Emerging Tech Impact Radar: Security 2 **AI-Based Security Operations**

Published 16 November 2022 - ID G00766277 - 101 min read (By Elizabeth Kim, Swati Rakheja)

Analysis by: Dave Messett and Nat Smith

Description: "Artificial intelligence" is a term covering everything from supervised learning, unsupervised learning, natural language understanding and deep neural networks to augmented intelligence. Creating actionable and trustworthy insights from enormous volumes of data through AI is a field receiving an increasing level of investment. Many early breakthroughs with AI were related to detecting advanced threats via preexecution file analysis or postexecution behavioral profiling. But AI-based security operations will be leveraged for postdetection actions, including alert prioritization, augmented threat detection/hunting, playbook creation and the automation of specific incident response (IR) processes. All this will speed up and increase the efficacy of alert triage, enhance alert enrichment, enable better correlation of low level alerts and telemetry across multiple source systems and ultimately improve analyst accuracy and response times.

Attack prioritization is the classification and arrangement of alerts and incidents into a logical order of operation, where the most-high-risk incidents can be remediated first. Risk, in this context, can be assessed based on a combination of severity of attack, likelihood of true positive detection and potential impact to the business. These factors themselves are evaluated leveraging appropriate contextual information such as privileges of the user involved, criticality of the system impacted and sensitivity of the data stored. Attack prioritization can also identify incidents requiring more detailed, human

investigation, arranging ones that are likely to be more critical to the top of the list to ensure they are executed first.

AI-based detection speeds investigations by correlating and aggregating connected alerts. Core to augmented detection is alert enrichment — automatically identifying additional information that may be required for a forthcoming investigation process and acquiring, normalizing and graphing that data ahead of time. Playbook creation comes next, determining optimal procedures based on what has been successful in the past. AI identifies and either suggests, or in more trusted scenarios, executes the next steps in real time, thus saving the analyst the cycles needed to think through these stages. Whether approached individually or altogether combined, AI-based security operations increase the speed at which an analyst can gather the relevant inputs, conclude an investigation, identify and execute the required responses, and move on to the next task.

Sample Vendors: BluVector, Cybersec, Cyware, Exabeam, LogPoint, LogRhythm, Rapid7, Sangfor Technologies, ServiceNow, Siscale (Arcanna.ai) and Stellar Cyber

Range: 1 to 3 Years

The majority of AI use in security products continues to focus on detection. However, as vendors continue to look for new ways to differentiate, AI utilization within security operations will be widely adopted over the next one to three years. The technology has been and is expected to be further pioneered in products targeted at security operations buyers, especially buyers of SIEM, SOAR, NDR, XDR and EDR. This technology is not likely to evolve into its own market, so the range to maturity will inevitably take time both for development and integration by the security vendors and for widespread upgrades to be deployed. However, as more solutions become available leveraging these technologies, the desire to port this technology into other security products will stretch the applicability of using AI in security operations, just as AI in detection is broadly seen today.

Mass: High

Mass is high. The shortage of skilled security practitioners will continue to drive an increased appetite for automation within the security operations field, and AI will be strongly leveraged across a range of products to deliver enhanced security outcomes at greater speed. This will be witnessed across all industries and across companies of all sizes. The benefits will be most recognizable by larger, more sophisticated organizations that currently utilize detection and response technologies more broadly and by MSSPs on behalf of their downstream client bases. This is because these are the organizations most focused on proactive attack detection and therefore are the ones struggling with an inundation of alerts that currently need manually triaging and prioritizing. They are also the organizations that have security operations centers (SOCs) and therefore face the challenge of creating playbooks for their staff to work through under prespecified conditions. AI will reduce the manual workload across all these areas, freeing up skilled resources to focus on less repetitive and more critical activities. There will be impact in less mature organizations as well, however, with the evolution of AI increasing accessibility to proactive attack detection by ensuring these activities no longer demand a substantial workforce of highly skilled security analysts.

Recommended Actions:

- Unless you are planning to fully embrace AI-based security operations technology in its entirety, there is a natural progression from AI-based detection. Plan first for prioritization, then hunting and then playbook creation.
- Clearly establish the real-world benefits AI integration brings to your customers. It is not enough to simply communicate that you have AI-based operations — you must clearly link the technology to a unique and differentiated value.
- Ensure transparency of your AI to provide customer confidence that the AI is trustworthy, unbiased and auditable.

Recommended Reading:

- Emerging Technologies: Patterns in How Providers Position AI for Security Attack Detection

- How to Start and Scale Responsible AI for Business Value

Digital Ethics

Analysis by: Elizabeth Kim

Description: Digital ethics comprises the systems of values and moral principles for the conduct of electronic interactions among people, organizations and things. Key areas where digital ethics should be applied include social and mobile technologies, social interactions, cloud and security, data and analytics, autonomous technologies and freedom, AI/smart robotization and the value of work, and predictive algorithms and decision making.

Range: 1 to 3 Years

Digital ethics is 1 to 3 years away because digital ethics has moved beyond a mere concept to a practice that organizations are implementing. Over the past year, a growing number of organizations have declared their AI ethics principles, frameworks and guidelines, and some organizations already have digital ethics practices. Gartner predicts that, by 2024, 30% of major organizations will use a new "voice of society" metric to act on societal issues and assess the impact on their business performance. The voice of society will put more pressure on both governments and public/private organizations to use technology ethically.

New guidelines (such as the Ethical Framework for Artificial Intelligence In Colombia, a new AI regulation in the EU, and the U.S. FTC's Using Artificial Intelligence and Algorithms) and increased board-level attention will further drive the adoption of digital ethics. In addition, when more organizations understand that digital ethics strengthens the organization's positive influence and reputation among customers, employees, partners and society, they will try to adopt and communicate digital ethics practices more. It would be similar to how we observe the prevalence and importance placed by organizations on diversity, equity and inclusion (DEI) initiatives today.

Mass: High

The impact mass is high because digital ethics is a business practice discipline relevant to a multitude of (if not all) industries. It is applicable to practically all organizations and consumers using emerging technologies, so technology providers need to consider ethical impacts during product design and development for transparency and adherence to design principles. Additionally, the probability that unintended consequences will occur is high as the use of technology creates distance between morals and actions.

The impact of digital ethics to existing technology markets is low because it does not replace existing technologies. Digital ethics is a new concept, but there is still an implication to technology and service providers (TSPs). First, providers of emerging technologies such as IoT, 3D printing, cloud, mobile and AI should offer more guidance to customers. Second, there is opportunity for TSPs to help organizations develop new governance models and processes as well as the necessary technology to control new technologies.

Recommended Actions:

- Develop a repeatable practice to identify and assess digital ethics issues arising from adopting emerging technologies by leveraging Tool: Assess How You Are Doing With Your Digital Ethics.
- Define a digital ethics code of conduct that reflects the organization' s values related to the safety, privacy and commitment to transparency linked to product development and the services provided. Also create accountability with an obligation to report a violation without retaliation.

Hyperautomation in Security

Analysis by: Mark Wah

Description: Hyperautomation in security refers to the adoption of hyperautomation technologies to realize business benefits and outcomes such as improved security outcomes, profit margins, operational metrics, and offering

differentiated products and services. Security service providers have invested in hyperautomation technologies like process mining to identify common tasks to deliver a service and automate these processes strategically. Hyperautomation within MSSPs, MDR providers and NDR providers help differentiate the service by offering higher-value capabilities like proactive threat hunting, automated response playbook and IR. Several security service providers are able to leverage hyperautomation effectively to improve analyst-to-customer ratios and minimize manual tasks, hence improving margins.

There are many other areas in the broad security market where hyperautomation is applied. The examples highlighted here showcase unique outcomes that drive transformative results.

Sample Vendors: Apiiro, Aqua Security, Atos, Darktrace, Expel, IBM, Lightspin, Microsoft, Palo Alto Networks, ReliaQuest, Secureworks, ServiceNow, Splunk and Sysdig

Range: 1 to 3 Years

The range of hyperautomation in security is one to three years. This is because of traction in the security service market arising from, for example, MDR that provides competitive differentiators and ubiquitous application of AI capabilities within cloud security products such as CNAPPs and security service edge (SSE). The ROI for the MDR cohort was evident in the market share data for some of the top performers (see Market Share: Managed Security Services, Worldwide, 2021). For products within cloud security, hyperautomation technology applications accelerate time to market with differentiated capabilities.

Hyperautomation in security exists in multiple areas, ranging from products to services. There are many facets of hyperautomation implementation within security — from using AI products for attack detection in multiple security product categories (as described in Emerging Technologies: AI in Security Attack Detection) to workflow and response automation within SOAR. There are also many other hyperautomation technologies that can be leveraged to address security use cases

— from process or task mining to low-code application platforms (see Emerging Technologies and Trends Impact Radar: Hyperautomation for examples).

Mass: High

The overall mass is high because hyperautomation delivers the expected value in many industries with the right application. For service providers with mature security operations, hyperautomation is a low-hanging fruit to capitalize on. As product and service providers demonstrate the benefits of hyperautomation, the overall mass will increase further.

Hyperautomation is also being facilitated on platforms within XDR, where metrics like mean time to detection (MTTD) and mean time to response (MTTR) are optimized. The integration points, workflows, playbooks and other capabilities enable hyperautomation to achieve specific outcomes like an automated response to a validated threat. In some cases, traditional tasks of Tier 1 and Tier 2 SOC analysts are automated, providing opportunities to upskill SOC analysts and improve SOC metrics. Some hyperautomation technologies applied are SOAR, process mining, API integrations with security products and bots to enable these outcomes.

Cloud security products such as CNAPPs have relied on hyperautomation technologies to digest vast amounts of data stored on modern data platforms such as a graph database. Some vendors are able to apply graph data science to enable use cases such as attack path analysis and support cloud-native security operations use cases.

Recommended Actions:

- Focus hyperautomation efforts on labor-intensive or repeatable processes within security operations that will benefit MSSPs, MDR providers and large enterprises rather than complex operations that require human judgment.
- Assess the implementation cost and desired outcomes (such as expected labor hours saved over a period of time) compared to the investment cost before diving headfirst into hyperautomation implementations. This can be achieved by leveraging tools such as the Gartner Use-Case Prism (see Toolkit: Discover and

Prioritize Your Best AI Use Cases With a Gartner Prism and Beyond RPA: Build Your Hyperautomation Technology Portfolio)

- Develop key metrics such as operational metrics (MTTR, MTTD) and business metrics (profit margin) to help drive a successful hyperautomation implementation. Note that the metrics that drive the desired outcomes may not be directly related to the specific areas being automated.

Secure Access Service Edge

Description: Secure access service edge (SASE; pronounced "sassy") delivers multiple converged network and security capabilities, including software-defined WAN (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), firewall and zero trust network access (ZTNA). SASE is primarily delivered as a service and enables dynamic zero trust access based on the identity of the device or entity, combined with real-time context, and security and compliance policies.

SASE is a market developing from the convergence of five contributing security and network segments: SD-WAN, firewall, SWG, CASB and ZTNA. While retaining capabilities and use cases from the contributing segments, this market also has its own unique characteristics. The most transformative of these is the change from on-premises-based appliance products to cloud-based services. Several vendors offer completely converged solutions already, and other vendors offer intermediary steps, usually consolidating five products into two. Convergence of operation and convergence of management, cloud adoption and remote-first work are some of the main drivers for buyers moving to SASE. Capabilities continue to evolve; however, serving those capabilities from the cloud edge is fundamental to SASE. There are components of SASE that reside on-premises, and everything that can be served from cloud edge should be. Therefore, products with all SASE capabilities integrated into a single, on-premises appliance are not considered a SASE solution.

Sample Vendors: Broadcom, Cato Networks, Cisco, Cloudflare, Forcepoint, Fortinet, Juniper Networks, Netskope, Palo Alto Networks, Skyhigh Security, Versa Networks, VMware and Zscaler

Range: 1 to 3 Years

SASE architecture is one to three years away from early majority adoption. The 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey suggests that 16% of organizations surveyed already have SASE. An additional 25% of organizations intend to have SASE deployed by the end of 2022, and a further 27% believe SASE will be deployed by the end of 2023.[1]

Multiple SASE vendors have all five contributing elements within a single, converged offering. These vendors continue to mature, improve and expand functionality with viable offerings today. Other vendors converge parts of the SASE solution, such as SWG, CASB and ZTNA, into a stand-alone offering, such as SSE. This portion of SASE will integrate with another converged solution, such as SD-WAN and firewall (WAN edge), creating a two-vendor SASE solution. The presence and viability of two forms of SASE (single-vendor or two-vendor solutions) further demonstrates SASE' s traction in the market.

Mass: High

SASE mass is rated as high, based on forecast growth, the convergence of five security and network subsegments, and growing interest from Gartner clients. Changes to security product architecture and buyer preference are sizable, giving SASE a particularly large influence on the security market. The changes required for existing offerings in the contributing segments to evolve to a SASE product (cloud edge-based solution) are significant. Appliance-based products must transform to cloud-native services, not merely cloud-hosted virtual machines (VMs). Additionally, the cloud-native services also need multiple geographically relevant and highly available points of presence (POPs) on the cloud edge, which may require substantial investment or partnerships from vendors.

Recommended Actions:

- Create a flexible solution that allows buyers to start either with pieces of your offering or the entire SASE solution. Not all buyers are ready to replace their existing security and network elements, so a strong migration path will meet buyer needs and result in buyer preference.
- Invest in advanced SASE element capabilities. SASE' s rapid adoption from buyers has attracted many vendors, and minimal capabilities will soon be insufficient to attract buyers.
- Develop cloud-native components as scalable modules. Continued innovation and investment by other SASE vendors will require the agility and efficiency that can only be delivered from a cloud-native architecture to remain competitive.
- Build a network of distributed POPs through colocation facilities, service provider POPs or infrastructure as a service (IaaS) to reduce latency and improve performance for network security services.

Vendor-Delivered Service Wrappers

Description: Vendor-delivered service wrappers (VDSWs) are a result of a technology vendor creating the necessary managed service delivery aspects as an additional option to couple with the vendor' s product. VSDWs help reduce end users' adoption friction for security products, given the challenges in managing security talent required to operate the technology. MDR, managed endpoint detection and response (MEDR), managed vulnerability management (MVM) and managed data loss prevention (DLP) are examples of a growing number of services delivered by vendors on their own products.

Sample Vendors: Bitdefender (MEDR), CrowdStrike (MEDR), Cybereason (MEDR), Deloitte (managed XDR), HelpSystems (MDR, MVM, managed DLP), IBM Security Services (various IBM security products), Microsoft (managed XDR), Optiv (managed XDR), Palo Alto

Networks (MDR), Proofpoint (managed DLP), Rapid7 (MDR, MVM), Secureworks (managed XDR), SentinelOne (MEDR), Sophos (MEDR), VMware (MEDR) and WithSecure (MEDR)

Range: 1 to 3 Years

The VDSW trend is expected to reach an early majority in the next one to three years as technology buyers and customers continue to demand more outcome-based deliverables rather than specific product features and functionality.

The range of VDSW offerings can vary based on the underlying technology. They can be available as co-managed or outsourced for the outcomes intended by the product. Co-managed offerings require that the vendor and partner/customer share responsibility for technology operation and content development of covered assets where applicable. There are use cases where the vendor requires the partner/customer to provide integrations or change management support where applicable. For outsourced offerings, the vendor is responsible for end-to-end service delivery applicable to the provided technology, including platform administration, triage, remediation, standards compliance and reporting. MEDR is a good example that has gained market traction and is offered by many EDR vendors. The rise of some of these offerings within the broader MSS market highlights the demand for outsourced offerings (see Market Share: Managed Security Services, Worldwide, 2021). A few EDR vendors are evolving their offerings beyond EDR use cases and getting closer to an MDR offering.

VDSWs are offered direct to market, via partnerships with service providers, or both. VDSWs should not be confused with SaaS-delivered platforms or a one-time professional services engagement to deploy a product, both of which result in turning over responsibility to the end customer for ongoing administration.

The trend to early majority will take time as some segments, like MEDR and MDR, are well-established and consistently growing, with many existing and new technology vendors offering a VDSW. Meanwhile, other segments, like DLP, have only a few technology vendors offering a VDSW, and others yet are just beginning to realize the trend. Furthermore, when technology vendors opt for a direct-to-market approach, intensified competition and channel conflict with the partner community will result as technology

vendors and traditional managed service providers and MSSPs compete for these product-centric service add-on opportunities.

Mass: High

The mass of VDSWs is high due to the impact it will have on historical channel norms and demarcations between vendors and partners. On one end of the spectrum, vendors have historically created and sold technology to service providers via various channels, including direct to partner and by way of distributors. On the other end of the spectrum, buyers, who historically owned responsibility for delivering internal business outcomes and looked to providers for technology, are now looking to consolidate vendors and shift the responsibility for internal business outcomes to providers.

As evidenced by the cross-section of sample vendors above, VDSWs will cut across most security segments as technology vendors seek to standardize processes and efficiencies around their technology to standardize outcomes delivered by the technology. VDSWs will be highly impactful to the conventional channel partner ecosystem as vendors navigate the service delivery market and service providers realign portfolios to accommodate the shift in service delivery.

These evolved partnerships between vendor and service provider will allow service providers to accelerate time to market with new services, while reserving the option to move those services in-house in the future with those investments front-end-loaded by previous sales. Service providers will refocus internal resources on differentiating the end-service delivery to the customer from the original VDSW. For example, where a VDSW is more generalized than specific to an industry or use case, it will need to be bundled with a service provider' s tools and services to deliver the last mile of a more industry-specific service delivery outcome.

Recommended Actions:

- Achieve service delivery capabilities by implementing the applicable people, processes and technologies needed to provide a consistent service delivery experience or by acquiring an MSSP with capabilities aligned to your technology portfolio.

- Offer a white-label VDSW to channel partners as an optional add-on to lower the barrier for partner adoption and accelerate time to market.
- Integrate with customer tools and workflows like SIEM, SOAR, XDR, IT service management (ITSM), remote monitoring management (RMM) and operation automation platforms in addition to mechanisms. This will ensure you don't limit customer flexibility or conflict with other providers in the environment when delivering direct to market.
- Address channel conflicts from the service delivery perspective, including transitions between servicing partners when an end customer desires to change partners while retaining your technology.

Cloud-Locked Semiconductors

Analysis by: Bill Ray

Description: A semiconductor, such as a system-on-chip (SoC) or embedded processor, can be locked to use only a specific cloud service by design — routing all communication through a security circuit. This mechanism can be used to restrict communications to a specific cloud provider, such as Microsoft's Azure platform, providing a high level of security and protection from hacking.

Alternative systems are generally software-based, authenticating communications and commands based on an installed cryptographic key. Such systems remain vulnerable to a low-level attack that manages to rewrite the device firmware, replacing the keys or bypassing the authentication process. Locking the semiconductors to a specific cloud provides a measure of protection even if the endpoint operating system has been compromised in this way. A similar mechanism is used by cellular networks, which use a removable SIM with embedded credentials locked to a specific network operator — this security remains in place even if the software of the smartphone is completely compromised.

Having the hardware locked to a specific cloud passes responsibility for the security of communication to the cloud provider, simplifying product development for the IoT

developer. However, it does make it impossible for the developer to change cloud providers at a later stage, and redundancy resilience must be considered.

Sample Vendors: MediaTek, Microsoft, NXP and Qualcomm

Range: 3 to 6 Years

Several vendors, including MediaTek, NXP and Qualcomm, have products in this space. However, adoption has been slow, and the required ecosystem is taking time to build. Other cloud companies have focused their initial efforts on software solutions, further slowing mainstream adoption. Therefore, we don’ t expect to see adoption scale before 2025.

Customers still seem content being locked to a specific cloud provider. Azure is already a critical partner in many enterprises, so being locked in by hardware is considered a small price to pay for the additional security that Azure Sphere can provide. Being locked into a specific hardware vendor is more of a concern, so product launches from additional partners will be critical.

Limited availability of semiconductors has discouraged adoption by product developers, but that is changing, although more slowly than anticipated. This will encourage competing cloud providers to explore the possibility of providing comparable services. Amazon and Google both have software-based solutions offering similar capabilities, but we expect at least one of those companies to offer cloud-locked hardware within the next two years. This will drive greater adoption.

Mass: Medium

The ability to offload a significant proportion of the security to a cloud provider is undeniably attractive. We expect cloud-locked semiconductors to be used across a very wide range of applications, although they will continue to compete with software-based solutions, with the majority of cloud providers offering both alternatives to their customers. Software options, such as Amazon Web Services (AWS) IoT Device Defender and Google’ s Cloud IoT Core, provide comparable functionality but without the hardware integration that makes the security of Azure Sphere so robust. IoT sensors, activators and

gateways can be secured without the developer having to invest in the skills or equipment necessary to manage secure systems.

Cloud providers will clearly play an important, and increasing, role in the management of the security of IoT endpoints, across a wide range of industries and applications. Mobile operators, which have an equivalent system in the SIM chip, will also be competing to provide security services of this type.

Recommended Actions:

- Create a cost-benefit analysis by establishing how much Azure Sphere, or a similar system, could reduce the cost of development and comparing that to the cost of hosting applications on the Azure cloud.
- Model the long-term implications of cloud-locked semiconductors by establishing the circumstances under which you would wish to change cloud providers, and then estimating the probability of such circumstances arising.
- Work with your existing cloud provider(s) to understand when, or if, they may offer cloud-locked semiconductors.

Cloud-Native Application Protection Platforms

Analysis by: Mark Wah, Lawrence Pingree

Description: Cloud-native applications are being delivered at an incredible pace, with deployment multiple times a day becoming common among mature application development teams. This includes adoption of containers and Kubernetes where workloads can be deployed in hybrid or multicloud environments. The current set of capabilities to secure cloud-native services range from application security vendors' offerings to cloud security posture management (CSPM) and cloud workload protection platforms (CWPPs), along with hyperscalers' native security services.

A cloud-native application protection platform (CNAPP) is an integrated set of siloed capabilities to reduce friction between engineering and security and to protect the life

cycle of cloud-native applications. CNAPP capabilities include elements of CWPP and CSPM with a shift-left focus and integrations with the CI/CD pipeline to address security risks. This also includes scanning of open-source software (OSS), container images, infrastructure as code (IaC) and policy as code (PaC) elements. Kubernetes security posture management (KSPM) is an important capability to support the popular container orchestration platform.

Cloud-native workloads are usually ephemeral, and traditional stand-alone protection that requires agent deployment will be operationally challenging. CNAPP capabilities that can help enable rapid development by seamlessly integrating in the development process will be favored.

Sample Vendors: Aqua Security, IBM (Red Hat), Lacework, Lightspin, Orca Security, Palo Alto Networks, Rapid7, Snyk, Sysdig, Trend Micro and Wiz

Range: 3 to 6 Years

The range for CNAPP is three to six years as the capabilities to secure cloud workloads, from development to production, have advanced for most vendors with thriving startups aimed at addressing DevOps and engineering security challenges. The adoption of CNAPP depends on end-user cloud maturity levels (see Advance Through Public Cloud Adoption Maturity). Some have adopted CWPP capabilities to protect the IaaS footprint to meet an immediate need for security coverage. Several CNAPP vendors have enabled snapshot scanning to address runtime security use cases. There is a rise in shift-left capabilities among CNAPP vendors to address DevOps and engineering needs and provide much needed context to application security outcomes. This was achieved through native capabilities and acquisitions observed in late 2021 and early 2022.The IaaS footprint is likely due to "lift-and-shift" approaches that are not taking advantage of cloud-native capabilities. It is difficult for some enterprises with varying cloud maturity and adoption to rightsize and modernize their cloud workload. Some CWPPs adopted by end users have offered CNAPP capabilities, but the adoption of core capabilities depends on the end user's cloud maturity. End users have mostly led with cloud configuration capabilities

within CNAPP such as CSPM, given the agentless approach and quick time to value from the visibility perspective. Born-in-the-cloud enterprises and new cloud projects within enterprises can adopt CNAPP capabilities more easily, which will fuel growth.

Mass: High

The overall mass is high for CNAPP due to the alignment to customer segments across multiple industries. Born-in-the-cloud or cloud-first enterprises will benefit the most from CNAPP capabilities. CNAPP is also important to hybrid customers, and many vendors have extended their capabilities to address hybrid use cases. The CNAPP set of capabilities appeal to a broader set of user and buyer personas. This is also evident within two Hype Cycles where CNAPP is represented: Hype Cycle for Workload and Network Security, 2022 and Hype Cycle for Application Security, 2022. Hybrid enterprises that are investing for the longer term will view CNAPP as a desirable platform to accommodate a diversity of workloads and an enabler for cloud-native workloads. Security operations personas such as security analysts and IR analysts have leveraged CNAPP products in their workflow, given the rich data within these platforms. Many CNAPP vendors have enhanced these use cases recently to support security operations use cases. This aligns with the observations described in Emerging Technologies: Future of Cloud-Native Security Operations. As CNAPPs expand their capabilities and enable additional user and buyer personas, their importance will grow and support the broader vendor consolidation trend (see Predicts 2022: Consolidated Security Platforms Are the Future).

Recommended Actions:

- Align product portfolios toward CNAPP capabilities (see Innovation Insight for Cloud-Native Application Protection Platforms) with shift-left integrations within development to help meet both security and engineering requirements.
- Establish strategic and complementary partnerships if technology gaps are difficult to fill with current capabilities, and consider acquisitions if conditions are favorable.
- Enable capabilities that help customers bridge the gap to evolve from lift-and-shift workloads to cloud-native services securely.

Composable Security

Description: Composable security does not have a rigid technical standard or blueprint but instead leverages a variety of architectures and technologies. Composable security is about architecting security to align to new requirements coming from edge computing and digital business initiatives. It' s also about building and aligning different security controls and components of a security ecosystem as interoperable, modular and dynamic capabilities. A good ecosystem example is a cloud platform marketplace where users can select security functions or capabilities that are compatible on the platform to compose business applications with security functions to meet compliance or privacy requirements. The aim here is to better integrate with and offer native support for digital security approaches that involve a higher degree of integration and aid in enabling automation, orchestration to improve detection and remediation capabilities.

Range: 3 to 6 Years

The estimated distance to the early majority target is anticipated to be from three to six years. This is because the adoption of solutions that align to this architectural model is expanding fast. The rise of citizen developers and fusion teams will drive demand for composable security functions to enable rapid development of secure composable applications. So, while vendors will try to protect their turf by trying to remain as "proprietary" and siloed as long as they can, there is an increasing need for security solutions to become more dynamic, automatable and interconnected. What will prevent composable security from reaching early majority in a shorter-than-expected time frame has to do with low awareness within enterprises of this technology approach. However, the increasing impact of business transformation and composable business initiatives will drive the need for a composable security approach, which is expected to grow at a relatively fast speed.

This emerging technology will be driven by security vendors, product leaders and product managers looking to integrate security functionalities into their products in a more modular and open approach. Such an approach is particularly needed as security can be shared by different players in the supply chain ecosystem.

Mass: High

The impact to the market is high, with many (if not all) sectors involved. A good example is the continuing emergence of SASE solutions, an emerging technology that fairly closely mirrors a composable security approach. Here, a single platform incorporates a variety of networking and security functions, with an obvious significant impact to those broad markets.

This market evolution is likely to impact the market in two ways:

- Through a composable architecture, security features will increasingly be integrated into nonsecurity products, therefore having composable security supporting interoperability across security products and nonsecurity offerings. This will challenge the current status quo as provisioning security will increasingly shift to nonsecurity players (i.e., business application and public cloud providers). However, it will also provide opportunities for specialist security vendors to develop joint go-to-market initiatives and develop OEM commercial partnerships. Here, security providers have the ability to support hooks — in other words, a plug-in API — so that developers can plug into the control flow of the code they would be developing.
- Security solution offerings will evolve to become multiproduct functionally integrated microservices and delivered via SaaS-based APIs. A good example of this kind of evolution comes from AWS security services, where users can use modules, such as AWS CloudTrail, AWS Config, Amazon GuardDuty, Amazon Inspector and AWS Security Hub, to build/compose a security operations stack. Currently, composability is achieved focusing on proprietary solutions from large infrastructure security players. But over time, it is likely that composability will expand to an ecosystem of vendors. This may be the best way for smaller vendors to cope with the challenge brought about by large security portfolio vendors adopting composability. In other words, they could introduce modularity by linking up product capabilities, such as by joining open multivendor environments through APIs.

Recommended Actions:

- Plan to factor in the implementation of the interoperability and modularity required to support your clients' evolving requirements (see A Technical Guide to Composable Application Architecture).
- Develop modularity of controls through the implementation of concrete architectural frameworks such as API-first architecture or out-of-the-box integrations that enable integrations with heterogeneous environments.
- Achieve composability through different steps, starting with the publishing of APIs for automation and logging development, and progressing to the creation of an open multivendor ecosystem of cost-benefit capabilities.

Cyber-Physical System Security

Description: Cyber-physical system security (CPS-Sec) solutions enable organizations to securely manage increasingly interconnected environments — and related threats — to guarantee safety, availability, security, reliability, resilience and privacy. The need for a comprehensive and coordinated security approach will require organizations to deploy tools that cover the entire cyber-physical risk spectrum, across IT, OT, IoT, industrial IoT and physical environments. The objective of CPS-Sec is to secure engineered systems that orchestrate sensing, computation, control, networking and analytics that interact with the physical world (including humans). When secure, they enable safe, real-time, secure, reliable, resilient and adaptable performance.

Security TSPs focusing on asset-centric enterprises will be increasingly required to develop an overarching product architecture strategy in order to be relevant across the cyber-physical dimension. Product capabilities in demand will range across the spectrum of an adaptive security model, from preventive-centric tools (such as network firewalling and endpoint security tools) to detection mechanisms (such as system monitoring and inventorying) and predictive solutions (like threat intelligence).

Emerging CPS-Sec use cases where controls apply across IT, IoT, OT and physical environments include:

- Real-time visibility and asset discovery offering overarching inventorying and remediation features across IT, IoT and OT environments
- MDR and IR services
- Vulnerability assessment and penetration testing
- Threat intelligence

Sample Vendors: Armis, Barracuda, BlackRidge, Booz Allen Hamilton, Cisco, Claroty, Cybelius, Dragos, Elbit Systems (Cyberbit), FireMon (Cyber Asset Manager), Forescout (CyberMDX), Forta (Tripwire), Fortinet, Hexagon (PAS), LOCH, Nozomi Networks, Ordr, OTORIO, Palo Alto Networks, Radiflow, Sasa Software, SCADAfence, Sepio Systems, Tenable and Verve Group

Range: 3 to 6 Years

CPS-Sec technology is three to six years away from the early majority target as a result of its having reached 20% to 60% of the installed base of customers. The rationale behind this rating assumes that the pressure to review the security strategy in the majority of enterprises has been proceeding at a steady pace following the:

- Convergence of IT, OT, IoT and physical systems
- Increasing focus of threat actors toward the exploitation of new and old vulnerabilities across legacy infrastructures and "greenfield" deployments

This is contrasted by the lack of regulation and penalties overall, but on the heels of the Oldsmar water utility, Colonial Pipeline and JBS attacks, this is likely to change.

What's new with CPS-Sec compared with previous years is the shift to an asset-centric security discipline as opposed to information/data security or network-centric security. In other words, putting the CPS at the center, starting with asset

discovery, and wrapping other security features around it, all done on a platform equals a CPS protection platform.

Security and risk management (SRM) leaders operating in CPS-rich industry sectors (such as oil and gas, manufacturing, mining, energy and utilities, and healthcare) are expanding their security approach and activities beyond the traditional area of information security. This is being driven by awareness of business exposure to new risks arising from digital transformation initiatives, along with the growth of targeted attacks by ransomware gangs and nation-state-sponsored actors.

Mass: Medium

Gartner estimates the overall mass impact on products and markets for CPS-Sec to be medium. The specific volume of mass is high due to the varied adoption by vertical industries of CPS infrastructure and their vertical-specific use cases. But the density, which translates into the level of advancement pushing existing product capabilities forward, is medium. This comes as a result of the use of CPS-Sec capabilities advancing quickly, with their impact being felt by more than one industry or job role. Overall adoption is driven by new threats faced with newly integrated physical systems and a limited set of security technology controls that can be implemented on CPS endpoints.

Providers of traditional security tools will have to expand capabilities to remain relevant to enterprises facing threats from the cyber-physical dimension.

Recommended Actions:

- Develop and demonstrate security features that, while helping mitigate threats, preserve OT safety and reliability, such as operating on a passive mode to limit disruption.
- Align product capabilities to demonstrate relevance to specific industry-vertical requirements and architectures, as in healthcare and manufacturing, where there are very distinct priorities and concerns around safety and business support.

Decentralized Identity

Description: In current identity systems, users are not the owners of their identity and associated data; rather, these are controlled by a service provider, government or employer. The data is stored in centralized repositories that act as a honeypot for attackers, raising security and privacy challenges. Decentralized identity (DCI) or associated self-sovereign identity (SSI) systems aim to address these challenges with traditional identity systems. They use technologies such as blockchain or other distributed ledger technology (DLT) to decentralize an identity system and distribute it across a large number of nodes or participants. It offers a variety of cryptographically verifiable identities that rely on a decentralized and distributed identity trust fabric (ITF) instead of a centralized registration authority. DCI approaches are generally built with a user-centric approach, focused on allowing users to potentially gain more control over their identity and associated data. It offers users a reusable and portable identity that can be leveraged for multiple use cases across organizations. Data exchange between parties can be facilitated through verifiable claims exchange (VCE) protocols built using zero-knowledge proofs and zero-knowledge claims to avoid unnecessary exchange of personal information.

DCI implementation involves multiple technical and nontechnical components, including decentralization technology, identity wallet software, a trust framework, ITF and verifiable claims. It also requires the establishment of an ecosystem — that is, the end users and the organizations/systems that issue and accept these different credentials and claims.

Sample Vendors: 1Kosmos, IBM, ICONLOOP, Mastercard, Microsoft, NuID, Ping Identity, SecureKey, Sovrin Alliance and Workday

Range: 3 to 6 Years

The range is three to six years mostly due to the lack of interoperability and sufficient standards, disparate implementations of DCI sources, and the lack of a standard approach. There has been significant investment in the space with total

venture capital investment reaching $476 million from 2016 through 2021 and several governments exploring DCI/SSI-related wallet use cases. However, for the technology to move forward, there needs to be clear value establishment for users. Most DCI implementations are small scale with limited base of users, verifiers and issuers. In absence of critical mass for any of these participants, the adoption will not kick off due to lack of ecosystem. Currently, there are no large-scale networks that are widely accepted. Most vendors today lack a clear strategy on how to build a differentiated user experience (a factor critical to gaining users on the network) and retaining the established users.

Mass: High

Gartner assesses the mass of DCI as high, given the broad-based interest by a number of verticals, and the fact that the problem space of digital identity breach exists across most verticals. The technology addresses the privacy and security challenges for both individuals and enterprises. DCI supports privacy-centric approaches by offering users more control over their identity and associated data. Thus, once large-scale DCI networks are established, it will make the need to establish a new identity for each digital interaction redundant, impacting current IAM and service provider models. And by moving away from centralized identity repositories, enterprises can abstract themselves from the associated challenges, including reduction of identity validation costs, associated data storage and maintenance cost, and compliance and regulatory pressure. The government and banking verticals have the strongest general interest in the wider DLT landscape.

Recommended Actions:

- Ensure compatibility with existing standards while keeping a note of any changes and evolutions in current standards.
- Explore participation in public-sector opportunities such as large-scale pilots in the EU.

Digital Risk Protection Services

Description: The digital risk protection service (DRPS) market is composed of TSPs offering solutions developed to protect critical digital assets and data exposed to external threats. These solutions provide visibility into clear (surface) web, deep web and dark web sources to identify potential threats to critical assets and provide contextual information on threat actors and the tactics and processes utilized to conduct malicious activity. DRPS provides support in four areas — mapping, monitoring, mitigating and managing the impact on critical digital assets — that ensure business operations are preserved.

Sample Vendors: Bfore.Ai, BlueVoyant, Bolster, CloudSEK, CTM360, CybelAngel, Cyberint, Cyber Intelligence House, CYFIRMA, Flashpoint, GroupSense, HelpSystems (PhishLabs), LookingGlass Cyber Solutions, Microsoft (RiskIQ), Rapid7 (IntSights), Recorded Future, ReliaQuest (Digital Shadows), SafeGuard Cyber, SOCRadar and ZeroFox

Range: 3 to 6 Years

The range is three to six years because, while there is recognition and interest for this technology, it is not considered crucial by many industries. However, the pace of investment growth in this technology and its transformational effect on buyers focused on heritage vulnerability assessment are fairly rapid. This is particularly influenced by the increasing need to have visibility into external-facing assets to help prioritize mitigation/remediation efforts and reduce exposure. The high level of merger and acquisition (M&A) activity impacting the market is a sign of the interest this capability is receiving. Among the most popular use cases for DRPS that we encounter are:

- Digital footprinting (such as mapping internal/external assets and identifying shadow IT)
- Account takeover protection (such as protection from credential theft)
- Fraud detection (such as phishing and credit card compromise)

- Brand protection, a service focusing on the discovery of malicious activities impacting brand reputation (such as cybersquatting of digital assets such as domains and impersonations of executives)
- Data leakage detection (such as IP protection)
- High-value targeting monitoring/executive protection
- Takedown services

The DRPS space is still emerging, with close to 75 vendors aligned to this market. Vendor capabilities vary and may be limited by a vendor' s ability to provide a comprehensive solution. Some vendors have a best-of-breed approach, where they are heavily focused on niche DRPS use cases; however, many are expanding to support more than one use case.

Mass: Medium

The impact of DRPS on existing products and markets is now medium. The shift from low to medium impact is justified by an acceleration in adding DRPS capabilities to existing products. This is due to an increased interest in protecting external-facing digital assets from cyberthreats. As DRPS overlaps with some complementary mainstream security offerings, such as threat intelligence, social media protection, endpoint protection platforms (EPPs), secure email gateways (SEGs) and MSS, DRPS functionalities are increasingly available as an extension of existing capabilities. Here, providers have been able to expand offerings by adding DRPS to their service catalogs as an integration to their core capabilities, as well as offering stand-alone DRPS. But large-enterprise needs will drive demand for comprehensive and closely integrated DRPS and threat intelligence capabilities and support consolidation of heritage threat intelligence and DRPS use cases.

New providers are expanding capabilities to cover the whole spectrum of digital risks, stretching to the cyber-physical layer and public cloud environments. This is

creating new opportunities and expanding the reach to new buying roles, such as chief marketing officers, chief privacy officers and chief information officers.

Recommended Actions:

- Focus your product positioning strategy by targeting separately reactive and proactive buyers with matching solutions. Offer targeted capabilities with the aim to expand into a solution set rather than an all-in-one bundle.
- Align to emerging security requirements by developing premium targeted services that will also help to improve the perceived value of the tools.
- Consider "build, buy, partner" to provide comprehensive DRPS and threat intelligence solutions with optional integrated threat intelligence platform (TIP) capabilities. This is where the market is heading.

Encrypted Traffic Analysis

Description: Encrypting traffic on the sending device is relatively inexpensive and all but ensures that no one who intercepts the traffic can read its content. While encryption can protect an organization's data and communications, it is also a good tool for bad actors to attack and infiltrate an organization. Unless an organization is able to decrypt the traffic, which may not be possible (or legal) in many cases, then an organization's inspection technology may not be able to detect the malicious activity. Additionally, even when decryption is possible, it is computationally expensive, leading to overloaded or significantly decreased performance. An embarrassing amount of traffic in organizations today goes uninspected simply because it is encrypted. This is not acceptable. Gartner inquiries show that 80% to 90% of network traffic crossing the edge is encrypted (see Securing the Enterprise's New Perimeters).

Encrypted traffic analysis can help. Without decrypting the traffic, the patterns of communication in the traffic can be used to fingerprint and identify malicious activity. Frameworks such as open-source JA3, which was first published on GitHub in 2017, are often the starting point. Encrypted traffic analysis measures characteristics of the traffic that are not obscured with decryption, from simple things like the source of the

communication, to more complicated analysis that recognizes patterns in the size and frequency of the packets in the traffic. These patterns become behavioral fingerprints of the encrypted communication, and they are compared to behavioral fingerprints of known malicious communications.

Sample Vendors: Arista Networks, Blue Hexagon, Cisco, Corelight, Darktrace, ExtraHop, IronNet, Juniper Networks, Sophos and Vectra

Range: 3 to 6 Years

The range is three to six years. Despite this technology becoming more popular with NDR vendors today, the results are not always reliable. It may require a few more years to improve the accuracy of detection before the technology appeals more broadly to other security markets. Several NDR vendors have been using these techniques for a couple of years and continue to improve the methods and fingerprint libraries. After some experimentation, most depart from JA3, retaining some of the methods and concepts, but using AI (usually ML) to improve the efficacy of their implementation. Some of these vendors believe it may be possible, in time, to remove the need for decryption at all. Beyond the improved visibility and detection this would enable, it would greatly simplify an organization' s obligation to comply with privacy regulations for employees and customers.

Mass: Medium

The mass is medium. Despite broad applicability, this technology is evolutionary: Not all detection products struggle with encrypted traffic. For example, most endpoint technologies examine communications or payloads only after they have been decrypted by the device. In addition, this technology is likely to remain a feature of other products.

Recommended Actions:

- Formalize a strategy to cope with detection in increasingly encrypted environments. Evaluate encryption metadata analysis to determine if this is a good fit for your solutions. Presume that all traffic will be encrypted in the near future.

- Research JA3 and JA3S to familiarize yourself with some concepts of Transport Layer Security (TLS) fingerprinting. As JA3 is an open-source project, there is a lot of research and commentary in the public domain on this.

External Attack Surface Management

Analysis by: Elizabeth Kim and Ruggero Contu

Description: External attack surface management (EASM) refers to an emerging set of capabilities that continuously discovers internet-facing enterprise assets (such as systems, web applications, IPs, domain names, SSL certificates and cloud services) and associated exposures. Examples include exposed servers, credentials, public cloud service misconfigurations, deep dark web disclosures and third-party partner software code vulnerabilities that could be exploited by adversaries. EASM has emerged to better manage the attack surface, which has grown more difficult due to the extended perimeter as organizations become more digital.

Sample Vendors: Bishop Fox, Censys, Coalfire, CrowdStrike (Reposify), CybelAngel, Cyberint, Cyberpion, CyCognito, Darktrace (Cybersprint), Detectify, Firecompass, IBM (Randori), LookingGlass, Microsoft (RiskIQ), NetSPI, Palo Alto Networks, Pentera, Recorded Future, Team Cymru and Tenable (Bit Discovery)

Range: 3 to 6 Years

The range is three to six years because end-user adoption is still relatively low. Gartner estimates adoption to be between 5% to 20% of the way to the early majority target. On the other hand, there is continued interest in EASM, with Gartner observing end-user EASM-related inquiries quadrupling in 2021 compared with 2020. The hype around EASM still outweighs the actual implementations of EASM. Awareness and understanding of the value of EASM are still fairly limited among security professionals. Not all organizations know why they need to understand what all their assets are or why they should put a budget behind the effort. On the other hand, more vendors, including service providers such as

MSSPs/MDR providers, are entering this space (natively or through acquisitions), creating a degree of more market hype. Gartner predicts that, as EASM is increasingly incorporated into other security products, the adoption of EASM bidirectional integrations will accelerate.

Mass: Medium

EASM has the potential to benefit organizations across multiple industries, but is a complementary technology. EASM use cases can range from asset management and exposure management to cloud security and governance, third-party risk assessment, and M&A due diligence. Organizations are tasked with managing a growing attack surface due to their technological environments becoming increasingly complex and dispersed, both on-premises and in the cloud. New technologies and business initiatives (such as SaaS applications), new ways to generate revenue, OT, IoT, CPS and supply chain touchpoints pose new threats. EASM can support organizations' initiative toward a more continuous threat and exposure management through continuously discovering known and unknown digital assets. Additionally, EASM performs analysis of asset exploitability for prioritizing mitigation/remediation of vulnerabilities and exposures (e.g., misconfigurations, open ports, data leakages and unpatched vulnerabilities).

EASM does not replace existing technologies but is highly complementary to many of them. EASM complements vulnerability assessment, threat intelligence, cloud security and security testing (such as breach and attack simulation, penetration testing as a service, and automated penetration testing and red teaming tools). Gartner predicts that, over the next three to five years, EASM will be incorporated into these markets. This is evidenced by the ongoing market consolidation and acquisitions of EASM vendors that is happening at a rapid pace. Recent examples include the following:

- IBM acquired Randori.
- Recorded Future acquired SecurityTrails.

- Team Cymru acquired Amplicy.
- Tenable acquired Bit Discovery.
- Microsoft acquired RiskIQ.
- Mandiant acquired Intrigue. Mandiant was subsequently acquired by Google.
- CrowdStrike acquired Reposify.

Security testing providers such as Bishop Fox, NetSPI and Pentera have natively expanded into EASM. CyCognito, Randori and Firecompass are examples of EASM vendors that support security testing.

Recommended Actions:

- Partner, build or buy adjacent technologies to better sustain market evolution toward a more comprehensive solution offering. Examples of adjacent technologies include vulnerability assessment, security testing, CAASM, security rating services, threat intelligence and digital risk protection services.
- Invest in educating the market by communicating how EASM complements an organization' s existing security stack and processes. EASM is net new spending for most organizations as it doesn' t replace any tools. Additionally, there is still a degree of market confusion among organizations on the distinction of EASM with other similar technologies.

*** Attention: research are originally in English and I have translated it into Chinese by Google Translate as instructed by Peter. In case of any discrepancy between the English version and the Chinese version, the English version shall prevail.*