EBOOK

2024 and Beyond

Identity & Security Trends & Predictions

Saviynt

Table of contents

Saviynt

Introduction

As part of our annual tradition, Saviynt executives and partners reflected on top identity trends for 2024. Leaders weighed opportunities, highlighted concerns, and suggested responses for security practitioners and the enterprises they're defending.

Here are a few big ideas worth following in the new year.

TREND NO. 01

1

Identity security becomes a U.S. public company board matter.

Is your cyber program disclosure-ready?

Earlier this year, the U.S. Securities and Exchange Commission adopted new rules on cybersecurity risk management, governance, and incident disclosure for public companies. According to the SEC, the updates meet a need for more "consistent, comparable, and decision-useful" disclosures of material impacts to investors, companies, and the markets connecting them.

Companies must report material cybersecurity incidents on a Form 8-K within four days of determining materiality. Disclosure requirements include describing cyber risk management programs and strategies to the public. PwC spotlights policies and procedures, risk assessment, and controls and controls monitoring as areas that companies must diagnose in order to prove disclosure capabilities. For boards, this raises four important questions:

- **Are our policies in line with specifications from recognized industry frameworks?**
- **Is a risk assessment policy in place, and are findings absorbed into our cyber strategies?**
- **Do budgets reflect a priority for enterprise cyber risk management?**
- **How mature and/or effective are our controls, as evaluated against industry frameworks?**

> "These **regulations will kick off more evaluations, more assessments, and will require companies to reassess the controls they have in place.** Depending on findings, more digital transformation and modernization will likely be required."
>
> **Paul Zolfaghari,** President, Saviynt

For many enterprises, this work will expose how little access visibility exists. Security teams will then adopt more "identity-first" security practices.

In particular, companies will need to quickly disclose incidents that could have material impact, such as a breach of customer data. To do that effectively, they need to be able to quickly diagnose what the malicious actor had access to, what they actually did with that access, and whether it was material. That requires a security platform with strong identity-centric controls to prevent, detect, respond and recover.

Companies will also need better reporting capabilities to digest and remediate anomalous activity. Progress here can simplify information sharing within departments and to the board – and also help internal auditors understand risk posture, capabilities, and constraints.

How to respond to this trend:

Build an identity data warehouse that centralizes identity, access and activity data.

Expand the aperture of your identity security conversations. In particular, don't neglect managing access for third-parties. Reduce supply chain risks by improving onboarding efficiency, simplifying lifecycle management, and ensuring zero standing privileges.

TREND NO. 02

2

AI supercharges identity security– and becomes table stakes for mature cyber risk programs.

Unmet AI promises have left security professionals disillusioned for years. Nuisances like immature technology and marketing hype have added to the disappointment.

Various AI capabilities now exist, and no matter where an enterprise starts, it must incorporate this technology. We've reached an era where **AI-powered identity security is a mature cyber risk program imperative.**

> "Artificial intelligence, machine learning, and advanced data science are central to identity security transformation. A new era of identity security starts now, as companies control and design processes using behavioral attributes."
>
> **Jim Routh,** Chief Trust Officer, Saviynt

Gartner points out how generative AI (GenAI) will soon disrupt identity and access management by providing new user and administrative experiences via natural language that were once inaccessible. They suggest GenAI will also eventually add more consistent and contextual security controls.

But, GenAI may need some seasoning before enterprises deploy it at scale. More immediately, enterprises can introduce other AI (and machine learning) capabilities to better analyze user behavior, detect vulnerabilities, and simplify security program operations.

According to Vibhuti Sinha, Chief Product Officer at Saviynt, the convergence of ready technology and challenging macroeconomic conditions means now is the time for AI adoption.

“Reducing governance costs by 50% is a new norm target. Every security leader is being asked to reduce manual overhead and build more efficient processes, without compromising security effectiveness” shares Sinha.

Michael Davis, Partner/Principal, Ernst and Young LLP reinforces the idea that AI-driven identity tools may help organizations meet security goals, despite resource constraints. Through improved data access, personalized recommendations, and automated decision-making, organizations enhance end-user experience and support the principle of least privilege.

“The efficiency gains offered by AI allow leaders to allocate their limited resources toward broadening control coverage and collaborating with stakeholders to strategically advance identity security in alignment with business objectives”.

Today, leading identity platforms may already incorporate AI. This means more contextual understanding of the identity landscape and benefits like automatically evaluating access rights and usage patterns.

Security teams may also find AI transforming employee or vendor onboarding, for instance, by comparing access entitlements to peers.

In addition, generative AI tools may be deployed to detect anomalies and suspicious activities in real-time, enabling rapid response. Other use cases include uncovering fraudulent activities related to identity, such as phishing scams and social engineering through pattern learning.

Routh believes AI’s various learning mechanisms makes it particularly useful for security professionals today: “Behavior data are great indicators of potential threats. Once normal patterns are established for users, behavior deviations can trigger automated responses in real-time.”

How to respond to this trend:

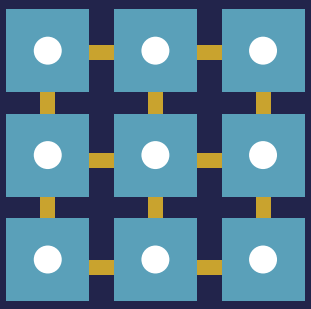
Up to 15% of a manager’s time is applied just to access recertifications for regulatory compliance. **Enterprises should capture ‘low hanging fruit’** for AI including access activity reviews and assessments and more lifecycle automation.

Embrace behavioral profiling to reduce the need for human oversight and long wait times for approvals. Explore how AI better enforces least privilege, resulting in lower operating costs, better user experience, and improved risk management.

TREND NO. 03

3

Three's a party, four is a crowd: Managing your vendor's vendors.



Companies must solve for these indirect trust relationships

Few organizations manage identity risk beyond their third-party vendors. The problem is, they still inherit issues at the fourth or fifth levels.

This year, companies will emphasize comprehensive attack surface management as the operational, regulatory, and reputational effects of cybersecurity breaches grow.

We've raised concerns around third-party users, but increasingly enterprises' partner organizations now own multiple relationships. These are the "n'th parties" who enjoy provisioned access throughout the value chain. Companies must solve security for these indirect trust relationships.

Consider this: More than 98% of organizations have a relationship with at least one breached third-party vendor. Third-party vendors are also five times more likely to exhibit poor security.

In 2024, we predict more companies will target governance that extends to third-, fourth-, and nth-parties. This approach necessarily requires a converged governance model, whereby a security leader links identity governance and administration (IGA), privileged access governance, and third-party access governance functions to manage every identity for any access.

"Fourth-party" risk management demands that enterprises embrace principles of least privilege and zero trust access. By identifying nth party risks, eliminating them when possible, and restricting the access of untrusted parties to corporate assets, an organization can guard against supply chain exploits.

> Enterprises must now manage outside parties completely on trust. Security solutions must be flexible enough to control and integrate with various systems, platforms, and applications no matter where the nth party exists.
>
> **Vibhuti Sinha**
>
> Chief Product Officer, Saviynt

How to respond to this trend:

Emphasize integration between security capabilities and solutions to manage third-, fourth-, and nth-parties across all access points, platforms, and applications.

Prioritize time-bound access management including controls that support capabilities like temporary privilege elevation for contractors or automatic access removal when a contract ends.

TREND NO. 04

4

Perspective, Platforms, and Your Personnel: Key fronts for beating CISO burnout.

Staying upbeat while fighting cyberthreats, shrinking budgets, and staff turnover is a tall task. Today's CISOs find themselves perpetually overworked and often alone. Add in worries about personal liability, and it's clear why 60% of CISOs report having burned out in the past twelve months.

CISOs operating at diminished capacity can devastate an organization's cyber resilience. Prolonged burnout may mean disengaging from essential cyber program management, monitoring, incident reporting, and hiring. As well, it may lead to less enthusiastic observation of trends and useful vendor technologies.

Combating these issues isn't a one-size-fits-all, suggests Gopal Padinjaruveetil, Chief Information Security Officer of the Auto Club Group. "First, leaders must come to grips with the reality that this job is stressful. As pressure and fatigue mount, they instinctively think they're doing something wrong. Often, they're not."

This isn't to say burnout is an inevitability, however.

"But acknowledging times of genuine emotional impact is part of healthy role acceptance," guides Padinjaruveetil.

From here, CISOs need to address three linchpin areas that worsen symptoms leading to burnout.

First, they must define explicit risk tolerance expectations with other C-suite leaders. "There is no scenario where CISOs can prevent breaches entirely, and this type of thinking is crushing," offers Padinjaruveetil. CISOs and their executive peers need to balance expectations against available tools, cyber program maturity, and resource support, Gartner suggests.

Next, they need to recognize that cyber defense is a weak link sport. Instead of trying to be world-class on every front, enterprises must avoid being especially bad at any point in the system (e.g. avoid perfection and look for glaring vulnerabilities)

"Great identity architecture is a must-have," shares Padinjaruveetil, "But remember that social engineering manipulation is your biggest adversary and where enterprises are actually most vulnerable." Organizations must embrace cyber defense as a team, and secure buy-in from every stakeholder.

Finally, CISOs must collectively push back against the individualism that characterizes the role and security industry. Normalizing the reality of cyber attacks and breaches by sharing data about threats and mitigation, reminds CISOs that they don't have to be superhuman.

> "As pressure and fatigue mount, they instinctively think they're doing something wrong. Often, they're not."
>
> **Gopal Padinjaruveetil**
> Chief Information Security Officer of the Auto Club Group

How to respond to this trend:

Define your specific risk appetite and tolerance levels. This isn't a CISO-only decision; every executive needs to buy-in. Push back if the answer is zero-risk – that's an impossible way to run a business.

Set CISOs up for success. Adopt tools that support continuous risk monitoring, proactive threat identification and mitigation, and contribute to overall security maturity.

Support open-source projects like the Open Cybersecurity Schema Framework (OCSF). Actively contribute to help spur adoption, don't just ingest information and leech off the schema.

TREND NO. 05

5

Adiós admin-time authorization, runtime is ready.

A few months ago, Gartner cast a vision for replacing implicit trust with a discipline of continuously assessing risk based on identity and context.

Modern enterprises struggle here–often as user, group, and identity counts swell making granular management difficult. The dynamism associated with complex enterprise applications also stretches conventional security controls.

Fortunately, a promising identity security evolution is underway: runtime authorization, the practice of permitting or denying access to an application or resource in real-time.

A budding marketplace of ready-to-use authorization solutions means that security leaders can now incorporate ongoing business context from key systems of record to make access decisions. This means a needed shift from evaluating permissions based purely on policy.

> "Runtime authorization that incorporates business context shows **real progress toward Zero Standing Privilege.** Companies that embrace this will gain momentum along the Identity Security maturity curve."
>
> **Anirudh Sen**
> VP, Products and Experience, Saviynt

Security leaders will still bump into challenges (particularly in the cloud) as the granularity, volume, and ephemeral nature of these workloads push the limits of runtime authorization offerings. And currently, enforcing authorization is technology-stack dependent.

The practice should improve, however, as standards develop to help data synchronization across popular apps and services. This could include industry providers uniting around a shared standard of pre-built connections linking systems of records, enterprise applications, infrastructure resources, and other services.

According to Anirudh Sen, VP, Products and Experience at Saviynt, the ability to capture changes in an enterprise's business systems, including across CRM, HRIS, ERP, or ITSM – and reflect these in access decisions marks a genuine Zero Standing Privilege posture.

How to respond to this trend:

Get granular. Fine-grained decision making around human and machine identity use cases requires policy management capabilities that can handle a high volume of access requests for apps, APIs, compute resources, and more.

Invest in policy management. More funding, partnership, and engineering will begin flowing toward this capability. Enterprises will want to reevaluate a dynamic approach to authorization and consider investing in automated Identity Policy as part of a broader control strategy.

TREND NO. 06

6

Growing frenzy for FedRAMP

Late last year, the FedRAMP Authorization Act was signed as part of the National Defense Authorization Act (NDAA). The effort codifies FedRAMP as the standard for security assessment and authorization for cloud computing products and services that process unclassified federal information.

Services providers have embraced the standard, and the number of "In Process" cloud service offerings increased by 50% over the last two years. In 2024, we believe more enterprises will explore FedRAMP authorization. Absolutely, these companies want to do business with the government, but many recognize that achieving FedRAMP alignment proves broader security rigor.

> "This external validation of cloud security is meaningful for any organization. Of course, for those selling to the US government, but increasingly to those doing business in financial, healthcare, and other regulated markets."
>
> **Andrew Whelchel,**
> Lead Solution Engineer
> Public Sector, Saviynt

Consider the benefits to any party that does business with a FedRAMP authorized provider. These may include

- **Cost and time savings over doing independent security assessments or vendor evaluations**
- **Enhanced insights into existing controls**
- **Confidence in assessment validity**
- **Faster path toward cloud services adoption**

For many, the authorization provides a proverbial stamp-of-approval, and offers commercial companies a sense of where to look for advanced, highly secure cloud solutions. In addition, FedRAMP providers often incorporate security functionality across their entire product suite–even for non-FedRAMP solutions.

Beyond what potential FedRAMP authorization signals to the marketplace, we also expect the federal government to continue sponsoring CSPs as it reaps benefits intrinsic to cloud products.This means would-be CSPs need to boost security readiness, including identifying their own product risks and aligning with secure providers. The opportunity extends to non-US companies who want to sell a cloud service offering to the U.S. government.

FedRAMP designation is part of the modern CSP's platform value proposition. Security leaders must not fall behind, and should start now to shore up issues that will inhibit FedRAMP Authorization. "Standing privilege, in particular, is a worthwhile starting point," notes Whelchel. "Solving this is essential for complying with the various controls and enhancements within the Access Control family objectives."

This includes embracing the principles of least privilege limiting user and application access rights to the bare minimum necessary for their respective roles as a complement to broader Zero Trust strategies.

How to respond to this trend:

Build the visibility of your vulnerable identity and application assets with a comprehesive risk inventory — this will help hone the direction of your response strategy.

Least privilege controls (keeping user and application access rights to the minimum necessary for their role) is a vital component of a NIST-based Zero Trust strategy, **Begin to develop a comprehensive least privilege policy** that outlines the approach, including how rights are granted, reviewed, and revoked. This is a complex undertaking, but a step-by-step strategy can coax buy-in from top management all the way down to individual users.

Saviynt

Want to talk to an **identity and security expert?**

SCHEDULE A CALL

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time.

The Saviynt Identity Cloud brings together identity governance (IGA), granular application access, cloud security, and privileged access (PAM) into the industry's only enterprise-grade SaaS solution.

Learn more at **Saviynt.com**

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com