Deloitte.

Identity Solutions

Emerging Identity Trust Services

Building trust, bolstering reliability

Trust is the foundation of all business. But with global supply chains, remote work, the Internet of Things (IoT) and e-commerce making it increasingly difficult to know exactly who you are dealing with, verification by password—once the standard—is no longer sufficient.

With Deloitte's Emerging Identity Trust Services, your organization can strengthen its cybersecurity stance by reducing dependence on passwords, which are increasingly vulnerable to breaches and attacks. With advanced measures such as passwordless authentication, biometrics, and adaptive authentication, we'll help you bolster your cybersecurity posture while creating an exceptional user experience. After carefully assessing your needs, we can design (or source) and implement your emerging identity solutions, seamlessly integrating them with your existing architecture to let you focus on outcomes instead of outputs.

Our Emerging Identity Trust Services

1. Identity proofing and verification

An essential part of Emerging Identity Trust Services, our identity proofing and verification offerings help ensure identity across public and private sectors.

Identity proofing is the end-to-end process of verifying the identity of individuals attempting to access an application or service.

Identity verification, a capability within identity proofing, is the process that confirms a valid identity is associated with the correct individual.

Notable emerging features of identity proofing include:

- **Machine learning and artificial intelligence (AI)** to analyze validity of the supplied document.
- **Advanced biometrics and liveness detection** to compare the picture of the applicant on the document to the selfie.
- **Fraud mitigation** through watchlists, authenticity checks, pattern analysis, and risk scoring.

Our identity proofing and verification methods can be combined and tailored to your organization's specific requirements to establish a high level of confidence in an individual's identity before granting that person access to sensitive information or services.

Reasons to implement:

Identity theft:
Fraudsters may steal or impersonate someone else's identity to gain unauthorized access to resources, services, or financial accounts. They may also use stolen documents or personal information to pass the identity verification process.

Weak or inadequate authentication methods:
Some authentication methods, such as knowledge-based verification relying on static personal information, can be vulnerable to breaches and data leaks. If personal information is compromised or publicly available, it becomes easier for fraudsters to bypass your verification process.

User experience:
Striking a balance between security and a seamless user experience can be challenging. Strict verification processes, especially those involving multiple steps or biometrics, can be time consuming and frustrating for users, potentially leading to abandonment or dissatisfaction.

Cross-border verification:
Verifying identities across borders can be complex due to variations in identity documents, formats, and verification systems. Different countries may have distinct standards and practices, making international identity verification especially challenging.

Evolving fraud techniques:
Fraudsters continually adapt and develop new techniques to bypass identity verification processes. This includes exploiting vulnerabilities in systems, leveraging advanced technology, or social engineering techniques to deceive individuals or organizations.

Our capabilities:

- **Strategy/road map:** Developing your strategy for identity proofing and verification is the first step toward implementing tools or frameworks to address challenges.
- **Implementation:** Deloitte has extensive experience in implementing tools, features, and frameworks to address identity proofing and verification challenges. Technologies that can be implemented include multi-factor authentication, biometric technologies, data protection tools, logging and monitoring tools, AI tools, and fraud detection tools.
- **Operations:** In addition to implementation services, Deloitte provides operations services to help maintain and monitor identity proofing and verification tools.

2. Zero Trust

Deloitte's Zero Trust solution is a security framework requiring all users—whether inside or outside your organization's network—to be authenticated, authorized, and continuously validated for security configuration and posture before being granted (or permitted to keep) access to your applications and data. Zero Trust assumes there is no traditional network edge; networks can be local, in the cloud, or a combination, with resources and workers located anywhere.

Reasons to implement:

Increased need for workforce mobility and flexibility:
Many businesses are moving to remote and virtual working models, increasing the need for transparent and strong approaches to identify, manage, and reduce risk.

Push toward digital transformation:
Increased use of emerging technologies, such as cloud and machine learning, increases the surface area for vulnerabilities and the need to keep your organization's security at the heart of modernization.

Increased outsourcing of "core" services:
To achieve desired efficiencies and flexibility, organizations are expanding not only the number of business operations that are outsourced but also activities that are considered critical services, including cybersecurity. This has increased the need for broader cybersecurity programs.

Increased scale, complexity, and frequency of cyberattacks:
Data breaches are often a top concern for executives responsible for the security of highly confidential information. Increasingly, cybersecurity and cyber resilience are two of the top trending topics on board agendas.

Our capabilities

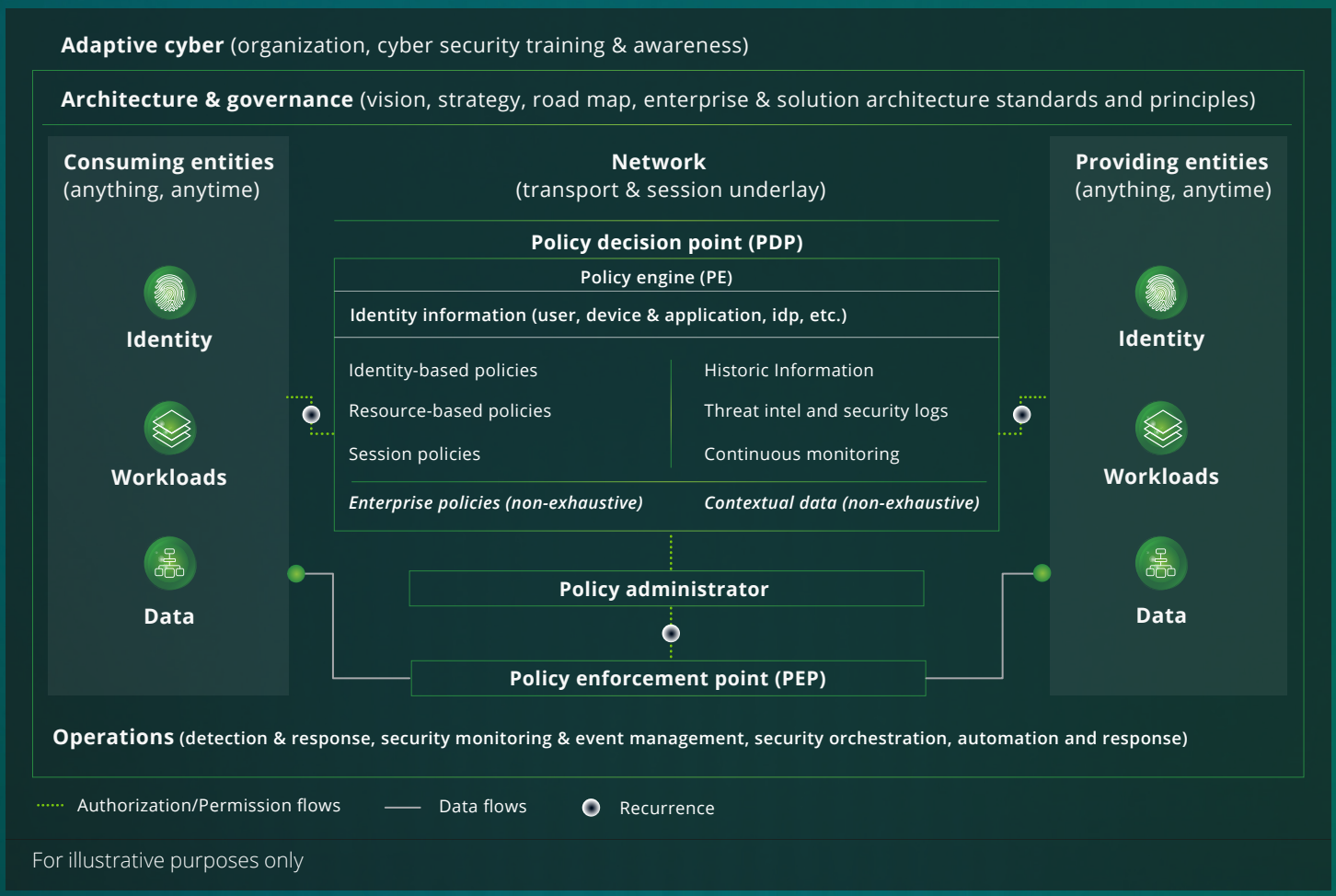
Zero Trust architecture

- Deloitte's functional architecture helps to define a customized Zero Trust reference architecture that is well aligned with your organization's Zero Trust strategy and ambition.
- The functional architecture takes the seven key National Institute of Standards and Technology (NIST) Zero Trust principles into consideration and outlines key Zero Trust architectural building blocks.
- In addition, the architecture is based on the Deloitte Zero Trust domain model and is accelerated by our Zero Trust domain assessment tool.

Deloitte accelerators | Zero Trust architecture

Deloitte created a functional architecture that is a valuable baseline to design Zero Trust reference architectures.

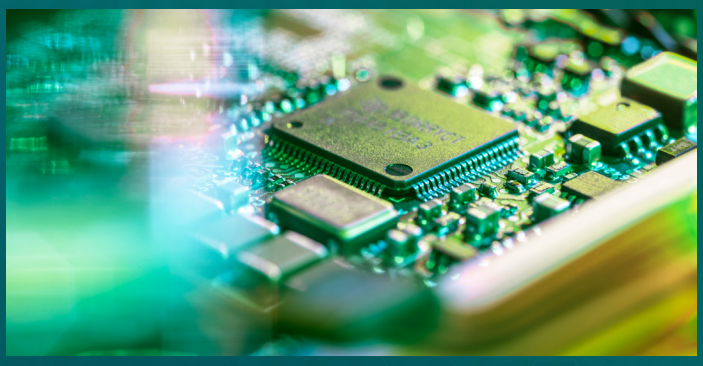
Overview: Deloitte's functional Zero Trust architecture



For illustrative purposes only

Zero Trust domain model and tool

- Our Zero Trust model is built upon nine strong foundational domains that represent business drivers and areas of an end-to-end transformation.
- To design your organization's Zero Trust journey, we built a model and tool that seeks the capabilities and respective requirements per domain and maturity stage.
- These accelerators contribute to the current maturity assessment and identification of initiatives to fill the gap toward the to-be status and ambition.



Deloitte accelerators | Zero Trust domain model and tool

Deloitte built a model and tool that seeks to support conducting comprehensive reviews and assessments.

Overview: Deloitte's Zero Trust domain model & tool

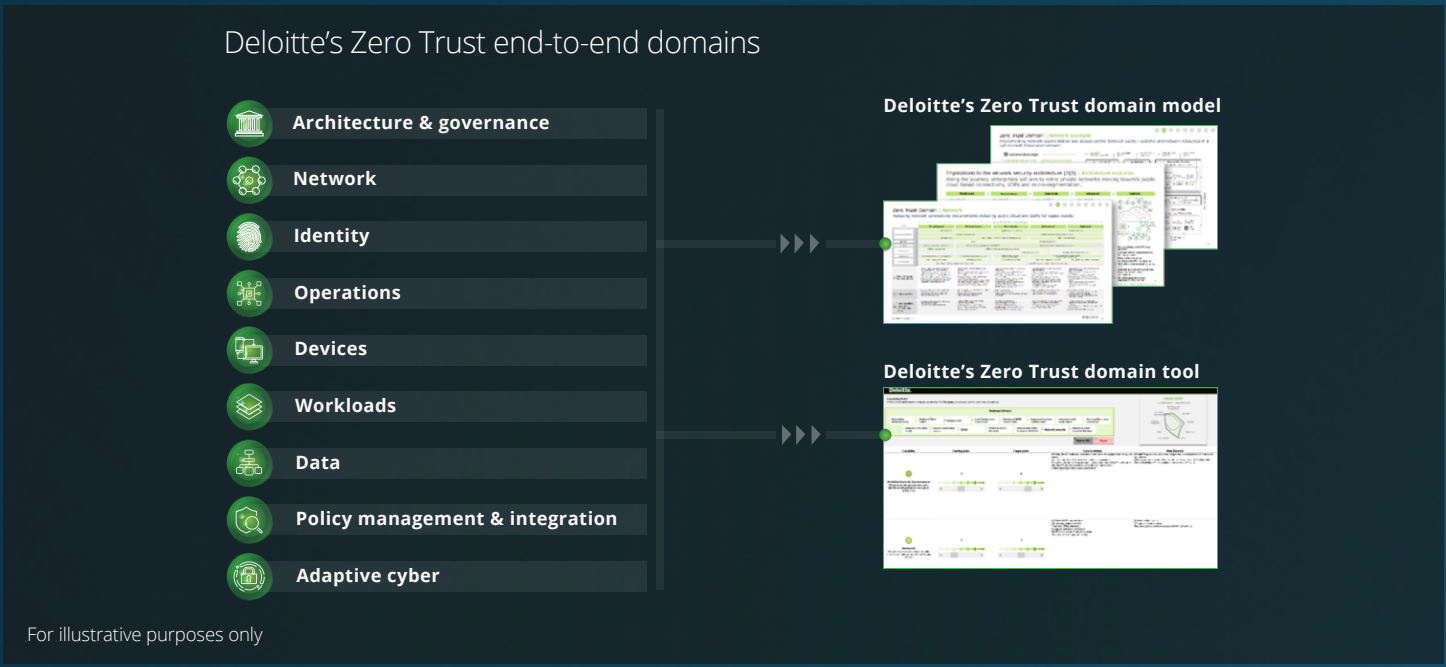
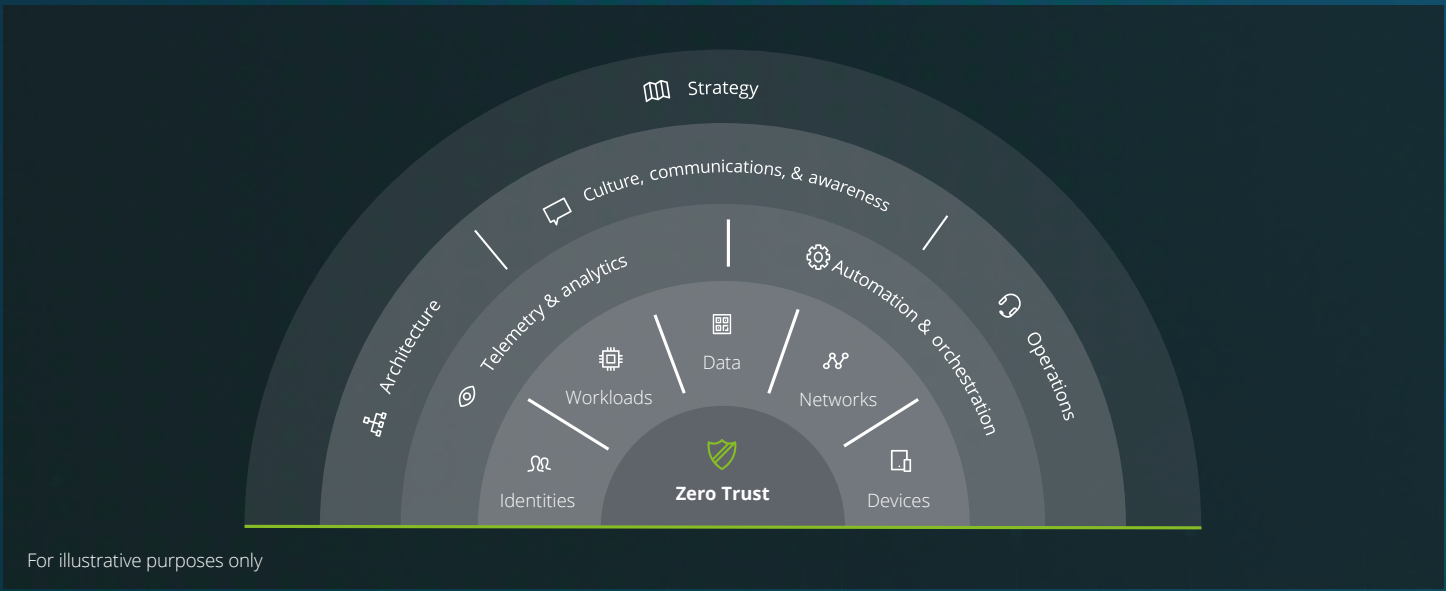


Figure 1 | Deloitte's Zero Trust framework



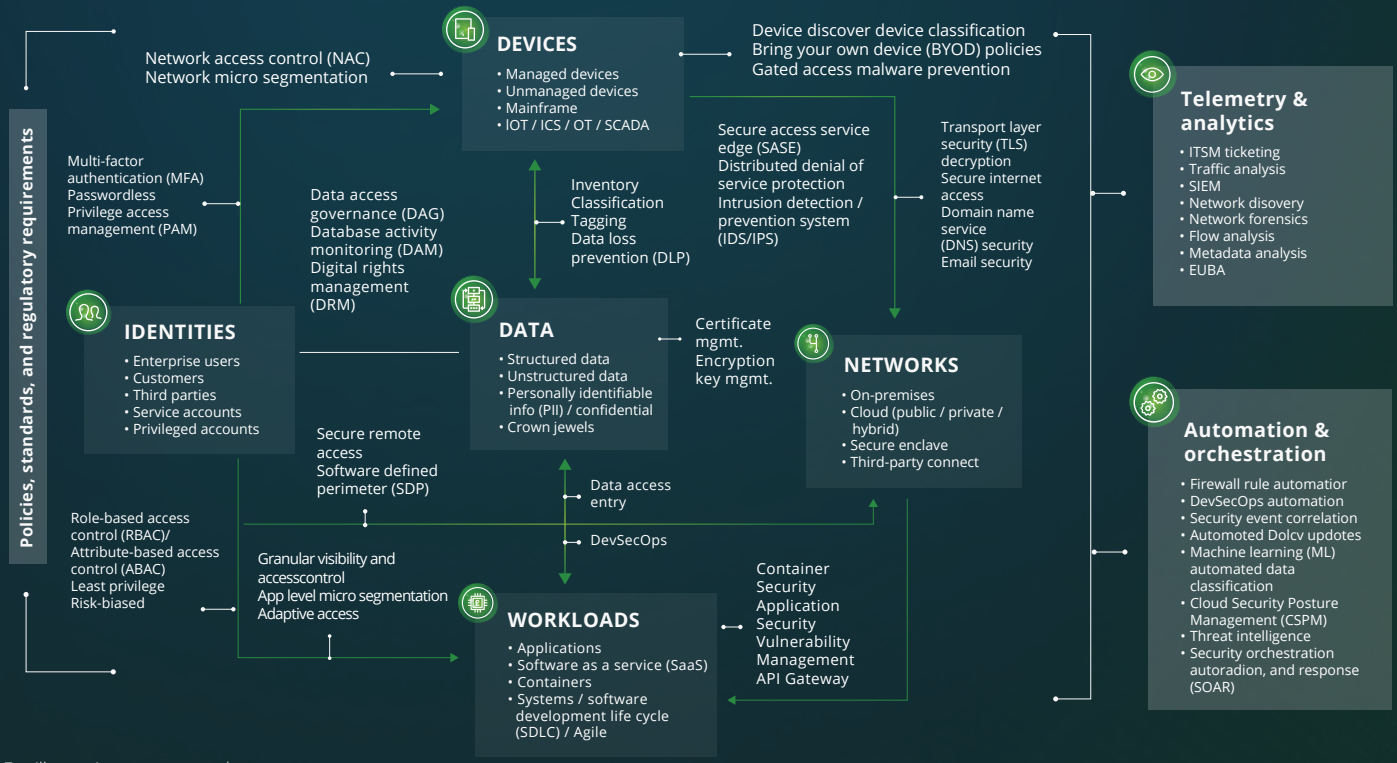
Deloitte's Zero Trust framework is built upon strong foundational capabilities across five core domains: identities, workloads, data, networks, and devices. The framework emphasizes the importance of identity-based access control decisions and the need to shift toward user profile, entitlements, authorization, and acceptable usage pattern.

- Identities are the new "perimeter" in a Zero Trust architecture. The framework emphasizes identity-based access control decisions to enhance security.
- Workloads hosted on legacy infrastructure or in cloud environments should be hardened, segmented, and monitored on a granular level. Adaptive actions, such as limiting access or blocking uploads to specific applications, should be implemented.
- Data lies at the heart of an effective Zero Trust strategy. It should be discovered, inventoried, governed, classified, and tagged to inform access control decisions. Data should also be protected through obfuscation, encryption, and advanced data loss prevention mechanisms.
- Networks carry traffic between identities, devices, and workloads. Controls should segment, monitor, and analyze network activity, operating on the assumption that all network connection requests are inherently untrustworthy.

- Devices, including managed and unmanaged endpoints, as well as smart devices should be continuously assessed for risks and threats. Compliance with defined security policies should be evaluated.
- The framework also includes an enabling layer, which involves telemetry and analytics systems for event correlation and advanced analysis, as well as automation and orchestration capabilities for proactive security posture. The governance layer encompasses architecture principles, culture communications, awareness, and organizational change management updates. The outer ring focuses on aligning the Zero Trust strategy with business drivers.
- By implementing strong capabilities across the core domains and enabling layers, organizations can establish an agile and dynamic security foundation that is resilient to organizational change and adaptable to modern business, workforce, and technology trends. Deloitte's Zero Trust framework provides a comprehensive approach to cybersecurity, enabling organizations to protect sensitive enterprise data and improve their overall security posture.

Illustrative reference architecture

This illustrative Zero Trust reference architecture shows an end-to-end approach to network/data security that encompasses the five Zero Trust domains and the interconnecting infrastructure between them.



For illustrative purposes only

Deloitte's approach to implementing Zero Trust:

Not all organizations use a big-bang approach to implement Zero Trust. By using an evolution approach rather than a revolution approach, Zero Trust can be implemented in the following stages, with nominal business interruptions.

- Establish a baseline: Identify user base, critical apps/services/ data, third-party integrations, business processes and technology requirements, and capability gaps.
- Set the strategy: Prioritize initial use case(s) in low-risk environments to help reduce disruption.
- Pilot and test: Identify proof-of-concept (PoC) candidates/ timeline, monitor progress and risks, and document lessons learned.
- Implement incrementally: Taking an iterative approach, implement one discipline/use case at a time and conduct user awareness training as required and capture metrics/reporting on potential impact to an organization.

3. Advanced authentication

Increase in identity theft and account takeovers in recent years has necessitated enhanced digital authentication to help organizations protect their customers and their online presence. Advanced authentication is a sophisticated approach that combines active, passive, and account-level data* to calculate the risk score of a login attempt and determine the authentication level needed.

*Active data: What you know/are/have. Passive data: Collected transparently to the customer, e.g., device data, session information, cursor movement. Account-level data: Collected based on past account information and cross-channel transactions, e.g., machine learning.

Reasons to implement:

- **Weak or inconvenient authentication** of user accounts creates opportunities for malicious users to hijack legitimate accounts.
- **Unsecured exchange of identities and attributes** between systems creates foundational authentication issues that compromise security across the organization.
- **Complex access and authorization policies** make it difficult to adapt to ever-changing regulations and market conditions.
- **Passwords** continue to be one of the weakest links in the digital life cycle.

Our capabilities

Deloitte uses the layered approach to implement advanced authentication and detect fraud.

1. **Authentication using basic credentials:** Using user ID/password and knowledge-based authentication (KBA)
2. **Third-party data sources:** Using external data for customers' identity verification
3. **Device data:** Fingerprinting the customer device and building an internal negative database
4. **Session monitoring:** Analyzing the session logs to detect bot activities (system attacks and fraudulent attacks)
5. **Behavioral/voice biometrics:** Utilizing passive biometrics, such as accelerometer data for mobile devices, typing speed, reaction times, and voice pitch/tone
6. **Clustering and link analysis:** Leveraging machine learning analytics to perform link analysis at account level and device level to detect anomalies

4. Access management

Access management refers to the processes and practices used to control and manage user access to resources, systems, and data within an organization. It encompasses the policies, technologies, and procedures that govern the authentication and authorization of users to determine that they have relevant levels of access based on their roles, responsibilities, and business needs. Our access management offering has the following key components:

- **Authentication:** The process of verifying the identity of a user or device. It ensures that users are who they claim to be before granting access to resources.
- **Authorization:** Once a user's identity is authenticated, authorization determines the level of access they are granted based on their role, permissions, and policies.
- **Role-based access control (RBAC):** RBAC is a widely used authorization model that assigns permissions and access rights to users based on their predefined roles or job functions within an organization. It simplifies access management by associating permissions with roles and managing access based on those roles.
- **Access policies and controls:** Access policies define the rules and criteria for granting or denying access to resources. These policies are typically based on business requirements, compliance regulations, and security leading practices.
- **Centralized user access management:** This creates a secure repository of identities for administration.
- **Periodic access reviews:** This ensures your users have the right access to the right resources and prevents prolonged, unwanted access.
- **Audit and monitoring:** Continuous monitoring and auditing of user activities, access requests, and system events are crucial for detecting and mitigating potential security incidents.

Reasons to implement:

- Attaining a common understanding of the enterprise-wide **identity program risks and issues**
- **Exponentially increasing user access proliferation** (on-prem and cloud), inconsistent entitlement management, and siloed policy enforcement
- **Enhancing governance** over distributed/disjointed provisioning processes for high-risk apps with a scope limited to elevated infrastructure access and capacity limited to the corporate directory
- **Ongoing regulatory compliance pressure** and a need for an efficient identity governance process for access reviews
- **Integrating identity governance and administration (IGA) principles** within other processes and groups

Our capabilities

- **Risk and compliance-focused approach for IGA** – Designing an IGA program that weaves in the required risk and control aspects from the very beginning of the program helps your organization save costs, reduce risk, and improve compliance.
- Deloitte offers a range of **scalable IGA solutions** that address different client issues around identity governance even in the most complex of environments. We provide unique value through the following identity benefits:
  - **A mature methodology for role management** to pilot and adopt concept of roles across the enterprise
  - Consistent **compliance with privacy and security requirements**
  - **A global talent pool** with years of experience on a range of market-leading IGA products

To learn more about how your organization can benefit from adopting these emerging identity capabilities and enhance its overall security posture, please reach out to any of the below contacts.

Anthony Berg
Principal
Identity & Access Management Leader
Deloitte & Touche LLP
antberg@deloitte.com

Naresh Persaud
Managing Director
US Cyber & Strategic Risk
Deloitte & Touche LLP
napersaud@deloitte.com

Laxman Tathireddy
Principal
Emerging Identity Trust Leader
Deloitte & Touche LLP
ltathireddy@deloitte.com