SAVIYNT

Identity and Security Trends & Predictions:

2022 AND BEYOND

INTRODUCTION

Last year was supposed to be a return to normal. But for security professionals, the uncertainties ballooned; one writer detailed the whirlwind – cyberattacks, virtual work, executive orders, cloud expansion – resulting in more intertwined IT ecosystems and vulnerabilities.

Still, companies proved resilient. They established new operating norms, supported dispersed staff, and navigated digital-first demand for products and services. New cybersecurity challenges surfaced, but so did opportunities. In 2022, enterprises will press deeper into unknowns.

Security leaders must reckon with the modern risk landscape, accelerating Zero Trust demands, competing transformation initiatives, coordinated cyberattacks, and unique access issues with the rise of machine identities. No roadmap through these exists. Enterprises must rely on foresight and preparation. Consider the trend insights and guidance in this report an ideal starting point.

In these pages we examine research and collect insights from cybersecurity experts, system integrators, and technology providers. We also lay out actionable steps your organization can take to prepare for success in the year ahead. With these in mind, here are ten trends worth following.

TREND NO. 01

Increased Attacks on Critical Infrastructure

↓ HOW TO RESPOND

Last April, the cyberattack on Colonial Pipeline thrust infrastructure security into the mainstream. The world learned what CISOs know: modern criminals are brazen, agile, and capitalize on security exploits with ease.

Security Boulevard shares how this attack **signified the everyday devastation potential of ransomware**. Because DarkSide (the Russian perpetrators) gained access to Colonial Pipeline's systems by exploiting an inactive account that didn't use multifactor authentication, "it puts pressure on businesses to assess similar risks within their own network of systems."

Disturbingly, the human toll of infrastructure attacks boosts their attractiveness. Last year, cybercriminals also targeted water treatment facilities and wiped out nearly 20% of the U.S. meat processing capacity of JBS Foods, the world's largest meat supplier.

Systems that house high-value assets and information are increasingly vulnerable – especially as maintenance costs for outdated technology and processes multiply. For many enterprises, this depletes resources that might otherwise be used to strengthen and modernize.

In a letter sent to corporate executives last year, White House Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger noted that "threats are serious and they are increasing," highlighting how cybercriminals are no longer just interested in data theft, but disrupting operations and creating chaos.

Companies must consider go-forward responses – particularly as offices including the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Management and Budget issue new directives surrounding Zero Trust and cybersecurity preparedness. Given that attackers breached Colonial Pipeline through a compromised account with privileged access, it is no surprise that the OMB highlights specifics under the "identity" pillar of the Zero Trust model: Guidance includes applying automation and enterprise-wide identity management to access software applications.

Armed with advanced methods like phishing, credential stuffing, and social engineering – and boosted by the promise of huge payouts – cyberattackers are just getting started. As this trend continues, enterprises must stay cautious, particularly in securing favorite attack vectors (like identity) within IT or OT devices, and SaaS, IaaS, and PaaS.

How to respond to this trend:

Take a "lifecycle management" approach to every identity: Apply intelligence and analytics to discover identities and consolidate them within a governance framework.

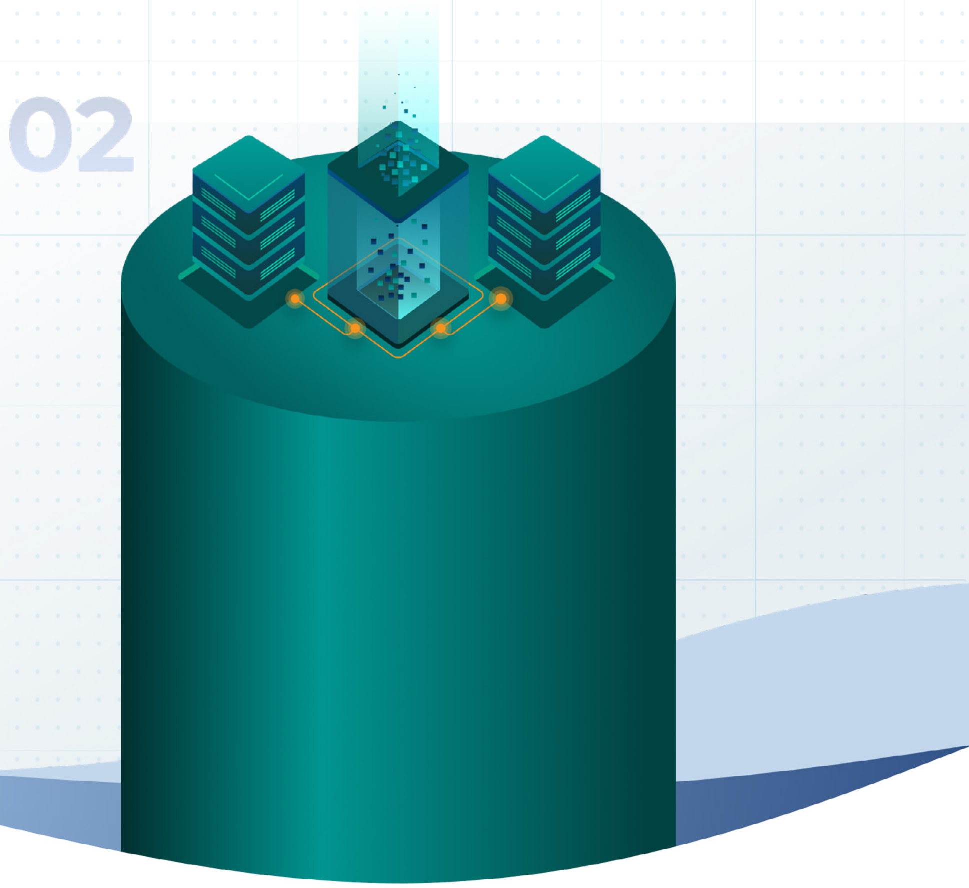
Free up your human first responders: Introduce AI/ML to parse security anomaly noise and use k-nearest neighbor (KNN) algorithms to improve predictive analyses.

Employ risk-based decision making to address excessive access. This includes limiting the number of privileged accounts, utilizing a Zero Standing Privilege model, and ensuring a just-in-time approach to privileged access.

TREND NO. 02

Growing Interest in Cybersecurity “Mesh” Strategies

↓ HOW TO RESPOND



The evolution of cyberattacks and distributed cloud workloads and applications creates a “perfect storm” for IT leaders, suggests Gartner. These changes require that security professionals “integrate security tools into a cooperative ecosystem using a composable and scalable cybersecurity mesh architecture (CSMA) approach.”

This model amends the old view of protecting the traditional IT perimeter with a more modular approach. With CSMA, security leaders apply policies at the identity level to protect devices and resources. These policies extend across the access path – from data to workload to application – creating integrated security from individual components.

A notable opportunity within CSMA is the emphasis on composability, scalability, and interoperability. **This moves security teams from managing fragmented, individually configured services to deploying best-in-class solutions that work together to mature security posture.**

CSMA relies on aggressive assumptions including the availability of widely composable security services and common frameworks/architectures (like analytics, identity management, threat intelligence, and API security controls). These must work together to protect everything from cloud applications to end users. Effective mesh strategies also require stronger centralized policy management and governance.

For mesh strategies to succeed, Anurag Rai, Principal, Cyber Security Services at KPMG highlights the need to understand exactly what needs solving – and then choosing the right mix of extensible technologies. “Cybersecurity solutions are historically siloed. Don’t start combining tools until you know what needs to be part of your mesh.”

As CSMA popularizes, questions remain:

- Will enterprises dually invest in complimentary principles of Zero Trust and CSMA on the path to modernization?
- Do enough best-in-breed solution providers integrate to deliver enterprises' intended security outcomes?

Last year, CSMA generated significant buzz. Is the approach sustainable or simply good in theory? Time will tell.

> By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a cooperative ecosystem will reduce the financial impact of individual security incidents **by an average of 90%.**
>
> **Gartner**
> Top Strategic Technology Trends for 2022

How to respond to this trend:

Reimagine your legacy perimeter and shift to "identity based" to handle growing cloud platforms and SaaS use. Apply a Zero Trust framework, built on Zero Standing Privilege to improve security.

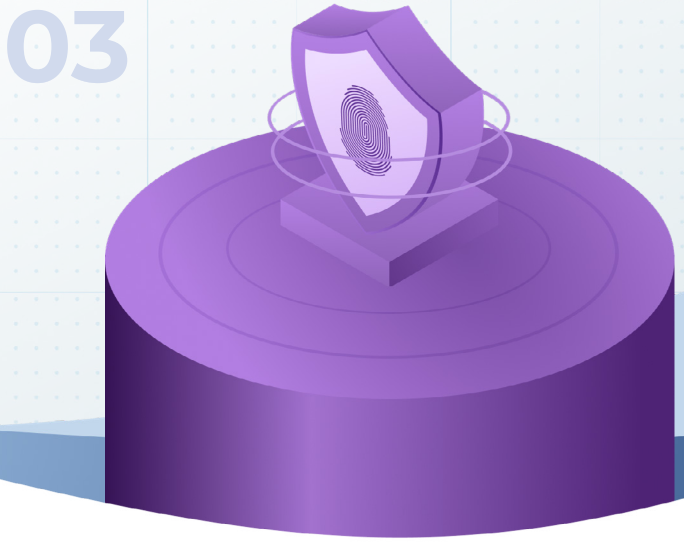
Examine existing security infrastructure and assess opportunities for connecting currently siloed products.

Establish KPIs and routinely measure mesh strategy effectiveness. "Going down the project integration path with no proven ROI is the fastest way to kill sponsorship and funding," shares KPMG's Rai.

TREND NO. 03

‘Go time’ for Zero Trust

HOW TO RESPOND



Last year, we predicted a Zero Trust increase as cyberattacks dismantled confidence in perimeter-based security and a “trust but verify” model for identity access management.

This year, we expect mass movement from framework *acceptance* to *implementation*. According to VentureBeat, 82% of security and risk professionals now say that Zero Trust is an “essential strategy” for their company – and nearly 60% expect to begin Zero Trust efforts in the next six months.

Late last year, the White House **issued** an executive order essentially mandating Zero Trust architecture for federal agencies by 2022. To achieve an optimal level of Zero Trust maturity, the Cybersecurity and Infrastructure Security Agency (CISA) suggests that companies:

- Continuously validate all identities in real time
- Centralize access authorization across all cloud and on-premises systems and resources
- Leverage machine learning (ML) to analyze access patterns within the organization on an ongoing basis
- Constantly monitor and validate the amount of access that each connected device is granted
- Safeguard data access with real-time risk analytics
- Enforce micro-perimeters around all assets and resources in the environment
- Ensure that all traffic is encrypted
- Integrate continuous identity validation into all inter- and intra application workflows

As Zero Trust implementations grow, we anticipate a range of challenges to emerge.

For example, growing use of modern applications and cloud services requires ways to enforce access controls and governance. SaaS use also introduces disparate security requirements that stretch legacy processes and tools. Companies will need scalable means to inventory assets and existing access levels – and establish where sensitive data and access reside.

Endpoint devices, enterprise computing resources, and networking and infrastructure components **must exchange** information seamlessly across the entire IT ecosystem. And all parts of the data and endpoint security architecture need to work together with security analytics and identity governance and access management solutions.

In response to these challenges, we predict adoption of **converged platforms** that unite capabilities like privileged access management, identity governance and administration, application access governance, and data access governance. Business processes now blur the lines between various types of identities and access. No longer do organizations need extensive (and distinct) product suites to secure varying identity types.

As a principle, Zero Trust is widely accepted. In 2022, the hard work of operationalizing will begin.

How to respond to this trend:

Establish a Zero Trust roadmap that starts with rigorous assessment and extends to critical capabilities and controls.

Prioritize the role of identity (and a modern identity solution) when considering platforms that integrate with existing security and compliance tools.

Don’t neglect internal alignment. “In many cases, Zero Trust implementation pain comes from consensus,” suggests Laxman Tathireddy, Principal at Deloitte & Touche LLP. “It’s important that security, application, and network infrastructure teams contribute and sign-off on strategy and end goals.”

TREND NO. 04

Multi-Cloud Management Mayhem

HOW TO RESPOND

In a recent survey of public cloud users, 81% of respondents said they are working with two or more providers. “Most organizations adopt a multi-cloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions,” says Michael Warrilow, VP Analyst, Gartner.

Deploying multi-cloud for services like compute or storage has clear advantages around performance, compliance, and resilience. But it “adds an extra layer of management complexity – especially if multi-cloud adoption develops in an ad hoc manner,” suggests ZDNet.

Given the way organizations implement cloud assets and workloads, these services are more vulnerable to data breaches, phishing or DDoS attacks, and ransomware. Enterprises must deploy strong security practices to ensure availability, protect sensitive information, and maintain regulatory compliance.

As multi-cloud adoption expands, we expect visibility, security, and governance issues to heighten. CISOs will wrestle with questions like:

- How do I improve risk insights and gain a single view of all identities, assets, workloads, policies, and settings across my multi-cloud environment?
- How do I reduce manual compliance efforts and apply automation to controls management?
- Where can I apply just-in-time, time-bound, and just-enough access to reduce privileged access sprawl?

According to Accenture, legacy identity tools and processes actually compound the difficulties of these questions as they “lack the scope and capability to secure access to the cloud.”

Although cloud providers and customers **share** security and compliance responsibilities, customers are responsible for management and configuration of Identity and Access Management (IAM) controls in their own environments. Often, varied cloud roles, infrastructure, applications, and services lead to misconfigurations – resulting in exploitable vulnerabilities like unused permission accumulation, especially **at scale**.

Further, the traditional, backward working model for security control building is increasingly inadequate:

> "Building security controls one-by-one to meet the authorization models of individual cloud providers won't work with multi-cloud. Enterprises must start with more technology agnostic frameworks. Start by understanding every identity, persona, or workload that interacts with your clouds, then apply individual management nuances as needed."
>
> **Anurag Rai**
> Principal, Cyber Security Services at KPMG

Multi-cloud management solutions must not be people-centered, shares James Quick, Director, Solutions & Advisory at Simeio. "Software automation can mitigate the known risk of chronic staff shortages in cybersecurity. There are hundreds of thousands of unfilled cybersecurity roles out there – so use RPA, leverage AI and ML, and prioritize automation investments to ease internal burdens."

Additionally, given distinct control capabilities across cloud providers, we anticipate a growing appetite for a "homogenous" control plane experience. Although a truly centralized management offering does not exist, platforms that offer a unified, cloud-native management experience will be in demand.

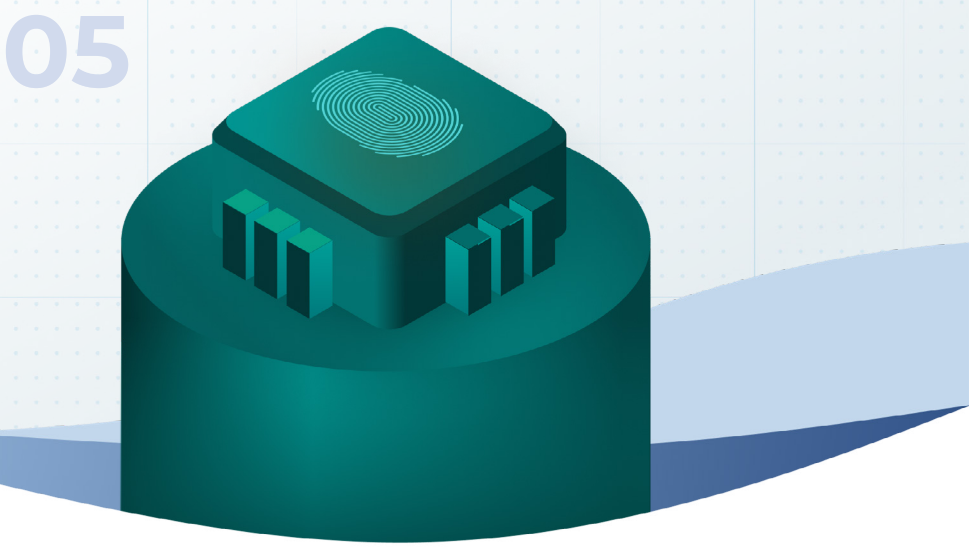
How to respond to this trend:

- **Start all security efforts at ground zero – managing identities.**
- **Prioritize precise visibility (e.g. - deploy solutions that give you an exact view of access across your entire infrastructure and application ecosystem.)**
- **Integrate with federation tools to link cloud accounts and individual identities. Don't risk errors from manual cross referencing.**

TREND NO. 05

Rise of the Machine... Identities

HOW TO RESPOND



In a recent security webinar, Forrester posed an unsettling question: “*Do you know how many software bots, physical robots, or internet of things (IoT) devices are connected to your network?*"

Today, digital transformation campaigns spawn thousands or millions of new machine identities. Non-human tools boost productivity, but they also widen threat surfaces. According to TechCrunch, machine identities are the least understood and poorest protected part of enterprise networks.

Research from Identity Defined Security Alliance (IDSA) **finds that** 83% of companies saw an increase in the number of identities accessing system resources last year. Types include bots, serverless functions, software-defined infrastructure, administrative roles in cloud accounts, scripts, and other infrastructure-as-code artifacts – identities with no operator or human intervention.

Forrester now **predicts** the number of non-human identities to “grow at more than twice the pace of human identities.” Today, organizations desperately need robust machine identity governance and more secure IoT and IIoT ecosystems.

> By some estimates, non-human or non-people identities **outnumber human identities by hundreds or thousands to one.**
>
> **SecurityBrief by TechDay**
> Rise of the Machine Identities

As we’ve shared, machine identities fundamentally behave as privileged users. Enterprises must view them as a security threat – and elevate privilege on a just-in-time basis and deactivate the privilege when the identity is inactive.

Computer Weekly also describes needed responses for security conscious enterprises:

- Businesses must work to eliminate shared accounts so that all human or non-human entities interacting with systems have an identity that can be managed and used for applying the Principle of Least Privilege [...]
- PAM systems, therefore, must support privileged non-human identities for machines, processes, microservices and containers in both production and development environments or DevOps, where this model is followed

Just 40% of CISOs and IT leaders **say they** have an enterprise wide strategy to manage machine identities. Most have either no strategy (18%) or a limited strategy for certain applications or use cases (42%).

Machine identity growth is explosive – clearly, there is much management work to be done.

How to respond to this trend:

Avoid manual or siloed controls with point solutions. Bring machine identity management under a comprehensive IGA/PAM strategy.

Prioritize visibility and continuous monitoring – this helps you establish privilege level understanding, access revocation/changes, succession policies, peer and usage data intelligence.

TREND NO. 06

Push Towards Passwordless

HOW TO RESPOND

Last year, more than 60% of data breaches involved stolen credentials – and "credentials are the skeleton key," explains Gabe Bassett, senior information security data scientist for Verizon Security Research. Many enterprise accounts, including service accounts, still rely on static credentials. Often, they maintain privileged access to software and processes (and run without operator intervention through automation).

In 2022 and beyond, we expect security leaders to abandon both the "set it and forget it" mentality and static passwords to grant sensitive access.

As 1Kosmos **guides**, "[Static controls have] proven ineffective; that is why password-based breaches and identity fraud persist. The bigger problem is the dynamism and ephemerality of digital identity – which has led to the emergence of passwordless authentication and digital identity proofing."

VentureBeat **dubs passwordless** as one of identity and access management's most defining trends. They tie this evolution to the rise in virtual work – suggesting that a displaced workforce needs a Zero Trust based approach to passwordless authentication to stay secure.

Simeio's James Quick connects this to the larger meta-narrative "that every user must now be treated as a privileged user." He cites the frequency of cyberattackers compromising ordinary user credentials and then moving laterally as a reason for passwordless.

Vibhuti Sinha, Saviynt's Chief Product Officer, sees this evolution as essential for reducing system exploits and impact:

"Going passwordless is akin to reducing a blast radius; by lessening the potential of 'system hooks', enterprises reduce fallout from breaches or data leaks."

Increased **support** of authorization protocols, including FIDO2, from hardware and software vendors fuels passwordless momentum, according to Andre Priebe, CTO, iC Consult. "In the past, passwordless depended on proprietary technology. Now we can use standard technology, hardware, operating systems, and processes." Additionally, he acknowledges growing user comfort with biometrics in personal device use, noting that IT system application for simple, phishing-resistant, and privacy-enhancing sign-in experiences is an obvious next step.

In 2022, expect wider embrace of the idea that identity must be both immutable and tamper-proof (i.e., based on factors/attributes other than passwords) and that access permissions need hardening against exploit. Slowly, inertia and perceived security weaknesses are being overcome. Organizations will aim for access policies to be contextual, conditional, and based on least privilege.

How to respond to this trend:

When rolling out a passwordless security approach, start incrementally. Apply learnings for subsequent rollouts across the IT landscape.

Do not underestimate the importance of User and Administrator training during the transition to passwordless. These facilitate faster, better adoption.

Consider the IT risks of passwordless when users need to re-prove their identity. For example, when replacing hardware for a remote employee. Assess alternatives like AI-based identity proving scenarios where supervised interaction isn't required.

TREND NO. 07

Necessity of Shared Intelligence Initiatives

HOW TO RESPOND

Despite remarkable technology advances within the cybersecurity industry, threat intelligence (TI) sharing remains mostly ad-hoc – filled with blindspots, disunity, and delays.

DarkReading describes information sharing as a “critical aspect of any security strategy,” however, the fragmented nature of service providers often impedes enterprises’ ability to identify, validate, and respond to threats.

This year, we believe the corporate cybersecurity ecosystem will aggressively partner around shared intelligence. In particular, we expect movement beyond informal, peer-level relationships to deliver broader protections with scope, scale, and speed.

McKinsey suggests better TI sharing will help leaders filter out the most pertinent intelligence and protect critical data assets – without abandoning basic IT support needs.

Consider one initiative: the Cyber Threat Alliance. This not-for-profit membership organization facilitates information flow across dozens of cybersecurity companies, bridging vendors’ partial visibility, and the patchwork of tools, technologies, services, and research that exist. Today, the alliance acts as a ‘force multiplier’ of defense and automates sharing of more than 200,000 malicious indicators per day.

Also gaining traction is The Financial Services Information Sharing and Analysis Center, which shares threat intelligence and incident information across nearly 7,000 financial-services institutions.

Enhancing security with open standards will also boost security insight collaboration. IBM’s Cloud Pak, for instance, leverages open-source Sigma rules and STIX patterns to bridge security insights across multi-cloud environments.

Other promising work is underway with SIEM and endpoint providers. McAfee **offers a** collaborative platform with all the components for operationalizing threat intelligence, including global TI feeds, local intelligence creation, real-time sharing of threat information across the IT infrastructure, security information and event management.

More **recently**, Bitdefender, a leading cybersecurity company protecting hundreds of millions of endpoints and systems worldwide, announced a threat intelligence sharing partnership with Recorded Future, the world's largest provider of intelligence for enterprise security.

To address obfuscated risk across IT ecosystems and multiple monitoring tools due to identity proliferation, we've **established** an Identity Risk Exchange. The solution consumes and exchanges risk data across key GRC and risk platforms (including popular SIEM, UEBA, and vulnerability management tools) for better cloud security. This is an important, early step toward seamless integration across popular risk monitoring tools.

Cyberdefense is historically reactive. But operationalizing threat intelligence means safer ecosystems for everyone. Shared security insights are the cornerstone.

How to respond to this trend:

For security product vendors: apply a standards and API based approach to product development. Providing necessary interfaces for TI and risk signals sharing will accelerate initiative progress.

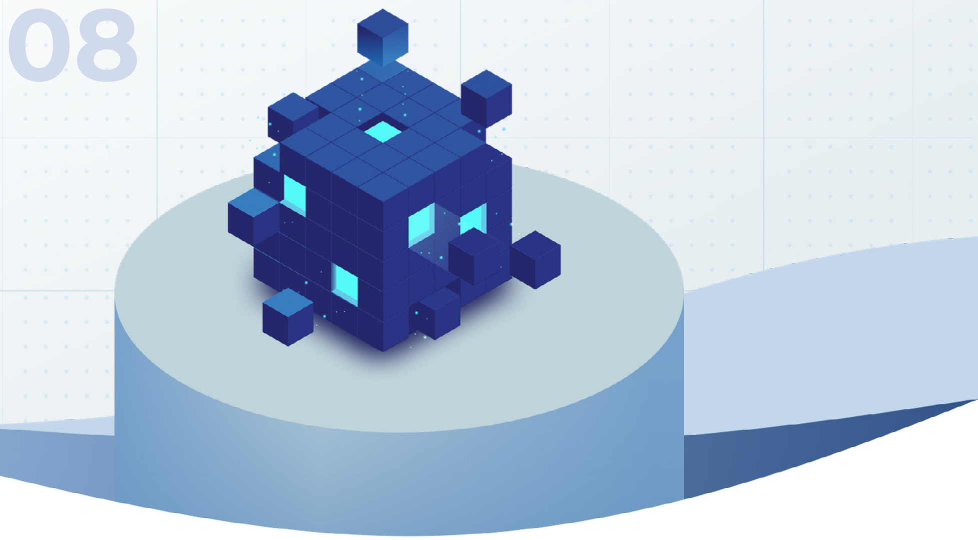
Invest resources to build an open consortium to share information with other vendors and operate at scale.

For organizations: Mature beyond rudimentary use cases. Correlating data from various sources (and responding proactively) is essential to detect sophisticated attacks. Understand that with enriched data you may retrieve false positives; don't be discouraged. Expect this as part of an incremental maturing process.

TREND NO. 08

Mass Convergence of Identity and Security Platforms

HOW TO RESPOND



The historical arc of identity in technology is long, but bends toward convergence. In 2022, the merging will intensify, creating new efficiencies.

Companies today are always transforming *something*. The downside of these modernization ventures? An explosion of tools, interfaces, dashboards, alerts, and, yes, identities. The chaos demands a centralized hub to manage data, attributes, and information.

We've **termed it** "converged identity."

In a recent Total Economic Impact **report on** Saviynt's Enterprise Identity Cloud, Forrester notes how many companies deal with onerous identity and access governance responsibilities using a "combination of on-premises, homegrown tools that require internal coding, regular maintenance and upgrading, and significant management time." **CISOs simply do not have the resources to integrate, manage, and maintain point solutions and wrangle IAM sprawl.**

> By 2025, converged IAM platforms will be the preferred adoption method for AM, IGA and PAM in over 70% of new deployments, driven by more comprehensive risk mitigation requirements.
>
> **Gartner**
> 2021 Magic Quadrant for Access Management

To boost risk-awareness, enterprises will look for converged identity governance, granular application access, cloud security, and cloud privileged access to draw the security perimeter at identity. Efforts will also target IoT/Bot governance and Third-Party Access.

In addition, they will pursue better defined identity business workflows – particularly as vendors incorporate identity insights and analytics into security platforms.

For 2022, we expect extended offerings – centered on identity – that improve security leaders' visibility. According to ITProToday, **these extended detection and response** (XDR) solutions will combine cloud, endpoint, network, and log data with a data processing engine to expose malicious operations. "This could fill a gap for organizations struggling to gain visibility into their cloud workloads for critical applications," shares Dave Gruber, a senior cybersecurity analyst at ESG Global.

Aggressive M&A among cybersecurity vendors is fast-tracking this convergence. Microsoft's spending spree last year **netted them** four new cybersecurity offerings. Security Magazine **observes** how vendors with acquired tools (like IGA & PAM) now talk about their tools as "platforms."

Enterprises must exercise caution, however. Often marketers hype "converged identity" despite a lack of true solution convergence. Alternately, genuinely converged platforms simplify, unify, and streamline the workflows across distinct tools – while being robust enough to handle modern ecosystems.

"While converged offerings may improve security elasticity, visibility, and scalability, for some solutions, questions remain about automation, interoperability, and user-friendliness," offers Yash Prakash, CSO at Saviynt."

Still, we don't expect this uncertainty to derail convergence. Deloitte's Tathireddy highlights how a shift to outcome-based service models can help de-risk converged identity and security:

"Enterprises may not need to find individual tools, purchase licenses, and navigate implementations. They can engage third parties and pay for services to help them achieve their identity and security goals, not simply get guidance on point solutions. The model makes identity product companies and system integrators more accountable and interested towards outcomes."

How to respond to this trend:

Prioritize simplicity for end users to improve converged platform adoption.

Consider a cloud-built platform that combines multiple identity management capabilities and has an open framework to support solution integrations.

Once identity and security goals are defined, evaluate outcome based engagements. At a minimum, ensure that solution vendors have a story around convergence – versus offering only a point solution.

TREND NO. 09

Demand for Better Third-Party Access Governance

HOW TO RESPOND

Last year, Morgan Stanley disclosed that corporate client data was stolen in a data breach that involved a stock account maintenance vendor. In April, the infamous hacker group ShinyHunters compromised a third-party identity warehouse and exposed over 56 million KYC data files from Upstox, India's second-largest stock broker.

Security professionals still recall the 2013 cyberattack on Target, when hackers breached a refrigeration services vendor and stole credit card data of 41 million individuals. The estimated **expense** of the breach: $292 million.

Harvard Business Review points to misleading mindsets as a **key reason** for weak third-party security: "Products are usually purchased for the value-added features they provide, not because they are secure."

As third-party related incidents rise, we expect organizations to increase monitoring and assurance activities for this segment.

"Historically, enterprises were far too focused on managing employee identity and access. But third-parties often have as much, or more, access risk and they need to be managed better," suggests Saviynt CEO, Amit Saha. "Especially because upstream governance is often weaker for third parties."

Forbes **builds on this**, noting a lack of discipline around third-party access management and knowledge gaps resulting in standing, privileged access:

"You might have one department that notifies the HR team they're bringing a new contractor on board, but they're managing the process in a distributed fashion. Once the contractor has completed the job, there's no ownership of notifying HR or IT that the contractor has left."

In many cases, enterprises don't grasp the extent of third party access, particularly as external collaboration within cloud-based applications like Microsoft 365 grows. Companies may have a limited supplier database, for instance, but because of capabilities like self-registration and guest invites, external identities stay disconnected and "fragile governance and lifecycle management for third parties persists," finds iC Consult's Priebe.

This year, expect companies to push suppliers for more stringent security controls. “The focus will shift to ensuring that identity-based perimeter is robust enough to identify and manage threats from external contractors,” says Saha.

Data will also play a larger role in providing context to third-party threats in the coming year. “Today, assessing third-party security risk requires a much more data-driven approach to identify and understand risk,” says Jonathan Dambrot, Partner at KPMG. He observes that third-party security has largely been driven by shared assessments in the past, but that approach is no longer enough to keep up with the modern risk landscape, or build trust with partners and customers.

We predict increased efforts to include more inline identity proofing, security monitoring, and continuous verification. For example, allowing contractors or less-known operators to prove themselves out using external digital identity validation and then applying least privilege authorization.

Other intelligent identity practices will grow in popularity, including streamlining the suspend/deactivate/rehire process to secure access.

How to respond to this trend:

Inventory your partners, suppliers, and contractors to understand your third-party access exposure – then define what the right level of access and relationship should be.

“Consider additional investments in identity security platforms and ID proofing technology — along with AI and machine learning security solutions — to continuously verify identity, monitor third-party risk signals, and respond appropriately to remediate emerging threats,” shares KPMG’s Dambrot.

Be careful that poor user experiences and complexity within identity lifecycle tools don’t undermine efforts to manage third parties’ digital identities. Complicated processes, governance, and platforms may impact user and IT buy-in.

TREND NO. 10

Mainstreaming Blockchain in Identity

HOW TO RESPOND

Fragmented identity, access, and authentication experiences still mark IAM and IGA architectures. To solve this, we foresee mainstream application of blockchain (and decentralized identity) – alongside movement away from more rigid, centralized, and federated infrastructures.

One overview of decentralized identity describes a trust framework in which identifiers (such as usernames) are replaced with IDs that are self-owned, independent, and enable data exchange using blockchain and distributed ledger technology.

According to Microsoft, a decentralized approach brings benefits for three key audiences:

- Users - own and control digital identities and protect privacy with highly secure user experiences.
- Organizations - engage with less risk, use electronic data verification, and improve transparency and auditability.
- Developers - design user-centric apps and services and build true serverless apps that store data with users.

> “Decentralized digital identity is not just a technology buzzword: It promises a complete restructuring of the currently centralized physical and digital identity ecosystem into a decentralized and democratized architecture.”
>
> **Forrester**
> Prepare For Decentralized Digital Identity: Security SWOT, January 21, 2020

In a decentralized framework, a verified issuer (e.g., government or employer) provides credentials to a user who stores them in a digital wallet. The user is able to present these credentials to a service provider who can consume and confirm prevalidated identities and verified credentials.

Many cybersecurity vendors now suggest that existing systems for handling digital identities no longer work. A popular alternative is a **fully decentralized IAM**; one that gives entities self-sovereignty over the verification and authentication process via multiple digital workflows powered by blockchain.

Gartner **writes that** because ecosystems are still immature, fully decentralized identity implementations will not fully overtake traditional, centralized identity systems in the near future. However, they note that enterprises must "be prepared to support BYOI mechanisms from multiple decentralized identity networks, especially if [your organization] is responsible for other IAM technologies, such as access management, identity governance, and administration and identity proofing."

"But even with identities increasingly distributed or decentralized, enterprises need to solve for compliance and improved transparency," guides Saviynt's Prakash.

We forecast near-term use cases to include enterprises consuming and supporting decentralized identities from various sources and third-party vendors. In these instances, enterprises will need agile third-party access governance solutions to "hook" into existing HR processes as part of identity proofing and continuous verification/credentialing.

How to respond to this trend:

Uncover any blockchain POCs within your organization. For these, understand identity lifecycle management, how keys are managed, and explore ways to correlate activities/transactions (while preserving privacy) when establishing a governance model.

Discern regulatory requirements before building a threat model. Model should account for how blockchain will specifically be used in the business. Assess each attack vector and then develop a defense-in-depth strategy.

Conclusion

For the thoughtful security leader, exploring trends is more than intellectual sport. Each trend raises real-world security implications; and while the trends we highlight may not materialize exactly as described, action steps that accompany reflection may drive real success.

Act now: Consider machine identity sprawl, harden vendor governance, assess converged identity platforms, and anticipate decentralization in your security roadmap. As you weigh your approach, identify a partner to ride the modernization wave with you.

SAVIYNT

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 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.

Want to talk to an identity and security expert?

Schedule a Call Today

Thanks to Our 2022 Identity & Security Trends & Predictions Contributors

KPMG

Deloitte.

simeio™

iC CONSULT

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.