Gartner Research

CISO Foundations: 5 Questions CISOs Should Ask About IAM

Oscar Isaka, Henrique Teixeira, Sagar Patel

22 January 2024

Gartner®

CISO Foundations: 5 Questions CISOs Should Ask About IAM

Published 22 January 2024 - ID G00792334 - 9 min read

By Analyst(s): Oscar Isaka, Henrique Teixeira, Sagar Patel

Initiatives: Cybersecurity Leadership; Build and Optimize Cybersecurity Programs

> Identity and access management is a foundational, yet complex, component of every cybersecurity program. To enable digital business outcomes, cybersecurity leaders must move beyond compliance-based IAM and fully integrate IAM into the cybersecurity strategy.

Overview

Key Findings

- CISOs often do not see the identity and access management (IAM) function as a program, leading to a siloed approach that casts IAM as a purely operational activity.
- CISOs often lack comprehension of the IAM program and fail to align it with the security initiatives in the prioritization and planning of projects and initiatives.
- IAM metrics are often performance-oriented, technical and inward-looking, and lack business context that is useful for CISOs and C-level executives.
- Credential compromise is the leading cause of breaches, yet traditional security controls often don't include IAM-specific use cases.
- The broad adoption of cloud services, digital supply chains and a rise in remote access by employees working from anywhere has positioned identity as one of the primary control planes for cybersecurity.

Recommendations

CISOs and cybersecurity leaders looking to expand synergies between IAM and cybersecurity should:

- Educate themselves on the pillars of the IAM program and align it with the cybersecurity strategy.

- Ensure comprehension of the IAM practice in detail by understanding its maturity and gaps so it's appropriately leveraged for planning and prioritization activities.
- Add visibility to the IAM program by aligning it to outcome-driven metrics. Incorporate them to measure the efficiency and coverage of IAM's controls and functions programmatically.
- Become familiar with identity threat detection and response (ITDR) concepts and measures by assessing detective and response controls in place and bridging the gap with existing prevention controls.
- Enable zero trust, and optimize the organization's cybersecurity posture by embracing identity-first security.

Strategic Planning Assumption(s)

Introduction

Remote work, digital transformation and zero trust have recently made IAM a core element and key enabler of the cybersecurity strategy of any organization. However, Gartner inquiry data shows that cybersecurity leaders are seeking more information about the IAM domain, demonstrating a lack of expertise in the area. How can they bridge the cybersecurity and IAM disciplines? CISOs and cybersecurity leaders need to seek answers to five fundamental questions covered in this research to understand how to leverage IAM as a cybersecurity — and digital business — enabler.

Analysis

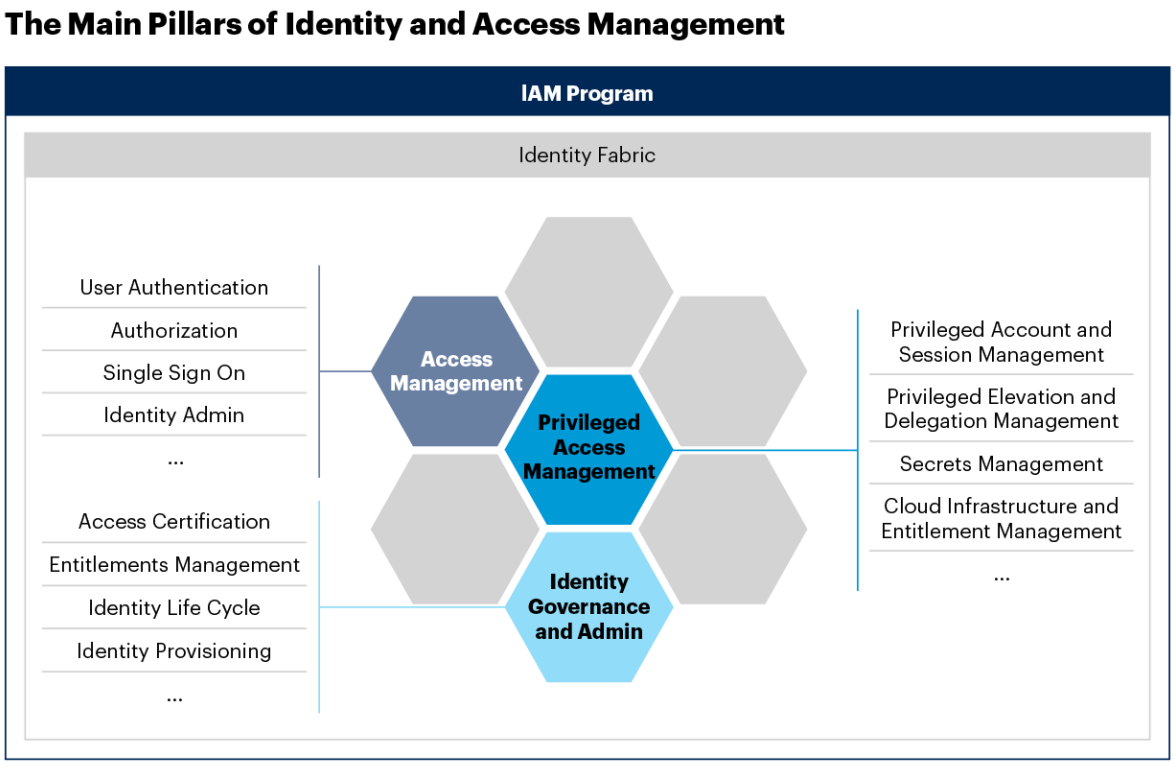
Question 1: What Are the Main Pillars of IAM?

Traditionally, CISOs were not directly involved in IAM operations. Regulatory and compliance requirements have changed this relationship, and CISOs are required to represent the IAM practice in the overarching security strategy and its benefits.

Privileged access management (PAM), identity and access governance (IGA), and access management (AM), supported by a strong IAM program, are key pillars in a cybersecurity strategy (see Figure 1). It is important to understand how they not only satisfy requirements, but also align with the wider digital strategy goals of the organization.

Understanding these pillars will enable cybersecurity leaders to be more aligned with industry terminology, internally communicate about individual IAM requirements and understand the appropriate group of competencies. It will allow the CISO to speak with more confidence about the needs of IAM and cybersecurity as related strategies, as well as understand the specific needs and overlapping benefits of both.

Figure 1: The Main Pillars of Identity and Access Management



IAM Program

CISOs and cybersecurity leaders should adopt a formal program management approach to engage business stakeholders, govern IAM activities, address project and program risks, and accomplish desired business outcomes. This is not a project, but a crucial component of every cybersecurity program. A well-governed program is crucial to success as it requires several deliverables, many of which compete for budget and resources (see IAM Leaders' Guide to IAM Program Management).

Access Management

Access management is the tools, techniques and processes to establish, enforce and manage runtime access controls for internal and external types of identities, interacting with cloud, modern standards-based web and legacy web applications. Multifactor authentication (MFA), API access control and single sign-on are some of the capabilities in this area relevant to the CISO and the cybersecurity strategy.

For more information on access management, see:

- IAM Leaders' Guide to Access Management
- Quick Answer: How Does IGA Differ From AM?
- Critical Capabilities for Access Management

Identity Governance and Administration

IGA are the tools, techniques and processes to manage the digital identity life cycle and govern user access across on-premises and cloud environments. It is responsible for ensuring the right people get the right access to the right resources (for example, applications and data) at the right time for the right reasons. Identity life cycle, segregation of duties, access certification and auditing of IAM are relevant topics within the practice for the CISO (see IAM Leaders' Guide to Identity Governance and Administration).

Privileged Access Management

Privileged, administrative or excessively empowered accounts remain one of the primary targets of attackers and are often responsible for significant breaches. The appropriate management of privileged access enables the principle of least privileged and significantly helps streamline the mitigation of security, operational and business risks created by the inherent power of administrative privileges. Account discovery, privileged operations model, just-in-time controls and secrets management, and machine identity management are relevant topics for CISOs.

For more information on PAM, see:

- IAM Leaders' Guide to Privileged Access Management
- Critical Capabilities for Privileged Access Management

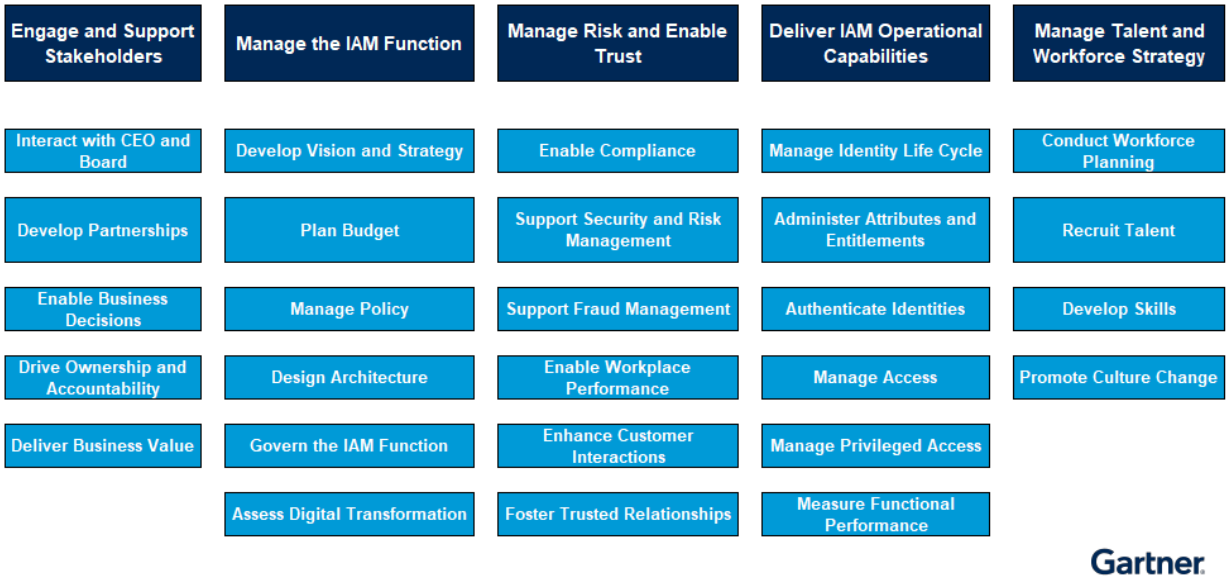
Question 2: How Can I Effectively Prioritize/Plan IAM Work?

Understanding IAM in detail ensures that CISOs and cybersecurity leaders grasp the complexity and depth of the practice and how its controls can be orchestrated to enable better security. The IAM program allows CISOs to establish a governance structure to the IAM work, understand the vision and how it feeds into an appropriately prioritized roadmap and align the enterprise security initiatives. For more information, see A Successful IAM Program Begins With a Vision and Communicate Plans and Manage Program Risks With the IAM Roadmap.

The IT Score for Identity and Access Management can be leveraged as a starting point to assess and evaluate current IAM maturity, identify strengths and weaknesses, prioritize activities and projects, and support establishing an IAM program.

The functional activity map in Figure 2 is a view of what the IT Score for IAM encompasses. For more information, see IAM Leaders' Guide to IAM Program Management.

Figure 2: Functional Activity Map for IT Score for IAM



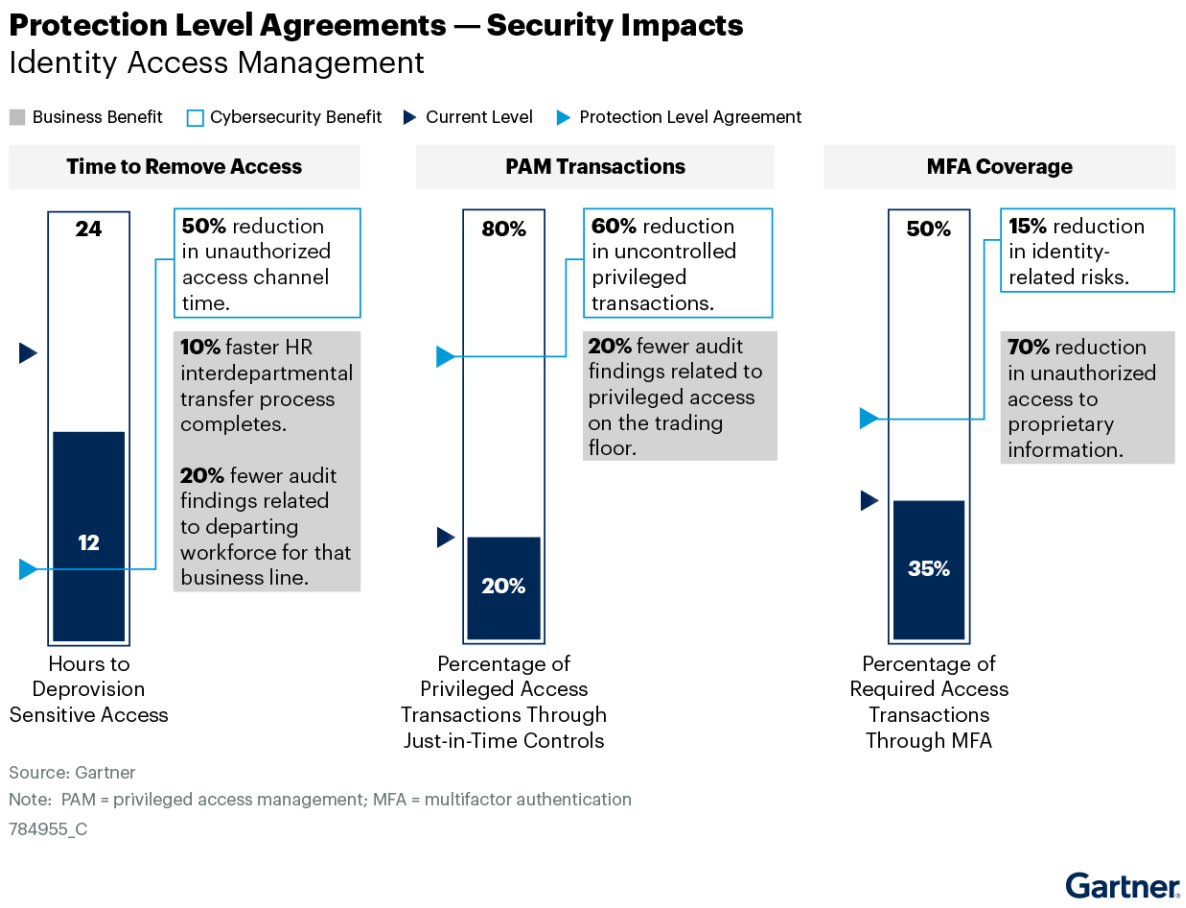
Gartner

Question 3: How Do I Show the Value of IAM Investments?

IAM investment decisions are often made in isolation, with organizations taking a tactical approach to solve a specific problem. This limits the organization's ability to create defensible metrics to measure and support investments to the overall IAM program; as well as align it with the cybersecurity strategy and business goals. Gartner's outcome-driven metrics (ODM) and protection-level agreements (PLA) are a great way to achieve both. They measure cybersecurity outcomes achieved by specific investments, constructed by aligning what is measured to the desired protection outcome of the investment. In this manner, ODMs simultaneously reflect protection levels and value for investment as well as raise awareness to the rest of the C-suite regarding the important role of the IAM function in the security and risk management strategy.

As shown in Figure 3, Gartner recommends you start by benchmarking three primary protection-level ODMs for IAM (also see Use Outcome-Driven Metrics to Drive Value for Identity and Access Management).

Figure 3: Protection-Level Agreements — Security Impacts



These ODMs are defined in The Gartner Cybersecurity Business Value Benchmark, First Generation. Many more ODMs are defined in Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security.

Question 4: What Role Does IAM Play in Protecting My Organization From Breaches?

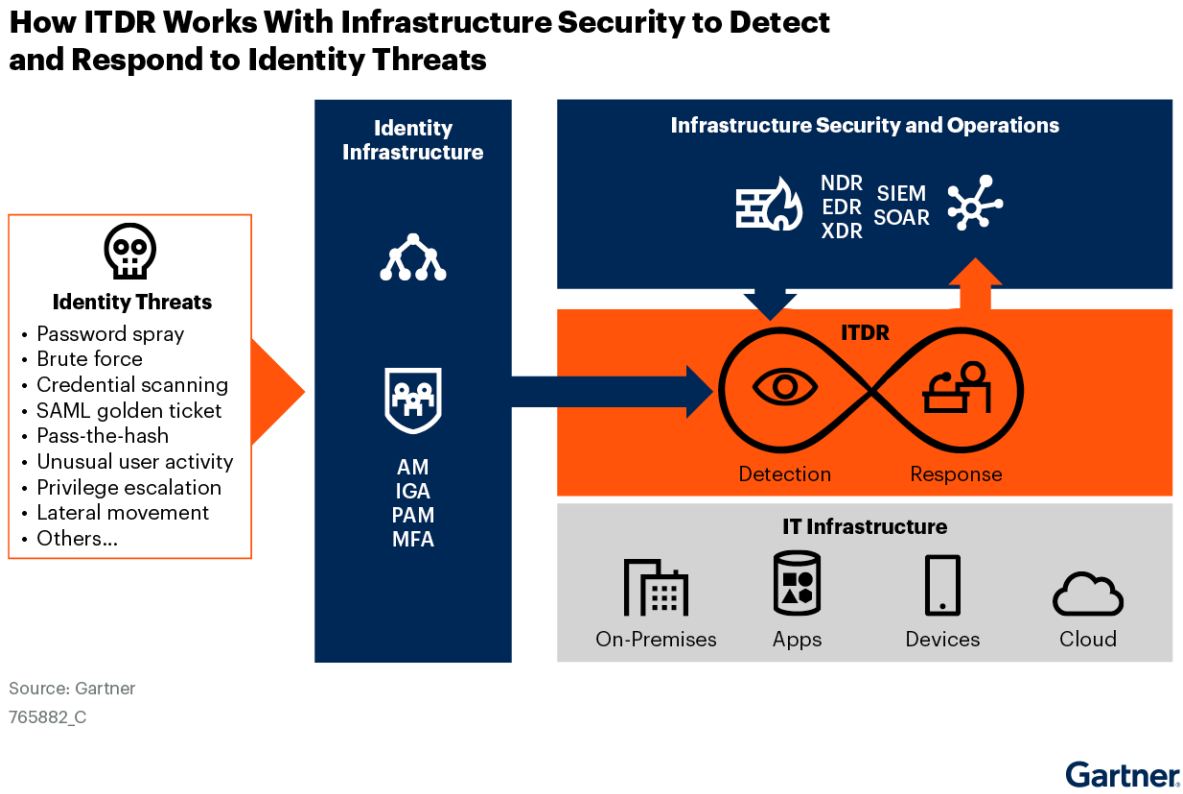
Prevention is a foundational part of every cyberattack preparedness plan. This includes documenting key elements of the identity infrastructure and assessing whether proper preventive controls are in place to protect them (see the four areas discussed in the first question). However, there is no such thing as fail-proof prevention. Organizations must be prepared for the highly probable scenario that controls can be bypassed (see Maverick* Research: You Will Be Hacked, So Embrace the Breach).

Credential misuse is the most popular path to security breaches in 2022. [1] There is an active initial access broker marketplace for stolen credentials. [2] There are well-known attacks against MFA. [3] And sophisticated attackers are now targeting the IAM infrastructure itself.

> **Identity threat detection and response is a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools and processes to protect identity systems. It works by implementing detection mechanisms, investigating suspect posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure.**
>
> *— Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response*

ITDR unifies tools and best practices to protect the integrity of identity systems, which is necessary even for mature IAM and infrastructure security deployments. The focus of ITDR is to work as second and third layers of defense (see Figure 4), after the foundational preventive mechanisms identified above are in place.

Figure 4: How ITDR Works With Infrastructure Security Operations



For more information on identity threat detection and response, see:

- Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response
- Quick Answer: Who Is Responsible for Identity Threat Detection and Response?

Question 5: What Is the Benefit of Identity-First Security?

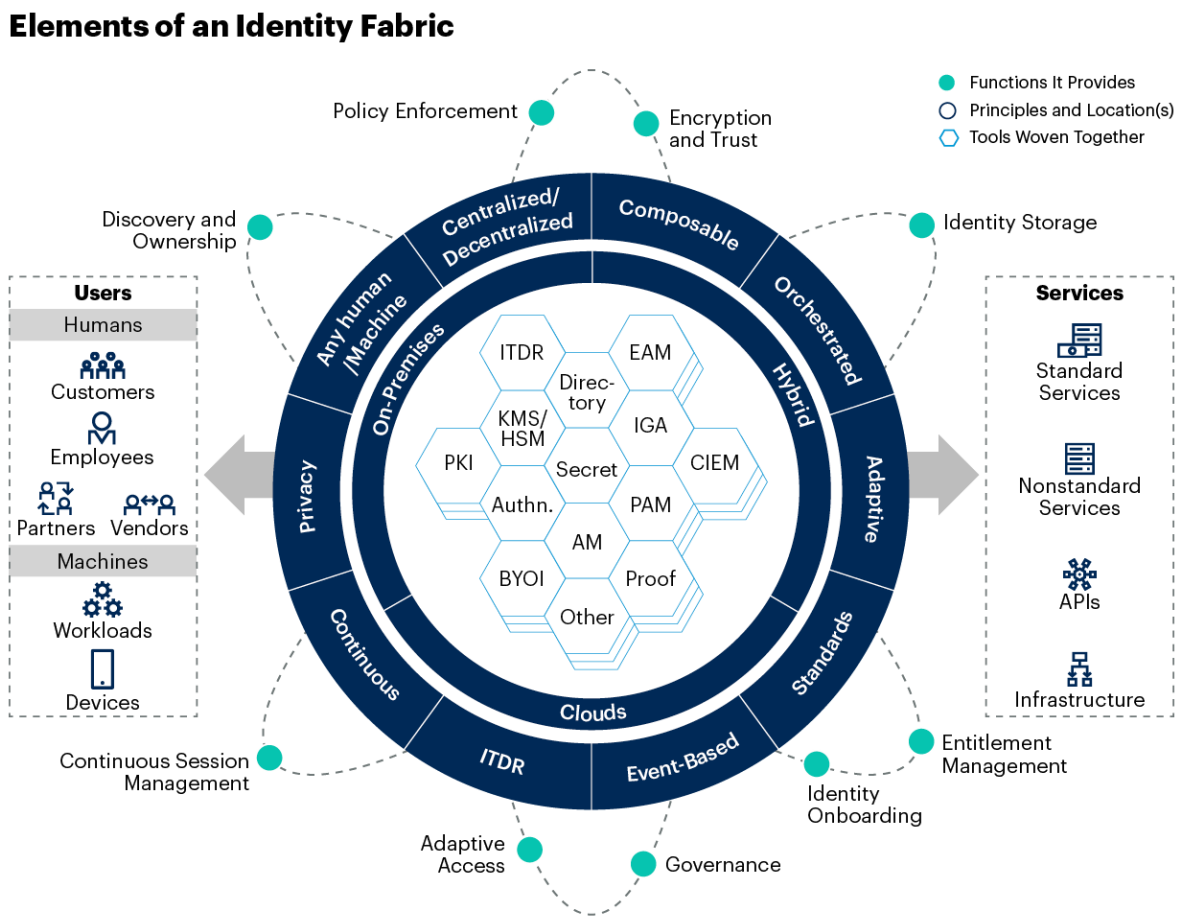
Identity-first security is an approach that makes identity-based controls the foundational element of an organization's cybersecurity architecture. It marks a fundamental shift from reliance on static perimeter-based controls that have become obsolete due to decentralization of computing resources, channels, entities (human and machines) and devices to adopting access policies that are consistent, and focused on flexible, scalable, continuous and context-driven dynamic controls. Identity-first security is one of the important goals in an effective IAM program.

In the current dynamic threat landscape, trust and risk must be assessed at every moment, and changes must be reflected immediately across all sessions. IAM is well-placed to deliver this approach to support a continuous and adaptive zero-trust security capability. Access decisions need to be made quickly and wisely, and potentially changed rapidly to react to an active threat; yet, most IAM deployments are still so process-driven that they cannot react quickly.

To achieve an identity-first security strategy, instead of focusing on specific IAM tools and capabilities, cybersecurity leaders should focus on end-to-end use cases. For example, there are numerous components involved in an API security strategy, including API gateways, an access management tool, a secrets management tool and public key infrastructure (PKI), among others. All of these components need to work together to effectively deliver the control. The objective is to achieve an integrated and extensible framework, where IAM along with security and risk management tools and processes can be used interoperably.

Figure 5 illustrates how IAM components can be viewed as elements within a connected ecosystem or identity fabric that enfolds multiple use cases. For more information, see Identity-First Security Maximizes Cybersecurity Effectiveness.

Figure 5: Elements of an Identity Fabric



Acronym Key and Glossary Terms

Notes

Evidence

[1] 2023 Data Breach Investigations Report, Verizon.

[2] Compromised U.S. Academic Credentials Identified Across Various Public and Dark Web Forums, FBI.

[3] D. Goodin, Lapsus$ and SolarWinds Hackers Both Use the Same Old Trick to Bypass MFA, Ars Technica.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription. IAM Leaders' Guide to Privileged Access Management

IAM Leaders' Guide to Identity Governance and Administration

IAM Leaders' Guide to IAM Program Management

Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

What You Must Know About Identity and Access Management in 100 (Short) Tweets

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Equip your cybersecurity function for greater resilience.

Download Now

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

Webinar

Generative AI's Impact on Cybersecurity and the CISO's Role

Explore how GenAI impacts security best practices.

Watch Now

Conference

Gartner Security & Risk Management Summit

Join your peers for the unveiling of the latest insights at Gartner conferences.

Reserve Your Spot

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 866 263 8917

International: +44 (0) 03301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Gartner®