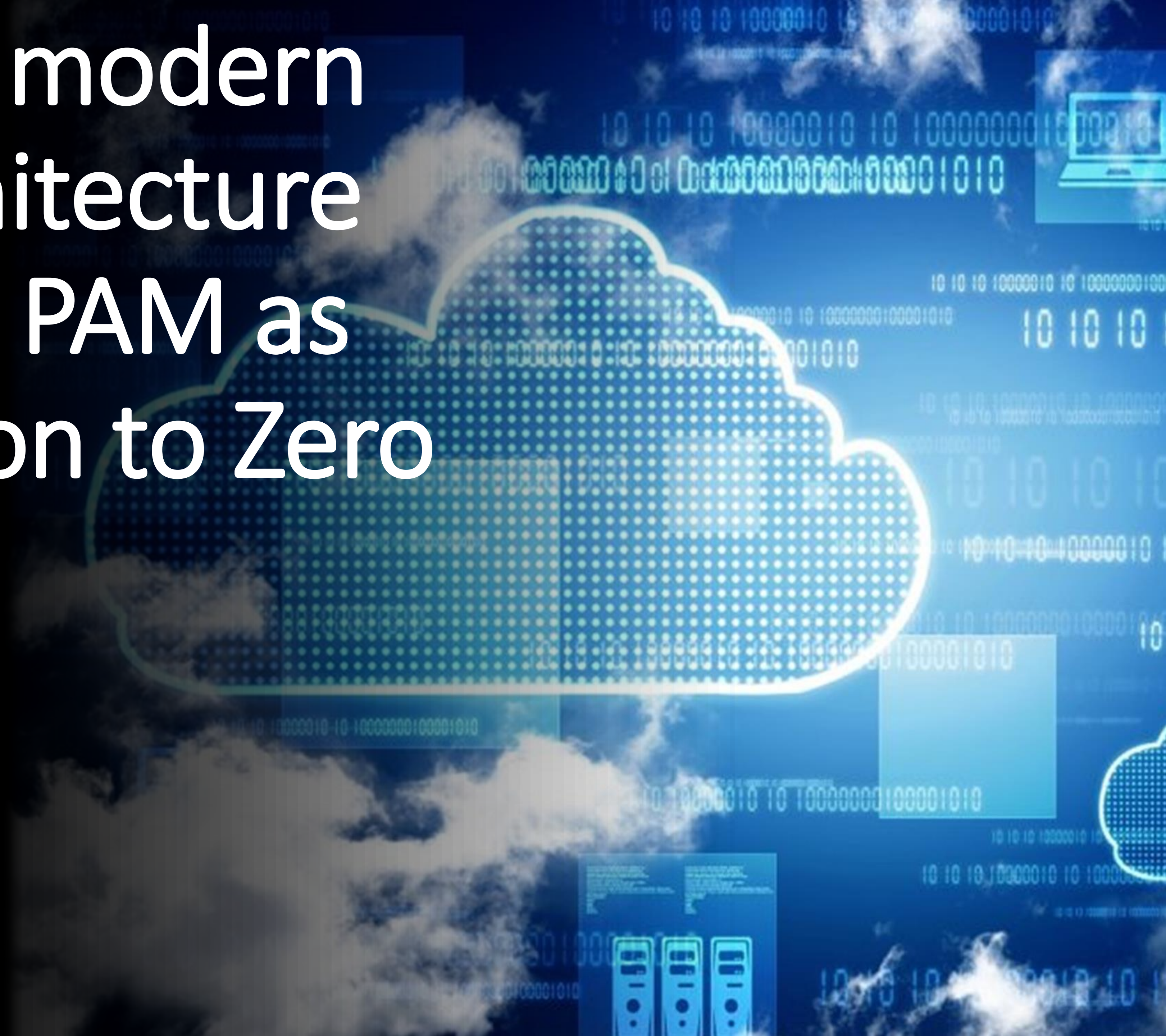
Empowering modern Security Architecture with IGA and PAM as the foundation to Zero Trust



Cullen Landrum, CISSP

Calvin Gurka

The information provided in this presentation is confidential and is provided for general understanding and guidance only.

This presentation may contain forward-looking statements within the meaning of the federal securities laws, which involve substantial risks and uncertainties, and are based on management’s beliefs, based on currently available information. Actual results could be materially different.

The development, release, and timing of any features or functionality described for our products that are not currently available remains at our sole discretion on a when, and if available, basis and may not be delivered at all and should not be relied on in making a purchasing decision.

Discussion Points

Digital Transformation

Cybersecurity Risk

Zero Trust Principles

Identity Defined Security

Identity Strategy

SailPoint BeyondTrust

Identities

Data

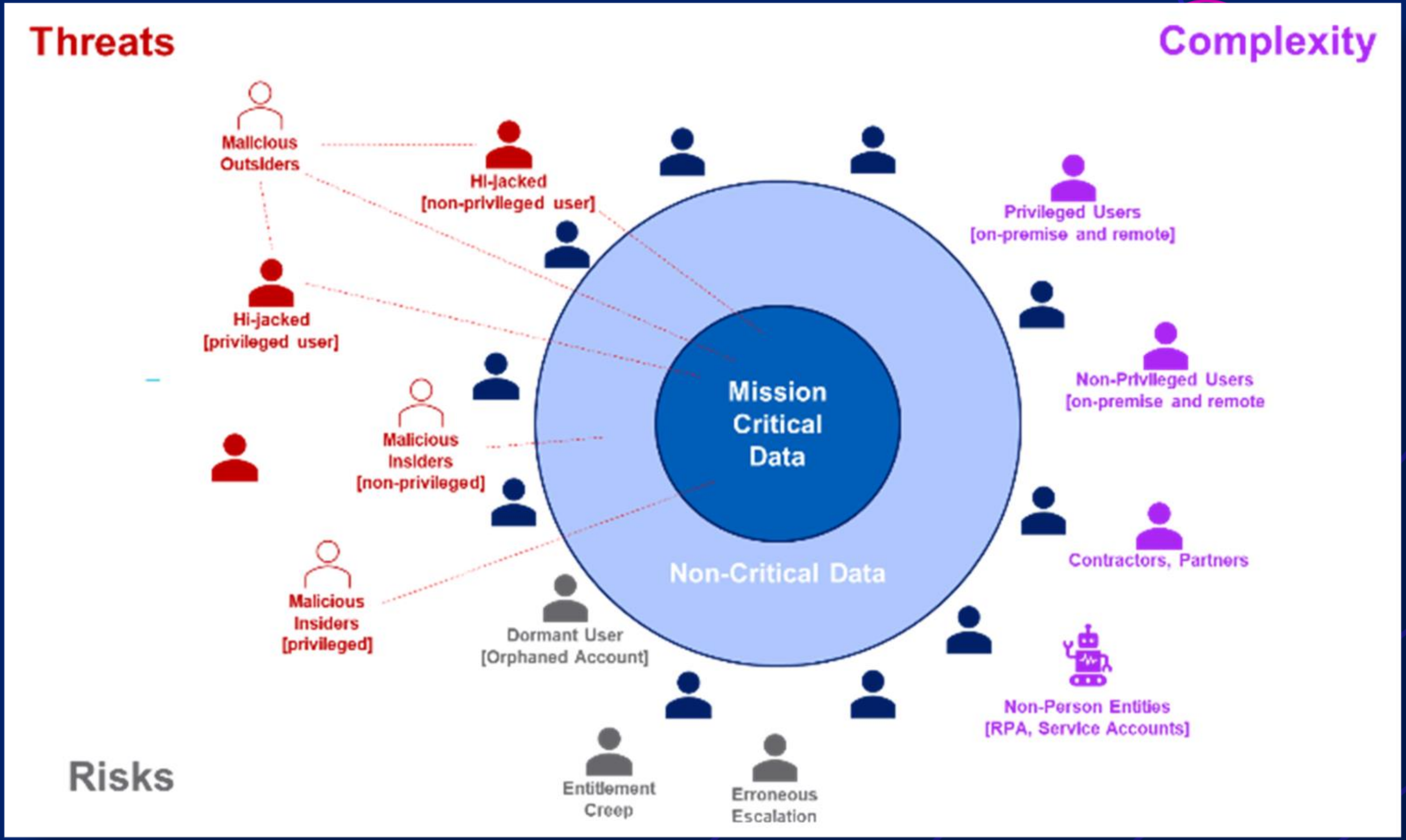
Applications

Cloud

SailPoint BeyondTrust

Threats, Complexity, Risk

- Lack of centralized visibility
- Lack of automation
- Inconsistent processes
- Stale & toxic access
- Overexposed resources
- Lack of alerting and integrated response



Threats
Complexity
Malicious Outsiders
Hi-jacked [non-privileged user]
Hi-jacked [privileged user]
Malicious Insiders [non-privileged]
Malicious Insiders [privileged]
Mission Critical Data
Non-Critical Data
Privileged Users [on-premise and remote]
Non-Privileged Users [on-premise and remote
Contractors, Partners
Non-Person Entities [RPA, Service Accounts]
Dormant User [Orphaned Account]
Entitlement Creep
Erroneous Escalation
Risks

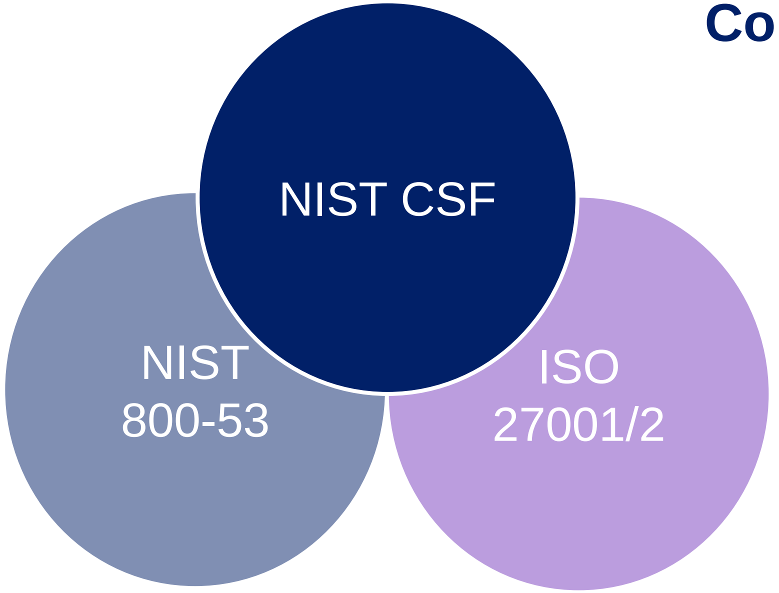
SailPoint BeyondTrust

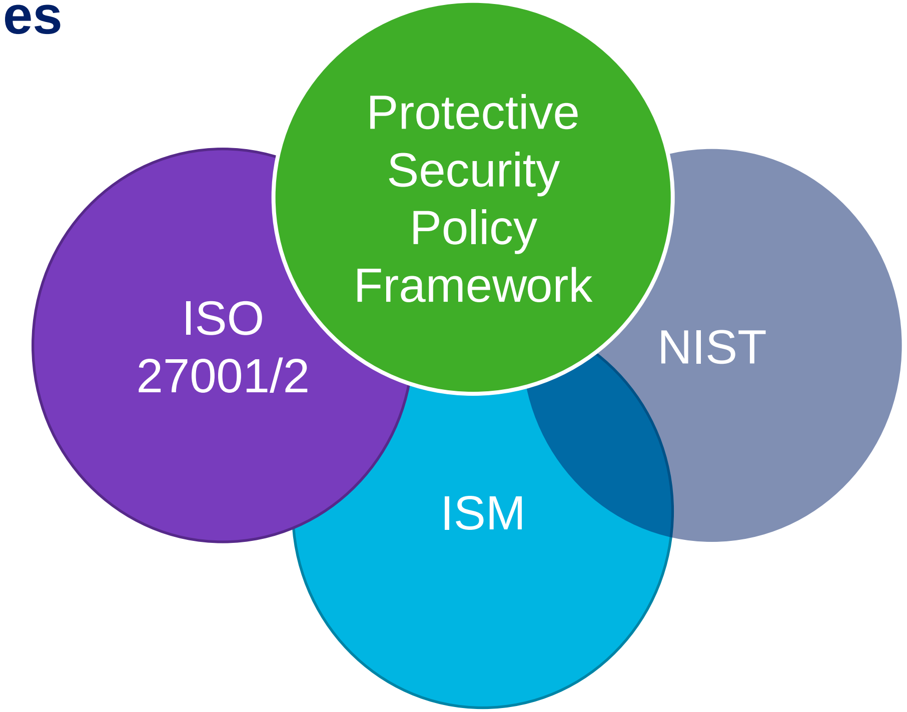
Cybersecurity Frameworks & Identity Centric Security

Cybersecurity Frameworks

IDENTIFY | GOVERN PROTECT DETECT RESPOND

Risk-based assessment
Subcategories
Control Families
Audit





Zero Trust Principles

- Paradigm Shift
- Identity-centric
- Least Privilege
- Context-aware
- Automation
- Continuous Evaluation

SailPoint BeyondTrust

Identity Governance

Everything, Everywhere, Everyone

See Everything

… Everywhere

- Visibility
- Applications
- Systems & Infrastructure
- Data
- Users

Govern Everything

… Everywhere

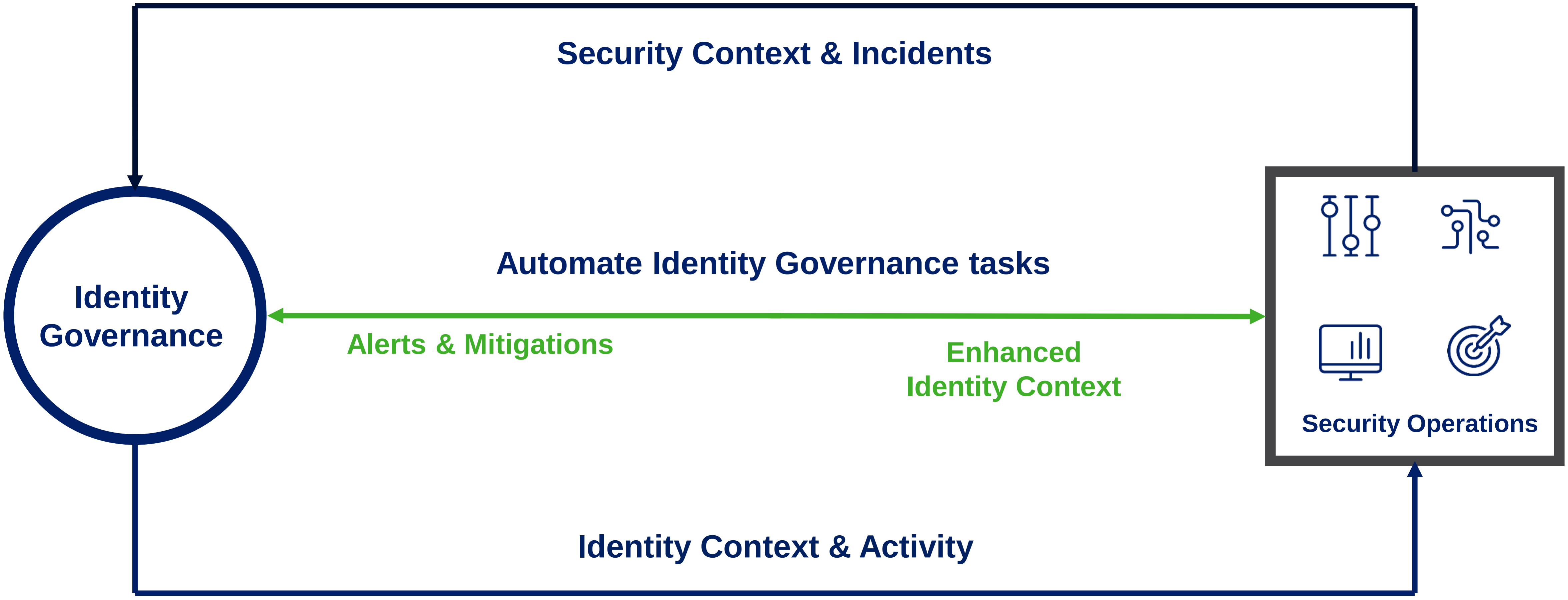
- Access Models
- Policies and Controls
- Predictive/Detective
- Continuous Evaluation

Empower Everyone

… Everywhere

- All Users
  - Employees
  - Partners
  - Contractors
  - Processes

Security Operations Integration



Security Context & Incidents

Automate Identity Governance tasks

Identity Governance

Alerts & Mitigations

Enhanced Identity Context

Security Operations

Identity Context & Activity

SailPoint BeyondTrust

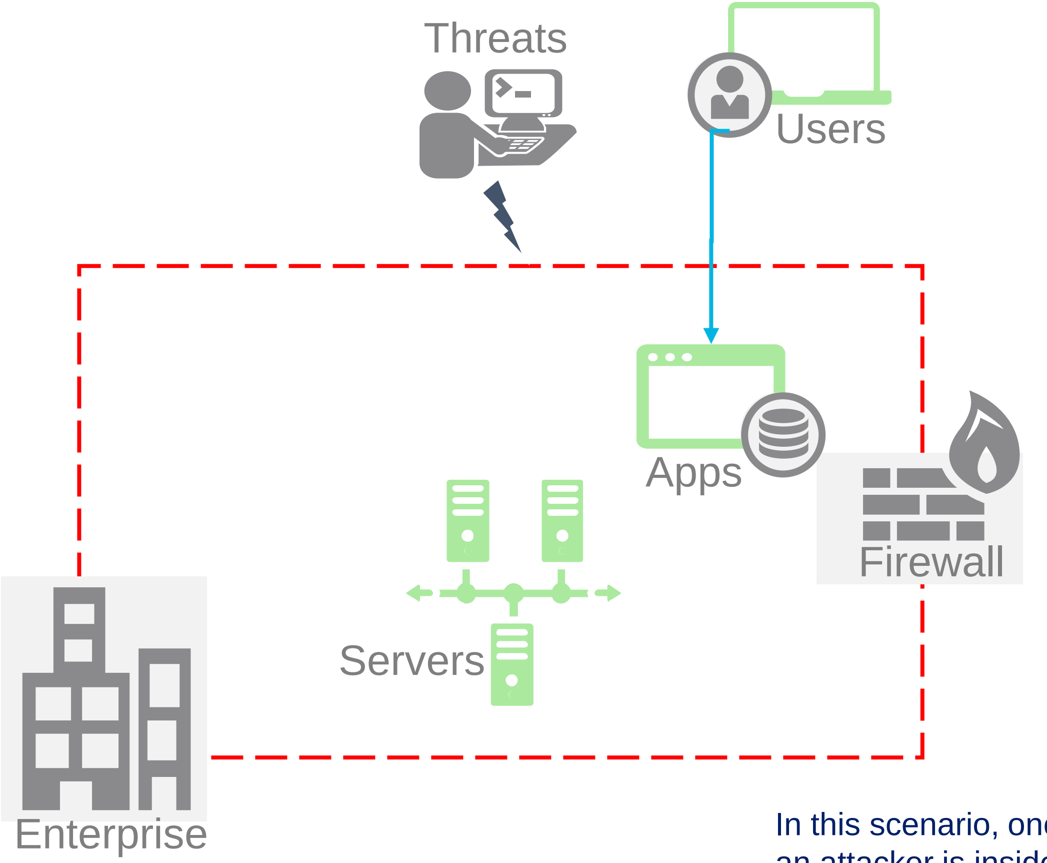
BeyondTrust

The Path to Zero Trust: Start with Identity Security and Least Privilege

Traditional Security vs. Zero Trust Security

Perimeter Based Security

Physical and Digital Barriers

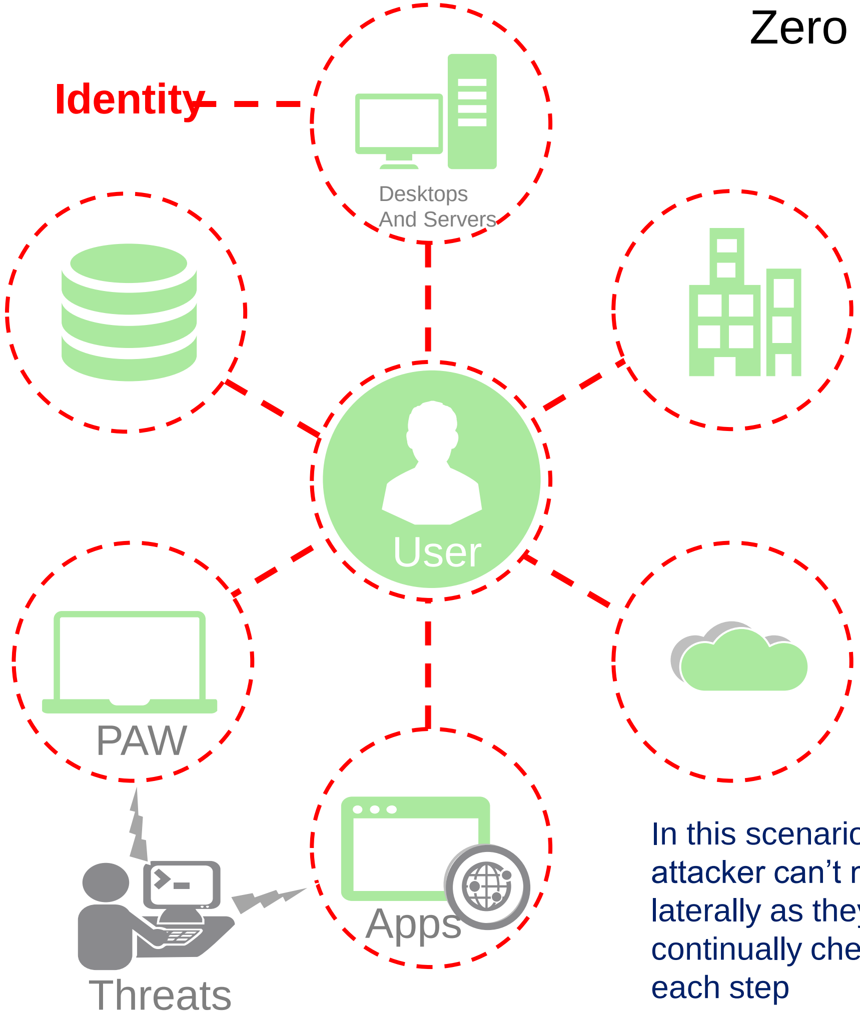


In this scenario, once an attacker is inside, they can move laterally

Identity Defined Security

Continuous Verification

Zero Trust



In this scenario, an attacker can't move laterally as they are continually checked at each step

SailPoint BeyondTrust

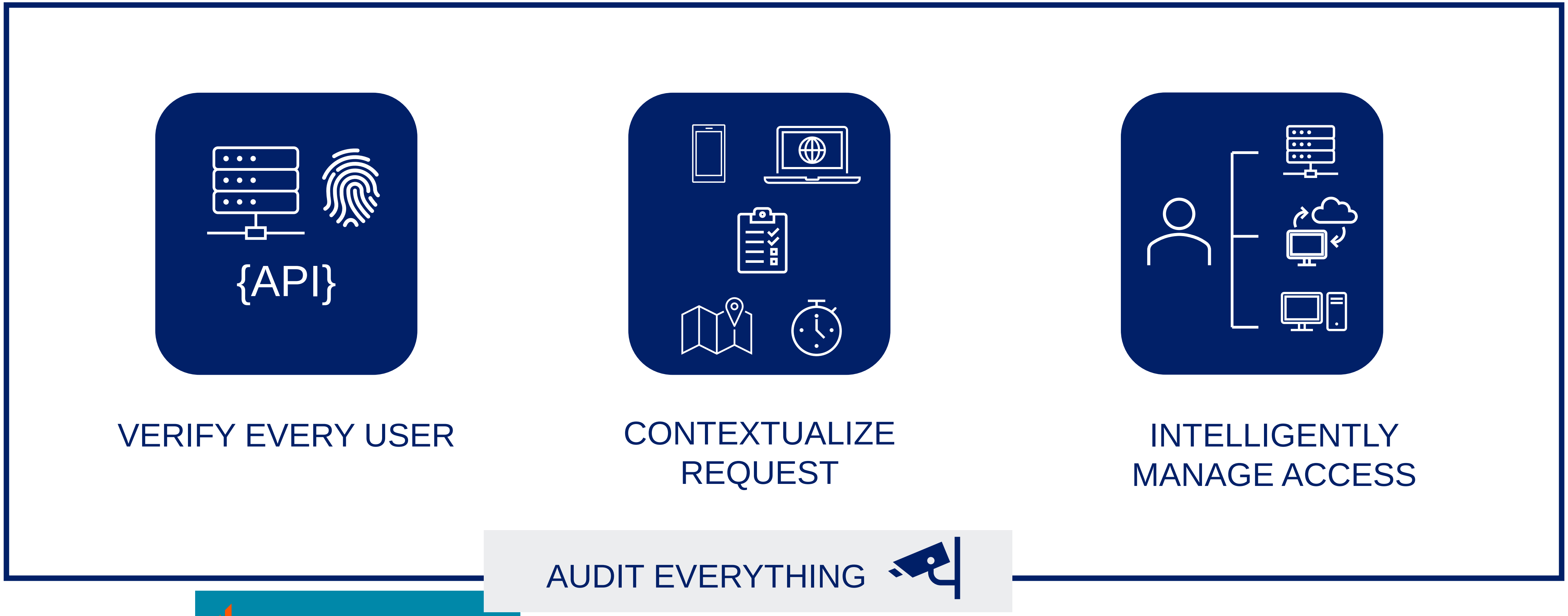
Why a Zero Trust Approach Now?

Traditional Perimeter-based Defense is Obsolete

Ever-expanding Attack Surface

Government Mandates and Corporate Standards

Never Trust. Always Verify



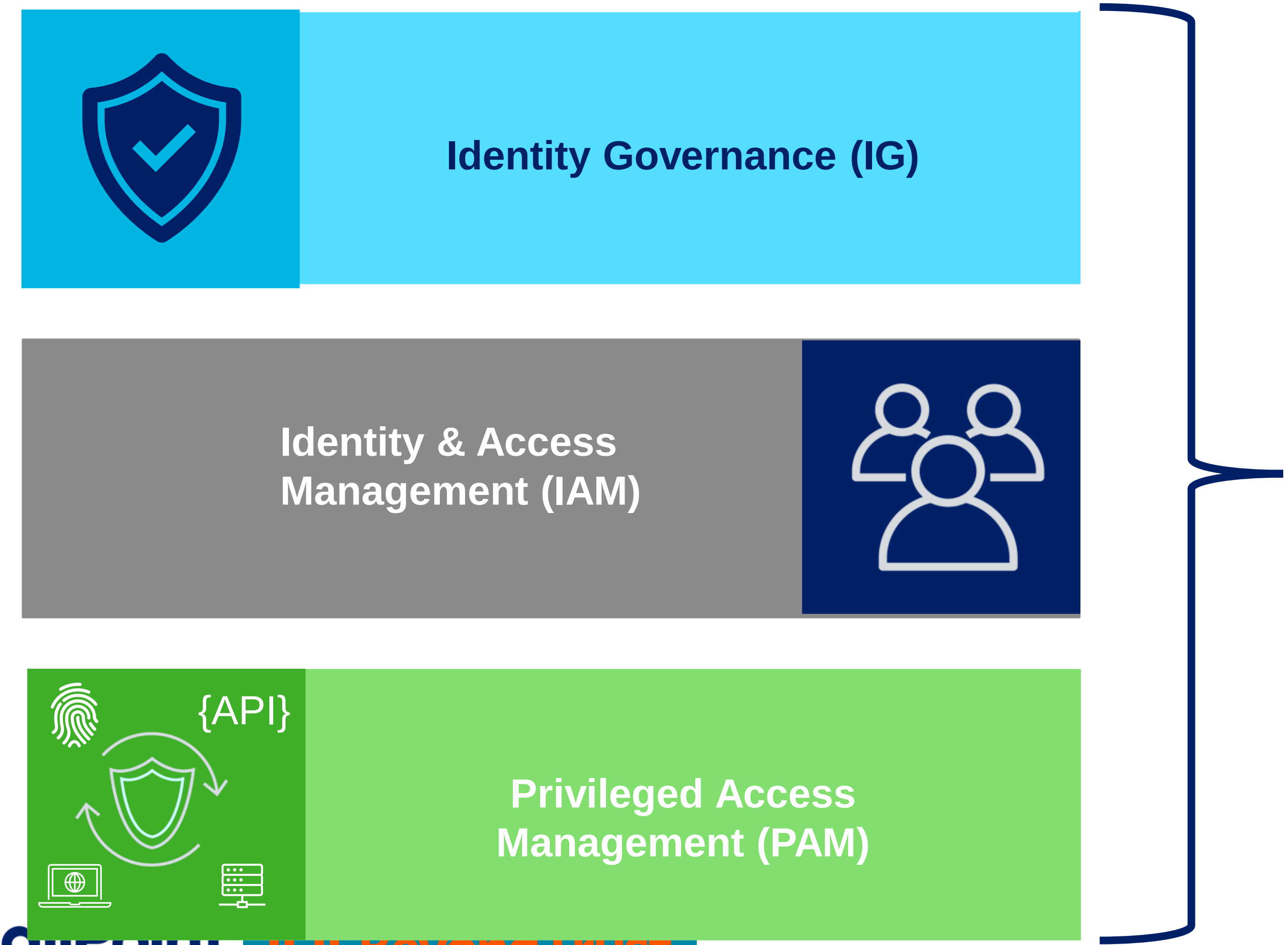
VERIFY EVERY USER

CONTEXTUALIZE REQUEST

INTELLIGENTLY MANAGE ACCESS

AUDIT EVERYTHING

Zero Trust is not a single product



Identity Governance (IG)

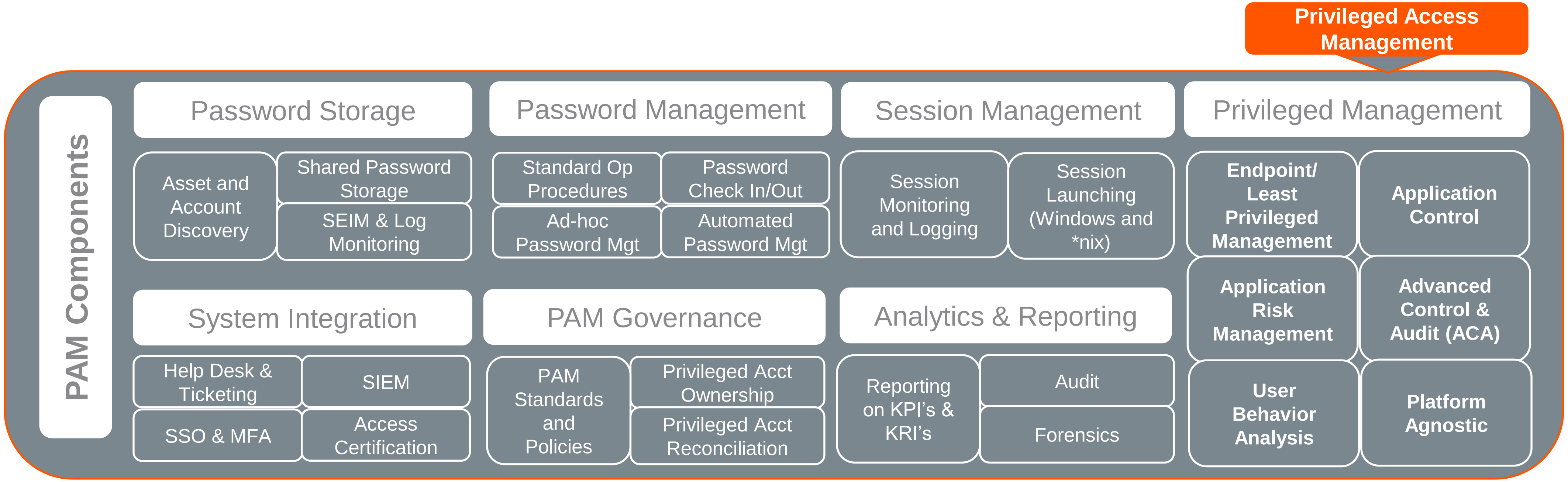
Identity & Access Management (IAM)

Privileged Access Management (PAM)

IG + IAM + PAM

- Likely already in your organization
- Provide end-to-end identity security automation
- Provide coverage and governance for all human and non-human identities (privileged and non-privileged)

Defining Privilege Access Management



Privileged Access Management

PAM Components

Password Storage

- Asset and Account Discovery
- Shared Password Storage
- SEIM & Log Monitoring

Password Management

- Standard Op Procedures
- Password Check In/Out
- Ad-hoc Password Mgt
- Automated Password Mgt

Session Management

- Session Monitoring and Logging
- Session Launching (Windows and *nix)

Privileged Management

- **Endpoint/ Least Privileged Management**
- **Application Control**
- **Application Risk Management**
- **Advanced Control & Audit (ACA)**
- **User Behavior Analysis**
- **Platform Agnostic**

System Integration

- Help Desk & Ticketing
- SIEM
- SSO & MFA
- Access Certification

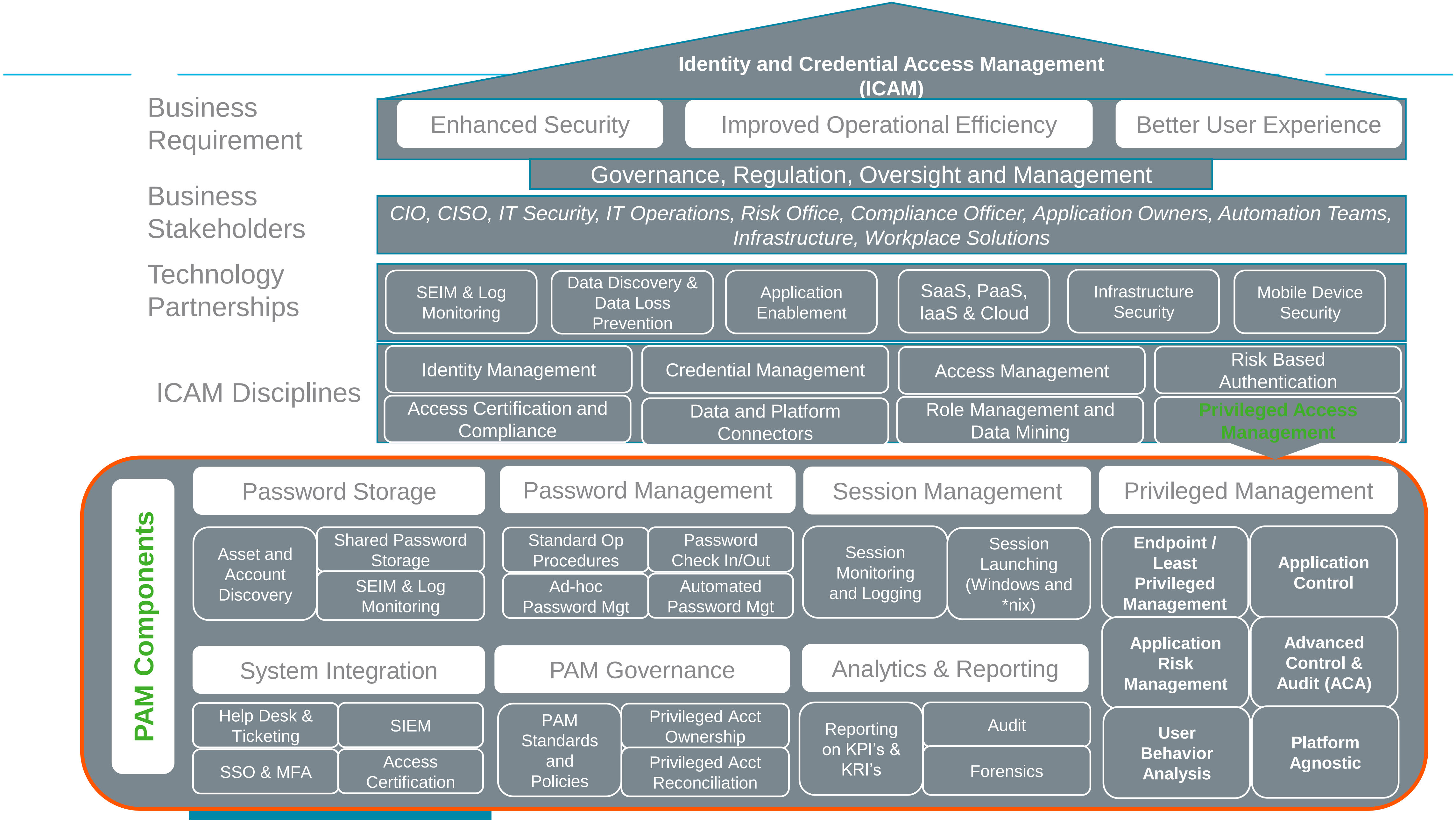
PAM Governance

- PAM Standards and Policies
- Privileged Acct Ownership
- Privileged Acct Reconciliation

Analytics & Reporting

- Reporting on KPI's & KRI's
- Audit
- Forensics

Complete Identity Governance Model



Identity and Credential Access Management (ICAM)

Business Requirement

- Enhanced Security
- Improved Operational Efficiency
- Better User Experience

Governance, Regulation, Oversight and Management

Business Stakeholders

CIO, CISO, IT Security, IT Operations, Risk Office, Compliance Officer, Application Owners, Automation Teams, Infrastructure, Workplace Solutions

Technology Partnerships

- SEIM & Log Monitoring
- Data Discovery & Data Loss Prevention
- Application Enablement
- SaaS, PaaS, IaaS & Cloud
- Infrastructure Security
- Mobile Device Security

ICAM Disciplines

- Identity Management
- Credential Management
- Access Management
- Risk Based Authentication
- Access Certification and Compliance
- Data and Platform Connectors
- Role Management and Data Mining
- Privileged Access Management

PAM Components

Password Storage

- Asset and Account Discovery
- Shared Password Storage
- SEIM & Log Monitoring

Password Management

- Standard Op Procedures
- Password Check In/Out
- Ad-hoc Password Mgt
- Automated Password Mgt

Session Management

- Session Monitoring and Logging
- Session Launching (Windows and *nix)

Privileged Management

- **Endpoint / Least Privileged Management**
- **Application Control**
- **Application Risk Management**
- **Advanced Control & Audit (ACA)**
- **User Behavior Analysis**
- **Platform Agnostic**

System Integration

- Help Desk & Ticketing
- SIEM
- SSO & MFA
- Access Certification

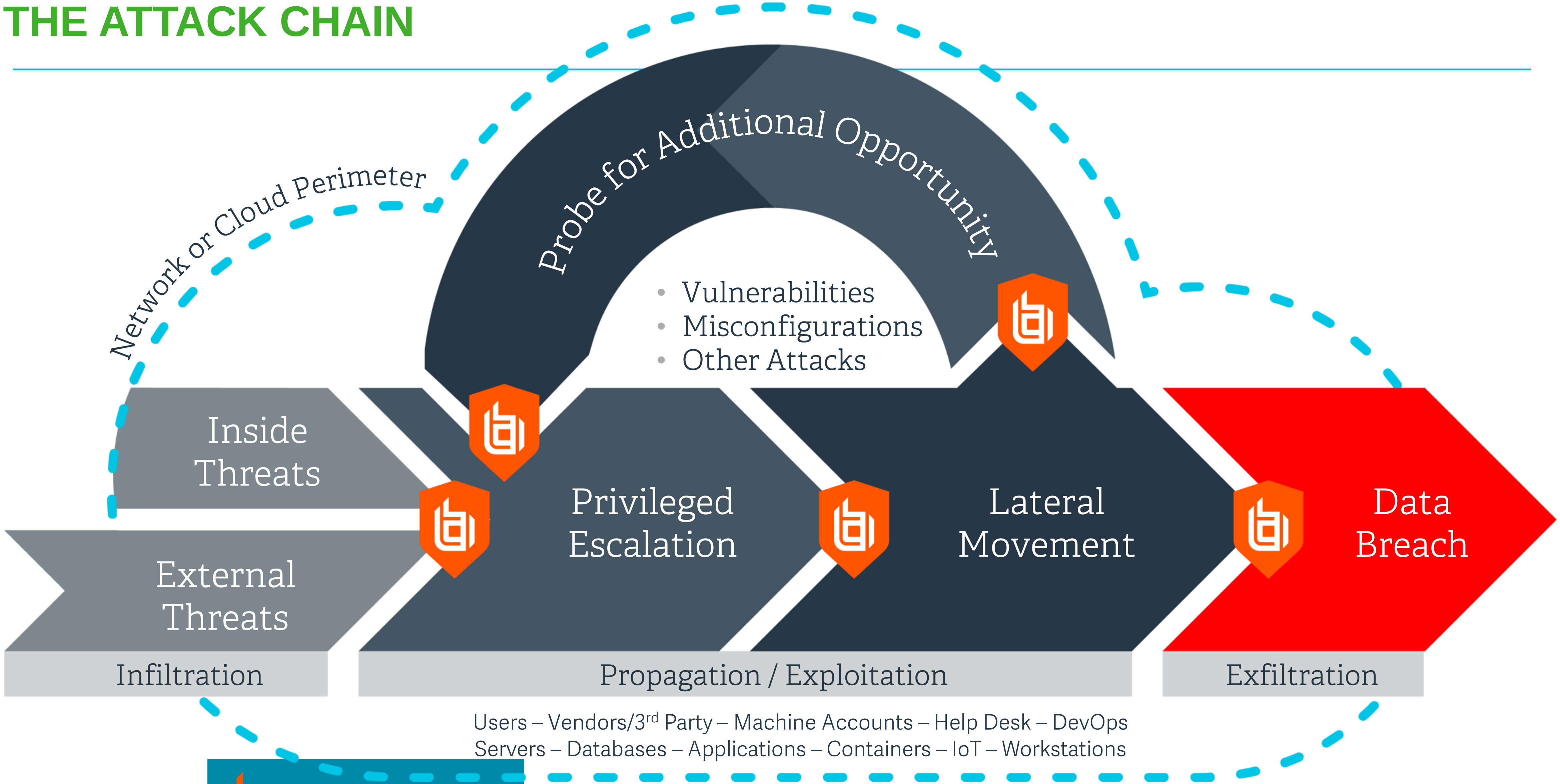
PAM Governance

- PAM Standards and Policies
- Privileged Acct Ownership
- Privileged Acct Reconciliation

Analytics & Reporting

- Reporting on KPI's & KRI's
- Audit
- Forensics

THE ATTACK CHAIN



- Vulnerabilities
- Misconfigurations
- Other Attacks

Infiltration

Propagation / Exploitation

Exfiltration

Users – Vendors/3rd Party – Machine Accounts – Help Desk – DevOps
Servers – Databases – Applications – Containers – IoT – Workstations

SailPoint BeyondTrust

BeyondTrust

SailPoint®

Thank You