Deloitte.

Identity Trifecta

Zero Trust . Cybersecurity Mesh Architecture . Identity Fabric

MAKING AN IMPACT THAT MATTERS since 1845

Identity Trifecta

Around the globe, digital identities are becoming increasingly indispensable for organizations of all kinds - private companies, government bodies and civil society organizations - and for the people and organizations they serve.

But as organizations are increasingly automating, abstracting, and outsourcing their business processes to technology, and boundaries between online or offline, local or cloud, are fading more than ever, the question of how to stay in control is pressing.

Combine this with more sophisticated cyberattacks, and we understand the pressure on security teams and business leaders alike to secure their digital transformation. There are solutions. Combining Digital Identity with Zero Trust Architectures allows us to build trust in an untrusted world.

Our partners

SailPoint · Ping Identity · BeyondTrust · H-Kare Solutions

Identity Trifecta | Zero Trust . Cybersecurity Mesh Architecture . Identity Fabric

New technological capabilities will be more effective when strong cyber strategies are part of the picture.

How will you harness these emerging technologies for business value while ensuring that your cyber strategies and investments keep pace?

For starters, a zero trust approach should be central to your efforts involving new technology.

Zero Trust Architecture enables modern enterprise environments by:

Strengthening security posture

Remove the assumption of trust from the security architecture and authenticate every action, user, and device, which enable a more robust and resilient security posture.

Simplifying security management

Address foundational cyber issues, automate manual processes, and plan for transformational changes to the technology landscape and the enterprise itself.

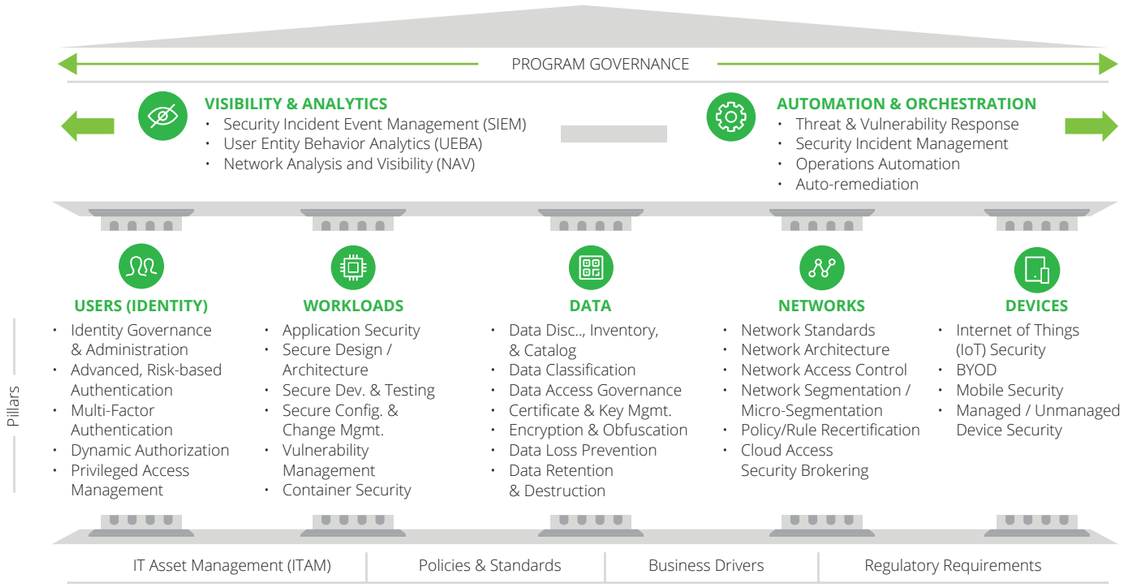
Improving end user experience

Provide seamless access to the tools and data needed to work efficiently.

A zero trust implementation is much more than a technological implementation, it is also a **business and cultural transformation** that is dependent on culture, communications, and awareness.

Deloitte's Zero Trust framework

A Zero Trust model is built upon strong foundational capabilities across five fundamental pillars: user, workload, data, network, and device.



Promises of Zero Trust model

As a modernized infrastructure requires that we approach security differently, Zero Trust can help leverage new capabilities and opportunities to close the transformation gap and become more agile and efficient

Challenges of traditional model			Benefits of Zero Trust	
Fix Location	An organization's infrastructure is known / easily identified by the adversary, with no ability to adjust or adapt based on threats	→	**Evasive**	Fully-integrated and cohesive approach that protects the organization regardless of where connections are coming from
Perimeter Centric	Even with layered defenses, a significant breach in an organization's wall/perimeter can be catastrophic (e.g., ransomware)	→	**Ubiquitous security**	Isolation and identification of user, device, resource and the data being processed by each of them in combination with a high degree of orchestration and automation results in a secure and resilient environment
Limited Visibility	Threats are identified as they hit the perimeter, defenses largely focus within the borders of the corporate network	→	**Increased Visibility**	Active defense technologies, analytics such as anomalous detection, machine learning, artificial intelligence (AI) and real-time data inventory and catalog allow organizations to gain broader, real-time visibility into their threat landscape
Reactive	Security teams take action when an attack is identified and hope that their layered defenses hold and allow for rapid containment	→	**Predictive**	Organizations can anticipate adversary movements, adapt and adjust 'in the field', and initiate preemptive action if necessary, contextualized by a data inventory that enhances situational awareness of where sensitive data is stored and processed

Identity Trifecta | Zero Trust . Cybersecurity Mesh Architecture . Identity Fabric

Identity Fabric Layer Overview

Following the principles of CSMA, it is essential to establish a Identity Fabric comprising solutions that support composable, distributed and collaborative capabilities.

Principles of Cybersecurity Mesh Architecture

Composable

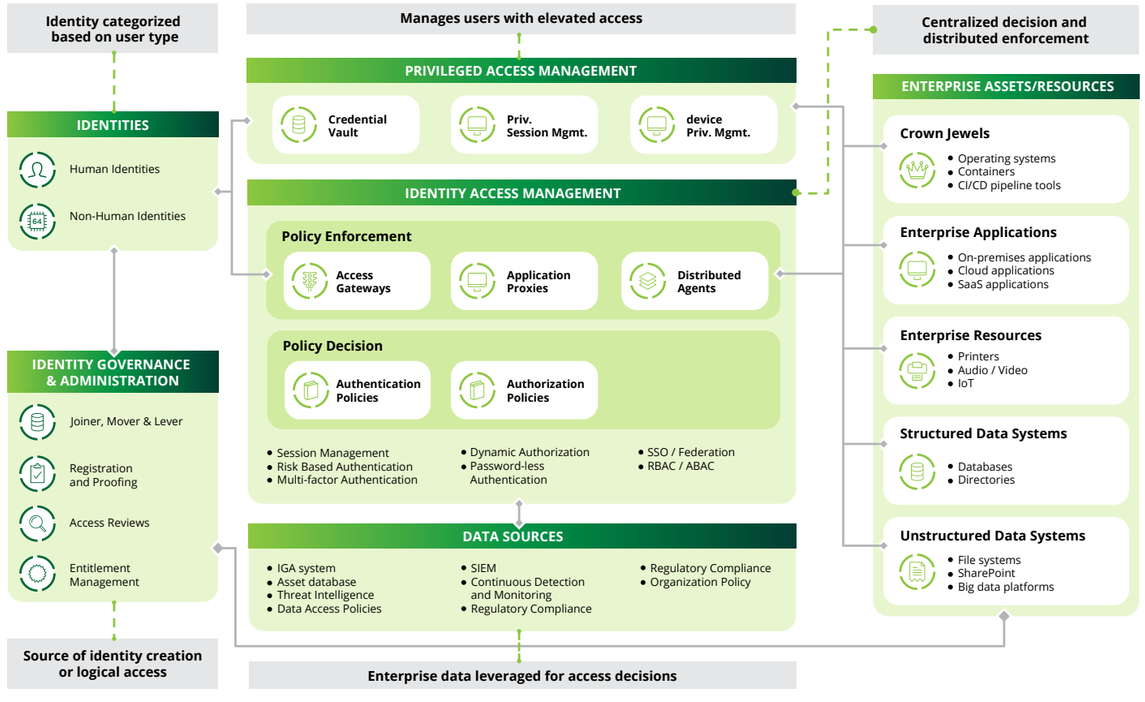
Choose tools that are composable: provide APIs for inversion of control, provide mechanism for entitlement management (admin time) or dynamic externalized (runtime) authorization

Distributed

Choose tools that can run in a distributed manner: support standards-based authentication (OAuth/OIDC/SAML), support standardized attribute lookup via OIDC or SCIM support

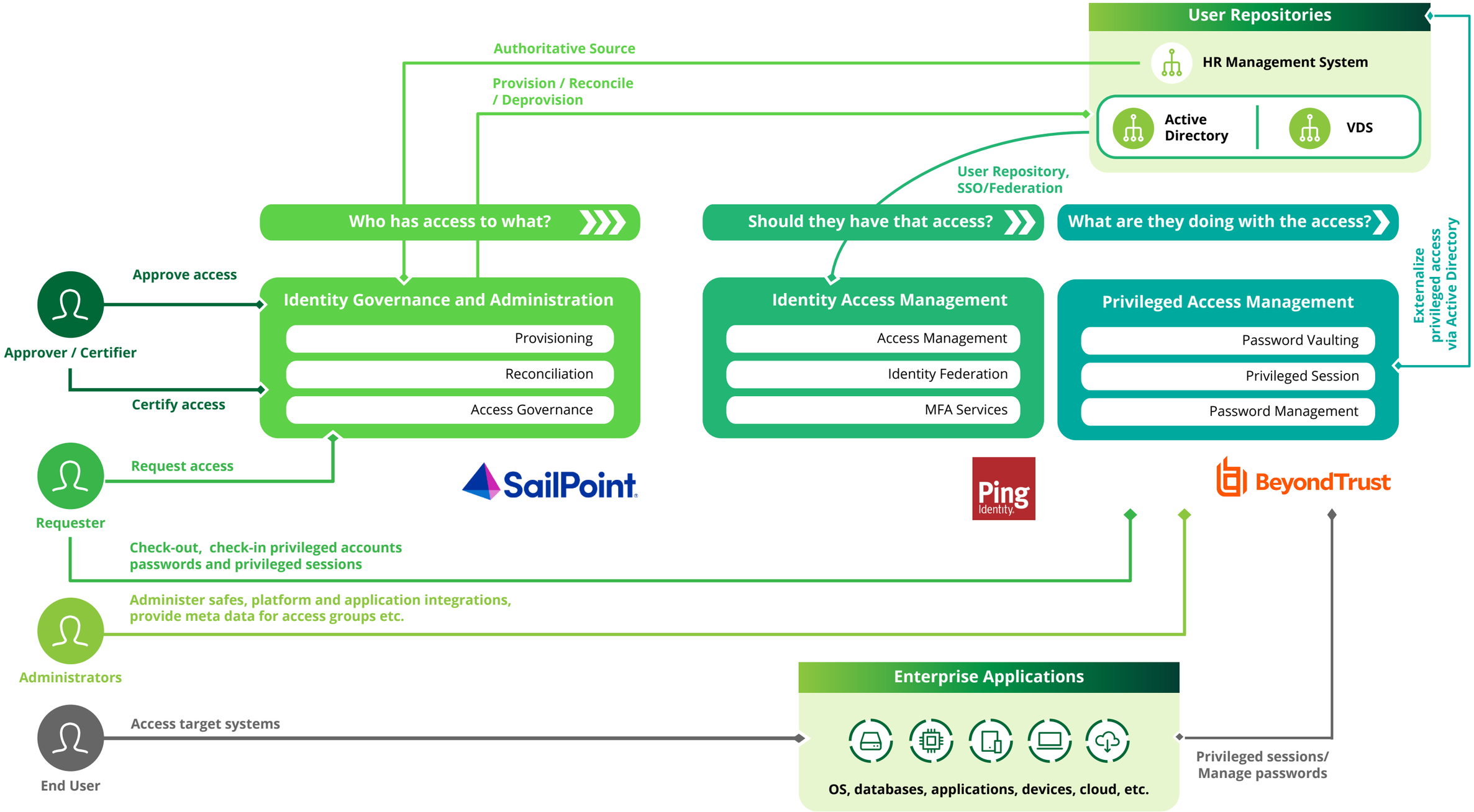
Collaborative

Choose tools that are collaborative: share and consume risk signals (OpenID continuous access evaluation protocol/shared signals and events framework), extensible security analytics capabilities



Identity Trifecta | Zero Trust . Cybersecurity Mesh Architecture . Identity Fabric

Identity Trifecta - IGA, IAM and PAM



Digital identity services

Password Management
- Password Synchronisation
- User Self-Service Password Changes
- Password Policies
- Lost/Forgotten Password Recovery

Privileged Account Management
- Privilege Session Management
- Privilege user Password Management
- Root/Admin User Tracking
- Service Account management
- Transaction Management

Role Based Access Control
- Role based Provisioning
- Exception management
- SOD Definition/Enforcement
- Role Operations Management
- Role Engineering
- Role Lifecycle Management

Access Management
- Simplified Sign-on
- Device Authentication
- Internal Access Management
- External Access Management
- Single Sign-On
- Risk/Adaptive/Strong Authentication
- API Security

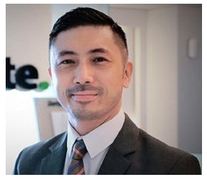
Access Governance
- Access Recertification
- Reporting
- Risk Profiling
- Access Remediation
- Access Reconciliation

Identity Administration
- Delegated Administration
- Central Administration
- User Self-Service Access Requests
- Request/Approval Management
- Automated Provisioning
- Identity Verification
- Identity Account consolidation

Identity Trifecta | Zero Trust . Cybersecurity Mesh Architecture . Identity Fabric

Contact us

Eric Lee
SEA Identity Leader
Delotte Singapore
ewklee@deloitte.com
+65 6800 2100



Alex Cheung
Partner
Deloitte Indonesia
alecheung@deloitte.com
+62 21 5081 9609

Gonzales, Ronald Allan
Partner
Deloitte Philippines
gonzgonzales@deloitte.com
+63 27 730 5290

Jiravachara, Parichart
Partner
Deloitte Thailand
pjiravachara@deloitte.com
+66 2034 0130 | ext=40130

Ho, Siew Kei
Partner
Deloitte Malaysia
sieho@deloitte.com
+60 3 7610 8040

Deloitte.

Designed by CoRe Creative Services. RITM1277459