Identity and Security Trends and Predictions:
2021 and beyond

The pandemic forced a new way of working. Organizations transitioned millions of staff, fast-tracking remote work. Across the globe, executives doubled-down on cloud migration and digitization. Some dubbed it the shift from “cloud speed to COVID speed.”

As challenging as the year was, new opportunities emerged. Corporates reprioritized cyber resilience to deal with new and increased attack surface. While the pandemic exposed tool, practice, and mindset shortcomings, it also spurred product innovation and partnerships. Often, enterprises transformed overnight.

Time will tell what 2021 holds. But new mindsets, rapid innovation, and advanced persistent threats signal significant changes for identity and security professionals. For this eBook, we examined research and collected insights from cybersecurity experts, system integrators, and technology providers. We also connect practical action steps to each trend. With these in mind, here are eight trends worth following.

TABLE OF CONTENTS

1

Trend No. 1: Increased vulnerability through remote working

The mass and sudden transition to remote work was even difficult for the most vigilant CISOs. Moving millions of workers from secure corporate networks to WFH exposed vulnerabilities – and expanded attack vectors for threat actors.

In 2021, Forrester **predicts** that insider incidents will be responsible for 33% of breaches, nearly a double-digit increase over last year. Their study cites three contributors:

- The rapid push of users, including some outside of companies’ security controls, to remote work
- Employees’ job insecurity
- Increased ease of moving company data

This is the first time many employees have worked remotely, and few practice security hygiene. As social engineering, ransomware, and phishing attack sophistication grows – including novel attacks targeting social apps or COVID-themed emails – dispersed workers have a more significant role in protecting the enterprise than ever before. IT is no longer a walk down the hall. Similarly, without physical co-location, there are **various** authentication factors that can no longer be assumed. Workers and workdays are now spread across time zones. As the 8-to-5 schedule morphed to fit workers’ irregular, at-home routines, stretched information security teams struggle to keep up with network monitoring. As workers change positions, get fired, or vendor contracts end, access permissions must also be revisited–further complicating the IAM/IGA lifecycle. ZDNet **warns** of issues caused by blended personal and professional work on corporate devices. Most concerning is the reality of weaker residential internet infrastructure versus the hardened enterprise-grade security of corporate offices. “Once an attacker compromises a home user, they’ll wait for the user to connect to the corporate VPN and take it from there.”

> “CISOs cannot control and manage network security settings, see users router settings or assess connection security. As corporate perimeters crumble, the need for endpoint security health and user behavior analysis grows more urgent.”
>
> – YASH PRAKASH, CHIEF OPERATING OFFICER AT SAVIYNT

A Ponemon Institute **study confirms** that personal device use and remote collaboration spurred new attacks. Consider:

- **60% OF COMPANIES** have already experienced a cyber attack during the pandemic
- **51% SAY** that malware or exploits got past their defenses
- **42% OF COMPANIES** report that they have no idea how to defend against attacks aimed at remote workers

60%

of companies have already experienced a cyber attack during the pandemic

Last year, COVID-19 had a profound effect on physical health. In 2021, we believe it may have a similarly devastating impact on organizational health.

How to respond to this trend:

- **INTEGRATE ENDPOINT SECURITY AND IDENTITY SOLUTIONS** to support contextual decision making
- **CONSIDER ROLE OR ID-BASED ACCESS** that is time-bound and well monitored to gain control and visibility into the utilization of privileged access
- **ENABLE IDENTITY SECURITY THROUGH THE CLOUD** to keep up with growing corporate applications and services – and to maintain continuous compliance monitoring

2

Trend No. 2: New (and persistent) challenges to cloud adoption

Remote work is only one facet of enterprise movement to the cloud. Other workload migrations are underway as companies capitalize on the flexibility, elasticity, and scalability of cloud services. However, the variety of cloud service models in use introduce a new set of challenges. In particular, we see issues related to expanding SaaS, IaaS, and PaaS adoption:

SaaS

Critical business functions such as ERP, HR, and CRM will deploy as-a-service. Companies must meet compliance mandates to ensure necessary Segregation of Duties (SoD) policies across diverse applications. Organizations will also require deeper visibility into managed and unmanaged users/devices accessing SaaS applications.

IaaS & DevOps

Usage promotes devOps models in which developers spin up environments like virtual machines and containers and push them to production using automation. But immature automation here can circumvent security practices — enterprises must consider DevSecOps and Privileged Access Management. As the Solarwinds hack reminds, organizations must also vet service vendors and ensure proper controls and operating standards. For example, reassessing global shared administrative access privileges typically used by legacy applications. Companies must also contend with compliance management and threat analytics for IaaS workloads.

Remote work is only one facet

of enterprise movement to the cloud

PaaS

Includes platforms used to build and deploy applications in cloud-based runtime environments or to invoke API-based services. Companies must enable API Security and web and mobile Application Access Management.

Additionally, enterprises need to harden data management practices as the use of cloud-based collaboration platforms like Microsoft 365, Box, and Dropbox grows. BYOD model popularity means basic data encryption is no longer enough.

As cloud use normalizes, companies should plan to “manage privileges, access, and ensure configuration management,” guides Prakash.

“In the cloud, everything is now an identity,” says Vibhuti Sinha, Chief Cloud Officer at Saviynt. He notes how identity management & governance is no longer confined to employees and contractors. “Virtual machines, databases, containers, mobile phones – even the billions of IoT devices – have identities that need to be managed.”

Another concern is how enterprises overestimate the responsibility of public cloud providers. Sinha notes how hackers carried out the recent **Capital One breach** through an insecure infrastructure component. With a shared responsibility model, providers like Microsoft or AWS control data center security infrastructure that hosts customers’ resources. Customers themselves are responsible for securing access to the existing data resources.

Cloud benefits are clear, and movement from on-prem is certainly worthwhile. But optimizing and securing workloads in the cloud is not as easy as just lift-and-shift.

How to respond to this trend:

CONSIDER A COMPREHENSIVE CLOUD SECURITY ARCHITECTURE that includes privileged access management, identity governance and CASB solutions to manage risks on cloud services outside your direct control

SUPPORT RAPIDLY GROWING HUMAN AND MACHINE IDENTITY MANAGEMENT; consider guest access management, BOT access governance, operational technology integration, and application and privileged workload discovery

3

Trend No. 3: All in on Zero Trust

Forrester now estimates that 80% of data breaches connect to compromised privileged credentials, including passwords, tokens, keys, and certificates. As threat vectors expand, organizations are actively replacing the traditional “trust but verify” model for managing access.

In its place: zero trust security.

Zero trust is not a technology; it is a mindset. The philosophy assumes that attackers exist inside and outside a network, so no user or machine is to be implicitly trusted. Sue Bohn, Partner Director of Program Management at Microsoft **sees zero trust** as the cornerstone of a new era for security and governance – with **identity at the center**.

As threat actors increasingly use malware and social engineering to steal credentials and take over accounts, enterprises must strengthen their security posture. Saviynt sees a movement away from standing access and ‘superusers.’ Taking their place are zero standing privilege and just-in-time provisioning. MJ Kaufmann, security specialist at Saviynt, **suggests** environments that only allow elevated privileges temporarily can narrow potential attack scope.

We also expect deeper monitoring and risk-based analyses of access requests in addition to micro-segmentation and multi-factor authentication investments. For example: artificial intelligence and machine learning assess the reasonability of requests or flag potential compliance violations and anomalous request behaviors. Microsoft’s Bohn suggests monitoring suspicious behavior and using “continuous access evaluations to terminate sessions in real-time” to improve zero-trust standing.

Like Vanessa Gale, Head of Identity and Access Management at Origin Energy, **mentioned** during the CONVERGE 20 Roadshow, we also believe that SMBs are the next wave of zero-trust adopters:

Zero trust is not a technology;

Zero trust is a mindset.

> “It isn’t only companies like Google considering the concept. Smaller organizations realize that they can’t rely on network controls and office settings, and are also creating new perimeters. [They] need to take a zero-trust approach and utilize access management controls to support it.”
>
> **– VANESSA GALE, HEAD OF IDENTITY AND ACCESS MANAGEMENT AT ORIGIN ENERGY**

Similarly, we anticipate interest in another use case – applying zero trust to the myriad unmanaged IoT devices on organizations’ networks. However, companies will deal with visibility issues as few devices support traditional authentication and authorization processes. To enable zero trust, companies will invest in smarter device identity technologies and ongoing behavior verification.

Zero trust will accelerate as companies realize how essential continuous risk evaluation now is. As Saviynt CEO Amit Saha admits: “A single risk assessment at login is no longer enough.”

How to respond to this trend:

BUILD YOUR SECURITY PERIMETER AT IDENTITY. In particular, reduce always-on privileges, and add “right-sized” access for all human and machine identities

INCORPORATE CONTEXTUAL IDENTITY INFORMATION (such as average peer usage or requestor’s role permissions) and device information, user behavior, and analytics into access request processes

4

Trend No. 4: Healthcare data in the crosshairs

Recently, the former director of the U.S. Cybersecurity and Infrastructure Security Agency, **warned** hospitals and healthcare companies about a devastating ransomware from a Russian cybercriminal group. His message: assume it is inside your house.

The warning followed **alerts from** the FBI and other federal agencies warning of "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."

Today, a healthcare data record may be valued at $250 per record on the black market compared to $5.40 for the next highest value record (a payment card), according to **one report**. As hackers take advantage of health organizations' time and pressure constraints, ransomware payments are also inflating.

In a recent discussion at Saviynt's CONVERGE 20 roadshow, Intermountain Healthcare's Michael Allred **reinforced the idea**, noting how compromised personal data is the first step toward the billions of dollars in available federal financing for Medicare and Medicaid.

Experian **describes** the coming year as a 'cyber-demic,' calling COVID-19 vaccine rollout information and personal healthcare data "particularly vulnerable."

Information Week **notes how** healthcare providers' "critical need for resilient systems to address surge care capacity" indicates a mass, coming cloud migration. Cloud use cases will include patient data storage and access, querying and analyzing clinical datasets, health tracking between medical devices and EHR applications, responsive platforms for telehealth delivery, and flexible workforce management models.

As **we've shared**, cloud migration makes it harder to control and secure access to PHI. Overall connectedness adds to cybersecurity risks, exposes health entities' need for systems resilience, and requires intelligent compliance to meet various SOX, PCI, NIST, and HIPAA/HITRUST requirements.

Further, network integrity is difficult because **of the volume** of interconnected devices and information sharing across vendors and partners (claims processors, bill collectors, accounting firms, claims clearinghouses, medical transcriptionists, etc).

In 2020, 90% of the breaches Experian serviced were healthcare or telehealth related. Meanwhile, **new statistics** show a 45% increase in cyberattacks against the global healthcare sector since November — over double an increase of 22% against all worldwide industries in the same time period.
In 2021 and beyond, expect the trend to continue. As Bloomberg **guides**: "Attackers know that organizations are so desperate to build ventilators, or to stop people from getting sick, and they are trying to exploit that."

How to respond to this trend:

SET RISK-BASED ACCESS POLICIES; apply data analysis to classify data appropriately

CONTINUOUSLY MONITOR USER ACCESS to ensure control effectiveness

5

Trend No. 5: (Even more) Evolution of data privacy regulations

On November 3, 2020, California's approved Proposition 24, a ballot measure creating the California Privacy Rights Act (CPRA). The measure **expands the state's** previous privacy law (CCPA) – itself only a few years old. Among other changes, the CPRA introduces a new regulated category of "sensitive personal information" and provides consumers new access and opt-out rights.

Nationally, the senate is considering **several other** proposals for data privacy and security legislation. Pending outcomes affect how U.S. businesses conduct online activities with respect to issues like IoT, annual reporting and certification requirements, and personal data use in facial recognition.

Whether CCPA will become an example for other states or a blueprint for countries considering an alternative to GDPR remains to be seen. Meanwhile, China announced **its own initiative** to set global standards on data security.

Other significant data regulations were approved last year, including Brazil's **Lei Geral de Proteção de Dados** (LGPD) and Thailand's **Personal Data Protection Act** (PDPA). The LGPD closely models the EU's GDPR and requires companies to adopt security, technical, and administrative practices to protect consumers' data.

Thailand's PDPA goes into effect May 31, 2021, and includes some of the GDPR's stricter requirements, including the need for data protection officers, greater protection for sensitive categories of data, and an extraterritorial reach. Violators face both the risk of fines and criminal prosecution and imprisonment.

Wired **reports** the California law puts pressure on Congress to act at the national level, even as businesses protest the idea of patchwork state requirements. No matter how ambitious legislation grows, we have entered a new age of evolving regulation. Companies need to consider overarching Identity Governance and Administration (IGA) and, by extension, Identity Access Management (IAM) and the means to manage user identities and govern access to personal data to satisfy changing the law.

We expect non-compliance issues to grow as companies wade through changes *and* attempt to harden the variety of processes – from HR onboarding to customer offboarding – that touch the data protected by the various legislations.

Despite uncompromising legislation and growing consumer expectations, Security Magazine **reassures**: establishing a privacy policy framework and utilizing a reliable, flexible identity platform will help companies meet the variety of control and safeguarding challenges presented in data regulations.

How to respond to this trend:

APPLY PRINCIPLES of least privilege and privacy by design

ADDRESS CONSENT MANAGEMENT and right to erasure

CONSIDER WAYS TO EASE AUDIT COMPLIANCE – such as automating self-service access requests to reduce log tracking

6

Trend No. 6: Modernizing the C-Suite

Examples of disunified C-suites are everywhere. Misalignment around digital transformation and related investments is a leading factor.

In many companies, leaders with low technology proficiency occupy the C-suite. Unfortunately, a view of digital transformation as a series of CIO or CTO-led tactics persists. But digitization blurs traditional role limits in the C-suite – and companies need to re-organize.

Consider, for example, digital activities such as product experience, customer journey analysis, and analytics. As Financier Worldwide **shares,** these "fall somewhere in between the remits of the CMO and the CIO and, as such, collaboration between these two executives must drive digital."

Next year, we expect new C-suite dynamics; roles will morph, and responsibilities will shift. In many cases, companies will add new titles in the executive office.

Adding a Chief Identity Officer

We recently dug up a fifteen-year-old article **proposing** the Chief Identity Officer role. The writer lauds the idea of a single office owning IdM solutions and user identities. The position wouldn't have the same concerns generalist IT leaders do; charging leaders to find solutions that enable the business, facilitate ease-of-use, and also maintain strict security guidelines. No doubt, the idea was ahead of its time. The conversation went cold until a few years when **an IAM analyst** posed a similar point:

"[making] identity management a larger part of the enterprise not only makes sense from a security and compliance perspective, but because good, clean, organized IdM data results in better running organizations."

-DAVE KEARNS, SENIOR ANALYST AT KUPPINGERCOLE

The message is prescient; IDG **writes how** the last decade broke the entire model of security. They, too, note how verifiable identity and management are at the center of security, lending credence to the idea of a C-level identity leader. Our team believes this is the year of a *new* CIO. According to Saha, "The Chief Idenity Officer is more than a CISO; he or she looks at the digital transformation of a business and how identity informs it."

Adding a Chief Cloud Officer

Similarly, we expect that in the next few years, more companies will employ a Chief Cloud Officer. WiPro **believes** that as cloud adoption speeds up, organizations will add an executive to "[...] not only spearhead cloud adoption policy but also expertly deal with the various business and technology issues that cloud computing introduces." These may include: maximizing cloud performance, establishing vendor relationships, managing security and ownership, and understanding cloud innovation and developments.

Vibhuti Sinha, Saviynt's Chief Cloud Officer, expects some Chief Information Officers to evolve into cloud leaders. Other enterprises, he shares, will add dedicated CCOs:

> "As companies SaaS-ify their operations, they need a cloud-focused leader with business acumen. This leader will have to battle legacy mindsets around running a company on traditional data centers versus moving to the cloud."
>
> **-VIBHUTI SINHA, CHIEF CLOUD OFFICER AT SAVIYNT**

Companies will depend on cloud officers to support internal infrastructure and product innovations, including securing the company's own platform or service. According to Sinha, they must also be evangelists – engaging the development and testing communities – while continuously enforcing security policies.

How to respond to this trend:

- **CONSIDER HOW INTERNAL IDENTITY AND SECURITY FUNCTIONS ALIGN.** And position these leaders in strategic places and ensure their contributions at the executive table
- **INCREASE THE VISIBILITY** and influence of the identity function during digital transformation

7

Trend No. 7: Entrance of new Identity Solutions

In years past, if an enterprise wanted to build out identity governance, it would have to bolt-on a separate privileged access product to manage certain accounts – such as those for IT administrators. The disparate tech added new challenges for companies modernizing their IT infrastructure in the cloud:

- Extended implementation times due to multiple stacks and solution parts
- Scaling difficulties due to the transient nature of cloud applications
- Complex operational support of multiple solutions and heterogeneous architectures
- Complex pricing and significant professional services investments
- Lack of risk awareness and governance

Adam Barngrover, Principal Solution Strategist at Saviynt, **reminds us how** critical assets have changed, with workloads spinning up and down within days and hours. Admins can now connect to the cloud executing privileged activities via direct console access, RDP, and command line. At each new access point, a new risk needs to be managed and monitored.

Although security-conscious organizations invest in integrations between PAM and IGA tools, they must still maintain and provision access to critical access across two systems. Given the complexities of integrating IGA and PAM, organizations may overlook governance. With convergence, risk awareness and governance is available on day zero.

In 2021 and 2022, we predict that more enterprises will introduce combined PAM and IGA into their cloud-migration plans. Purpose-built platforms that integrate the two disciplines – including adding privileged access directly in the endpoint system and securing privileged access to applications running in the cloud – will support this. Beyond this, SaaS-delivered, converged IAM platforms will be the preferred adoption method for IGA, AM and PAM in more than 45% of new IAM deployments by 2023, **suggests** Gartner.

As Simeio's Troy Keur shares: "These worlds are colliding quickly; it is simply illogical to manage privileged identities with separate workflows, systems, and governance."

How to respond to this trend:

BUILD COMPETITIVE ADVANTAGE and gain meaningful visibility with an integrated or converged identity solution

FOCUS ON NATIVE IGA INTEGRATION to unlock the benefits of "right-level" access for all user types–and establish appropriate governance controls

8

Trend No. 8: Improved security postures with AI/ML

Identity governance strategies have historically fixed on the question: "Who has access to what?" As the range of identities, including RPA, IoT, and service accounts grows in the cloud, enterprises must also ask, "What are these users *doing* with their access?"

Moving ahead, we expect more in-depth use of AI/ML technologies to improve risk awareness and decision making for identity-related business processes. One application area ripe for improvement is risk modeling.

Enterprises can take advantage of intelligent risk scoring – based on usage data, behavioral analytics, and peer group analysis – to optimize access certification, requests, role management, and other access management assignments and processes.

Eventually, we expect the elimination of human intervention in access decision-making. While this is not a 2021 revelation, automated access provisioning may soon normalize. For example, instead of providing a Salesforce admin 24/7 administrator privileges, access is granted in real-time and is task-specific – once the admin logs out, access is revoked. AI for adaptive decision making, including applying technologies that consider location data or device insights (like irregular mouse movements) is an emerging use case.

Deloitte **notes the** opportunity for behavioral analytics to create baseline markers of normal user behaviors. Alongside, NLP tools would develop user profiles and monitor for abnormal occurrences–and learn (and infer) from behavior patterns. This supports faster, frictionless identity related decision making.

We foresee more dynamic risk-based scoring that adapts to user behaviors and attributes, even across an ecosystem of devices, cloud-workloads, and user types. Enterprises will also invest in smarter Attribute-based Access Controls (ABAC) to manage modern identities. These tools incorporate intelligent analytics to create attributes such as user, object, action, or environment characteristics and dictate how a role can operate. Using automation for role-mining, security leaders will create authoritative identity sources.

Intermountain Healthcare's Allred **cites** his organization as an example of how frictionless ML-decision making will expand: "Reviewing user-behavior and auditing access for 50,000 users is simply not sustainable."

Simeio's Keur also anticipates more AI/ML-guided responses to outlying behaviors flagged by UEBA tools. He expects security leaders to connect user analytic tools to IAM solutions to move past "just giving users permissions and flying blind."

Identity intelligence powered by AI/ML improves risk awareness, reduces over-entitlement, helps companies identify inactive user accounts, streamlines certification efforts, and increases revocation rates. The ROI is too high to ignore.

In 2021, consider taking advantage of

intelligent risk scoring

How to respond to this trend:

DETERMINE WHERE GOVERNANCE CAPABILITIES NEED STRENGTHENING and look for AI/ML-based innovations from identity solution vendors

CAPTURE "LOW-HANGING FRUIT" benefits of automation for discovering and integrated new cloud workloads

Conclusion

Each of these trends highlight an opportunity to build a proactive security posture. Enterprises that consider these – and then make identity-centered decisions and investments in response – will outpace those that don't.

So take steps now to secure your workforce for the future. Reduce your access and compliance costs. Accelerate cloud adoption. Together **we can build** a modern approach to identity security.

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 Enterprise Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution. Learn more at **Saviynt.com**

Want to talk to an identity and security expert?

Schedule a Call Today