Devolutions

# Gartner Lists Top Security and Risk Management Trends in 2021


## THERE ARE EIGHT TRENDS IN TOTAL

Gartner has revealed its list of the top security and risk management trends that will shape the business landscape in 2021. There are eight trends in total, which have been grouped into three categories:

- **Location-independent security**, which is driven by the surge in remote workers, and the fact that identity — and not location — has become the de facto organizational perimeter.
- **Security organization evolution**, which places an emphasis on maturing information risk processes with regards to personnel (e.g., appointing cybersecurity experts to executive roles) and infrastructure (e.g., consolidating multiple security products into a single, centralized security platform).
- **Security technical evolution**, which focuses on ways to enhance privacy, security and compliance as workloads rapidly shift to the cloud.

Below are the eight trends as they are listed in the Gartner report, and not necessarily in order of priority. For each trend, we also include Gartner's recommendations for IT leaders who are responsible for security and risk management.

## Location-Independent Security Trends

## 1. Cybersecurity Mesh

COVID-19 has accelerated the relocation of end users and digital assets outside of the organization, which is driving a modern InfoSec approach — called the cybersecurity mesh — in which controls are implemented where they are most required, and in a way that is flexible, scalable, resilient and composable (i.e., components can be selected and assembled in multiple combinations to satisfy specific organizational requirements).

Typically, the cybersecurity mesh architecture is deployed in the cloud (although on-premises deployments are possible). Leveraging the public cloud supports various enforcement points, which can be associated with multiple distributed assets. This model also enables SaaS providers to provide customers with reliable, high-performance services.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following cybersecurity mesh strategies:**

- Shift focus, resources and investments to cloud-delivered, location-independent cybersecurity controls.
- Select intelligence technology and security analytics that are extensible (internal structure and data flow are unaffected/minimally affected, by new or modified functionality) and interoperable (enable the connection and integration of disparate tools in the ecosystem).
- Develop adaptive trust models that support secure, high-performance access to cloud apps.
- Choose vendors that have opened up their policy framework, so that the organization is not restricted to making policy decisions within various tools.

## 2. Identity-First Security

Identity access management (IAM) certainly is not new. However, COVID-19 has thrust this approach into the spotlight and elevated it from an optional best practice to an essential day-to-day requirement. Indeed, organizations no longer operate in a paradigm in which location determines the degree (or lack thereof) of security controls. Instead, all resources, applications, tools and network areas need to be perceived as potentially vulnerable and at-risk.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following identity-first strategies:**

- Implement controls such as single sign-on (SSO), multifactor authentication (MFA), and zero-trust network architecture. For enhanced visibility and security, some organizations may also want to implement proxies and cloud access security brokers (CASBs).
- Audit all remote access use cases, and build reference architectures for securing each one.
- Scrutinize all logging practices, security processes and procedures, and where necessary increase visibility and control. The focus must be on being proactive vs. reactive.
- Determine if there is sufficient specialized cybersecurity talent in-house to support these (and other) strategies. If not, then make recruitment a top priority. Given that the cybersecurity skills shortage in the labor market continues to grow, organizations — and especially SMBs — are encouraged to partner with a managed service provider (MSP).

## 3. Security Support for Remote Work Is Here to Stay

Remote working in one form or another has been in place for decades, and well before the pandemic, an increasing number of employees and contractors were contributing from a distance. However, COVID-19 dramatically accelerated the remote working migration. And while in some parts of the world workplaces are slowly welcoming back workers, a significant number will not be leaving their home office — at least not on a full-time basis.

As a result, organizations need to reinvent their pre-pandemic policies and tools, so that they make sense in a post-pandemic remote work environment. This approach includes developing multiple robust use cases that: define various end users (roles and functions); identify what kinds of devices end users have (and who owns them); determine what apps, data and network areas end users need access to; and identify where end users are located.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following strategies to support remote workers (including hybrid remote/on-site workers):**

- Leverage modern security architectures, such as the cybersecurity mesh and identity-first security (both discussed above).
- Involve senior IT leadership in determining the optimal models of computing.
- Minimize the risk of loss (intentional or accidental) by defining procedures that control access to applications and data, and the security controls that must be in place for governing access to those applications and data.
- Create multiple security profiles and architectural approaches. A generic "one-size-fits-all" plan for securing remote work is not functional or safe.
- Anticipate and take steps towards supporting remote work that can be 100% disconnected from the LAN. In other words, make decisions that embrace the reality that remote work is not a trend. It is now mainstream and permanent.

## Security Organization Evolution Trends

## 4. Cyber-Savvy Board of Directors

As organizations pay more attention to cybersecurity — especially in light of high-profile breaches such as the Solorigate attack — they are realizing that their leadership roster lacks the personnel required to evaluate the quality of cyber-risk information, and establish a strong and reliable security posture. To fill this insight gap, they are adding cybersecurity specialists to the Board of Directors, and in some cases, creating executive-level cybersecurity committees.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following strategies to support a cyber-savvy Board of Directors:**

- Seek to understand market trends and board priorities, in order to align (wherever possible) business needs with cybersecurity objectives.
- Get input from senior stakeholders, so they can provide meaningful advice on any changes to oversight and governance at the board level.
- Strive to make cybersecurity risk relevant to non-technical stakeholders by putting observations and recommendations in a business context.

## 5. Security Vendor Consolidation

While diversity in an organization is an advantage, using a large number of security products can increase complexity and cost. It can also lead to overlap, as organizations fail to optimize the functionality and potential of existing tools, and instead add new solutions to the stack. Security vendor consolidation can simplify operations, while at the same time help achieve regulatory and compliance requirements.

With this in mind, Gartner also points out that security vendor consolidation also carries inherent risks. These can include forced legacy products after acquisitions, limited threat intelligence, lack of product integration, vendor lock-in, and overlapping software terms and conditions. Furthermore, some "best-of-breed" security vendors may not achieve this level of excellence across their entire product line.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following strategies to support security vendor consolidation:**

- Do not expect consolidation to take place overnight. Typically, implementing this strategy can take two or more years to implement and optimize.
- Analyze both internal and external factors that trigger the need for vendor consolidation.
- During evaluation and due diligence, focus on a range of metrics including simplified operations, reduced total cost of ownership and total cost of security, and improved risk posture.
- Work with multiple senior stakeholders, including CIOs, CISOs, and CSOs, to develop a customized vendor consolidation strategy and approach. Ensure that the roadmap is realistic and achievable.
- Train staff on how to use new security products to their full potential. Appreciate that this is not just a procurement project, but also a change management challenge.
- Completely retire products that are no longer needed. Do not keep them in the environment due to the sunk cost fallacy (keeping something because it was purchased vs. because it makes sense to keep it), or because "it has always been in the environment."

# Security Technology Evolution Trends

## 6. Privacy-Enhancing Computation (PEC)

Functions like multi-party data sharing, data processing, and analytics in untrusted environments are becoming more complex and riskier in light of expanding privacy regulations and legislation — both on a regional (country) and global scale. Adding to the challenge is the fact that, historically, attempts to establish in-use data protection (as opposed to data protection at rest or in motion) has been notoriously difficult.

Privacy-enhancing computing (PEC) is an approach that leverages emerging technologies to safeguard data in-use in both trusted and untrusted environments. Gartner highlights three levels upon which PEC can be applied: data level (includes transformations on-the-fly controls like differential privacy and transformations to hide individual data values); software (combine specialized software with data transformations); and hardware (establishing secure hardware systems and trusted execution environments).

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following strategies to support PEC:**

- Assess data process activities that need to use personal data, in order to identify use cases for PEC techniques.
- Explore the viability of multiple models, such as homomorphic encryption, secure multi-party computation, private information retrieval (PIR), and others.
- Start experiencing now vs. later in order to ensure long-term readiness.
- Begin budgeting now to invest in valid PEC techniques and technologies, so that there is no financial obstacle to procurement and implementation down the road.

## Breach and Attack Simulation

Today's cyberattacks are potentially much more costly and devastating than in the past. Whereas hackers used to focus on destroying machines and wreaking havoc, today they are motivated to steal data and commit identity theft. In order to thwart hackers from invading endpoints and networks, organizations need to put their defensive systems to the test — and that is where breach and attack simulation (BAS) tools enter the picture.

BAS tools continuously evaluate an organization's defensive posture, which includes both the readiness of its security products and its workforce. While BAS is important, it should be used alongside other threat assessment approaches including penetration testing, bug bounties, and vulnerability scanning/prioritization.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following strategies to support BAS:**

- Align BAS testing with deployment/upgrades to key systems, bespoke applications, and new infrastructure.
- Implement specialized BAS exercises to reveal likely attacker paths to high-value assets.
- Leverage BAS to assess the effectiveness of existing security controls, detection capabilities, and incident response plans.
- Leverage BAS to prioritize future investment.

## 7. Managing Machine Identities

Driven by artificial intelligence and machine learning, nonhuman entities such as devices, apps, gateways, cloud services, virtual machines, RPA/bots, and other SaaS and IaaS workloads are at the leading edge of digital transformation. Managing machine identities focuses on establishing trust — and therefore security — across these digital identities. This approach can include the use of keys, X.509 certificates, secrets, and other cryptographic materials.

**Gartner advises IT leaders who are responsible for security and risk management to focus on the following strategies to support managing machine identities:**

- Determine how ownership and machine credentials should be managed across the organization.
- Map current and short-term machine ID management use cases against those that are available to be assessed.
- Integrate regulatory requirements into machine ID use cases — both existing and upcoming.

## Looking Ahead

After a year like 2020, it is understandable that the only thing we should definitely predict and expect in 2021 is uncertainty. However, amidst the chaos and change, these eight trends from Gartner will shape the narrative in security and risk management. Organizations that adopt and optimize these projects and strategies will find themselves in a much safer and more successful position in the years ahead.

**For additional insights, we highly recommend downloading the full Gartner report which can be found here. It is a free download, and a work email address is required.**