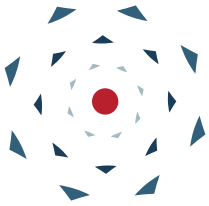


IDENTITY DEFINED
SECURITY ALLIANCE

WHITEPAPER

IDENTITY DEFINED SECURITY FRAMEWORK

Putting Identity at the Center of Security

INTRODUCTION

We live in an increasingly connected world. The issue of identity, and its inherent connection to security, is more important than ever. The explosion of cloud, mobile devices, and connected things, as well as the consumerization of information technology (IT), has increased the risk of a cyber security attack due to compromised identities, accounts and credentials. A high-profile breach can lead to significant financial and reputational harm.

In the last several years, identity has started the transition from an operational and user experience driven entity, to its current recognition as the core component of security. Despite the increase in credential related breaches and the shifting focus to identities and actions as the mechanism for insight into security events, the majority of organizations are still not leading with this premise. A lack of Identity and Access Management (IAM) maturity, an over-abundance of complex security technologies and confusion over where to start are just a few reasons that organizations miss this inherently valuable identity:security connection.

The Identity Defined Security Alliance (IDSA) was created to help organizations recognize the importance of bringing identity and security together, reducing the risk of a breach through identity-centric security strategies. More importantly, the IDSA is aimed at breaking the problems into common identity-centric security outcomes and implementation approaches – with the goal of providing guidance and tips for practitioners.

TODAY'S CHALLENGES

Today's investments in security solutions are yielding positive results, but a number of forces play a role in marginalizing their effectiveness. The majority of these solutions provide either a single-point defense mechanism, or require skilled security personnel who can detect, recognize and remediate a sophisticated attack. In addition, organizations and external threats have been evolving in numerous ways, including:

- Explosion in users, identities and environments
- Increased interconnectedness with customers and partners
- Massive amounts of data outside of IT controls
- Consumer-oriented technologies and concepts moving into the enterprise
- Malicious actors are becoming more sophisticated and organized
- Insider threats that are as real and perhaps even more lethal than outsider attacks

It's clear from the dynamic enterprise landscape that cybersecurity is relentlessly and cumulatively challenging. This evolution provides overwhelming evidence that a new security strategy is required to meet the changes in how we do business, as well as combat the threats that emerge every day.

IDENTITY DEFINED SECURITY

This new approach is grounded in four foundational concepts:

- Identity is a critical cyber security technology
- All aspects of cyber security must fundamentally work together if they are to achieve meaningful effectiveness
- Every business transaction, attack surface or target involves a credential and a service or piece of data
- Given the cumulative investment in security, each new investment is increasingly measured for its ability to make the whole more effective

It's these foundational concepts that have led to a new way of thinking about security – threading identity through end-to-end cyber security investments. This new approach:

- Leverages increasingly open and API-first technology stacks
- Steers the focus away from single point defense mechanisms to include a broader set of identity and security components
- Delivers a fresh, balanced set of detective and preventive controls
- Enables organizations to tackle security with a more precise, identity-aware and identity-specific approach

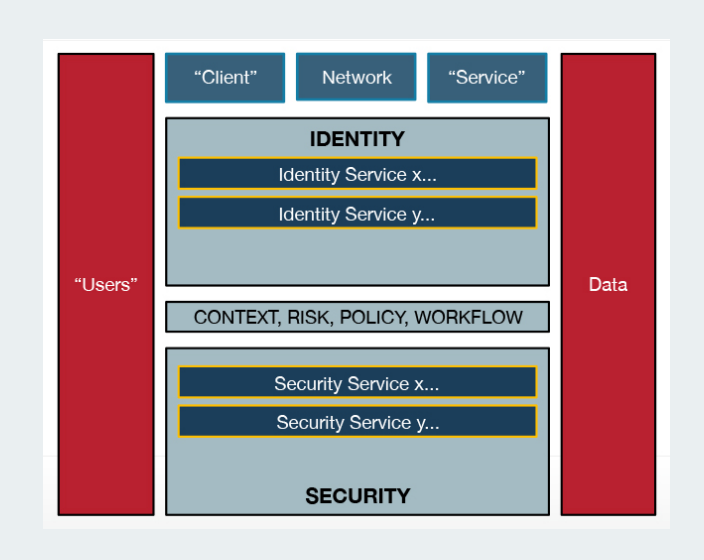


Figure 1: High-level Identity Defined Security Architecture

MAKING IDENTITY AND SECURITY WORK BETTER TOGETHER

In the past, identity has often operated outside of security. The goal of the IDSA is to move toward an identity-centric strategy by defining a framework for Identity Defined Security (IDS). It starts with a set of core technology components. These components are similar to those used in many discussions around digital transformation, hybrid access, Zero Trust, etc.

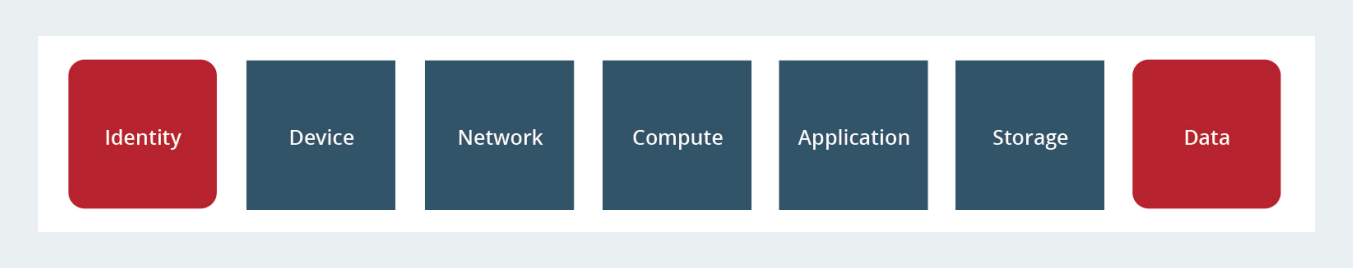


Figure 2: Identity Defined Security Technology Components

These core technology components serve two main purposes. They capture the different ways data is accessed across technology components illustrating the interaction between various actors (users, processes, etc) and the target data.

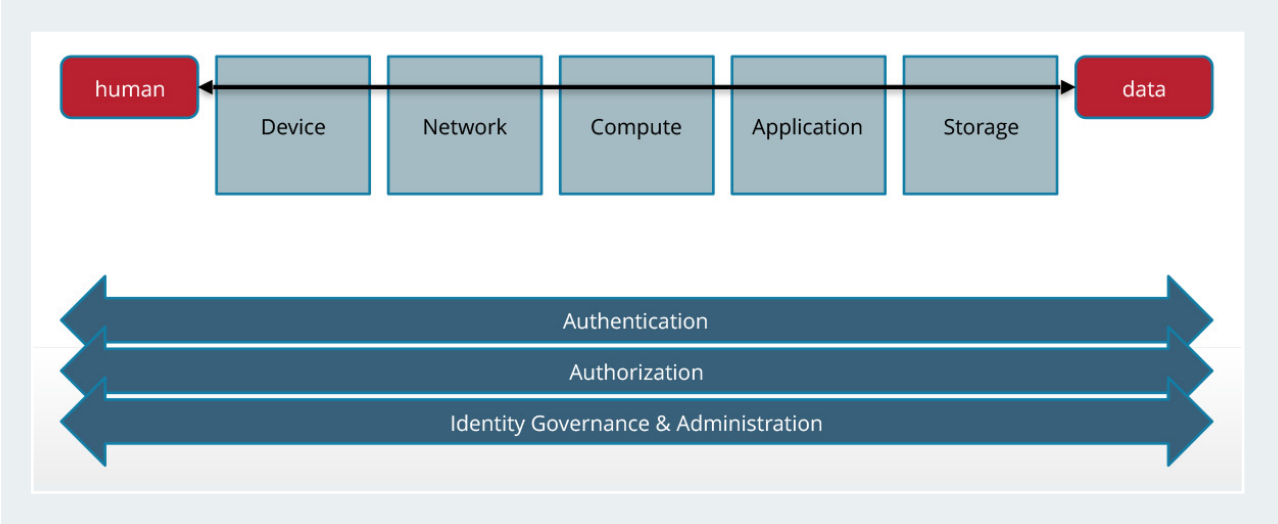


Figure 3: “Human to Data” Scenario Example

The core components also provide the foundation for the Identity Defined Security Reference Architecture illustrated in figure 4.

IDENTITY DEFINED SECURITY REFERENCE ARCHITECTURE

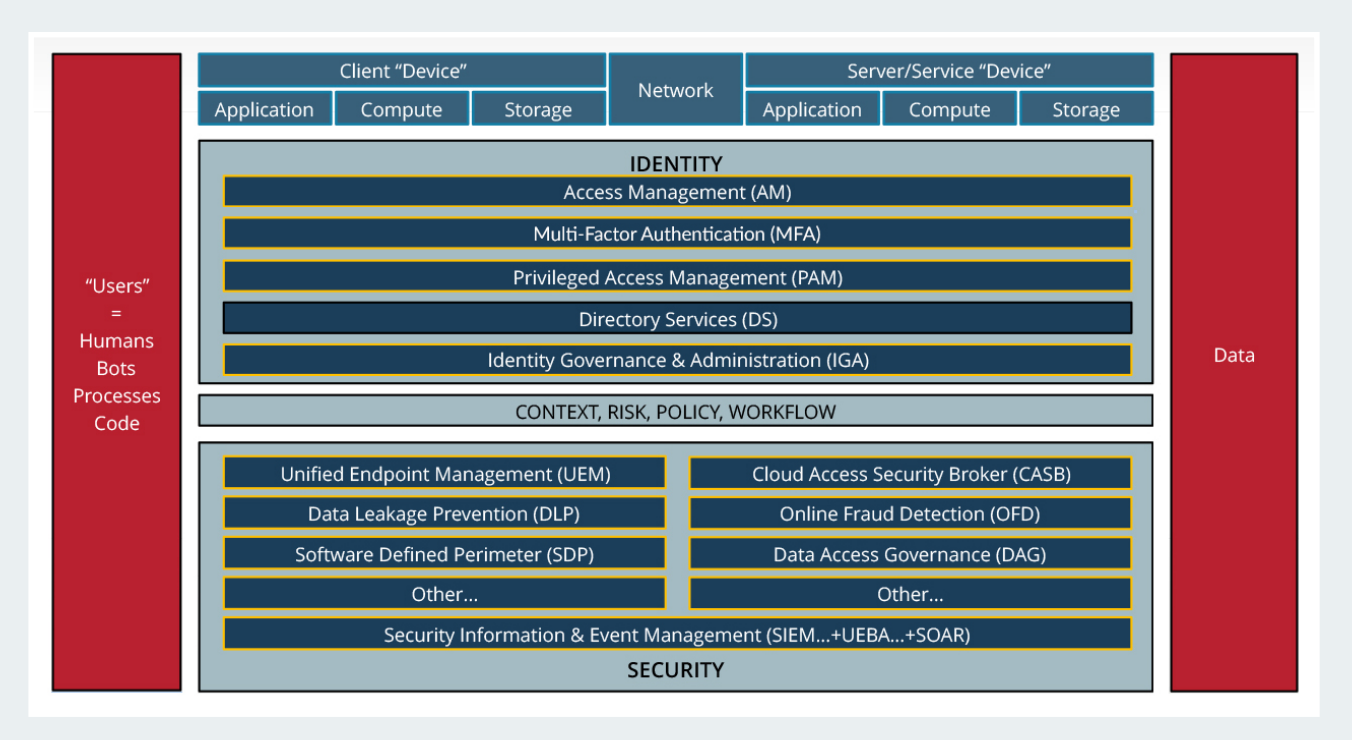


Figure 4: Identity Defined Security Reference Architecture

Getting Started – Identity Defined Security Framework

The Identity Defined Security Framework, collaboratively developed by leading vendors, solution providers and practitioners, provides organizations with practical guidance on implementing an identity-centric approach to security. It provides practitioners with a set of fundamental building blocks along with blueprints and best practices that help achieve security outcomes that support the needs of the business.

Identity Defined Security Outcomes

An Identity Defined Security Outcome is a desired result that improves an organizations security posture through identity-centric security and reduces the risk of a breach or failed audit.

Identity Defined Security Approach

Identity Defined Security Outcomes can be achieved through many different Identity Defined Security Implementation Approaches. These approaches are well-defined patterns combining identity and security capabilities that help organizations leverage an identity context to improve security posture.

Best Practices

The foundation of an identity-centric approach to security ideally begins with a mature Identity and Access Management (IAM) program but is not always required. An initial set of best practices defined by the IDSA focused on IAM fundamentals, serve as recommended hygiene tips related to the people and process, as well as the technology aspects of an IAM program, and augment the foundation of an identity-centric approach to security.

Below is an example of one identity-defined security implementation approach to achieve a specific identity-defined security outcome.

Outcome: Access is revoked upon detection of a high-risk event.

Description: Security related alerts or events captured by systems indicating that a potential breach of policy has occurred should result in the violating identities access being revoked in an expedited manner.

Value: Organizational exposure to defined policy breaches is monitored and reduced.

Approach: Integration of systems with security monitoring capabilities with identity provisioning capabilities

Components: Security Information and Event Monitoring (SIEM) + Identity Governance and Administration (IGA)

Description: A SIEM deployed in an organization's environment with security monitoring capabilities is integrated with Identity Governance initiating the remediation provisioning process.

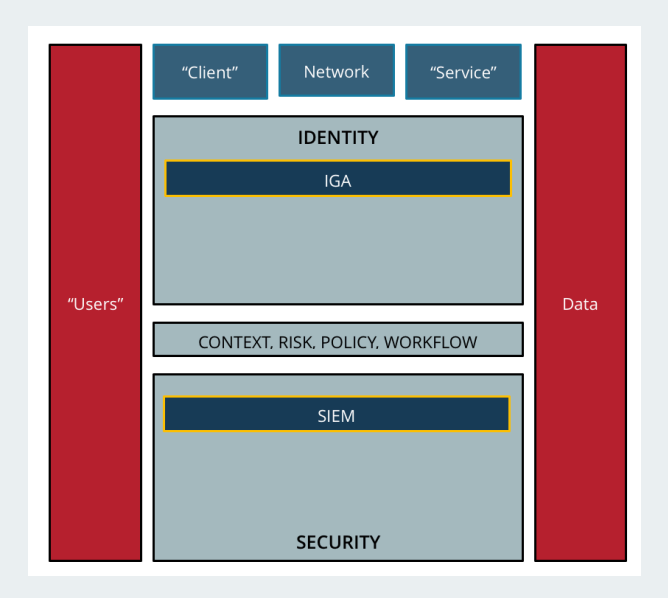


Figure 6: Approach using IGA and SIEM

1. A security policy is defined
2. Monitoring tool detects user violation of this policy
3. Monitoring tool creates alert/event
4. Details of alert/event sent to Governance solution
5. Governance solution revokes user entitlements/permissions used in violation through certification or direct de-provisioning
6. User cannot continue to violate policy based on reduction of entitlements

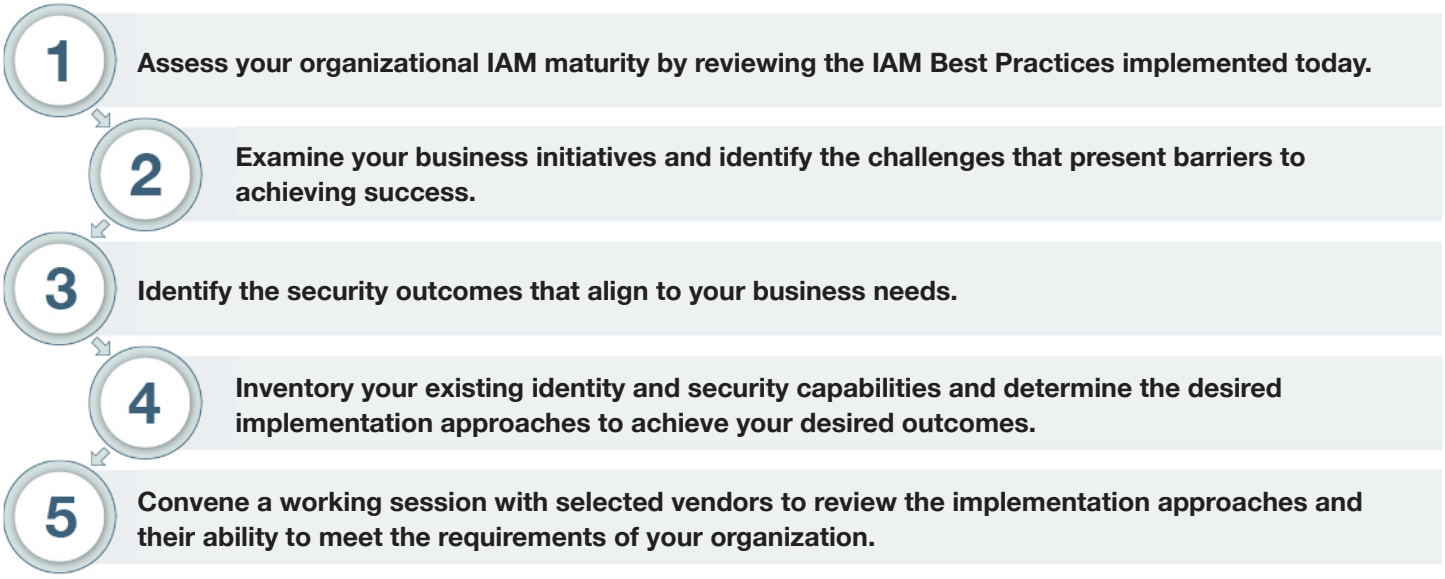
The current and complete library of Identity Defined security outcomes and approaches can be found on the IDSA website.

BRINGING IT ALL TOGETHER

The IDSA is a community of vendors, solution providers and practitioners that provide an independent source of education and information for reducing risk through an identity-centric approach to security. The IDS Framework is the vendor agnostic, practical guidance that organizations need to begin that journey.

Beyond the practical guidance, the IDSA provides a forum for vendors to collaborate on solving industry and customer challenges. In addition to the best practices, the implementation approaches detailed by the alliance give organizations a jump start on determining how solutions from the alliance members can help achieve security outcomes to reduce the risk of an identity-related breach or failed audit.

The path to identity-centric security will vary by business drivers and maturity, but the following is the recommended approach for how to apply the IDS Framework in your organization.



The IDSA is a community built from industry experts that represent practitioners, technology vendors and solution providers. Throughout your journey, use the IDSA as a source of information, as well as a place for continual learning from organizations who have achieved success.

ABOUT IDSA

The IDSA is a group of identity and security vendors, solution providers and practitioners that acts as an independent source of thought leadership, expertise and practical guidance on identity centric approaches to security for technology professionals. The IDSA is a nonprofit that facilitates community collaboration to help organizations reduce risk by providing education, best practices and resources.

We deliver on our mission through…

1. Cross vendor collaboration
2. Thought leadership content
3. Identity Centric Security Framework
4. Customer implementation stories
5. Virtual community for sharing experiences and validation

For more information about the IDSA visit www.idsalliance.org.