Top Security and Risk Management Trends 2021

Peter Firstbrook, VP Analyst
Zaira Pirzada, Principal, Advisory

30 March 2021

Gartner

Top Security and Risk Management Trends 2021

Published 30 March 2021 - ID G00738210 - 27 min read

By Analysts Peter Firstbrook, Zaira Pirzada

Initiatives: Security and Risk Management Leaders; Technology, Information and Resilience Risk

Organizations are finding that more computing assets reside outside their infrastructure, beyond legacy security controls. Meanwhile, executives recognize the increasing cybersecurity risk. Security and risk management leaders must leverage these top trends to adapt to change and ensure resilience.

Overview

Opportunities

- **Group Trend 1: Location-Independent Security**
  - The shift to remote work has accelerated security product migration to more modern cloud-delivered infrastructure and placed a greater emphasis on securing the identity of a user. As a result, a new architectural approach called the “cybersecurity mesh” was formed, and identity is now the de facto organizational perimeter.
- **Group Trend 2: Security Organization Evolution**
  - As information risk regulations tighten, organizations are putting an emphasis on maturing information risk processes. This has led to two trends arising. First, enterprises are appointing cybersecurity experts at the board level, which prompts greater scrutiny into what security leaders do. Second, in an effort to decrease security product complexity and focus vendor monitoring efforts, organizations are consolidating security products into security platforms that deliver a breadth of integrated security capabilities, rather than using individual products.
- **Group Trend 3: Security Technology Evolution**
  - As workloads rapidly shift to the cloud, privacy-enhancing computation methods are emerging to enable enhanced confidentiality and privacy in cloud environments, while breach and attack simulation tools facilitate the defense of these complex security stacks with continual security testing. Securing machine identities (e.g., devices and workloads) are also evolving into a critical security need.

Recommendations

Security and risk management (SRM) leaders seeking to capitalize on these trends should:

- **Group Trend 1: Location-Independent Security**
  - Plan security technology selection and adjust old processes for the new reality of permanent remote or hybrid work by creating a cybersecurity mesh foundation based on security analytics, intelligence and triggering, distributed identity fabric, and policy management and orchestration. Invest in how better to secure identities.
- **Group Trend 2: Security Organization Evolution**
  - Plan for vendor consolidation by evaluating the internal and external factors which drive the need for vendor consolidation and speak to cybersecurity risk in a business context in order to make it relevant to stakeholders who drive decision-making.
- **Group Trend 3: Security Technology Evolution**
  - Identify use cases for privacy-enhancing cryptography (PEC) techniques by assessing data processing activities that require the use of sensitive or personal data. Add breach attack simulation (BAS) to security resilience programs alongside other methods of managing security exposure. Assess the different tools that must be used for machine ID management.

Strategic Planning Assumptions

- By 2025, the cybersecurity mesh approach will support over half of digital access control requests.
- By 2025, three-quarters of large organizations will be actively pursuing a vendor consolidation strategy, up from approximately one-quarter today.
- By 2025, 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments or multiparty data analytics use cases.
- By 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% today.

What You Need to Know

The top trends covered in this research represent business, market and technology dynamics that SRM leaders cannot afford to ignore. They have the potential to transform an enterprise, and will accelerate in their adoption over the next one to three years. The accelerated speed at which disruption is occurring requires SRM leaders to have structured and proactive mechanisms in place to identify technology trends and prioritize those with the biggest potential impact on their competitive advantage (see Figure 1).

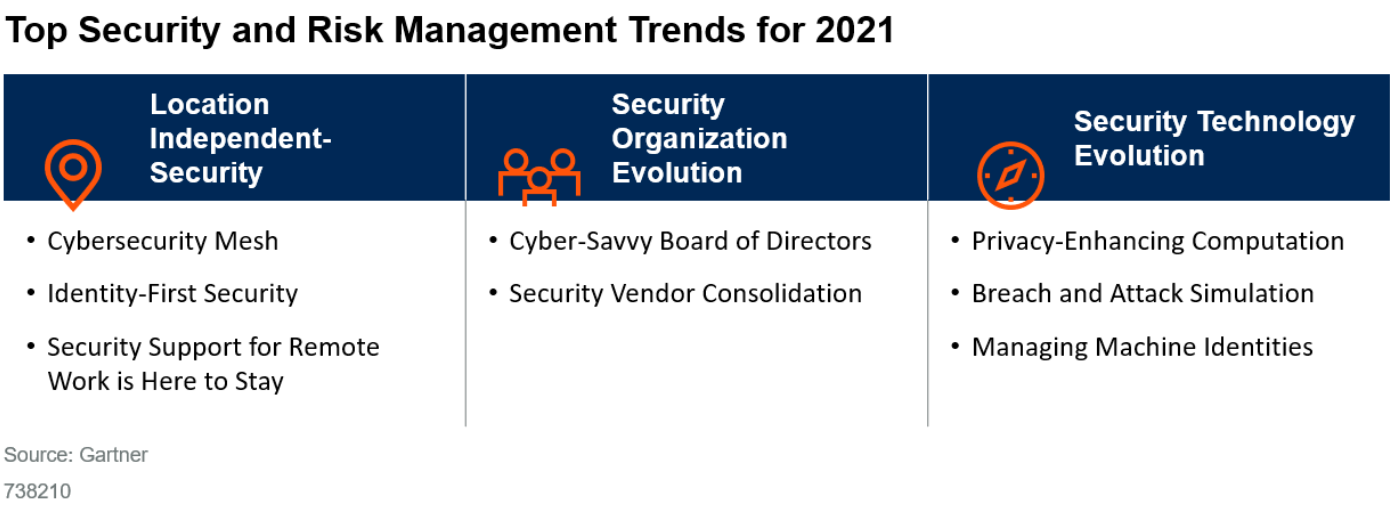
Over the past year, the typical enterprise has been turned inside out. COVID-19 has rapidly accelerated the modernization of information technology. A majority of the workforce formerly working in an office have shifted en masse to working from their homes. As more devices access sensitive company information in the cloud from home offices, the threat landscape increases. Organizations are accelerating their digital transformation journey at a profound rate to accommodate the new reality. Recognizing the cybersecurity danger to business goals, boards of major companies are now seeking cyber-savvy members.

With more transactions, data and employees moving beyond the traditional LAN perimeter, identity is now the new perimeter. Organizations need to know if all things accessed remotely are also accessed securely, and if they have the right technology to accommodate this ideal. Along with trust in human users, the growing need for reliance on and trust in digital identities also extends to machines like devices (e.g., the Internet of Things [IoT]) and workloads (e.g., containers). Privacy-enhancing computation is finally becoming a reality as well.

As the new normal takes shape, all organizations will need constant assurance, a forever-on defensive posture, and clarity in what they have and what they need to remain secure.

As we explore these trends in detail below, it is important to point out that they do not live in isolation. Rather, they are the response by leading organizations to longer-term challenges that are beyond the control of the SRM team. This analysis does not attempt to predict what will happen. Rather, we aim to describe what is significant about what we see happening in the cybersecurity discipline.

Figure 1. Top Security and Risk Management Trends 2021



Gartner

Location-Independent Security

Trend No. 1: Cybersecurity Mesh

Analysis by Jay Heiser

Description:

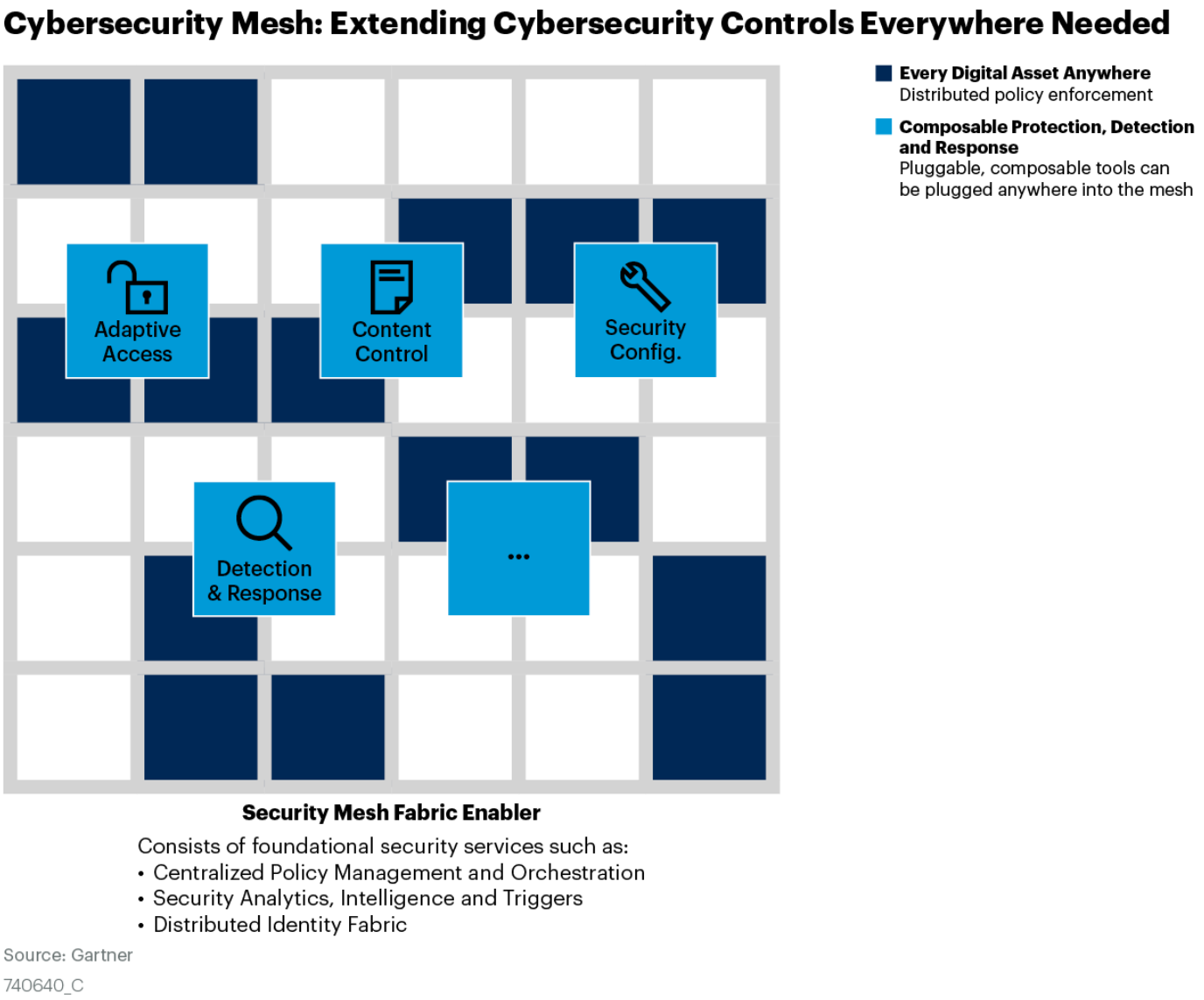
With many IT assets now outside traditional enterprise perimeters, IT leaders must rethink security. Enter the cybersecurity mesh architecture, a composable and scalable approach to extend security controls to distributed assets by decoupling policy enforcement from the assets being protected.

Why Trending:

Digital assets and individuals are increasingly located outside of the enterprise, which is forcing organizations to rethink their approach to security controls. Cybersecurity technology suppliers are helping their customers extend controls everywhere they are needed by using an architectural and delivery model that Gartner refers to as the “cybersecurity mesh” (see Figure 2).

A cybersecurity mesh is a modern security approach that consists of deploying controls where they are most needed, in a manner that is composable, scalable, flexible and resilient. Rather than every security tool running in a silo, a cybersecurity mesh enables tools to interoperate by providing foundational security services such as a distributed identity fabric, security analytics, intelligence, automation and triggers, as well as centralized policy management and orchestration.

Figure 2. The Cybersecurity Mesh: Extending Cybersecurity Controls Everywhere Needed



A distributed architecture decouples policy enforcement from the assets being protected, using a policy enforcement point (PEP) that comes in one of two forms: an agent or a proxy (whichever is most practical). The cybersecurity mesh also creates the fabric for tools to be loosely coupled, and to participate in a common environment where security analytics can enrich a common security intelligence function and trigger actions in multiple systems.

While it is possible to build a cybersecurity mesh architecture entirely on-premises, the typical deployment model is in the cloud. A public cloud deployment model ensures that enforcement points can be associated with an unlimited number of distributed assets. The use of cloud-architected enforcement and orchestration enables security-as-a-service providers to offer more resilient, higher-performance security services.

Implications:

The COVID-19 pandemic has accelerated the multidecade process of turning the digital enterprise inside out. We have passed an inflection point — most organizational cyber assets are now outside the traditional physical and logical security perimeters. However, our ability to control access to our critical digital assets has not kept up.

Today, cloud-based security services provide this function. Cloud computing offers the scalability and accessibility necessary to host security services that can reliably and conveniently support a global cybersecurity mesh. Offering technology on an as-a-service basis means that the vendor is responsible for routine maintenance and upgrades. The corporate cybersecurity team can concentrate on maintaining policy, while letting the vendor worry about the plumbing. Gartner's research indicates that 80% of organizations expect to be using security as a service by 2023.

All cybersecurity technologies are under pressure to accommodate countless forms of digital transformation, including the use of public cloud computing and reliance on personal mobile devices. Gartner believes a mesh approach is especially useful for cybersecurity. Organizations that want to prepare for a graceful transition to the next decade must reconceptualize their cybersecurity approach to a model that accommodates composability. For many organizations, the cultural issues of "this is not how we do security" will be more challenging than the actual implementation of a service-delivered model.

Actions:

IT leaders responsible for security and risk management should:

- Enable the organization's need for operations that can be conducted from any location by shifting to cloud-delivered, location-independent cybersecurity controls.
- Choose security analytics and intelligence technology that is interoperable and extensible: Additional security tools will be expected to plug into this technology, both by contributing additional data and by leveraging insight and being triggered through events.
- Challenge network security engineers to develop organizational adaptive trust models for secure and high-performance access to cloud applications.
- Beware of silos. Scrutinize vendor offerings for interoperability with cybersecurity controls and dashboards, in the form of APIs and integrations. Give priority to vendors that have opened up their policy framework, allowing policy decisions to be made outside the tool.

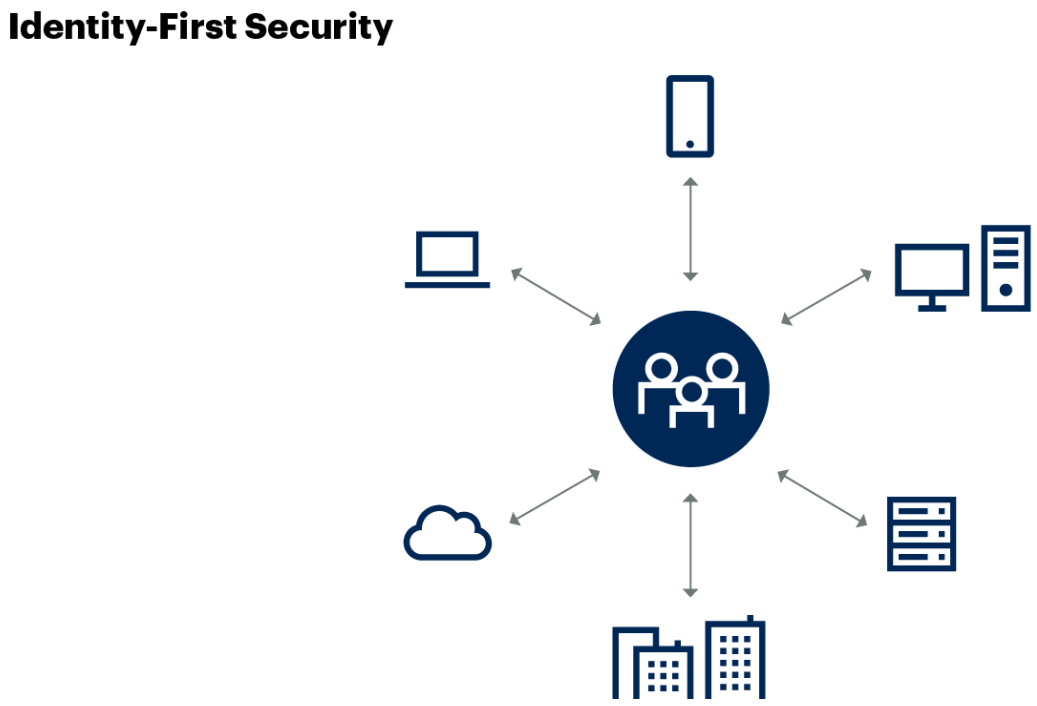
Trend No. 2: Identity-First Security

Analysis by Michael Kelley, Jeremy D'Hoinne

Description:

"Identity as the new perimeter" (identity-first security) has reached critical mass due to technical and cultural shifts, coupled with a now majority remote workforce as a result of COVID-19. Identity as the new perimeter demands a major shift in security priorities from traditional LAN edge design thinking. Identity-first security puts identity at the center of security design, as displayed in Figure 3 below.

Figure 3. Identity-First Security



Source: Gartner
738210_C

Why Trending:

For many years, the vision for access management (AM) was "identity as the new security perimeter," meaning access for any user at any time and from anywhere was an ideal. This was premised on working from the corporate network as the status quo. A good majority of organizations found no reason to change toward the ideal until COVID-19.

Even though culture aspects stalled, the technical capabilities that can enable this approach have been steadily maturing, and now represent the most dynamic of the categories using the cybersecurity mesh approach. AM tools now include single sign-on (SSO) into SaaS and internal applications for remote users; strong authentication through multifactor authentication (MFA) and session management controls brought the possibilities of this vision to life. The emergence of zero-trust network access (ZTNA) mostly completed it.

The ideal became a reality when COVID-19 forced international shutdowns and drove tremendous increases in remote work.

Implications:

The result of these technical and culture shifts is that “identity-first security” now represents the way all information workers will function, regardless of whether they are remote or office-based.

Legacy applications continue to challenge an identity-first approach. However, the market has provided complimentary approaches, leaving space for other modern remote access tools to facilitate access to these applications.

Finally, although much attention has recently been paid to the business value of the identity-first approach, less attention is being paid to the security ramifications of this approach. No longer can the location of an application (within a corporate perimeter or on the public internet) determine the security discipline which should be applied. Rather, all applications and resources must be approached from the perspective that they are at risk, and must be secured as though they have been exposed on the public internet. Moreover, the effort to secure and maintain the traditional network perimeter must be transferred or replicated to the new identity perimeter with a defence-in-depth approach, comprehensive tools, process, monitoring and policy.

Actions:

IT leaders responsible for security and risk management should:

- Inventory remote access use cases and create reference architectures for planning and validating secure approaches for each remote access use case.
- Develop a gap analysis between the organization’s existing access strategy capabilities (e.g. AM, VPN and ZTNA) and consider additional security tools like proxies and cloud access security brokers (CASBs) for additional visibility and control.
- Examine current security processes, procedures and logging practices so as to change practices for more visibility and control, all by way of a risk-adjusted approach.
- Evaluate the technical skills of the organization’s IT department, since many of these technologies require specialized skills, many of which a managed services provider (MSP) could provide.

Trend No. 3: Security Support for Remote Work Is Here to Stay

Analysis by Rob Smith, Jeremy D'Hoinne

Description:

The shift to remote work is here to stay. Security organizations are accelerating their migration to more modern security infrastructure and cloud-delivered security products.

Why Trending:

Prior to the global pandemic, remote working and access were typically reserved for executives, senior staff and employees based outside the office, such as field sales representatives. However, 2020 drove an unexpected and immediate change to the way organizations enable work. According to the 2021 Gartner CIO Survey, on average, 64% of employees are able to work from home, and two-fifths actually are working from home (see The 2021 CIO Agenda: Seize This Opportunity for Digital Business Acceleration). And according to CFOs, the majority of organizations plan to shift at least some employees permanently to remote work after the pandemic.

Implications:

For many organizations, this migration requires a total reboot of policies and tools fit for purpose for a modern remote workspace. They need to create use cases defining who the user is, what kind of device they have (and who owns the device), what apps and data content they need access to, and where in the world they are located (see Figure 4).

Figure 4. Key Components of an Employee's Remote Work Profile

Key Components of an Employee's Remote Work Profile

	Employee Role	Remote Work Strategy	Client Compute(s)	Application and Data
	• Access: – Applications – Structured Data – Unstructured Data (e.g., Email) • Technological Savviness • Fit to Remote Work • Risks Exposure	• Frequency: – Not Suitable – Impossible – Emergency Only – Occasional – Part Time – Most Time • Work Location – Fixed (e.g., Home, Co-working Space, Flex Office) – Mobile (e.g., Travel)	• Managed Laptop • Bring Your Own Device (BYOD) • On-Premises Workstation Accessed Remotely • Desktop as a Service (DaaS) • Virtual Desktop Infrastructure (VDI)	• On-Premises: – Public Facing – Internal – Air Gapped (e.g., SOC) • IaaS • SaaS
Stakeholder	Business Leaders	HR, Business, Finance	CIO	CIO
CISO's Role	Understand	Adapt	**Influence**	**Influence**

Source: Gartner
724856_C

Gartner

Once that is done, security teams can shortlist appropriate technology to provide appropriate security levels in order to mitigate risk while not affecting productivity.

As the organization's infrastructure and application landscape will evolve to adapt to the new remote work realities, security teams must leverage new security architectures, such as the cybersecurity mesh and identity-first security. They also must review how to secure, manage and monitor completely off-LAN employees. Remote work will also impact product licensing.

Actions:

IT leaders responsible for security and risk management should:

- Collaborate with senior IT leadership on which models of computing will be strategic in the organization's future.
- Define procedures for access to applications and data, securing data to minimize loss.
- Refrain from approaching distributed work security with a "one size fits all" plan. Prepare for multiple security profiles and architectural approaches.

- Adjust and plan technology and processes for the new reality of permanent remote work that can be completely disconnected from the LAN.

Security Organization Evolution

Trend No. 4: Cyber-Savvy Board of Directors

Analysis by Sam Olyaei

Description:

Large enterprises are now beginning to create an exclusive cybersecurity committee at the board level responsible for strategy and risk management. This committee is overseen by a qualified board member with subject matter expertise in cybersecurity.

Why Trending:

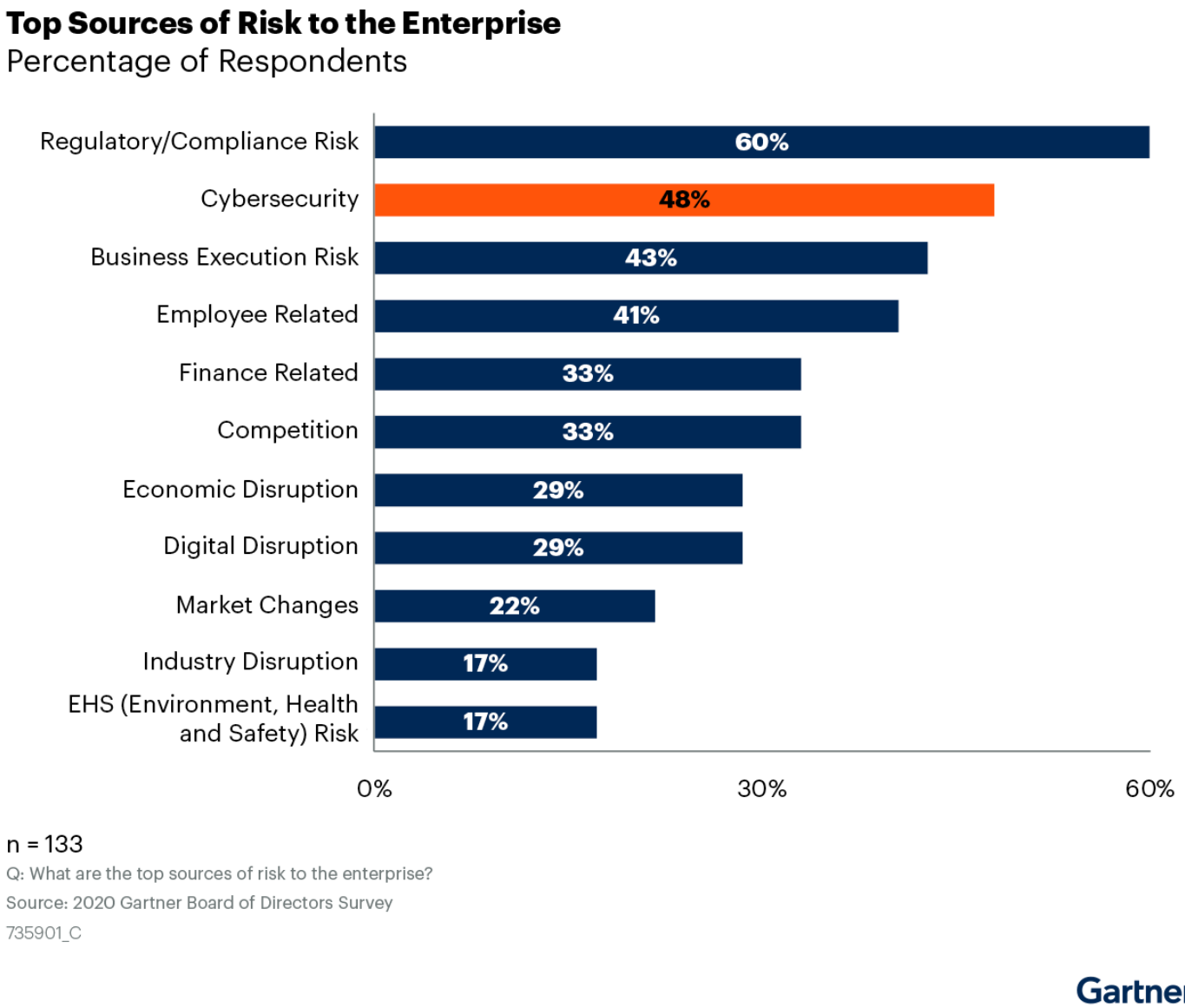
Interest in SRM at the board level is at an all-time high.

In 2018, 91% of large organizations have briefed their boards on their cybersecurity program at least once in the last year.

In 2019, four-fifths of respondents to Gartner's Security and Risk Survey said that cybersecurity-related risk influenced decisions at the board level.

In 2020, Gartner's Board of Directors Survey detailed cybersecurity-related risk to be the second-highest source of risk for the enterprise (see Figure 5).

Figure 5. Top Sources of Risk to the Enterprise



As boards give more scrutiny to cybersecurity, they are becoming less confident in their organization's security posture and the quality of cyber-risk information provided to them by management.

The reasons for this increased scrutiny and reduced confidence may include recent security incidents that disrupted business operations, changes to regulatory requirements necessitating board assurance, or some cultural disconnect between security and the business.

As a result of these changes, many boards of directors are forming dedicated committees that allow for discussion of cybersecurity matters in a confidential environment. These committees are often led and overseen by a member of the board who is deemed to be suitably qualified (current or former chief information security officers [CISOs] and third-party consultants may also play a role here). This allows for increased oversight across the organization, as well as ensuring that cybersecurity receives attention beyond that of committees such as audit, risk and technology committees.

Implications:

Board oversight and governance affects CISOs in three ways.

The first way is through the internal oversight component. CISOs should expect increased visibility of cyber-related risk at the business level, and thus more scrutiny and higher expectations. On the positive side, they are also likely to receive more support and resources if that rapport is built in a trustworthy manner.

Secondly, some boards have filled the role of cybersecurity committee head with former CISOs, while others have chosen consultants. Regardless of title, the board member is likely to have the experience of a full board member, with the necessary technical and cybersecurity knowledge to conduct oversight. The CISO will have to tailor communication and messaging plans to the role while expecting conversations to shift towards risk-oriented and value-driven exercises.

The third way is through the dynamics of the CISO's relationship with the full board. Since decision making may be handled by a board member or dedicated committee, the CISO may have less visibility and facetime in front of the other members and other committees. By the same token, other board members may feel ignored and/or out of the loop, especially if the conversations and deliverables get too technical.

Actions:

IT leaders responsible for security and risk management should:

- Anticipate potential business needs and changes in expectations by understanding board priorities, market trends and how good industry knowledge can influence outcomes.
- Work with other senior stakeholders to collectively add input on the change in governance and oversight at the board level.
- Speak to cybersecurity risk in a business context and make it relevant to stakeholders, so as to drive cybersecurity decisions based on business-relevant prioritization and investments.

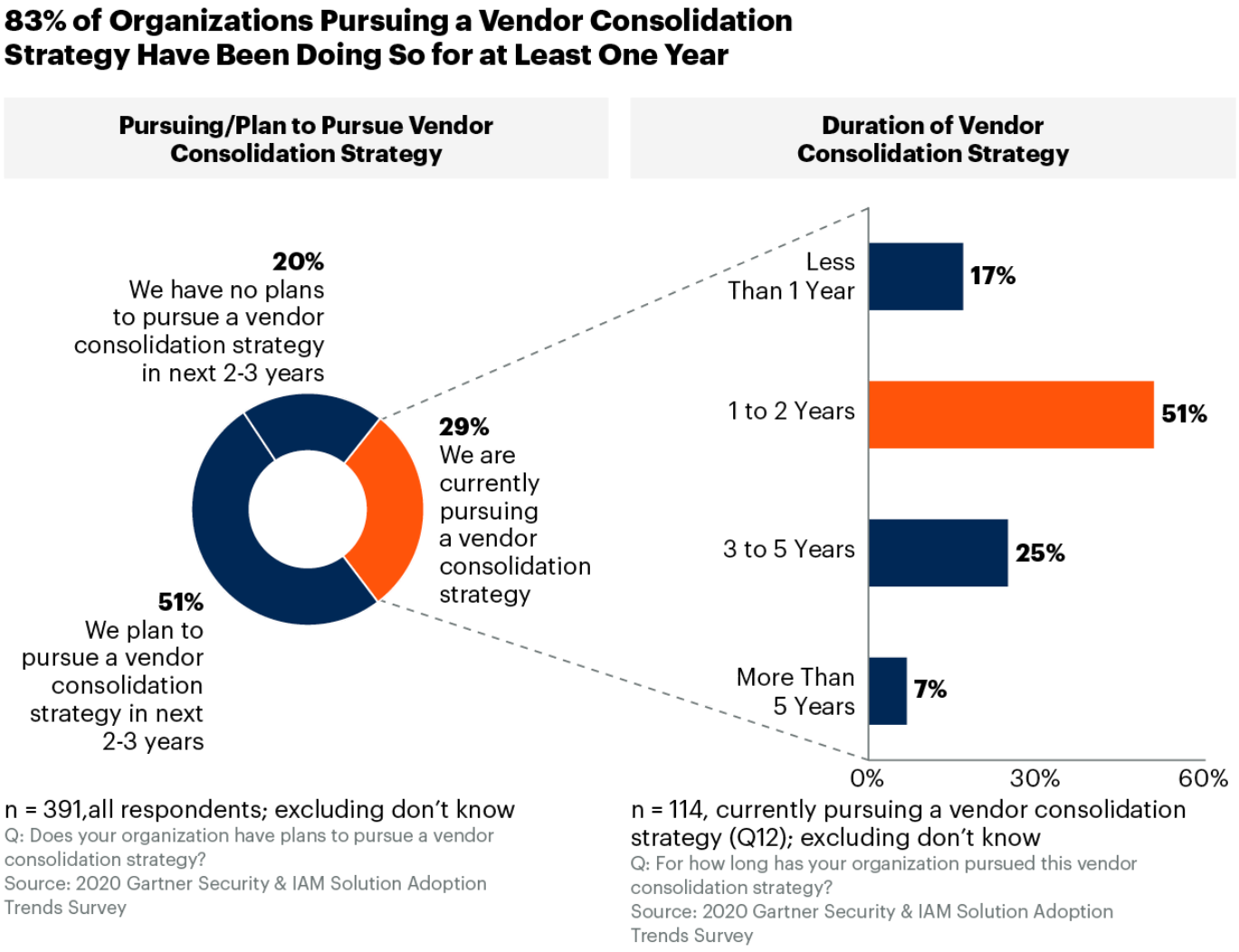
Trend No. 5: Security Vendor Consolidation

Analysis by John Watts, Peter Firstbrook

Description:

The large number of security products used by organizations drives up complexity and integration costs. This increases the complexity of security operations and results in a need to increase headcount. Organizations want vendor consolidation to simplify operations and reduce overall costs (see Figure 6).

Figure 6. Vendor Consolidation Spans Multiple Years



Why Trending:

In its 2020 CISO Effectiveness Survey, Gartner found that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio, with 12% of CISOs having 46 or more tools.

Organizations are now adopting enterprise license agreements (ELAs) with large security vendors offering a platform of products that are often integrated and managed through extended detection and response (XDR) product offerings.

Vendor consolidation can help to simplify operations and reduce overall costs. It can help with areas of concern, such as increasing regulatory requirements, as fewer larger vendors typically keep up with regulations more readily than point products.

Security products and vendors tend to follow business technology changes a few years after introduction as the new business technology practice takes hold and becomes mainstream. Rarely does security lead business enablement; rather, security is typically playing catch-up to secure what the business is doing after the fact. It is helpful to keep in mind that vendor consolidation and best-of-breed sentiments tend to ebb and flow over time in IT.

Implications:

Security vendor consolidation is challenging. In the survey, we found that 85% of organizations currently pursuing a vendor consolidation strategy had not reduced their vendor count in the previous year.

Security vendor consolidation alone does not necessarily reduce hard dollar costs. Acquiring new, more comprehensive platform solutions can lead to increased costs when organizations purchase more products than they are able to deploy, or when they have overlapping products with existing vendors which may not be fully replaced. However, the overall TCO may often decline as a result of preintegrated infrastructure components, reduced maintenance costs and fewer staff requirements for vendor-specific engineering skills.

Consolidating into fewer vendors can streamline operations and reduce complexity when compared to a best-of-breed approach. SRM leaders often seek upgrades to “best-of-breed” cybersecurity tools instead of maximizing the potential of existing tools, not realizing that tool improvement would be a more cost-optimal approach to improving security vendor portfolio effectiveness.

For those choosing a best-of-breed strategy, some risks include procurement roadblocks to onboarding new vendors, overhead required to manage vendor relationships, lower overall discounting, poor integration with solutions, and acquisition, solvency or partnership dissolution risks for those smaller vendors.

The vendor consolidation approach still carries risk, too. Vendor consolidation risks include vendor lock-in, overlapping software terms, forced legacy product retirements when acquisitions occur, lack of product integration and limited threat intelligence. In fact, some vendors may not provide “good enough” capabilities for some products that are well deserving of a “best-of-breed” approach. Both approaches in this case require good due diligence.

Actions:

IT leaders responsible for security and risk management should:

- Plan for a multiyear transition, as these strategies typically take two years or more to execute and realize the benefits.

- Plan for vendor consolidation by evaluating the internal and external factors that drive the need for vendor consolidation or best-of-breed vendor product strategies.
- Establish metrics to measure the expected business value of vendor consolidation, including measures such as simplified operations, reduction of total cost of security or improved risk posture.
- Collaborate with the CIO and CISO to agree on a vendor consolidation strategy. Work with other stakeholders, such as procurement and enterprise architecture teams, to formulate and plan for a realistic roadmap for transition.
- Provide security practitioners with new training and support as they migrate vendor products in order to fully deploy and utilize the new products that are introduced and fully retire products that are no longer needed.

Security Technology Evolution

Trend No. 6: Privacy-Enhancing Computation

Analysis by Bart Willemsen

Description:

Privacy-enhancing computation (PEC)involves emerging technologies that protect data while it is being used to enable secure data processing, sharing, cross-border transfers and analytics even in untrusted environments.

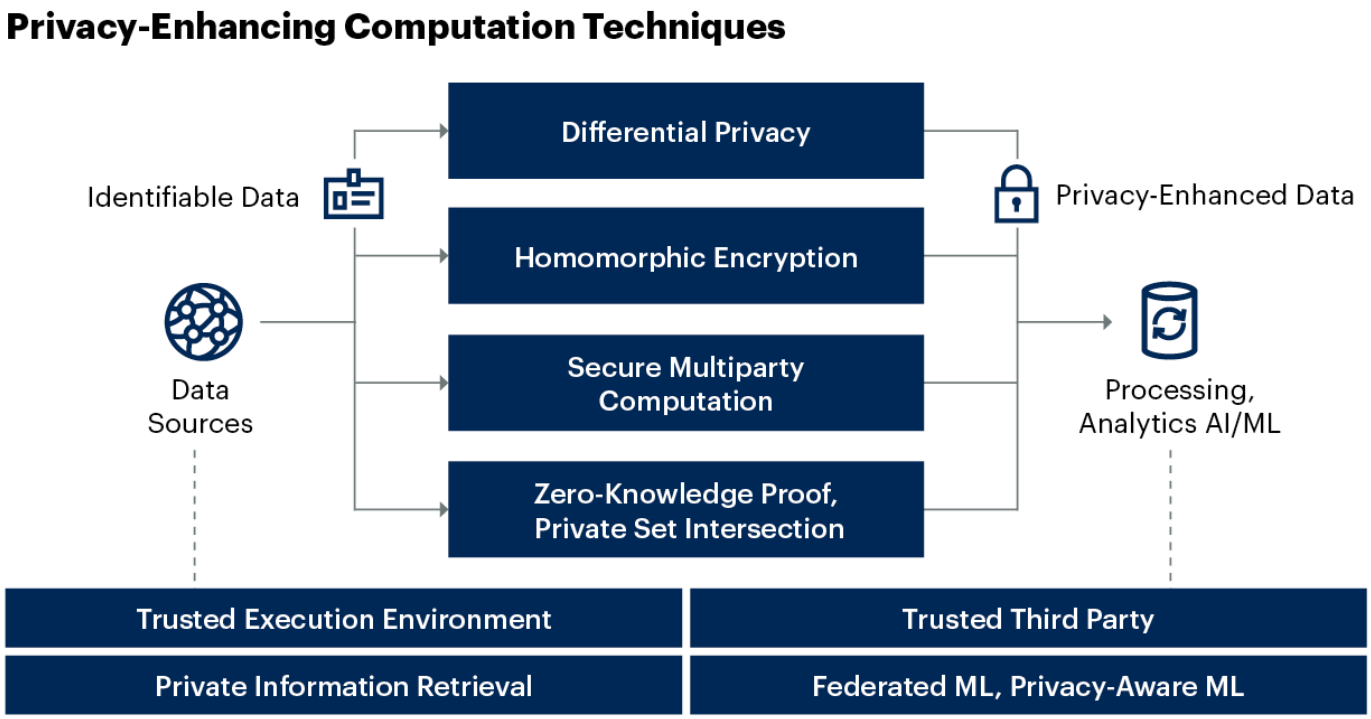
There are various individual privacy-enhancing computation techniques, but they can generally be applied on three different levels (see Figure 7):

1. **Data level** — Includes transformations to hide individual data values, such as homomorphic encryption or synthetic data, and on-the-fly controls like differential privacy.

2. **Software** — Software systems that combine data transformation with specialized software, such as secure multiparty computing (SMPC).

3. **Hardware** — Trusted execution environments and secure hardware systems, which implement security mechanisms in hardware.

Figure 7. Overview of PEC Techniques



Why Trending:

Global privacy and data protection legislation continues to expand, imparting various restrictions on the use of personal data. This will complicate multiparty sharing, data processing and analytics in untrusted environments. Historically, data protection while at rest or in motion has been solved; however, in-use data protection has been difficult or impossible. Multiple privacy-enhancing computation techniques are now becoming more viable in order to maintain confidentiality and protect privacy for data-in-use processes.

Implications:

The adoption of individual types of PEC techniques is nascent, but combined implementations are on the rise in use cases like fraud analysis, intelligence operations, data sharing, finance (e.g., anti-money-laundering [AML]) and healthcare.

Cloud providers have started to offer trusted execution environments (e.g., “confidential computing”). Other technologies, such as homomorphic encryption (HE), SMPC and private information retrieval (PIR), have transitioned from academic research projects to viable and influential commercial solutions.

PEC techniques aid, enable and allow cross-border data transfers, data sharing across multiple contributing entities without access to each other's underlying data, AI model training, and analytics and business intelligence (ABI) without touching regulated personal data.

Actions:

IT leaders responsible for security and risk management should:

- Identify candidate use cases for PEC techniques by assessing data processing activities that require the use of sensitive or personal data for data monetization and ABI.
- Assess the differences in the effectiveness and implementation needs of differential privacy, homomorphic encryption, secure multiparty computation, trusted execution environments and other approaches for these use cases.
- Start budgeting to invest for longer periods of time in applicable PEC techniques and begin experimenting soon and often to ensure long-term readiness.

Trend No. 7: Breach and Attack Simulation

Analysis by Pete Shoard, Jeremy D'Hoinne

Description:

Breach and attack simulation (BAS) tools are emerging to provide continuous defensive posture assessments, challenging the limited visibility brought about by annual point assessments like penetration testing.

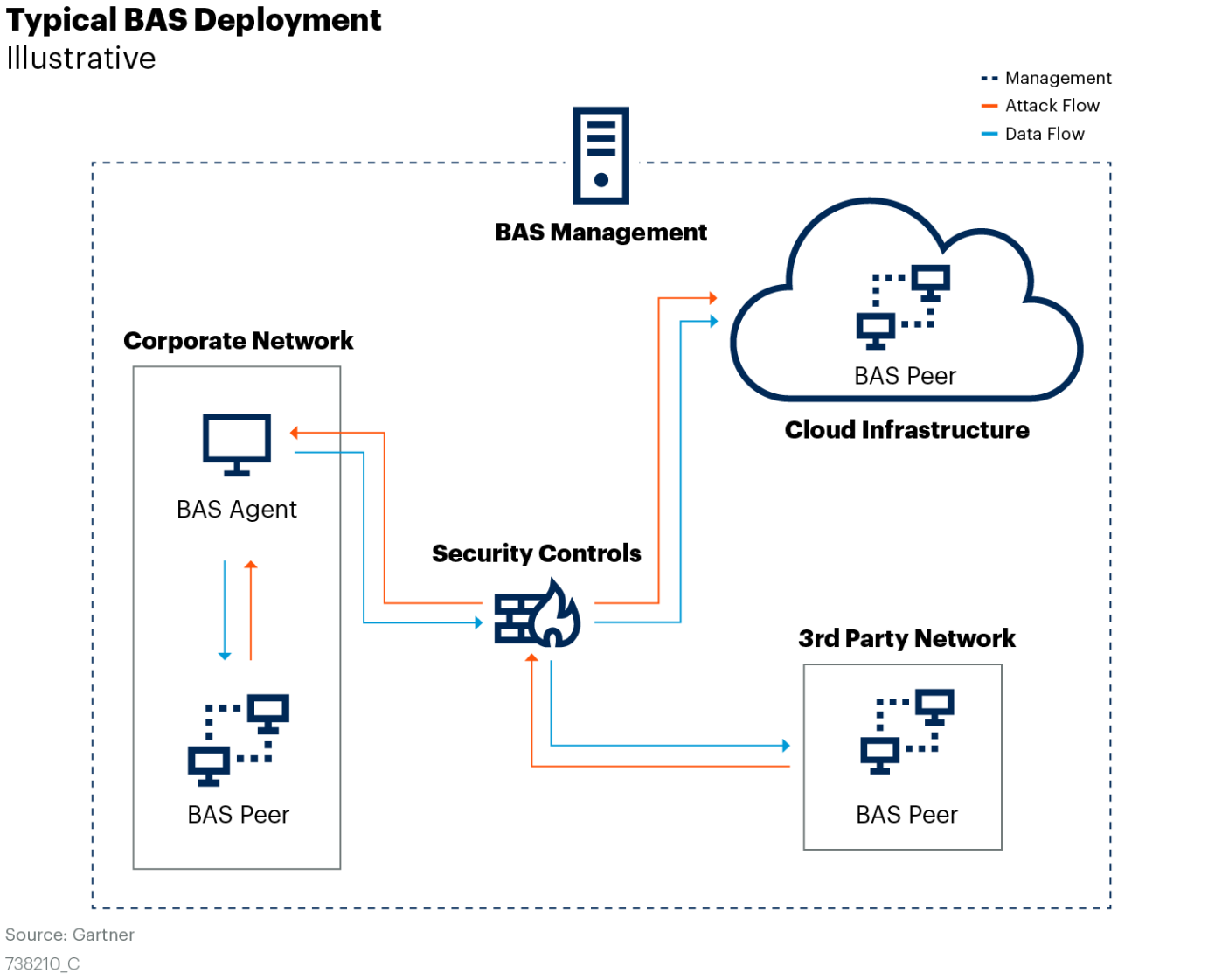
Why Trending:

Today, the importance of being adequately prepared for breaches grows with the constant evolutionary nature of costly cybersecurity attacks. Furthermore, the complexity of the modern security defensive posture is increasing with each new product. SRM leaders are looking for an easy, repeatable way to test the effectiveness of their defensive systems against attackers' tools in order to gain confidence that they have the right defenses in place and that they are correctly configured. BAS tools offer continuous testing and validation of security controls, utilizing a range of automated tools that simulate attack techniques and common attack types, such as those in the Mitre framework. This enables regular situational awareness that helps proactively identify and resolve gaps in security postures.

BAS testing can be aligned with the deployment of and upgrades to key systems, bespoke applications or new infrastructure to increase confidence in security controls and architecture. A typical BAS deployment is illustrated in Figure 8.

While attack simulations primarily test the organization's security posture against external threats, more specialized assessments might include an "attack path view," highlighting the risks to high value assets, such as confidential data. BAS equally provides training to help both defensive and offensive security teams to mature.

Figure 8. Typical BAS Deployment



Source: Gartner
738210_C

Implications:

When CISOs include BAS as a part of their regular security assessments, they can help their teams identify gaps in their security posture more effectively and prioritize security initiatives more efficiently.

BAS tools' ability to provide automatic testing for existing security controls immediately helps identify issues with the efficacy of security controls, configuration issues and detection capability. The ability to run this kind of assessment with only a few hours between the initial decision and the results enables better security assessments in near real-time.

BAS can speed up the assessment of new applications and critical infrastructure using attack techniques that are likely to be used in the real world.

BAS tools are still evolving and maturing, and are best aligned to the needs of experienced security teams. However, the power of continuous and repeatable testing can provide for a higher level of confidence in the defensive posture of the organization, and can be beneficial in developing security maturity. BAS should be used alongside other methods of managing security exposure, such as vulnerability scanning and prioritization, penetration testing and bug bounties.

Actions:

IT leaders responsible for security and risk management should:

- Use BAS to test the efficacy of security controls and help prioritize future investments.
- Use BAS tools to find likely attacker paths through the organization to highly sensitive assets.
- Improve the maturity of defenders by using BAS tools to test the effectiveness of current detection capabilities and incident response playbooks.
- Test new and prospective security controls using BAS tools.

Trend No. 8: Managing Machine Identities

Analysis by David Mahdi; Erik Wahlstrom

Description:

Managing machine identities (e.g., devices, workloads and their credentials) have become critical, as nonhuman entities are now at the leading edge of digital transformation. An enterprisewide machine identity management strategy is needed.

Why Trending:

As digital business continues to grow across all industries, so does the need for security and trust in digital identities. Machines and workloads are being leveraged at an increased rate due to the growth of digital business and trends towards digital transformation. Machine ID management aims to establish and manage trust in the identity of a machine interacting with other entities, such as devices, applications, cloud services or gateways.

Technology providers are starting to build tools that help clients manage machine identities across hybrid and multicloud environments. These providers now offer tools that scale and operate with modern cloud environments.

An enterprisewide machine identity management strategy is now imperative.

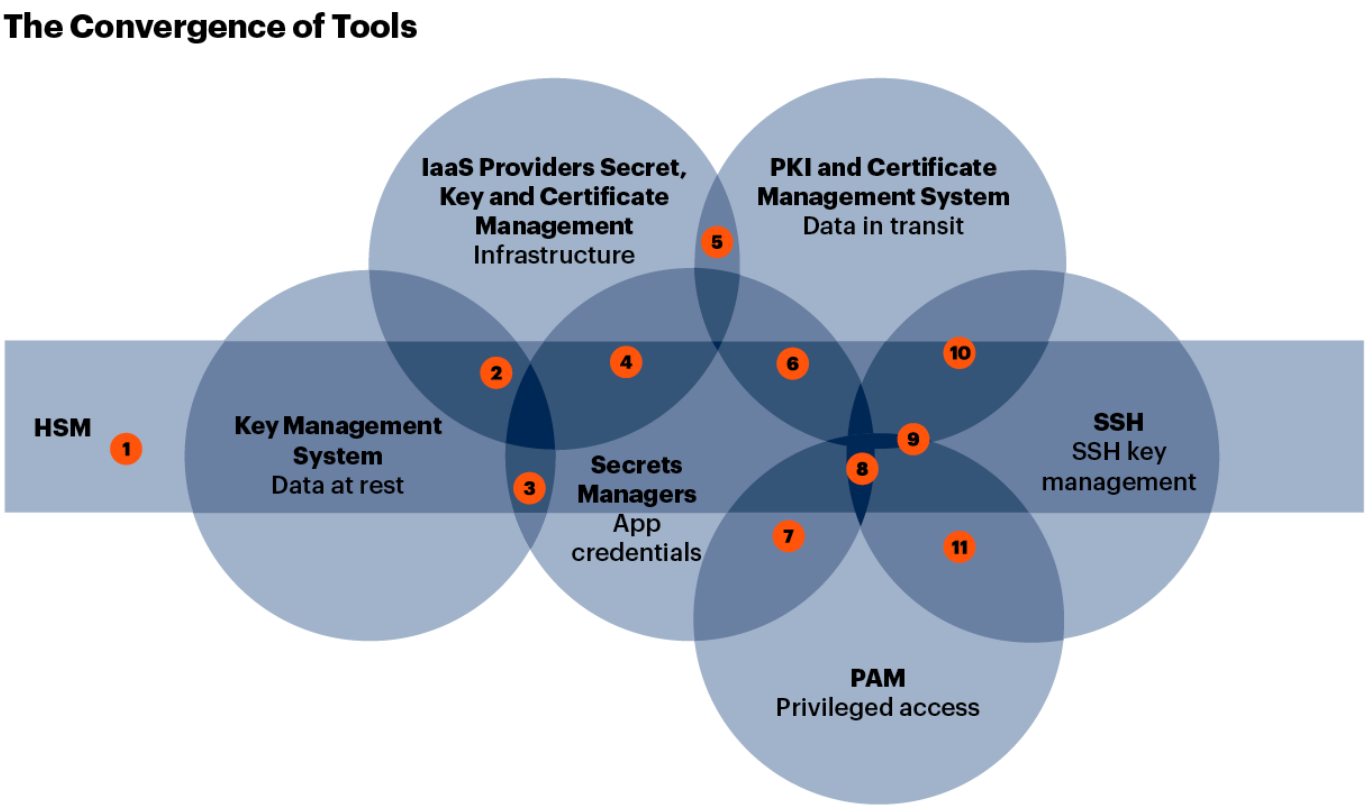
Machine ID management approaches handle the discovery and life cycle management of the credentials used by machines. This can include leveraging secrets, keys, X.509 certificates and other cryptographic materials that are used to strongly identify and authenticate nonhuman entities, such as containers, virtual machines, RPA/Bots and other SaaS and IaaS workloads.

Implications:

For clients, the notion of Machine ID management is still new. Machine ID management currently spans several technical areas (markets and vendors), and many clients are getting some benefit from already existing products, though only in limited fashion.

Figure 9 illustrates the convergence of tools within machine ID management.

Figure 9: Technologies That Converge on Machine Identities



Source: Gartner

Note: PAM offerings such as CyberArk, BeyondTrust, Thycotic providing DevOps tools and interfaces for DevOps toolchains to their Vault.

723409_C

Some forward-leaning organizations that have deployed early products in this space are saving time, avoiding outages and increasing their security posture. Integrations and single-pane-of-glass functionality are becoming more important evaluation criteria than previously expected.

Vendors in this space are now realizing that they need to acquire, build or partner with ancillary vendors in order to provide more holistic solutions in the machine ID space. The result here will likely be that vendors will conduct M&A in order to remain competitive and capitalize on this newly forming market.

The number of machines is growing at an increasing rate; this next decade will see more disruption and new entrants in various areas of business that capitalize on using bots and other kinds of machines. In order to offer higher value transactions and operations, security and identity must be built in at the foundation. Machine ID management offers the ability to create a strong foundation in order to capitalize on automation and overall digital transformation.

Actions:

IT leaders responsible for security and risk management should:

- Establish how ownership and machine credentials are (or will be) managed in their organization.
- Use the technology convergence diagram in Figure 9 to map the organization's current and short-term machine ID management use cases against currently available capabilities for assessment.
- Incorporate regulatory requirements into machine ID use cases and prepare for different teams' needs and the regulations that the organization has to meet after adopting machine ID management.

Evidence

Gartner's 2020 Security and IAM Solution Adoption Trend Survey: This study was conducted to learn which security solutions organizations are benefiting from and what factors affect their choice/preference for such solutions. The research was conducted online during March and April 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific region. Companies from different industries were screened for having annual revenue less than $500 million. Respondents were required to be at manager level or above (excluding the C-suite) and to have a primary involvement and responsibility in risk management roles for their organization.

The study was developed collaboratively by Gartner analysts and the Primary Research Team that follows security and risk management.

2020 Gartner Board of Directors Survey: A Gartner study to understand how boards of directors view the impact of technology on their enterprises. The primary research was conducted online during July and August 2020 among 133 respondents at midsize, large or global enterprises in the U.S., EMEA and APAC. Respondents were required to serve on a board of directors. If they serve on multiple boards, respondents answered for the largest company, defined by its annual revenue, for which they are a board member.

Remote work rates before, during and after the COVID-19 pandemic: In June 2020, Gartner surveyed over 4,000 employees across regions and industries to identify the current impact of COVID-19 on remote work behaviors and the long-term impact of COVID-19 on remote work preferences.

Gartner's 2020 CISO Effectiveness Survey: This study was conducted to identify the beliefs and behaviors of leaders who effectively deliver against key security outcomes. The research was conducted online during January 2020 among 129 heads of information risk functions globally across industries, geographies and revenue bands.

Document Revision History

Top Security and Risk Management Trends - 27 February 2020

Top Security and Risk Management Trends - 31 January 2019

Top Security and Risk Management Trends - 26 April 2018

Recommended by the Authors

Designing Security for Remote-Work-First Enterprises

Top Tips for Communicating Security and Risk to Business Stakeholders

CISO Effectiveness: A Report on the Behaviors and Mindsets That Impact CISO Effectiveness

Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?

Cost-Optimizing the Cybersecurity Vendor Portfolio

Securing the Enterprise's New Perimeters

Achieving Data Security Through Privacy-Enhanced Computation Techniques

IAM Leaders' Guide to Access Management

Managing Machine Identities, Secrets, Keys and Certificates

Utilizing Breach and Attack Simulation Tools to Test and Improve Security

Learn more.
Dig deep.
Stay ahead.

Follow these best practices to create a resilient, scalable and agile cybersecurity strategy.

The IT Roadmap for Cybersecurity

About Gartner

Gartner, Inc. is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow. Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Gartner®