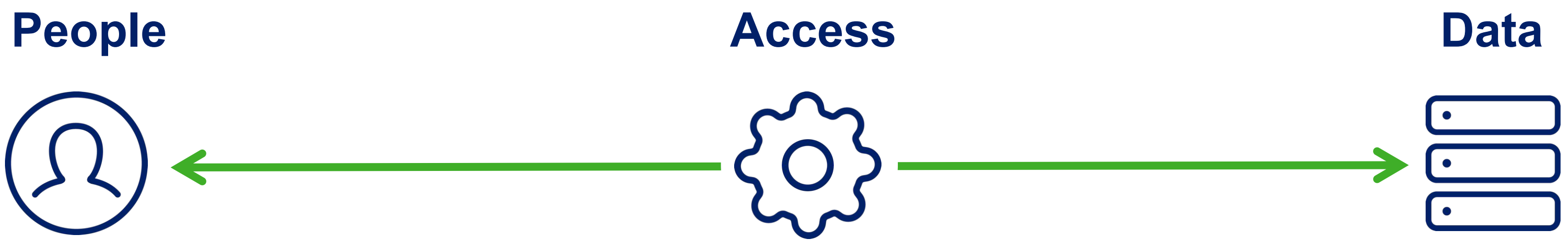
Role Based

System Defined

Attribute Based

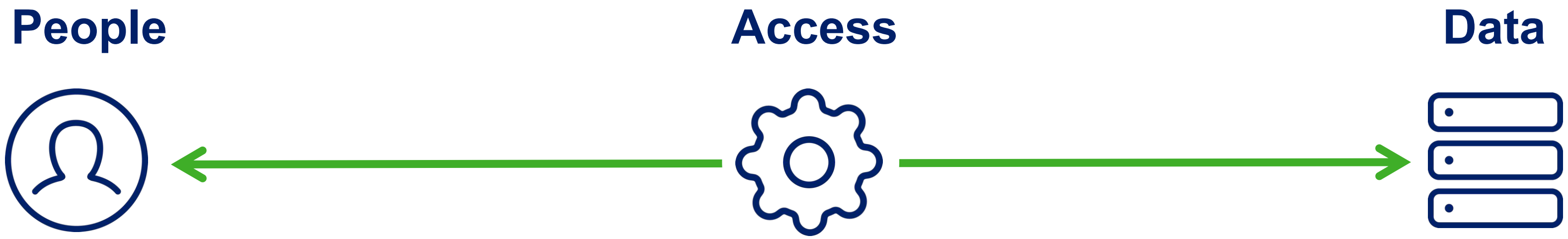
Vaulted Creds

Identity & Access Governance



Who has Access to What and Why…

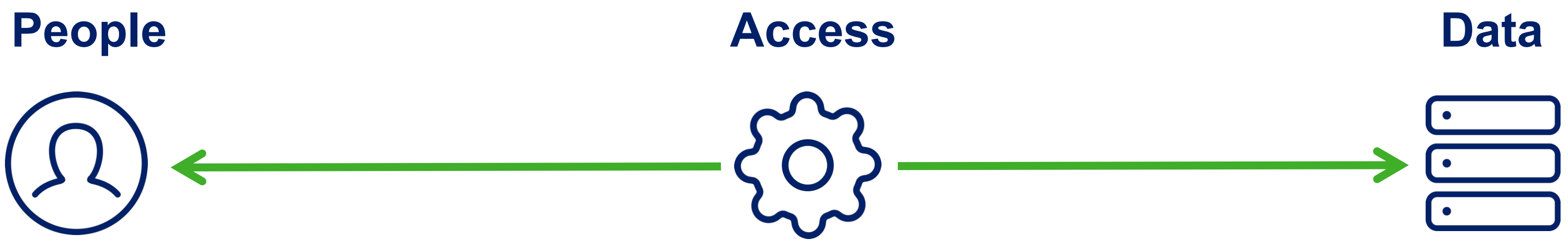
Identity & Access Governance

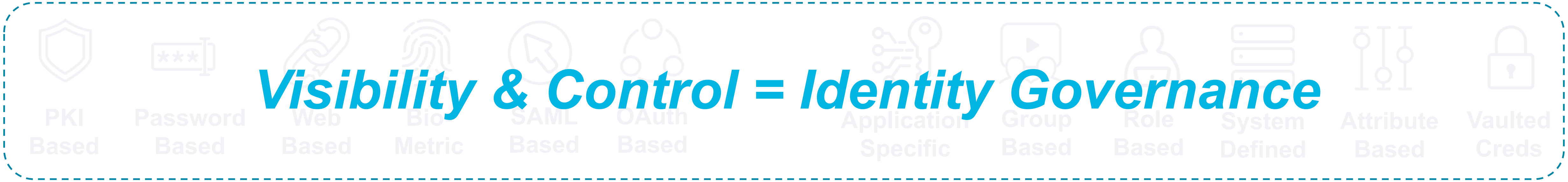


PKI Based
Password Based
Web Based
Bio-Metric
SAML Based
OAuth Based
Application Specific
Group Based
Role Based
System Defined
Attribute Based
Vaulted Creds

Automation, Delegation and Self-service

Identity & Access Governance





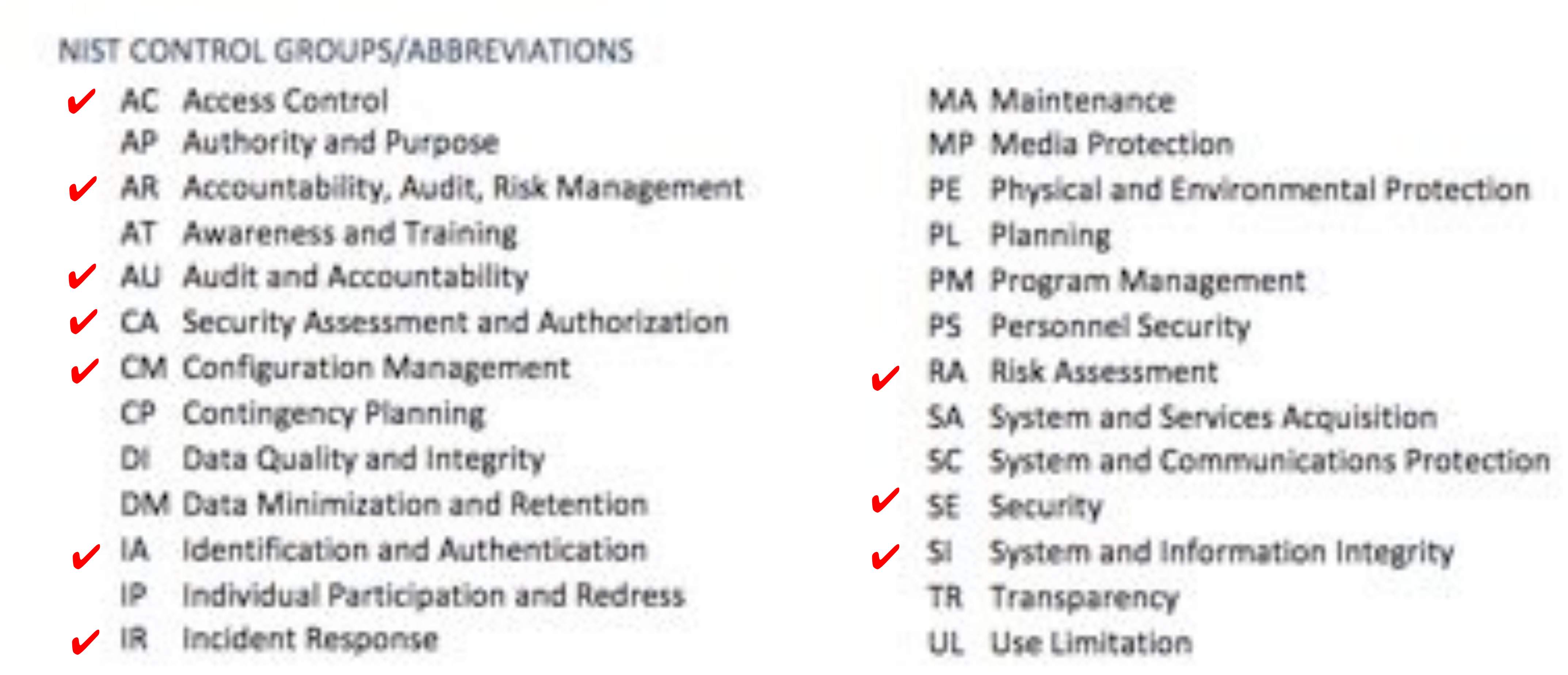
Visibility & Control = Identity Governance

Identity

Governance

Program Objectives

NIST 800-53 Control Groups



NIST CONTROL GROUPS/ABBREVIATIONS

✓	AC	Access Control
	AP	Authority and Purpose
✓	AR	Accountability, Audit, Risk Management
	AT	Awareness and Training
✓	AU	Audit and Accountability
✓	CA	Security Assessment and Authorization
✓	CM	Configuration Management
	CP	Contingency Planning
	DI	Data Quality and Integrity
	DM	Data Minimization and Retention
✓	IA	Identification and Authentication
	IP	Individual Participation and Redress
✓	IR	Incident Response
	MA	Maintenance
	MP	Media Protection
	PE	Physical and Environmental Protection
	PL	Planning
	PM	Program Management
	PS	Personnel Security
✓	RA	Risk Assessment
	SA	System and Services Acquisition
	SC	System and Communications Protection
✓	SE	Security
✓	SI	System and Information Integrity
	TR	Transparency
	UL	Use Limitation

Identity Governance Program Objectives

Increased Productivity

Enabling efficient & accurate user access

Lower Security Risk

Protecting access to applications and data

Sustainable Compliance

Staying compliant amidst mounting regulations

Cloud and on-premise applications and data…

Objective #1: Increased Productivity

Increased Productivity

- Joiner *MOVER* & leaver controls…
- Fine-grained access control…
- Delegated administration…
- End-user self-service…

Objective #2: Lower Security Risk

Lower
Security Risk

- Understanding access risk…
- Password management…
- File & access governance…
- De-provisioning & security response…

Objective #3: Sustainable Compliance

Sustainable Compliance

- Access reviews…
- Detective and preventive policy controls…
- Data ownership & responsibility…
- Reporting & analytics…

Identity-aware Infrastructure

Identity Context

Relationships

State

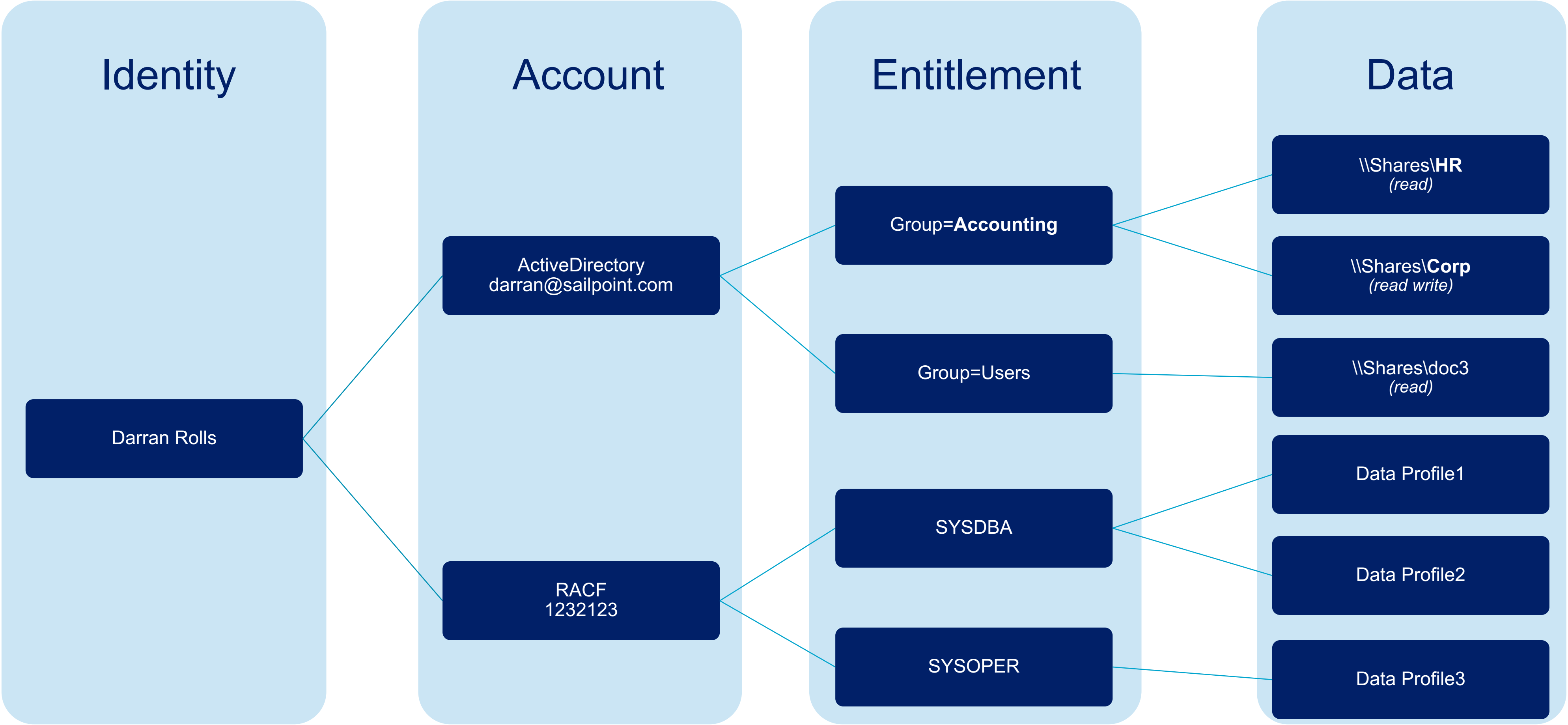
Policies

Controls

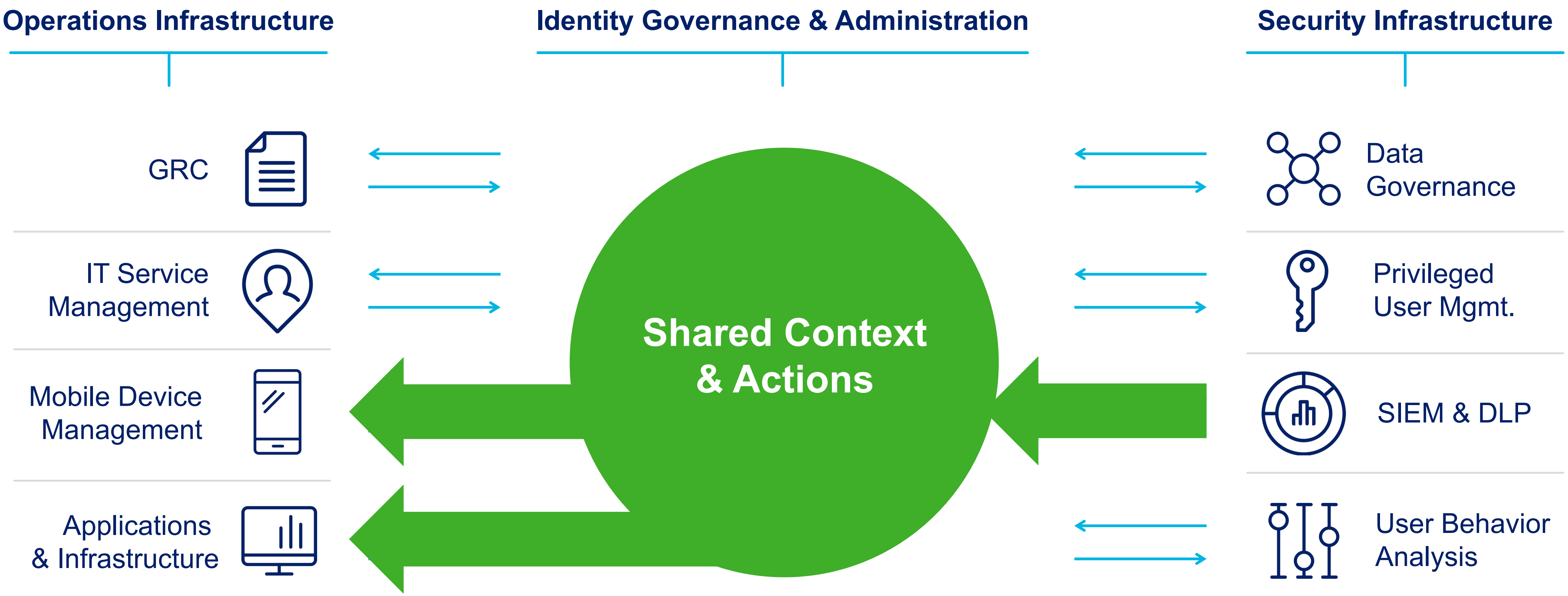
Meaning

History

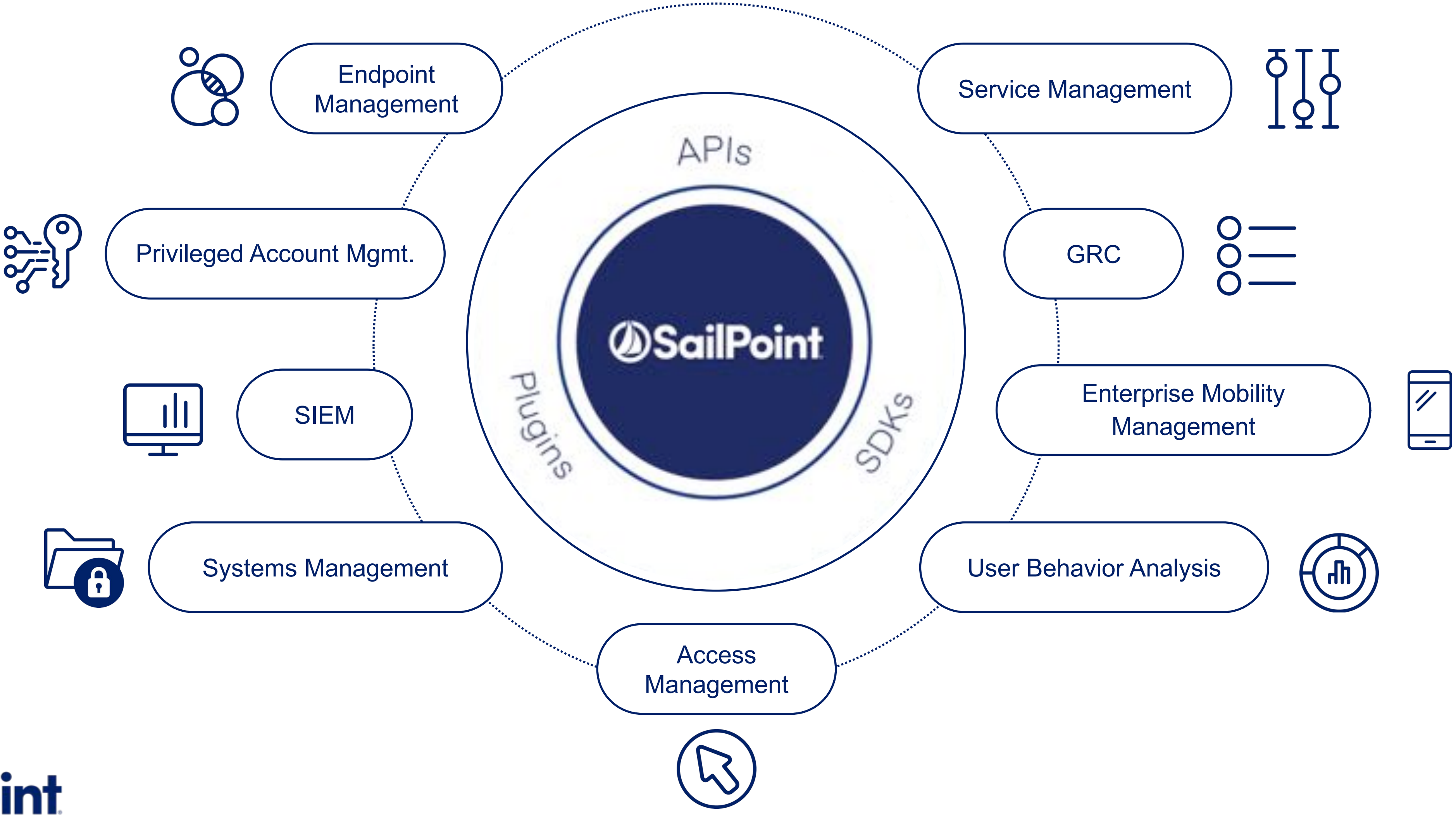
Understanding Key Relationships



Identity-enabled Infrastructure



SailPoint Open Identity Platform



SailPoint

darran.rolls@sailpoint.com
www.sailpoint.com