Hype Cycle for Security Operations, 2021

Published 23 July 2021 - ID G00747546 - 82 min read

ARCHIVED This research is provided for historical perspective; portions may not reflect current conditions.

By Analyst(s): Pete Shoard, Shilpi Handa

Initiatives: Security Operations

Security operations technologies and services defend IT systems from attack by identifying threats and exposure to vulnerability — enabling effective response and remediation. The innovations included in this Hype Cycle aim to help security and risk management leaders strategize effectively.

Additional Perspectives

- Summary Translation: Hype Cycle for Security Operations, 2021 (13 October 2021)

Analysis

What You Need to Know

This document was revised on 06 April 2022. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The acceleration in digital transformation has, over the past 12 months, affected organizational relationships with IT. Increases in remote work, use of mobile devices and cloud services have been notable, and they have facilitated a significant change in the way businesses need to function. Changes have brought about a shift in the types of threats that organizations are subject to and there is an emerging need to increase visibility to previously unmonitored third-party systems and services. It remains true that a large part of setting a security strategy for an organization is simply understanding the available security capabilities in the marketplace and their potential applications, and aligning these with risk-based requirements. Security and risk management leaders are unable to prepare for every eventuality and, therefore, must make intelligent, business-driven decisions about which security operations technologies they choose to manage the risks to their organization.

Security operations is not simply a department, team or set of technologies. It is a group of well-executed processes performed by personnel aiming to protect the organization from harm. Security operations personnel require modern security technologies to quickly detect and mitigate threats and reduce exposure. It is not always easy to find the skill sets or know which solutions to implement first. Organizations must therefore look to a range of managed security services (MSS) and cloud-delivered security technologies. Outsourcing and “as a service” offerings can provide levels of competency that can quickly be grafted into the organizations’ own operations. For more security-mature organizations that have established a dedicated team and have invested in a portfolio of security controls, constant enhancement is required to ensure that they are equipped effectively to fight external adversaries.

Technologically, the security domain has continued to be siloed, with much focus being directed toward specific domains, such as network detection and response (NDR) and operational technology (OT) security. At the same time, capabilities such as breach and attack simulation (BAS) join domains together, providing visibility and verification of that visibility, as well as response planning and effective response testing (see Top Security and Risk Management Trends 2021). The key trend across all technologies in the security operations space is greater API interactivity and availability. This extends the requirement for a set of technologies and services that can join together the findings from multiple systems. Gartner refers to this as the “cybersecurity mesh architecture” (see Top Strategic Technology Trends for 2021: Cybersecurity Mesh). Although, as a product, a single multiecosystem security control plane has yet to materialize.

Security and risk management leaders focused on network security controls with a greater alignment to prevention should read the sister document to this Hype Cycle, Gartner’s Hype Cycle for Network Security, 2021.

The Hype Cycle

Architectural complexity in corporate infrastructure is widening as organizations try to navigate their way through traditional IT infrastructure deployments, cloud-based deployments and hybrid approaches. Security operations technologies are designed to meet the diverse needs of modern organizations across these architectural challenges — providing greater visibility of threats and exposures, greater control, and faster response capabilities that work universally and cohesively.

The desire for a single platform to consolidate security capability continues to be prevalent in the market (see Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?). Extended detection and response (XDR) partially meets this challenge; however, it does so within the limitations of a single ecosystem. Therefore is best suited to greenfield infrastructure projects rather than organizations with broad, existing security investments. Continued use of artificial intelligence (AI) and automation continues to create interest, but by themselves, these technologies are not going to solve the challenges faced by security operations teams. This need for efficiency in security can also be met through the augmentation of internal security processes with offerings from service providers. Whatever an organization chooses to focus its security strategy on, it is clear that well-defined, directional and business-specific security requirements are the key to the efficient and effective use of security budgeting and resourcing.

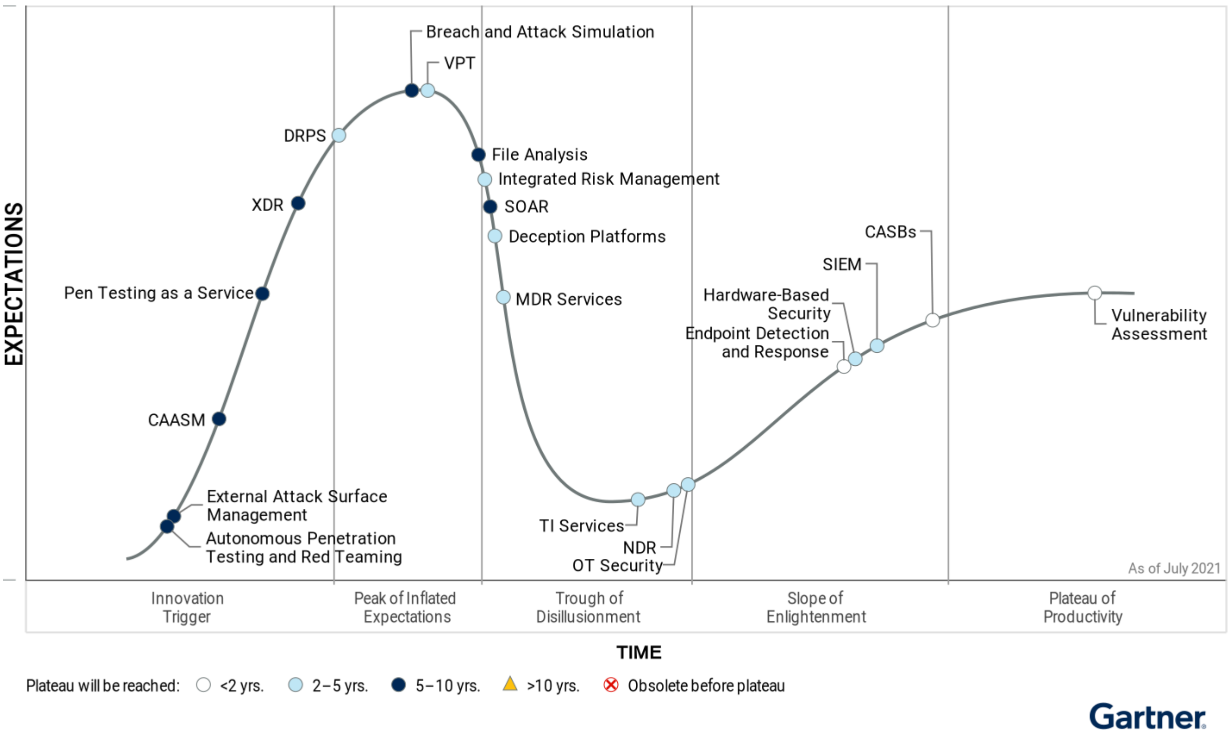
The demands of security are still heavily weighted in favor of effective processes and skilled individuals, with technologies becoming an enabler or efficiency-driver for an already effective SecOps team.

Organizations that have made significant investments in security tooling need to look to API integration to interact with new technologies. Decentralization has also become a significant theme. With cost closely linked to consumption, organizations can rarely afford to bring back all of their security data to a single location. Furthermore, with security capabilities frequently embedded in existing technologies, receiving an alert and asking a question of the sending system is becoming a logical and efficient way of managing the vast sums of data, and dealing with lesser understood scenarios.

Alongside greater adoption of cloud-based services and a focus on detection and response, a continuous assessment-and-exposure-based approach is emerging — with the majority of new entrants to the Hype Cycle featuring in this area. External attack surface management (EASM), autonomous security testing, and threat intelligence services all provide an inward-looking viewpoint toward an organization's infrastructure from the outside. This renewed approach to looking at exposure provides better enrichment for organizations to decide what really matters to them — without having to look at the threat landscape in a more general way and wonder if they are affected.

Turnkey and highly integrated solutions continue to trend upward. Smaller, less security-mature organizations are growing into new security operations requirements as they begin to become more dependent on connectivity and SaaS, and become dominated by compliance and regulatory requirements. Alongside turnkey requirements, consolidation is a key theme, with OT and IT security slowly converging. Differences in requirements are fading. Cloud access security brokers (CASB) are more frequently being associated with network security technologies such as zero trust network access (ZTNA) and SWG. Security and risk management leaders responsible for security operations should be looking to reduce overlapping capability across different technologies and become more risk-focused. This involves prioritizing issues that will genuinely impact their business, rather than those that receive media hype or simply sound bad.

Figure 1: Hype Cycle for Security Operations, 2021



Source: Gartner (July 2021)

Downloadable graphic: Hype Cycle for Security Operations, 2021

The Priority Matrix

Investments in technologies and services that align to security operations rarely provide immediate benefits. Such capabilities should be considered as consumable — that is, they require a process to fit into to become effective. Security risk should be managed in line with organizational priorities. Security operations must be designed to reduce risk and respond effectively to issues that may be damaging to productivity, the brand or both.

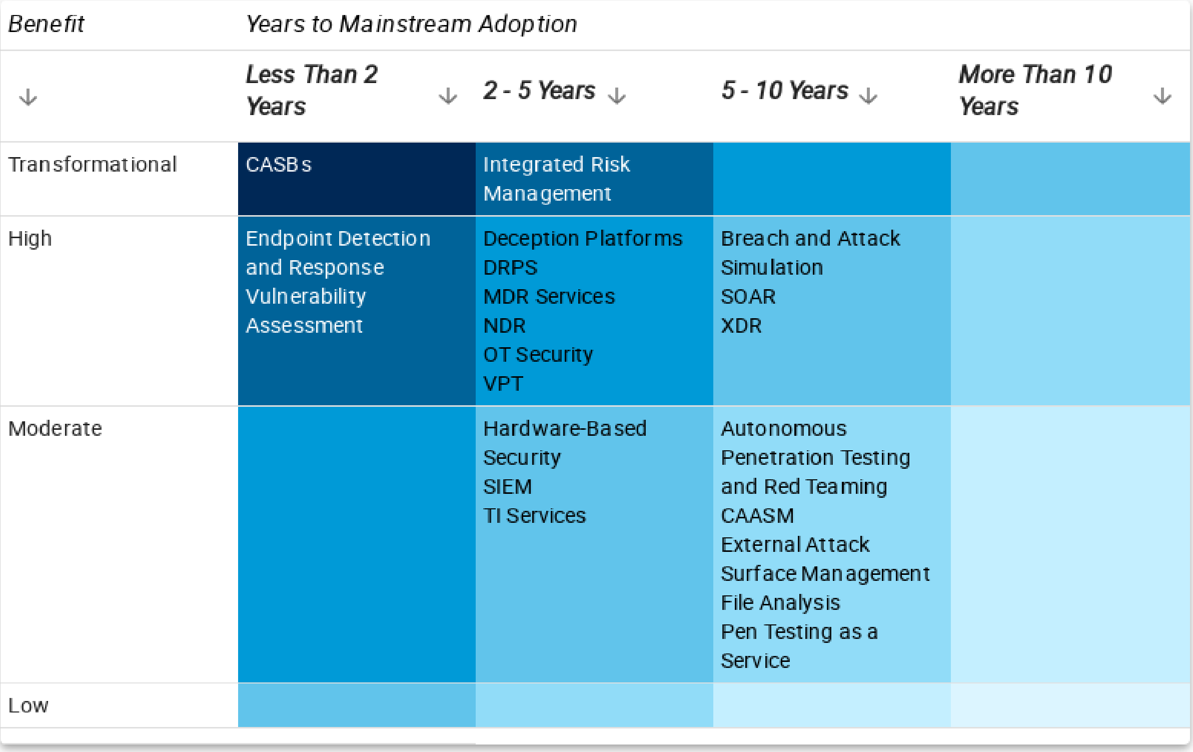
Organizations looking to invest in security operations services and capabilities should expect to have to regularly adjust their priorities to meet the changes in IT and the threat landscape. Continuing consolidation of security operations technologies has meant far more integration between different types of solutions. This integration is represented in the high benefits provided in areas such as security orchestration automation and response (SOAR) and XDR, but the adoption rates are reflective of the complexities in deployment and configuration. Some areas of security operations have seen wider diversification in more exposure-based technologies such as BAS, external attack surface management and penetration testing as a service (PTaaS). This has meant that organizations need more decision making data points to enable them to choose which threats or risks to tackle first. It is clear in almost every circumstance, security and risk management leaders must identify the outcome they require rather than the technology that they believe they require.

By focusing on risks, organizations can cut through the noise in security and provide transformational benefits. Organizations that can easily identify the event types that will impact their business in terms of brand damage or reduced operational capacity, stand a much greater chance of having an effective and measurable security operations capability. Furthermore, utilizing technologies that can consolidate information from an array of different SaaS providers in the market will offer visibility. This will only improve as more corporate functions migrate to these types of platforms and applications.

The idea of a truly automated security operations capability is unlikely to manifest itself on an end-to-end basis due to the pace of IT and the innovative nature of the adversary. However, developments in the security operations area continue to trend toward more consistent results derived from self-sustaining technologies that require less-skilled workers, and which can automate many of the more repeatable mundane tasks.

Table 1: Priority Matrix for Security Operations, 2021

(Enlarged table in Appendix)



Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	CASBs	Integrated Risk Management		
High	Endpoint Detection and Response Vulnerability Assessment	Deception Platforms DRPS MDR Services NDR OT Security VPT	Breach and Attack Simulation SOAR XDR	
Moderate		Hardware-Based Security SIEM TI Services	Autonomous Penetration Testing and Red Teaming CAASM External Attack Surface Management File Analysis Pen Testing as a Service	
Low				

Source: Gartner (July 2021)

Off the Hype Cycle

This year, Gartner has retired three profiles from the Hype Cycle for Security Operations:

- Network sandboxing has now evolved from a point-product to a feature of other products (such as a secure web gateway [SWG] or firewall) and has therefore passed the plateau as an individual technology.
- IoT security has changed focus to a development-centric approach and therefore no longer aligns with the aims and capabilities associated with security operations.
- Endpoint protection platforms (EPP) no longer address the nature of modern threats as it is no longer practical to focus on achieving 100% prevention and protection. Older EPP tools should be updated or replaced with ones that have endpoint detection and response (EDR) functionality.

On the Rise

Autonomous Penetration Testing and Red Teaming

Analysis By: Toby Bussa

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Penetration testing and red teaming activities have traditionally been heavily dependent on human testers and their toolkits of commercial and proprietary tools. A new market of solutions is emerging that can fully or semiautomate continuous or ad hoc network and infrastructure penetration test, and red team activities.

Why This Is Important

Security testing, like network penetration testing and red teaming, plays an important role in an organizations' capabilities to identify exposures, vulnerabilities and weaknesses in their defenses. Many organizations only test on an annual or ad hoc basis, rarely testing more frequently or even continuously in their environments due to the cost and lack of internal expertise.

Business Impact

- More frequent testing of infrastructure and the cybersecurity defenses of an organization helps find and mitigate weaknesses, gaps and operational deficiencies faster.
- More organizations can take advantage of penetration testing and red teaming capabilities without having to hire expensive experts when building an internal testing capability.
- Time to schedule and execute tests is shorter when an organization is not reliant on the schedule of a testing firm.

Drivers

- Vendors are adding more automation in their tools that can aid security operations teams

- Penetration testing tends to be an annual activity for many organizations due to the lack of budget and available resources, and to meet regulatory mandates or internal policy requirements

- Red teaming is still the purview of mature organizations that are prepared to benefit from these activities to validate and test the defenses and the "blue team." However, human-led red teaming requires a specific set of expertise, processes and tools that can be expensive to develop.

Obstacles

- As an emerging market, adoption is low and there is little feedback from buyers to validate the efficacy and value of these solutions.

- Acceptance of the test results from these solutions by auditors, assessors and third-party risk teams is still unknown. Organizations using automated testing solutions should confirm whether test results would be acceptable to applicable parties.

- Solutions still need people to operate them. This means managing the tools along with doing the work. This is done to determine scope, gather the necessary information (such as IP address ranges or excluded assets), configure the parameters of the test in the tool, and monitor the execution of the test until completion.

- Current tools cannot address all variations of penetration tests that buyers may require, especially those that require people to be on site, like wireless and physical intrusion tests.

User Recommendations

- Do POCs and other due diligence to confirm that the solutions being considered are fit for purpose and will meet the buyer's requirements. This is because the market is nascent and there is limited end-user experience with these tools.

- Confirm that the tools will be considered equivalent to the activities performed, and findings and results provided, by testing services providers. It is important in case you are planning to use these tools to address any audit or regulatory compliance requirements.

- Work with vendors in this space to help them refine and improve their solutions, and identify and prioritize new features and functionality, which benefit both parties.

Sample Vendors

FireCompass; Horizon3.ai; Pentera; Randori; Vonahi Security

Gartner Recommended Reading

How to Select a Penetration Testing Provider

Using Penetration Testing and Red Teams to Assess and Improve Security

External Attack Surface Management

Analysis By: Ruggero Contu, Mitchell Schneider, Elizabeth Kim

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

External attack surface management (EASM) refers to the processes, technology and managed services deployed to discover internet-facing enterprise assets and systems and associated vulnerabilities. Examples include servers, credentials, public cloud service misconfigurations and third-party partner software code vulnerabilities that could be exploited by adversaries.

Why This Is Important

While EASM provides similar capabilities with overlapping offerings such as DRPS, threat intelligence, third-party risk assessment and vulnerability assessment, vendor capabilities vary. Providers heavily focus on niche use cases and have been expanding globally.

EASM tools deliver five primary capabilities:

- **Monitoring** — Continuously scan the internet for domain-related environments (such as cloud services and external-facing on-premises infrastructures) and distributed ecosystems (such as IoT infrastructures).
- **Asset discovery** — Discover and map organization's external-facing assets and systems.

- **Analysis** — Evaluate and analyze asset attributes to determine if an asset is risky or vulnerable.
- **Prioritization** — Prioritize risks and vulnerabilities and provide alerts based on prioritization analytics.
- **Remediation** — Provide action plans on prioritized threat mitigation and the remediation workflow or integration with solutions such as ticketing systems and incident response tools.

EASM helps identify unknown assets and provides information about your systems, cloud services and applications that are available and visible in the public domain to an attacker/adversary.

Business Impact

EASM supports organizations in identifying risks from known and unknown internet-facing assets and systems. Security leaders can use EASM capabilities to understand and manage risks from their digital businesses, as it provides valuable context and actionable information from:

- Discovery of unknown digital assets (systems, IPs, domain names, SSL certificates, cloud services) across multiple environments (cloud, IT, IoT, OT). This visibility can also be extended to the organization's subsidiaries or third parties.
- Provide remediation/mitigation support of vulnerabilities and exposures (misconfigurations, open ports, data leakages, unpatched vulnerabilities) through prioritization of the assets, managed services and third-party integrations.

Drivers

- Digital business initiatives such as the shift to cloud infrastructure and platform services and SaaS, remote working, adoption of Internet of Things (IoT) technologies, and IT and OT convergence are some key areas where new security requirements are now emerging.
- Within these scenarios, EASM tools are being utilized.
- The tools help security professionals in understanding and reducing the unnecessary exposure to the internet and the public domain that could be exploited to prioritize the most critical exposures to be remediated.

Obstacles

- Security and risk management leaders should be aware that as EASM benefits from expanded visibility, there are tangible risks in the short to medium term M&A that will potentially impact investments made into startups in this space.

- To fully benefit from EASM solutions' capabilities, SRM leaders will be required to be able to leverage them in multiple areas (such as IT asset management, cloud management, vulnerability management, etc.), and not just security, with some degree of maturity and resources, such as dedicated or specialized personnel.

User Recommendations

- Review available EASM capabilities from providers of tools, such as DRPS or vulnerability assessment. You may have an existing commercial relationship in place, and their functionalities may be good enough.
- Review providers' capabilities as breadth of coverage (discovery), accuracy (attribution) and level of automation in supporting remediation activities as they vary considerably from vendor to vendor.
- Select an EASM service provider based on the recognized use case priority but also plan for longer-term requirements potentially stretching into DRPS use cases.
- Assess the level of preparedness in terms of skills, resources and maturity of your security organization, making sure to have appropriate resources to fully benefit from EASM capabilities.

Sample Vendors

Bishop Fox; Censys; CyberInt; CyCognito; FireCompass; ImmuniWeb (High-Tech Bridge); Informer Technologies; Palo Alto Networks; Randori; RiskIQ; Shodan

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Emerging Technologies: Critical Insights for External Attack Surface Management

Emerging Technologies: Critical Insights in Digital Risk Protection Services

CAASM

Analysis By: John Watts, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Cyber asset attack surface management (CAASM) is an emerging technology focused on enabling security teams to solve persistent asset visibility and vulnerability challenges. It enables organizations to see all assets (both internal and external) through API integrations with existing tools, query against the consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues.

Why This Is Important

CAASM expands beyond the limited scope of products that focus on a subset of assets such as endpoints, servers, devices or applications. By consolidating into a single repository, users can query to find gaps in coverage for external attack surface management (EASM) and endpoint detection and response (EDR) tools. CAASM provides passive data collection by using API integrations, replacing manual and time-consuming processes to collect and reconcile asset information.

Business Impact

CAASM enables security teams to improve basic security hygiene by ensuring security controls, security posture and asset exposure are understood and remediated across the environment. Organizations that deploy CAASM reduce dependencies on homegrown systems and manual collection processes, and remediate gaps manually or through automated workflows. In addition, such organizations can visualize security tool coverage and correct source systems of record that may have stale or missing data.

Drivers

- Full visibility into all assets under an organization's control to understand attack surface area and any existing security control gaps.
- Quicker audit compliance reporting through more accurate, current and comprehensive asset and security control reports.
- Consolidation of various existing products already collecting asset information into a single normalized view, reducing the need for manual processes or dependencies on homegrown applications.
- Access to consolidated asset views for multiple teams across the organization such as enterprise architects, vulnerability management teams and IT administrators, who can benefit from viewing and querying consolidated asset inventories.
- Lower resistance to collect data and gain security visibility from shadow IT organizations, installed third-party systems and line-of-business applications where IT lacks governance and control. Security teams need visibility in these places while IT may not.

Obstacles

- Resistance to "yet another" tool — Organizations with adjacent products that provide asset visibility may be challenged to justify the cost and addition of CAASM.
- Products may be licensed per asset consumed and become cost-prohibitive for very large organizations with millions of assets under management.
- Scalability of a single instance may be limited for extremely large environments, both for data collection as well as usability of the tool with excessive data points.
- Tools that can be integrated with a CAASM either do not exist (e.g., lacking API) or are blocked for integration by teams who own the existing tools.
- Reconciliation processes that conflict with source systems can cause confusion and frustration if the source system of record is not allowed to be corrected when errors are found.

User Recommendations

- Take advantage of POCs or free versions of products to try before you buy. Products are nondisruptive and easy to deploy, limiting the risk of purchasing a CAASM product and then needing to retire or replace it with another vendor.
- Determine the primary use cases you want to solve with CAASM such as achieving more comprehensive visibility into assets, auto remediation of security gaps, updating sources of records or easing compliance reporting burdens.
- Inventory all available APIs that can be integrated with the CAASM product and make sure you have user accounts available to integrate.
- Extend usage beyond core security teams to multiple users including compliance teams, threat hunters, vulnerability management teams and system administrators.
- Inquire with incumbent security vendors to understand what visibility they currently provide into assets and if they have a roadmap to provide CAASM functionality in the future.

Sample Vendors

AirTrack Software; Axonius; Brinqa; JupiterOne; Panaseer; Sevco Security

Pen Testing as a Service

Analysis By: Prateek Bhajanka

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Pen testing as a service (PTaaS) provides point-in-time and continuous application and infrastructure pen testing services which traditionally relied on human pentesters using commercial/proprietary tools. The service is delivered using a SaaS platform, which leverages a combination of automation and human pentesters to increase the efficiency and effectiveness of the results.

Why This Is Important

Pen testing (PT) is foundational in a cybersecurity program and mandated by various compliance standards. The PTaaS model delivers:

- Platform that enables faster scheduling and execution, and real-time communications with testers and visibility of test results.
- APIs in the platform to integrate with existing tools such as DevOps and ticket management to automate workflows.
- Large pool of testers with specific subject-matter expertise, which can be community sourced or vendors' in-house team.
- Outcome-driven approach.

Business Impact

PTaaS makes pen test services accessible to organizations irrespective of the size, revenue and maturity.

- On-demand and continuous scanning of internal and external infra. and applications.
- Optimizing the cost and also increasing the quality of output.
- Elevating the security posture of the organization.
- Integrating in DevOps and access to real-time findings delivered through the platform, enabling faster treatment of vulnerabilities.
- Performing revalidation of the vulnerabilities remediation.

Drivers

- With the increase in the number of cybersecurity threats in recent years and the COVID-19 pandemic accelerating the rate of attacks, it is imperative for an organization to harden their security posture. In order to elevate their security posture, an organization needs to identify their security vulnerabilities, prioritize and fix them in a timely fashion.
- Organizations are becoming more digital irrespective of their business, size, employee base, etc. and with the nature of cyberattack that can target anyone, they have to get their penetration testing done.
- PTaaS helps organizations with limited in-house security expertise to engage in a PT exercise in order to meet their compliance as well as risk management objectives.
- Security aware organizations looking to shift security to the left, can also leverage PTaaS to integrate in their CI/CD pipeline for their DevOps model.

Obstacles

- Selecting a suitable PTaaS vendor in the market will be difficult as comparing them will not be apples to apples. Vendors use one or combination of automation, human testers which are in-house or community led (vetted freelancers) to perform penetration testing for the client organization.
- Security testing market is overwhelmed with the number of options in the market. Vendors in other adjacent markets such as breach and attack simulation (BAS), autonomous pen testing and red teaming also contest for the same PT budget in an organization, making the PTaaS market more competitive.
- Most of the PTaaS vendors in the market focus only on the internet facing digital assets, like web apps and mobile apps, which will only partially fulfill the clients' requirements.
- Confusion between PTaaS and bug bounty programs, as many of the bug bounty vendors are also now offering PTaaS.

User Recommendations

- Evaluate whether organizations need a vulnerability assessment exercise or penetration testing exercise as both the services may appear similar with significant differences in cost and deliverables.
- Identify and evaluate the PT requirements that PTaaS vendors will be able to fulfill. PTaaS is well-aligned to application testing and external infrastructure testing. All the vendors' offerings will not be able to replace internal infrastructure pen tests, physical assessments, wireless assessments, etc.
- Choose a hybrid scanning model that includes both human and machine from PTaaS vendors in order to have the best of both worlds, effectiveness and efficiency.
- Select a PTaaS provider that fulfils all your compliance requirements when it comes to penetration testing and not just for internet facing infra and applications.
- Look for PTaaS players that provide customized and tailored guidance throughout the life cycle of their service, to mitigate the security skill gap.

Sample Vendors

Bishop Fox; BreachLock; Bugcrowd; Cobalt Labs; HackerOne; ImmuniWeb; NetSPI; Praetorian; Synack

Gartner Recommended Reading

How to Select a Penetration Testing Provider

Understand the Types, Scope and Objectives of Penetration Testing

XDR

Analysis By: Peter Firstbrook

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Extended detection and response (XDR) is a vendor-specific threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

Why This Is Important

Extended detection and response (XDR) is similar in function to security information and event management (SIEM) and security orchestration, automation and response (SOAR). However, XDR is differentiated by its level of integration and automation, ease of use, and focus on threat detection and incident response. XDR solution providers must also provide multiple security controls such as EDR, CASB, Firewall, IAM, IDS, directly.

Business Impact

XDR products can reduce the total cost of managing security incidents, improve the productivity of the incident response team and reduce the overall cybersecurity risk posture of the organization.

Drivers

Midsize organizations are struggling to address the alerts generated from disparate security components. These alerts are often not correlated together to provide a full picture of the incident nor contextualized by other security control points. Although existing SIEM and SOAR tools can provide a similar function, the cost, complexity, and ongoing maintenance of these tools are too high for the midmarket enterprise. The people and skills required to integrate and maintain a best-of-breed portfolio of security tools is too high. XDR tools are primarily marketed by security solution providers that have a portfolio of infrastructure protection products, such as EDR, CASB, SWG, SEG and NDR. More advanced XDR tools are focusing up the stack by integrating with identity, data protection and application access.

Obstacles

Only a small list of vendors can truly offer an XDR product. Committing to an XDR approach could lead to overreliance on a single vendor. Large vendors that can provide an XDR product often execute much slower than the best-of-breed startups in addressing new threats. All XDR tools require some integration with security products from other vendors, however integration of most XDR products is still low. The efficacy of security products is still an important factor and some solutions in a portfolio may be less effective than the best-of-breed competition. There is also the potential dependency on a single source of the threat intelligence and detection content provided by the XDR vendor. XDR tools lower but do not eliminate the need for knowledgeable operators and 24/7 monitoring. Note that a primary differentiator between XDR and SIEM products is that XDR does not meet the needs for long-term log storage for use cases outside of incident response, such as compliance or operations.

User Recommendations

- Work with stakeholders to determine whether an XDR strategy is right for the organization.
- Base decision criteria on staffing and productivity levels, level of federation of IT, risk tolerance and security budget, as well as tolerance for a single-vendor lock in, and presence of existing XDR component tools.
- Develop an internal architecture and purchasing policy that is in line with your XDR strategy, including when and why exceptions might be permissible.
- Plan future security purchases and technology retirements in-line with a long-term XDR architecture strategy.
- Seek security products that provide APIs for information sharing and automation with the XDR.

Gartner Recommended Reading

Innovation Insight for Extended Detection and Response

Market Guide for Security Orchestration, Automation and Response Solutions

At the Peak

DRPS

Analysis By: Mitchell Schneider

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Digital risk protection services (DRPS) are delivered via a combination of technology and services in order to protect critical digital assets and data from external threats. These solutions provide visibility into the open (surface) web, social media, dark web and deep web sources to identify potential threats to critical assets and provide contextual information on threat actors, their tactics and processes for conducting malicious activity.

Why This Is Important

It is easier than ever for cybercriminals to impact digital assets. Attacks are now more complex and voluminous, and they are disrupting business operations for organizations worldwide. The relevance of digital risk is not limited to security operations, but also other business functions, such as marketing, legal, compliance and fraud. Furthermore, DRPS is a highly outsourced function, as the need is often driven by the fact that many organizations do not have the necessary in-house skills.

Business Impact

- Identify exposed digital assets at risk
- Collect and perform analysis of mapped data with prioritization of risks and alerting and reporting capabilities providing actionable intelligence
- Enhance business resilience using people, process and technology (e.g., taking down an active threat and remediating on misconfigured environments)
- Improve security posture, which prevents future threats and business operational impact and implements effective protection against digital assets

Drivers

- The increasing interest in DRPS has been driven by its ability to support a broad range of use cases and user roles. Example use cases include: digital footprinting (e.g., mapping internal/external assets, identifying shadow IT); brand protection (e.g., impersonations, doxing, misinformation); account takeover (e.g., credential theft, lookalike domains and phishing sites); data leakage detection (e.g., protection of intellectual property and PII of employees and customers, as well as credit card data); high-value target monitoring (e.g., VIP/executive monitoring).

- Complexities in the management of risks are key reasons why organizations benefit from DRPS. These complexities include an expanding attack surface due to a more mobile workforce, higher reliance on e-commerce, regulatory compliance, cloud assets, digital business transformation, and the magnitude of information derived from monitored risk and security activities.

- Demand for DRPS has also been driven by the accessibility of such an offering for those small and midsize enterprises that originally could not benefit from threat intelligence (TI) services due to lack of specialized skills and resources on security. This is because of the less technical and more accessible nature of the intelligence made available by many DRPS providers, as well as the availability of a managed service type of offering.

Obstacles

- The DRPS space continues to expand with approximately 50+ vendors aligned to this market. The vendor capabilities vary and may be limited in their ability to provide a comprehensive solution. Some vendors have a best-of-breed approach whereby they are heavily focused on niche DRPS use cases (e.g., VIP/executive monitoring); however, many vendors are expanding to support more than one use case.

- Market growth is rapid and increasingly overlaps with complementary markets such as TI, endpoint protection platforms (EPPs), managed security service providers (MSSPs)/managed detection and response (MDR) providers and external attack surface management (EASM) capabilities.

User Recommendations

- Evaluate the capabilities and features of DRPS offerings and match them to the needs of users' security programs and business risks. Ask vendors what threats they cover and if they focus on one specific use case or many (e.g., phishing, dark/deep web monitoring, digital footprinting, data leakage and/or social media protection).

- Prioritize best-of-breed solutions to meet a specific urgent need, depending on the urgency and importance of the core use case. A good example would be threats arising from consistent look-alike domains and phishing domains requiring takedown services. Assess vendors based on takedown success rates and ability to work with ISPs and registrars in foreign locations.

- Prioritize solutions that include managed services in their offerings (especially if there are resource constraints), can predict and prevent issues from occurring in the first place, and have service-level agreements (SLAs) that ensure the fastest remediation time.

Sample Vendors

BlueVoyant; CyberInt; CybelAngel; Digital Shadows; IntSights; PhishLabs; Recorded Future; RiskIQ; SafeGuard Cyber; ZeroFOX

Gartner Recommended Reading

Emerging Technologies: Critical Insights in Digital Risk Protection Services

Emerging Technologies: Critical Insights for External Attack Surface Management

Breach and Attack Simulation

Analysis By: Jeremy D'Hoinne, Toby Bussa, Mitchell Schneider, Pete Shoard

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Breach and attack simulation (BAS) technologies allow enterprises to continually and consistently simulate multiple attack vectors against an enterprise's assets. BAS can test threat vectors such as external and insider, lateral movement and data exfiltration. BAS deployment leverages software agents, virtual machines, cloud platforms and other means to run simulations. Although there are similarities, it cannot fully replace red teaming or penetration testing.

Why This Is Important

The BAS market is growing, with two dominant use cases: security control validation and security posture assessments. Key advantages of BAS technology include the ability to provide continuous and consistent testing of security controls, and the help provided in prioritizing remediation actions to improve defenses.

Business Impact

BAS allows organizations to automate and run continuous security assessments that evaluate and assess a larger percentage of an organization's assets and on a more frequent basis. BAS continually adds new threats and expands the scope and depth of its capabilities.

Drivers

The most common use case for BAS is the automated testing and assessment of a company's security posture. Large organizations with mature security programs use these technologies primarily to ensure consistent defense and to test their existing security controls for configuration gaps and/or missing security visibility. Weekly, and sometimes daily tests are used to inform IT and business stakeholders about existing gaps in the security posture or validate that security infrastructure, configuration settings and detection/prevention technologies are operating as intended. BAS can also be used to validate if security operation center staff can detect specific attacks when used as a complement to red team or penetration testing exercises.

Obstacles

To grow as a market, BAS vendors not only need internal sponsors from teams such as the security operation center, application and network operations, validating the quality of the insights, but will also need to expand beyond the diagnostic and basic remediation guidance through standard frameworks.

BAS vendors must overcome deployment and maintenance challenges, and continue to differentiate from adjacent markets. Large enterprises already have too many diagnostics, from audit, vulnerability management, application security testing, and penetration testing engagements. BAS must not simply add to the mass, but provide directional guidance and enrichment to existing security assessments.

User Recommendations

- Evaluate the capability for a BAS technology to accurately and safely emulate attacks that mimic the threats actually faced by the organization.
- Prioritize your company's use cases, and then assess the BAS vendors' capabilities against those to determine which BAS would improve their existing security risk assessment, threat monitoring and vulnerability management practices.
- Evaluate the number of attack scenarios the provider can provide and the frequency to which these simulations are updated to reflect real-world attacks.
- Work with your auditors to determine whether BAS technology can be used to validate the efficacy of existing security controls.
- Ensure that the results delivered by the BAS product are actionable, prioritized and feed directly into response planning.

Sample Vendors

AttackIQ; Cymulate; FireEye; Picus Security; SafeBreach; XM Cyber

Gartner Recommended Reading

Quick Answer: What Are the Top Use Cases for Breach and Attack Simulation Technology?

VPT

Analysis By: Mitchell Schneider

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Vulnerability prioritization technology (VPT) streamlines the vulnerability analysis and remediation/mitigation process by focusing efforts on identifying and prioritizing the vulnerabilities that pose the greatest risks to the organization. The approach considers the exploitability of a vulnerability, asset or business criticality, the severity of a vulnerability and compensating controls in place.

Why This Is Important

VPT supports a risk-based approach to vulnerability management (RBVM). This class of products (and services) utilizes the telemetry from VA tools, configuration management databases (CMDBs) — although having a CMDB is not a requirement to utilize VPT — as well as application security testing (AST). VPT adds a layer of intelligence by leveraging analytics and various threat and vulnerability intelligence sources.

Business Impact

VPT solutions can be considered a form of automation that bring advanced analytics and vulnerability intelligence to reduce the human resource requirements of performing manual RBVM. The continued rise in the number of security incidents and breaches around the globe is driving many organizations to adopt VPT solutions to implement an effective, efficient vulnerability management program. The rise in incidents is also causing VA vendors to align more to the RBVM methodology.

Drivers

- The VPT market continues to grow rapidly, based on Gartner research and client inquiries, as well as sales of tools to support the process. VPT identifies more pragmatic risks to the organization and helps prioritize actions for vulnerability treatment — whether via remediation (e.g., patching) and/or compensating controls (e.g., intrusion prevention system [IPS] and web application firewall [WAF]). Moreover, the solution can provide savings in terms of operational full-time employee (FTE) costs due to better prioritization, as well as reduce the organization's attack surface, preventing the vulnerabilities from being exploited.

- RBVM is an iterative process, underpinned by the technology (e.g., VA and VPT), and triggers other processes, such as IT operations executing patch management. Moreover, performing manual RBVM is challenging. It requires intelligence and automation to successfully operationalize the process. Organizations cannot handle the traditional ways of prioritizing vulnerabilities via predefined CVSS scores because they need to account for exploits and business criticality to reflect the real score to the organization. In the case of VPT, these solutions perform the analysis of vulnerabilities in the context of the current threat landscape. For example, a vulnerability that is a low risk today might be a high-impact vulnerability tomorrow due to the public availability of an exploit, while the Common Vulnerability Scoring System (CVSS) score would remain relatively static.

Obstacles

- VPT solutions are typically leveraged by organizations that are higher in terms of vulnerability management maturity and should not be used until the basic vulnerability management processes are in place. VPT will not work if there are broken processes in the VM program.

- Vulnerability management (VM) is a foundational part of information security operations. However, prioritizing vulnerabilities according to a severity score results in a response that is based on a single metric. This metric-driven output is rarely based on risk, as factors such as threat activity and asset context are not considered.

- Organizations find the exercise of VM overwhelming because of the large number of vulnerabilities showing up in the reports, which adds to the friction between other business units and the security team. The most common client inquiries that Gartner receives include: “How do I identify the top 100 vulnerabilities in my VA report?” and “How do I prioritize those vulnerabilities that matter most?”

User Recommendations

- Implement a risk-based approach that correlates asset value to calculate a risk rating leveraging VPT solutions. This reduces the risk of being breached when prioritizing remediation activities.
- Augment VA tools with stand-alone VPT solutions for better prioritization or use existing VPT capabilities that assist with the effective methodology for real risk reduction. This enables vendor consolidation and places less effort on new training and tool deployment.
- Identify vendors with patching capabilities and SOAR integrations. This puts the security team in control of workflows. Evaluate if this approach is appropriate. If so, leverage remediation workflow automation and avoid using two different tools.
- Deploy VPT solutions that use the context of internal security controls to maximize existing security investments. This capability is immature across the market.
- Choose VPT solutions that aggregate vulnerability data from multiple sources to present action-oriented metrics.

Sample Vendors

Brinqa; Kenna Security; NopSec; NorthStar; Risk Based Security; RiskSense; ServiceNow; Skybox Security; Tufin Software; Vulcan Cyber

Gartner Recommended Reading

The Essential Elements of Effective Vulnerability Management

How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation

A Guidance Framework for Developing and Implementing Vulnerability Management

File Analysis

Analysis By: Michael Hoeck

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

File analysis (FA) software analyzes, indexes, searches, tracks and reports across multiple file and database sources. FA software reports on detailed metadata and contextual information to enable better information governance, risk management, data management actions, and the analytical assessment of unstructured and structured data.

Why This Is Important

FA solutions improve organizations' ability to manage ever-expanding repositories of unstructured/structured data. They increase visibility to disparate, unorganized sources of information, allowing IT teams to establish qualified operational efficiencies; compliance teams to improve insight to sensitive information, including personal information (PI); and security team exposure to areas of data access risk.

Business Impact

- FA solutions reduce business risk and inefficiencies by identifying access permission issues, locating and protecting intellectual property, and eliminating or quarantining sensitive data.
- Users gain actionable insights to optimize storage efficiency by identifying redundant, outdated and trivial (ROT) data.
- Management of information governance is improved, as FA solutions feed data insights into corporate retention initiatives and classify valuable business data.
- Lower business risk and storage utilization lead to savings.

Drivers

- The desire to mitigate business risks (including security, breach and privacy risks); identify sensitive data, optimize storage costs; and implement information governance
- The hype associated with the growing trend of privacy regulations, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which has greatly increased interest in and awareness of FA software
- The potential value of contextually rich data, which is capturing the interest of data and analytics teams

Obstacles

- Successful results from using file analysis software may be affected by a lack of data policy buy-in or consensus from key internal constituencies, including executive sponsorship.
- Establishment of action-oriented retention policies is required to defensibly delete redundant, outdated and trivial data identified by FA software.
- Although FA solutions and corresponding budgets resonate highest with compliance and efficiency use cases, budgeting aligned to data risk and analytics use cases may be challenged, requiring additional sponsorship.

User Recommendations

- Use FA software to better grasp the risks of an unstructured data footprint, including where it resides and who has access to it, and to expose another rich dataset for driving business decisions.
- Develop strong information governance principles by establishing, updating and enforcing retention policies, using the information gathered and remediation actions from FA software.
- Identify the potential risks of unknown data stored in structured database repositories often associated with applications.
- Clean up old file shares containing ROT data that can be defensively disposed of or relocated to optimize data infrastructure.
- Create data visualization maps to better identify the value and risk of the data, including the data owner.
- Use FA software to enable IT, line of business (LOB) and compliance teams to make better-informed decisions regarding classification, information governance, storage management and content migration.

Sample Vendors

ActiveNav; Data Dynamics; Ground Labs; Index Engines; Netwrix (Stealthbits); SailPoint; Spirion; Titus; Varonis; Veritas

Gartner Recommended Reading

Market Guide for File Analysis Software

Sliding into the Trough

Integrated Risk Management

Analysis By: Deepti Gopal, Jie Zhang

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Integrated risk management (IRM) combines technology, processes and data to enable the simplification, automation and integration of various risk domains across an organization. To understand and manage the relevant scope of risk, organizations require a comprehensive view across key risk and compliance functions, as well as critical business partners, suppliers and outsourced entities.

Why This Is Important

IRM has evolved to encompass risk and compliance management across a spectrum of risk domains, including technology risk and security risk. Building on the integration of monitored risk data at the execution layer provides a much-needed management layer of integrated data to support decision making. IRM delivers the combined technology, processes and data that fulfill the simplification, automation and integration of strategic, operational and technology risk management across an organization.

Business Impact

Regulatory compliance, digital business transformation, increasing cyber risks, and magnitude of information derived from monitored risk and security activities are key drivers to help skills-starved organizations benefit from this solution set. An IRM strategy enables the use of consistent tools, terminologies and processes across various risk domains relevant to the organization. The scope of an IRM project emphasizes the integration principle across risk-data silos and risk processes.

Drivers

Adoption, across all risk domains is still growing, as organizations:

- Look for opportunities to streamline and simplify their risk management and compliance-related activities and improve their understanding of risks through system integration with operational-level data sources, supported by risk program maturity assessment and consulting engagements, as well as augmentation of risk expertise and content through managed services.
- Reduce their overall spending by replacing multiple risk management solutions with a single, integrated solution.
- Midsize enterprises are more open to a single-vendor IRM solution to simplify and automate their risk management processes.

Obstacles

- Large enterprise buyers already utilize a broad array of legacy risk management tools and/or services that require replacing, upgrading and connecting to deliver an integrated risk management approach.
- A compelling business case for an IRM solution is closely linked to the size and complexity of the organization, restricting adoption in smaller companies.
- The majority of technology providers are positioning their capabilities to address all risk domain needs in a general-purpose manner, but in reality, they tend to support some specific domains better than others.
- Finding a common denominator among different risk functions within an organization is challenging — the tools are used by different users with different requirements, workflows, expectations and levels of acceptance.

User Recommendations

There is no single best product for all organizations across all use case domains included in the IRM definition (these include digital risk, vendor/third-party risk, quality risk, business continuity, internal audit, environment, health and safety, ethics and compliance, and legal risk). However, there are typically several good options to fit a specific set of requirements for your organization.

Buyers should:

- Capitalize on opportunities to align common risk management processes, terminology, data collection and technology tools to leverage IRM capabilities across a number of risk management domains.

- Align and focus on project and functional requirements around usability, scalability, ease of integration/implementation, geographic diversity and good customer support.

- Develop an IRM strategy by implementing a primary IRM use case and adding complementary point solution use cases, where needed, to address communication and business growth needs.

Sample Vendors

Cybersaint; Deloitte; Diligent; EY; LogicGate; LogicManager; NAVEX Global; OneTrust; PwC; Riskonnect; RSA; SAI Global; ServiceNow

Gartner Recommended Reading

Technology, Information and Resilience Risk Primer for 2021

Competitive Landscape: Integrated Risk Management

SOAR

Analysis By: Claudio Neiva, Craig Lawson, Toby Bussa

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

SOAR is a technology approach that combines incident/case management, workflows, orchestration and automation, response and threat intelligence management in a single platform. Incident management allows for knowledge capture and management, along with workflow mapping. Orchestration and automation adds machine assistance to human-lead processes and workflows. Threat intelligence management allows for the curation and automation of ingesting, processing and distributing intelligence.

Why This Is Important

Security orchestration, automation and response (SOAR) tools are flexible and can be applied to various security operations centers (SOCs) and broader SecOps use cases. Current buyers tend to be end-user organizations and security services providers with an SOC function, looking to optimize the efficiency, consistency and effectiveness of their threat monitoring, detection and incident response activities. Threat management use cases for SOAR are still emerging.

Business Impact

- SOAR solutions are being deployed mainly to assist the SOC team, to automate and orchestrate incident response processes combining human expertise and automation where applicable.
- Another benefit of this type of solution is the opportunity to reduce labor costs, taking advantage of automation. In addition, SOAR will not create all of your processes and workflows for you — it just helps you run them — so, unless you have a team with processes, SOAR may not be your starting point.

Drivers

- SOAR improves the optimization and execution speed of repetitive tasks that often torment SOC operations, especially in tasks that consume time and require little human expertise. This frees teams to spend more time on critical tasks and activities.
- SOAR solutions improve the triage process and prioritization of incidents to be managed by the SOC. SOAR increases alert fidelity and actionability by adding more context and data enrichment. This helps reduce noise due to the high volume of alerts that needs to be handled by the SOC team.
- Security orchestration and automation (SOA) as a capability is increasingly needed by security operations. SOAR solutions offer flexible SOA in the platform. However, SOA is also becoming more available as canned, baked-in functionality in other security technologies, such as email security solutions, to help improve analysis, triage and automate responses to threats.

Obstacles

- Security leaders might misinterpret SOAR solutions as a “silver bullet,” which will connect through integration alert functions to toolsets like firewalls, an intrusion detection and prevention system (IDPS), endpoint detection and response (EDR), and other security products. Instead, security leaders should think of the role of SOAR technologies as automation of existing well-proven processes: collecting inputs from security operations functions, such as alerts, and partial automation processes, such as incident analysis and triage.

- Organizations need to be prepared with documented processes in order to benefit from either manual workflow or automated workflow features.

- SOAR solutions will need to be managed and maintained in order to ensure maximum value is received. Resources to use and operate the tool are needed to address activities such as, monitoring for health, availability and performance of the solution, updates and patches, and maintenance of workflows and playbooks.

User Recommendations

- Assess the availability of development skill sets internally to develop SOAR’s required functionality. Security leaders should also review the time and cost this may add to the total cost of owning an SOAR toolset.

- Involve the entire security organization when scoping requirements for SOAR. Organizations must look beyond simply plugging a new technology into an SIEM, and instead engage with the wider security.

- Select an appropriate product based on buyer understanding, their applicable use cases, such as SOC optimization, threat monitoring and response, threat investigation and hunting, and threat intelligence management.

- Implement well-defined processes and playbooks before acquiring SOAR. Although SOAR promotes lots of benefits, not every security organization is ready for the tool and a considerable amount of time is required to develop playbooks..

Sample Vendors

Cyware; D3; Fortinet; IBM; Palo Alto Networks; Rapid7; Splunk; Siemplify; Swimlane; ServiceNow; ThreatConnect; ThreatQuotient

Gartner Recommended Reading

Market Guide for Security Orchestration, Automation and Response Solutions

SOAR: Assessing Readiness Through Use-Case Analysis

Is Your Organization Mature Enough for SOAR?

Deception Platforms

Analysis By: Rajpreet Kaur, Pete Shoard

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Deception platforms are centrally managed systems for organizations to create, distribute and manage an entire deceptive environment. These decoy workstations, servers, devices, applications, services, protocols, data elements or users are often emulated, essentially indistinguishable from real assets and identities, and are used as lures to entice, engage and detect an attacker.

Why This Is Important

Threat detection and response, production of local indicators of compromise (IoC), machine-readable threat intelligence (MRTI), integrated proactive threat hunting, and active attacker engagement are the primary use cases for deception tools. These platforms offer the ability to create network decoys of other types of devices, such as Internet of Things (IoT), operational technology (OT)/industrial control systems (ICSs) and healthcare, where many traditional active tools can't be deployed.

Business Impact

Security and risk management (SRM) leaders who want to develop a threat detection initiative can invest in deception platforms as a low-cost and high-impact complement for endpoint detection and response (EDR) and network detection and response (NDR) tools. Forward-leaning and mature clients can also benefit from the added value from deception platforms, such as generation of decoys that will increase an attacker's dwell time, or generation of local IOCs and other threat intelligence (TI).

Drivers

- **Active Directory protection:** Enterprises are utilizing deception platforms to detect attacks on AD and prevent attacks such as credential harvesting, exploitation of access rights and password spay. This helps the security teams to identify weaker/redundant configurations, such as expired accounts, and fix the misconfigurations and vulnerabilities being exploited by the attacker.

- **Ransomware:** Enterprises use deception platforms to identify ransomware attacks during the initial access, which is quite early in the ransomware kill chain. The endpoint decoys detect any ransomware attack, such as attempts to encrypt files and credentials stealing across different stages of the ransomware kill chain, making it easier to prevent the endpoint against such attacks.

- **Intuitive detection information:** The deception platforms offer intuitive information related to detection to help the security team identify the behavior and type of attack very easily. Few vendors use the MITRE ATT&CK framework to display the detection information on a real-time basis, making the alerts highly intuitive and easier for different security teams.

- **Cloud security:** With adoption of cloud, cloud-oriented deception support, such as Amazon Web Services (AWS) Simple Storage Service (S3) buckets and AWS Relational Database Service (RDS) databases, is being offered by the vendors. The vendors also offer a cloud version of their offering for clients that want to deploy it on the cloud.

- **SaaS-based option:** To make the deployment and management of deception platforms easy, few vendors have also started offering it as a SaaS-based fully managed model, making it an attractive proposition for enterprises with smaller security teams and a cost-effective model.

Obstacles

- **Perception:** The market perception is that these tools can only be utilized for complex use cases where enterprises have multiple security teams that are relatively bigger in size; hence they fail to find value in enterprises with smaller security teams.

- **Price:** As the vendors are adding more features into the platform, they are adding more subscriptions to it, which makes it relatively expensive and requires a business justification to get the budget allocated for it.

- **Overlapping technologies:** Few security technologies offer basic deception as an add-on feature; moreover, technologies like NDR, security orchestration, automation and response (SOAR) and EDR also offer respective detection and response features, undermining the capability of deception platforms.

- **Value proposition:** Gartner has often seen chief information security officers (CISOs) struggling to justify the cost of running a deception platform even after demonstrating its efficacy and value.

User Recommendations

- Identify the evolving use cases beyond the traditional network and endpoint decoys where deception platforms can be a game changer, and focus the evaluation toward these use cases.

- Prioritize deception-based detection approaches for environments that cannot use other security controls.

- Explore the option of utilizing the solution as a fully managed SaaS if you find deploying the entire solution complex to manage and time-consuming to maintain.

- Test the effectiveness of deception platforms by running a POC or a pilot on a production environment. Once deployed, prioritize alerts from the deception platforms as high-priority; these are high-fidelity alerts that need immediate attention.

Sample Vendors

Acalvio Technologies; Attivo Networks; CounterCraft; Fidelis Cybersecurity; Illusive; PacketViper; RevBits; Smokescreen; Thinkst Canary; TrapX

Gartner Recommended Reading

Improve Your Threat Detection Function With Deception Technologies

Applying Deception Technologies and Techniques to Improve Threat Detection and Response

Deception Solution Providers Must Prepare for Market Consolidation

MDR Services

Analysis By: Toby Bussa

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Managed detection and response (MDR) services leverage a combination of technologies at the host, the network and, increasingly, the cloud layer, as well as advanced analytics, threat intelligence, and human expertise to deliver 24/7 threat monitoring, detection and response. MDR providers undertake incident validation and investigation, and response actions to disruption, and they contain threats.

Why This Is Important

Attacks against organizations are relentless and increasing. Most organizations lack the resources, budget or appetite to build and run their own 24/7 modern security operations center (SOC) function, which is required to help them protect and defend themselves against attacks that increasingly cause more impact and damage to operations. MDR services enable organizations to procure modern SOC services to address this need and fill gaps in their threat detection and response coverage.

Business Impact

Organizations of all sizes that have not invested in threat detection and response capabilities are at risk, due to increasingly hostile external threats. This situation, combined with the challenge of finding, acquiring and retaining the necessary expertise and the right tools, makes building an adequate internal capability challenging. MDR services reduce the complexity of identifying the right mix of people, process and technology by enabling buyers to buy capabilities directly from service providers.

Drivers

- MDR services continue to expand beyond the traditional “turnkey” approach whereby the provider brings a predefined, or highly curated and supported, set of technologies. The expansion to supporting a broader set of log, data and alert sources has been well received by organizations that want more say over what is monitored, but it also puts pressure on providers to adapt and scale how they deliver their services, while delivering high-fidelity threat detection.
- Active responses by MDR providers are being required by buyers, especially in North America, and this challenges both parties to ensure responses are made in a coordinated and reliable way.
- In response to customer demand, MDR providers are adding foundational security operation capabilities, such as vulnerability management, log management and risk management, to their offerings.
- Cloud-native security operations solutions like security information and event management (SIEM), security orchestration, analytics and reporting (SOAR) and extended detection and response (XDR) with multitenant capability, MDR-friendly programs, and SOCaaS or “SOC in a box” offerings are enabling new MDR service providers.

Obstacles

- The number of MDR service providers continues to grow, with new ones becoming visible to Gartner at least weekly. This makes it more difficult for buyers to identify the best provider for their needs.
- Gartner hears of performance issues with MDR service providers and failed engagements due to misaligned expectations.
- Technology vendors with XDR solutions, which already offered managed endpoint detection and response (EDR) as a form of MDR, have started positioning their MDR services as managed XDR, which will likely increase buyers’ confusion.
- Managed security service providers (MSSPs) have added MDR offerings to their portfolios to address buyer demand and compete better — a development that further complicates buyers’ decision-making process.

User Recommendations

- MDR buyers should focus on outcomes, not technologies. Organizations underinvested in technologies like EDR and network detection and response (NDR) should favor an approach in which a vendor provides the tools and delivers the desired outcomes.
- Buyers lacking the staff and expertise to handle incident response activities once a threat has been identified, or that want to add threat-hunting capabilities, should assess MDR services.
- If there are existing investments in threat detection technologies, such as EDR, NDR and SIEM, MDR services that deploy their own technologies may be inappropriate. Consider services that can use existing technologies, and augment them to fill gaps.
- If technology management, compliance monitoring and reporting, and other managed security services are required, consider MSSPs, especially those that offer MDR-type services.
- Buy MDR services that offer transparency, that encourage engagement through modern user interfaces, and that have open communication channels with analysts and delivery teams.

Sample Vendors

Arctic Wolf; CrowdStrike; eSentire; Expel; F-Secure; FireEye; Rapid7; Red Canary; Secureworks; Trustwave

Gartner Recommended Reading

Market Guide for Managed Detection and Response Services

TI Services

Analysis By: John Collins

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Threat intelligence (TI) services provide knowledge about the cyberthreat landscape by documenting tactics, techniques, procedures, and identifying details of threats and threat actors. TI services provide tools to assist in operationalizing TI to instrument security products, but also educate end users about the threats they face. TI provides information about the who, what, why, how, and to a lesser extent when, based on technical and strategic analysis of adversaries and their tradecraft.

Why This Is Important

The people, process and technology components of security operations require constant updates on an organization's threat exposure. How can an organization protect itself against cyberthreats with no relevant understanding of adversary tactics, techniques and procedures (TTPs), or objectives? Threat intelligence has evolved to support a number of security operations and risk use cases from a large number of providers. This market is still yet to see meaningful consolidation of providers.

Business Impact

- TI deliverables assist in identifying strategic and tactical cyber risks, defining cyber risk to the business and focusing SecOps efforts.
- TI services facilitate an organization's understanding of their cyberthreat landscape, driving greater protection, increased detection, and response efficacy for threats that matter.
- Organizations utilize TI services through the use of APIs, marketplaces, portals and staff augmentation, simplifying the task of operationalizing intelligence in the environment.

Drivers

- Organizations are pushing for more relevant content in security solutions they are considering or already purchased. This has put pressure on technology vendors and security service providers to build, buy or partner with TI service providers. This will deliver a continuous stream of updated detection use cases, threat ratings and indicators based on current TI for their products and services to attract and retain customers.

- A consolidation of technologies in the security industry is pushing platforms, like SIEM, to increase TI service integrations, driven by increasing client demand for continuously updated detection content. New solution offerings like eXtended Detection and Response (XDR) (see Innovation Insight for Extended Detection and Response) require a TI core component, because of its ability to support use cases like threat hunting and deliver updated content buyers seek.

- Threat Intelligence frameworks have been high profile drivers in the TI services industry for a decade. The Mitre ATT&CK framework, based on TTPs derived from curated TI, arguably has the biggest impact on the security frameworks since public release in May 2015. Nearly every security solution and service provider is mapping their solution outputs to ATT&CK categories.This is primarily because of security operation (SecOps) user demand for a common taxonomy for sharing indicators and behaviors. Other standards like STIX/TAXII continue to see adoption by both users and vendors alike as a way to speed up the use of MRTI (machine readable threat intelligence)

- TI data is being leveraged to train models for data science driven security analytics for detection of adversary TTPs, which is inclusive of malware and behaviors. This driver is not exclusive to security product and service vendors as end user organizations with the tools and talent to generate their own algorithms are collecting internal and external TI data to improve their detections.

Obstacles

- TI is not well-understood by consumers and often not explained very well by sales or even TI experts. TI analysts often come from government, military or law enforcement backgrounds and their understanding and expertise of the threat landscape often does not translate well to the commercial sector.

- TI can be its own worst enemy when demonstrating clarity of value. Buyers of TI services report being overwhelmed with false positives or finding little value in the reporting in relation to their business or expectations, however realistic or inflated.

- There is a heavy focus on attribution of adversaries, but the reality is many organizations care, just not that much.They want TI operationalized, eliminate false positives and prioritize what's key in their environment without complexity and are not concerned with the five year plan or details of a nation state.

- Pricing for TI services may exceed the entire security budget for small and midsize organizations, increasing time to plateau.

User Recommendations

- Conduct periodic threat assessments to help identify where TI services are needed and ensure they align with your goals and ability to consume the deliverables. Assessments and vendor validation are not one time engagement due to the dynamic nature of the threat landscape and changing adversary goals.

- Evaluate the organization's appetite to consume TI services and match it with a provider(s) who can demonstrate value to the business and the SecOps team based on threat assessment findings and identified business risks. Expect to consume more than one commercial or open source intelligence (OSINT) service to improve visibility because no single TI service provider can see everything.

- Leverage multiservice TI service vendors for efficiencies, but only when the vendor can deliver on expectations. Merging features are creating comprehensive TI service platforms. However, a single vendor with multiple TI offerings often only meets expectations in some but not all organizational use cases.

Sample Vendors

CrowdStrike; FireEye (Mandiant); IBM; Intel 471; IntSights; Secureworks; Team Cymru; ThreatQuotient; TruSTAR

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

How to Use Threat Intelligence for Security Monitoring and Incident Response

How Gartner Defines Threat Intelligence

Use a Capability Matrix for a More Effective Threat Intelligence Program

Security Operations Primer for 2021

NDR

Analysis By: Lawrence Orans, Jeremy D'Hoinne

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Network detection and response (NDR) technology uses a combination of machine learning, rule-based detection and advanced analytics to detect suspicious activities on enterprise networks. NDR tools analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect abnormal traffic patterns, they raise alerts. NDR solutions monitor north-south and east-west traffic. These tools also provide threat hunting capabilities.

Why This Is Important

NDR is very effective in detecting suspicious traffic on networks, such as lateral movement or data exfiltration. It focuses on detecting abnormal behaviors, with less emphasis on more traditional signature-based controls, detecting known threats. NDR solutions also provide response capabilities. Responses can be automated (for example, sending commands to a firewall to drop packets) or manual (providing tools for incident responders to search through metadata for forensic analysis).

Business Impact

NDR solutions provide visibility into network traffic. The machine learning algorithms that are at the core of many NDR products help to detect anomalous traffic that is often missed by other detection techniques. The optional automated response capabilities help to offload some of the workload for incident responders. The threat hunting functionality provides valuable tools for incident responders.

Drivers

- **Low Risk — High Reward —** Implementing NDR tools is a low risk project, since the sensors are positioned out-of-band (they are not in the line of traffic, so they don't represent a point of failure or a "speed bump" for network traffic). Enterprises that implement NDR solutions as a proof of concept (POC) often report high degrees of satisfaction, because the tools provide much needed visibility into network traffic. The POC projects often result in the customer buying the solution, because they see value in the traffic visibility.

- **Encrypted Traffic Analysis —** As the volume of encrypted traffic grows, it becomes more challenging for traditional network security tools to analyze it. Multiple security research reports from leading vendors show growth in the frequency of instances where malware is delivered in an encrypted traffic stream. In the NDR market, vendors offer at least one of these three techniques for detecting anomalies in encrypted traffic. **JA3 signatures:** JA3 is a method of fingerprinting the handshake between a client and a server. By comparing handshakes in live traffic to the handshake patterns of commonly used applications, vendors can detect suspicious traffic. Nearly all NDR vendors support this technique. **Message lengths and time intervals between messages:** Monitoring this information is a proven technique for detecting suspicious traffic without decrypting it. Some vendors support this capability. **Traffic decryption:** Decrypting traffic so that it can be analyzed for malware is the most accurate technique, but only a few vendors support this capability.

- **Securing SaaS Applications —** Some NDR vendors offer the ability to monitor traffic destined for Microsoft 365 and other popular SaaS applications. These tools are good at detecting brute force login attempts and other suspicious behavior. Good CASB tools offer this functionality and more, but NDR vendors can add value where the customer does not already own CASB technology.

Obstacles

- NDR competes for budget with endpoint detection and response (EDR), increasingly extended detection and response (XDR) and sometimes user analytics, depending on the threat vectors that the prospective customers try to mitigate.
- Enterprises with a lower maturity security operation program might struggle to justify the expense for a technology that cannot simply be evaluated by counting the number of alerts it triggers.
- The response features of the NDR products are more recent and still evolving.
- Smaller organizations do not have the staff to support and operate a detection-only tool, but struggle to accept a fully automated response.
- False positives — they are inevitable with any behavioral-based detection tool. But NDR tools, once tuned, do not exhibit a chronic problem in this area and tend to trigger a relatively low volume of alerts.

User Recommendations

- Develop a strong understanding of the overall traffic patterns and specific protocol patterns in your enterprise network to gain maximum value from NDR.
- Carefully plan sensor deployment so that the most relevant network traffic can be analyzed. Proper positioning of the NDR sensors is critically important.
- Tune out false positives in the implementation phase (false positives may be triggered by vulnerability scanners, shadow IT applications, and other factors that may be specific to your environment).
- Select sensors that are sized appropriately for your network. Some vendors offer sensors that support up to 100 Gbps of line rate capture, whereas other vendors' sensors can only scale up to 10 Gbps.

Sample Vendors

Arista Networks; Cisco; Darktrace; ExtraHop; Fidelis Cybersecurity; FireEye; Gigamon; Plixer; Vectra; VMware

Gartner Recommended Reading

Market Guide for Network Detection and Response

OT Security

Analysis By: Katell Thielemann, Ruggero Contu

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Operational technology (OT) security is the practice of protecting critical production and operational systems and services in asset-centric enterprises. OT security addresses industrial control systems and use cases where physical state changes depend upon secure, safe and reliable function. As digital transformation efforts increasingly target operational and mission-critical environments, OT security is evolving into cyber-physical systems security, with security disciplines converging.

Why This Is Important

Once disconnected from IT networks, the convergence of OT and IT systems driven by business needs has created new security risks. They are compounded by remote connections from original equipment manufacturers (OEMs). Because operational systems are the centers of value creation, OT security is of major relevance to asset-centric organizations, such as those considered to be part of national critical infrastructure, and to any other industrial verticals with operations-centric environments.

Business Impact

Whether nation states targeting critical infrastructure (e.g., the 2015 attack on Ukraine) and intellectual property (manufacturing is often targeted for cyber espionage), or financially motivated hackers deploying ransomware, the number of attacks on OT systems has steadily increased over the past five years. The impact of operational disruption can range from mere annoyance to hundreds of millions of dollars, as well as reliability and safety impacts.

Drivers

- Whether because of attacks or an overall heightened awareness of the increased risks they face, asset-centric organizations are increasingly focusing their attention on the security risks they face outside of enterprise IT. At the same time, a growing number of vendors are offering specialized security platforms to help enhance situational awareness of assets, network topology and vulnerabilities, as well as to help with threat detection and mitigation.

- International standards, such as IEC 62443, European NIS and NIST 800 series, are also emerging to provide guidance; and in some industry verticals, security mandates such as NERC-CIP are already in place. Given the close relationship between critical infrastructure and national security, and the growing concerns of targeted attacks, government-led efforts are also likely to increase, adding to the growing list of existing national legislations.

- A converged cyber-physical systems (CPS) security discipline is emerging, driven by organizations paying more attention to the basics of OT security (e.g., firewalls, network segmentation), while adding “greenfield” new robotics or IIoT systems with modern technologies that introduce new risks across a cyber-physical continuum of threats.

Obstacles

- Because of their history of OT deployments disconnected from IT systems, organizations working on expanding their security and risk efforts outside of enterprise IT often face cultural, governance and security control challenges that prevent a one-size-fits-all approach to security. For instance, operations often run 24/7 and cannot be stopped at will.

- OEMs often contractually connect remotely into OT systems to maintain and update them. If not done securely with consistent policies, this creates additional risks. In some cases, OEMs also control the deployment of any updates, which hampers security efforts.

- Most OT systems have important safety and reliability requirements that prevent deploying security controls at will.

- Organizations also continue to face acute and growing shortages of OT security skills to foster and support IT/OT integration, and securely support digital transformation efforts.

User Recommendations

- Initiate risk discussions between IT security and OT teams, and determine the current extent of OT security efforts.
- Deploy OT asset discovery, inventory and network mapping security platforms.
- Determine immediate gaps, such as flat OT networks, lack of firewalls, open ports, vulnerable and unpatched operating systems, shared password, etc.
- Accelerate security awareness and skills training for converging IT and OT infrastructures.
- Focus on organizational and cultural trust challenges between IT and OT personnel.
- Collaborate with your procurement team to demand OEMs of OT systems ensure that their (future) systems are secure by design.
- Prepare for a future where CPS security emerges as a centralizing discipline for securing converging IT, OT, and IoT systems and bringing together asset-centric cybersecurity, physical security and supply chain security best practices.

Sample Vendors

Barracuda; Claroty; Dragos; Nozomi Networks; SCADAfence; Verve Industrial

Gartner Recommended Reading

Market Guide for Operational Technology Security

Establish Successful Executive Security Governance in an Integrated IT/OT Environment

OT Security Best Practices

Emerging Technologies and Trends Impact Radar: Security in Manufacturing

Climbing the Slope

Endpoint Detection and Response

Analysis By: Paul Webber, Jon Amato

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

EDR solutions can detect and investigate security events, contain attacks and produce remediation guidance. They must analyze user, process and system activity and device configuration. Reporting of user and device data is combined with direct intervention to detected events. Automated response and rollback of threats are desirable, integration and automation with other tools are key. Cloud hosting is predominant; some vendors can host on-premises for non-internet-connected systems.

Why This Is Important

All systems exposed to the internet, or attached to internal networks, are potentially at risk from attacks that often target vulnerable or unprotected systems. EDR is an essential part of the overall defense. It should be deployed to all managed systems in order to identify anomalous or malicious activity, reveal the tactics and techniques of advanced attacks and provide a means to respond to them.

Business Impact

- EDR is a must-have layer of protection for all industry sectors and should be applied to all devices and servers that connect to a network or handle corporate data.
- Early detection and rapid response are now vital, as prevention alone is not a viable way to approach contemporary threats and exploits.
- EDR is often stipulated as a mandatory security control in both internal and external policy.
- EDR provides the last means of defense when other layers fail to stop an exploit.

Drivers

- The nature of threats has changed. It is no longer practical to achieve 100% prevention and protection, and older EPP tools should be updated to have EDR functionality. Stealthy and state-sponsored adversaries, as seen in recent supply chain attacks, use advanced techniques to remain undetected and to bypass security controls.
- Remote work has accelerated the adoption of cloud-managed offerings, which now represent 60% of the install base and 95% of all new deployments.
- Fileless attacks are now a common component of all malware types, making the behavioral protection of EDR tools a critical capability to combat both advanced threats and an increasingly capable range of human-operated Ransomware campaigns.
- Advanced adversaries targeting an organization have shown they can disable protection solutions, making anti-tamper protection a critical facility. Comprehensive alerting and telemetry to facilitate early detection and fast response are also needed.
- As threats may target any system, EDR should now be a mandatory critical capability in the overall set of layered endpoint security controls, deployed to all managed endpoints and servers.
- The ability to rapidly respond in real time as incidents unfold is critical to containing the threat and stopping it from spreading.
- Augmenting existing vulnerability management programs and providing a means to reduce the attack surface is increasingly needed to ensure systems are not misconfigured and have no unpatched vulnerabilities.
- The collection of logs and events from EDR agents can also be used for retrospective threat detection and threat hunting.
- EDR tools often add the ability to manage adjacent risks such as the encryption of storage media, control of applications and internet activity.
- The increased stealth of advanced threats, human operated ransomware and state sponsored attacks, requires a new breed of security tools that work holistically together across all of the control areas of a complex attack.

Obstacles

- Adding detection and response features is now considered mainstream, though many organizations still lack the skills to use them.

- EDR adoption must be accompanied by investment in training responders, including “range” training that simulates real attacks.
- Organizations with few skilled staff should opt for managed detection and response services that provide monitoring, alerting and often triaging of alerts.
- Early definition-based agents needed frequent updates and used considerable amounts of system resources, leading to distrust of endpoint agents.
- Cloud-hosted workloads often have radically different “agile” deployment pipelines that preclude the use of traditional endpoint security tools. This usually results in a split environment, using separate tools for agile deployed workloads.
- Feature parity is not guaranteed for non-Windows systems. Consequently, endpoint security solutions for these systems lack the full EDR range of detection and response facilities.

User Recommendations

- Identify a single lightweight agent with remote deployment and low maintenance.
- Prefer cloud-hosted EDR solutions with faster time to value and vendors that provide automated processes.
- Target vendors that provide managed services themselves, including alerting, monitoring, incident response and managed detection and response.
- Favor vendors that can remove vulnerabilities and harden the endpoint against attack. They should provide direct access to endpoints to rapidly respond to issues.
- Look for third-party integrations with the ability to reuse existing investments like ITSM, authentication and threat intelligence.
- Specify tools with anti-tamper to ensure that agents are not disabled by attackers.
- Ensure data retention is adequate, uses archiving for cheaper storage and sends events and alerts to other security tools for longer retention.
- Seek ways to augment the solution with other security telemetry sources and integrated actions between tools, as provided by XDR systems.

Sample Vendors

Bitdefender; Cisco; CrowdStrike; Cybereason; FireEye; Microsoft; Palo Alto Networks; SentinelOne; Trend Micro; VMware Carbon Black

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

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

Hardware-Based Security

Analysis By: Neil MacDonald, Tony Harvey

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Hardware-based security uses chip-level techniques for the protection of critical security controls and processes in host systems independent of OS integrity. Typical control isolation includes encryption key handling, secrets protection, secure I/O, process isolation/monitoring and encrypted memory handling.

Why This Is Important

Adoption is increasing as hardware-based isolation capabilities are becoming standard in most hardware devices and cloud-based IaaS offerings, including emerging confidential computing offerings. These approaches strongly isolate parts of the system (and typically its security controls) from a breach of the application or OS. Interest in strong isolation techniques is rising in the face of ongoing disclosures of new types of side-channel attacks and requirements for cloud and data sovereignty.

Business Impact

If an OS is compromised, its security controls can be disabled and sensitive data in memory stolen; hardware-based security can prevent this. Hardware-based security can significantly reduce attack surfaces across computing devices, but these capabilities require support from operating system software and system management software. Upgrading to more recent versions of software and cloud providers, which use hardware-based security features, can materially increase system security.

Drivers

- The desire to extend trust from the hardware level of a system through the OS to applications and workloads, including containers that run above it. This root of trust needs a strong foundation in hardware.
- Software-based isolation of security controls is inevitably fallible and will be attacked, increasing interest in protection approaches rooted in hardware.
- The desire to use IaaS providers in potentially hostile parts of the world and protect these workloads from OS compromise or virtual machine and memory snapshotting is increasing.
- Most hardware platforms for servers and mobile devices, including Android and iOS devices, now include hardware-based isolation capabilities.
- Requirements for data sovereignty enabled by public cloud confidential computing offerings are driving demand for isolation approaches rooted in hardware.

Obstacles

- In public clouds, enterprises don't have access to the underlying hardware and must rely on hardware-based attestations provided by the CSP.
- Approaches to hardware-based confidential computing vary across microprocessor vendors, complicating application deployment using these techniques. No single approach covers all use cases. Abstraction layers, such as Asylo, may help but add another layer of complexity and are not widely adopted.
- Hardware-based security is strong, but may potentially still be broken by software flaws or side-channel attacks such as Spectre and Meltdown.

User Recommendations

- Patch and remain vigilant for unexpected breaches. For systems under direct enterprise control, implement a BIOS-level patching strategy to deal with exposures that require BIOS-level remediation.

- Make strong isolation of sensitive code and security controls a mandatory part of IT systems procurement, including IaaS.

- Evaluate the need for confidential computing capabilities only for the most critical applications in systems that move to public cloud infrastructure, to protect sensitive operations such as key management and sensitive intellectual property.

- Check for compatibility issues with third-party approaches that also use virtualization techniques, before activating Windows 10 virtualization-based security.

- Explore the use of hypervisor-based approaches with security rooted in hardware virtualization techniques as another way to achieve similar levels of strong isolation.

- Plan different strategies for different devices and server platforms as none of these mechanisms are interoperable.

Sample Vendors

Amazon Web Services (AWS); AMD; Apple; Bitdefender; Fortanix; Google; Hysolate; Intel; Microsoft; Samsung Electronics

Gartner Recommended Reading

Market Guide for Cloud Workload Protection Platforms

How to Make Cloud More Secure Than Your Own Data Center

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

Security Leaders Need to Do Seven Things to Deal With Spectre/Meltdown

SIEM

Analysis By: Kelly Kavanagh, Mitchell Schneider

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Security information and event management (SIEM) technology supports threat detection, security incident management and compliance through collection and analysis of security telemetry, as well as a wide variety of other contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze data across disparate sources, and operational capabilities such as incident management and response, dashboards and reporting.

Why This Is Important

Early detection of, and timely response to, security threats is a core element of effective security programs. SIEM supports an organization's ability to monitor security logs, alerts and other events to detect threats, prioritize and investigate them, and execute responses.

Business Impact

SIEM solutions improve an organization's ability to detect attacks, and improve incident investigation and response capabilities. However, they require an ongoing investment in resources (budget, expertise and staffing) for both technology operations and security event monitoring to realize their true value. SIEM tools also support other use cases (such as the reporting needs of organizations with regulatory compliance obligations, as well as those subject to internal and external audits).

Drivers

- Detection of, and early response to, threats from targeted and broad-based attacks is the primary driver for purchasing SIEM technologies. SIEM products have existed for a long time, but continue to evolve to address changing threats. These threats lie across a growing range of environments (SaaS, IaaS, OT and IoT), increases in the volume, velocity and variety of data sources, and increasingly constrained security resources and expertise.
- Modern SIEM solutions use a variety of techniques, including correlation, statistical analysis and machine learning to identify threats and other events of interest. Organizations are increasingly bringing infrastructure as a service (IaaS) and SaaS environments into the scope of monitoring via SIEM.
- OT and IoT environments represent challenges to monitoring with SIEM products, with a number of vendors developing native capabilities or partnerships with OT technology providers to enable coverage. SIEM vendors are introducing more advanced incident response capabilities natively or via integration with security orchestration, automation and response (SOAR) products.
- Buyers are increasingly seeking cloud SIEM offerings, although traditional on-premises deployment of SIEM is still relevant in cases where cloud options are not appropriate. The combination of new demands of SIEM products and the capabilities evolving to meet them keeps this mature market just off the Plateau of Productivity.

Obstacles

- Organizations may be challenged by requirements for SIEM platform management and for ongoing operations.
- Users must ensure the SIEM is configured to support the workloads required for data ingestion, management and analysis, and that the detection content, context feeds, dashboards, reports and response actions are configured correctly to meet the required use cases.
- Organizations can reduce this support effort by using SaaS or managed SIEM services.

User Recommendations

- Define use cases to establish the requirements for log management, user/entity monitoring, detection analytics, incident response management, and compliance reporting. It may be necessary that the SIEM tool has access to additional business context (such as user directories, configuration management databases and vulnerability assessment products).
- Document the network and system topologies, on-premises and in-cloud infrastructure, and where security controls are deployed. Estimates of log volume and event rate, and the number of log/data sources, should be documented for the initial use cases, and for those planned for the next 12 to 24 months.
- Plan to administer detection and response content in the SIEM and consider whether they require 24/7 monitoring.
- Evaluate cloud SIEM to reduce the effort needed to deploy and manage the SIEM platform.

Sample Vendors

Elastic; Exabeam; IBM; LogRhythm; Micro Focus; Microsoft; NetWitness; Rapid7; Securonix; Splunk

Gartner Recommended Reading

Magic Quadrant for Security Information and Event ManagementCritical Capabilities for Security Information and Event Management

Questions to Answer Before Adopting Cloud SIEM Solutions

CASBs

Analysis By: Craig Lawson, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud access security brokers (CASBs) provide crucial cloud governance controls for visibility, compliance, data security and threat protection by consolidating multiple types of security policy enforcement into one place for SaaS, IaaS and PaaS. Examples include authorization, UEBA, adaptive access control, DLP, device profiling, object encryption, tokenization, logging, alerting and malware removal. Majority of CASB deployments are cloud-based; on-premises deployments are rare.

Why This Is Important

CASBs are critical for organizations to secure usage of business-critical cloud services. The four key areas — visibility, compliance, data security and threat protection — are the primary value propositions for the usage of CASBs.

Business Impact

CASBs enable consistent security policies and governance across cloud services. Unlike traditional security products, CASBs are designed to protect data stored in someone else's systems, are suitable for organizations of all sizes in all industries and can demonstrate cloud usage is well-governed. With continued feature expansion, ongoing convergence with SWG/ZTNA and relative ease of switching providers, favor one-year contract terms over lengthier ones when selecting CASBs.

Drivers

- End-user organizations need to secure use of business-critical, cloud-delivered applications and infrastructure; secure general internet to prevent threats to users, regardless of their location; and improve access to existing services while taking advantage of zero trust concepts. Today, CASB is converging with SWG and ZTNA to deliver this “three-legged stool” concept to support all these use cases.
- With SWG vendors enabling secure use of business-critical, cloud applications and infrastructure, and CASB vendors expanding functionality for general internet security and access to existing services, security leaders are now able to successfully deliver on the above-mentioned three capabilities from an increasing number of vendors providing all three.
- The COVID-19 pandemic has increased focus on two specific use cases that CASB technology directly helps with: the huge shift to remote working and the continuously increasing use of cloud services critical to business.

Obstacles

- Lack of a focus on DLP can lead to frustration with a CASB as organizations fail to build comprehensive policies and manage false-positive rates.
- A subset of controls are offered by CSPs themselves, for example, Office 365's native security features and Salesforce Shield.
- Unclear organizational ownership of SaaS tenancy leads to a CASB implementation that fails to secure the SaaS adequately.
- Product consolidation failure in organizations where multiple CASBs exist through expanded licensing agreements.
- Overlapping CASB functionality from a number of vendors leads to duplication and confusion.

User Recommendations

- Examine vendor capabilities in four functionality areas: visibility, data protection, threat detection and compliance (see Magic Quadrant for Cloud Access Security Brokers for a more detailed analysis of these capabilities).
- Seek support for multiple modes of operation, namely forward proxy, reverse proxy (or RBI) and API for the best support of managed and unmanaged devices and cloud services via CASB.
- Aim to move to a single provider for CASB, SWG and ZTNA as these services are on strong convergence paths.

Sample Vendors

Bitglass; Broadcom (Symantec); Lookout (CipherCloud); McAfee; Microsoft; Netskope; Proofpoint

Gartner Recommended Reading

Magic Quadrant for Cloud Access Security Brokers

Critical Capabilities for Cloud Access Security Brokers

Magic Quadrant for Secure Web Gateways

2021 Strategic Roadmap for SASE Convergence

Market Guide for Zero Trust Network Access

Entering the Plateau

Vulnerability Assessment

Analysis By: Mitchell Schneider

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Vulnerability assessment (VA) solutions and services operate across on-premises, cloud or virtual environments. They discover, identify and report on IT, cloud, IoT and/or OT devices, operating systems, and software vulnerabilities; establish a baseline of connected assets and vulnerabilities; identify and report on security configuration of IT assets; and support compliance reporting and control frameworks, risk assessment and remediation prioritization, and remediation activities.

Why This Is Important

VA is a foundational component of the vulnerability management (VM) process, supporting security management and conformity with regulations and compliance regimes. Furthermore, vulnerability assessment is a key process in understanding and dealing with the organization's attack surface available to threat actors, which helps reduce the risk to IT and the organization.

Business Impact

- Weaknesses in infrastructure, systems and other assets will be abused by attackers for malicious purposes. This can lead to attacks like ransomware and data breaches.

- Many regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) 27001, require organizations to perform vulnerability assessments to remain in compliance and protect their assets.

Drivers

The VA market is mature; however, advancement and innovation continue to be applied in VA tools and services in the areas of discovery, prioritization and remediation/mitigation (e.g., tracking vulnerability remediation progress and workflow automation) to meet buyers' evolving requirements and needs.

Although compliance use cases are still strong drivers for leveraging VA tools, many organizations are implementing these solutions to help reduce risk and exposure, as well as improve and strengthen their overall security posture.

Depending on their maturity level, organizations typically pick one of the three delivery models for VA:

- Buying and deploying the tool/product, and operating it with internal staff. VA application and network scanners are both deployed on-premises. SaaS (cloud)-delivered VA products with network scanners are deployed on-premises in the enterprise network.
- Buying and deploying the tool, then having it operated by a third party such as a managed security service provider (MSSP) or managed detection and response (MDR) service provider.
- Outsourcing to a third party that provides managed vulnerability management services and uses its own proprietary technology or licensed commercial tool(s).

Obstacles

- VA solutions are relatively easy to implement; yet, they require resources and expertise that an organization may not have. Therefore, outsourcing VM to a security service provider might be an option. Also, risk-based prioritization of vulnerabilities is still not the norm for many VM programs as the tools are still maturing to improve this capability.
- The VA market is fragmented and characterized by a number of pure-play along with other vendors/providers from various security markets offering VA as part of their overall product/service portfolio. VA used to be simple, with a big scanner deployment covering the entire environment. But now things are different. Organizations may have one thing for their cloud systems (e.g., cloud security posture management), another for containers, the traditional scanner for the data center, a solution to assess OT assets and technologies, and their endpoint detection and response (EDR) tool providing VA capabilities for their end-user systems.

User Recommendations

- Evaluate vendors offering a combined solution, if your organization is resource-constrained or wants to consolidate vendors. More VA vendors are adding prioritization capabilities to their products — either complementary or through an add-on module.

- Evaluate and distinguish between the various deployment options and models available in the VA market, and understand how the technology fits the organization's requirements. Network scanning involves remote scans of network-connected devices, but will not work when devices are shut off. Agent-based scanning assists with getting vulnerability data from assets that are not always connected to the enterprise network. API-based scanning is often delivered from the cloud, but does not preclude scanning from on-premises appliances or software.

- Evaluate VA vendors that have strong built-in integrations with patch management and IT service management tools, which are aimed at streamlining the treatment process and closing the loop more effectively.

Sample Vendors

Balbix; F-Secure; Greenbone Networks; HelpSystems (Digital Defense); Microsoft; Outpost24; Qualys; Rapid7; Tenable; Tripwire

Gartner Recommended Reading

Market Guide for Vulnerability Assessment

A Guide to Choosing a Vulnerability Assessment Solution

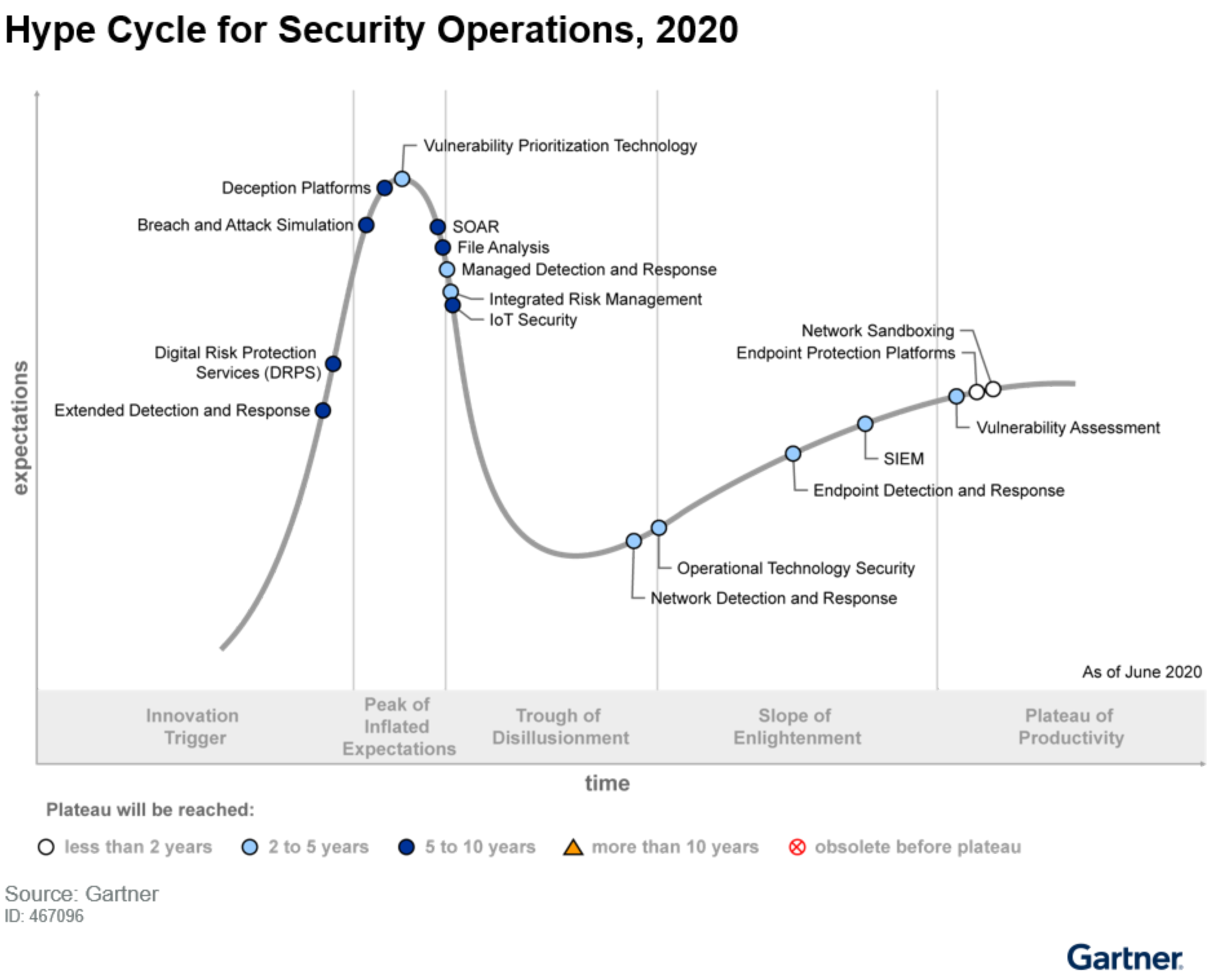
Toolkit: RFP for Vulnerability Assessment Tools

Solution Comparison for SaaS-Based Vulnerability Assessment Tools

Midsize Enterprises Must Prioritize to Achieve Effective Vulnerability Management

Appendixes

Figure 2: Hype Cycle for Security Operations, 2020

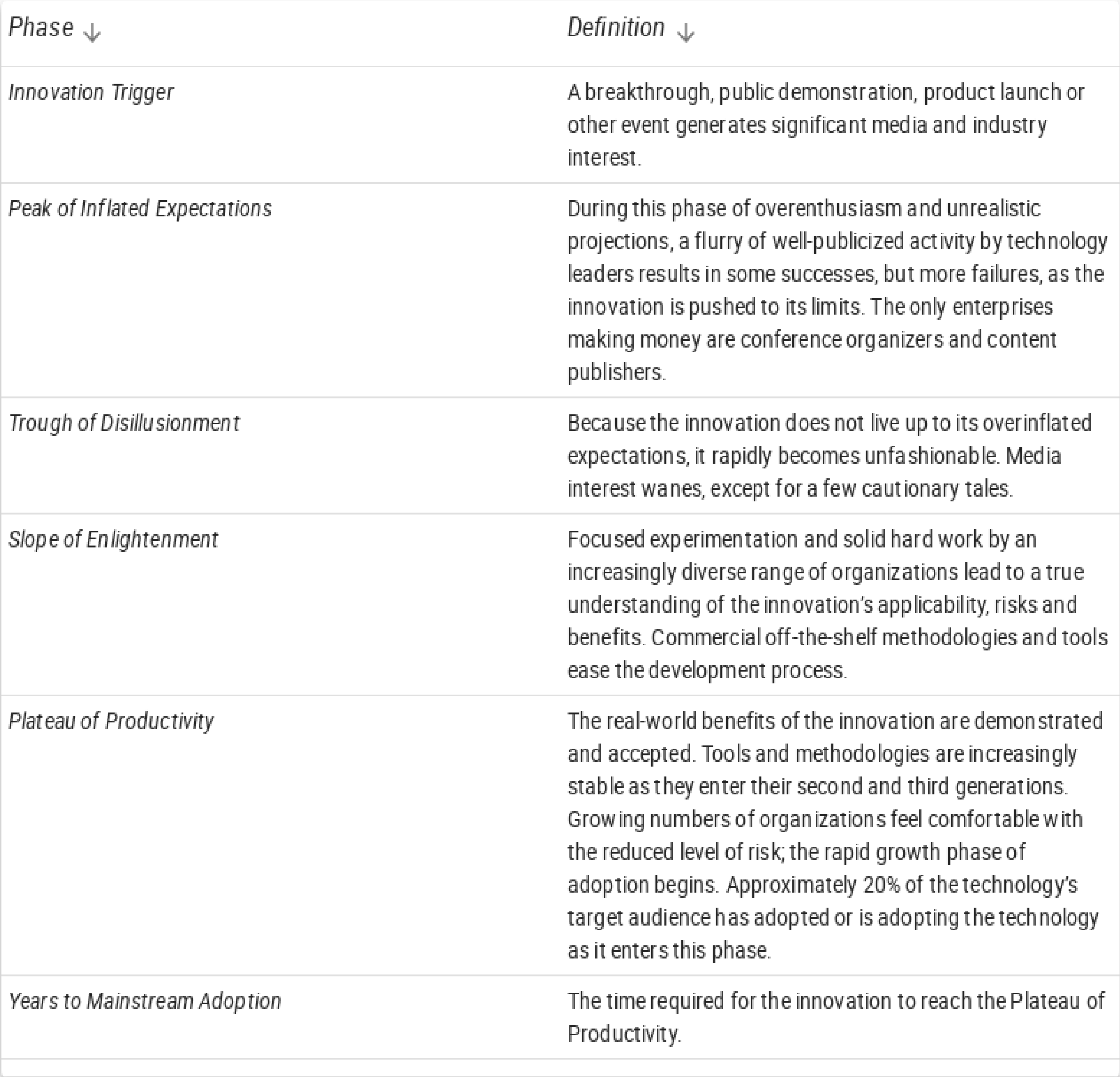


Source: Gartner
ID: 467096

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)



Phase ↓	Definition ↓
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2021)

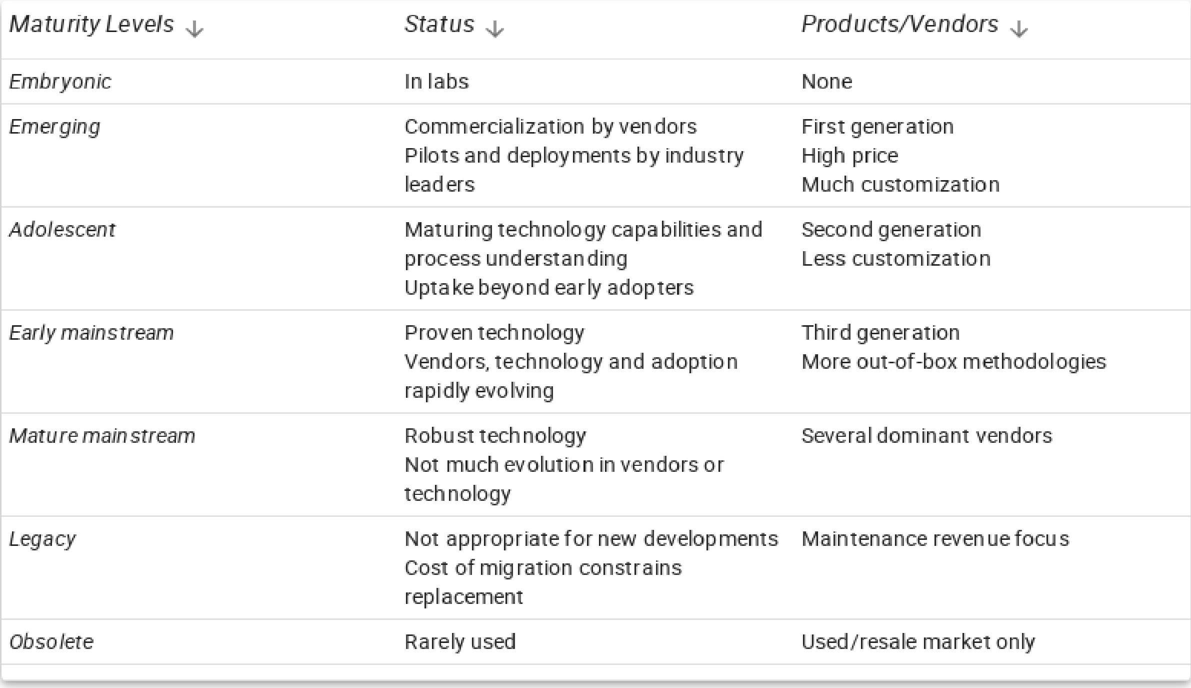
Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2021)

Table 4: Maturity Levels

(Enlarged table in Appendix)



Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2021)

Document Revision History

Hype Cycle for Security Operations, 2020 - 23 June 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner’s Hype Cycles

Create Your Own Hype Cycle With Gartner’s Hype Cycle Builder

Emerging Technologies: Top Trends in Security for 2021

Security Operations Primer for 2021

Top Security and Risk Management Trends 2021

SOC Development Roadmap

Cool Vendors in Security Operations and Threat Intelligence, 2H20

General Manager Outlook: Information Security Spending, 2Q21

Table 1: Priority Matrix for Security Operations, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	CASBs	Integrated Risk Management		
High	Endpoint Detection and Response Vulnerability Assessment	Deception Platforms DRPS MDR Services NDR OT Security VPT	Breach and Attack Simulation SOAR XDR	
Moderate		Hardware-Based Security SIEM TI Services	Autonomous Penetration Testing and Red Teaming CAASM External Attack Surface Management File Analysis Pen Testing as a Service	
Low				

Source: Gartner (July 2021)

Table 2: Hype Cycle Phases

Phase ↓	*Definition* ↓
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase	*Definition*

Source: Gartner (July 2021)

Table 3: Benefit Ratings

Benefit Rating	*Definition*
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2021)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2021)