Emerging Tech Impact Radar: Security

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

Product leaders can incorporate the emerging technologies discussed here to optimize opportunities coming from organizations’ need to secure new environments, protect against the expanded attack surface, consume security capabilities in new ways and create better efficiencies through automation.

Overview

Key Findings

- Public cloud adoption is driving the implementation of new security technologies that better cater to the protection requirements that many traditional security controls fail to match when it comes to securing cloud computing.
- New technologies and business initiatives (such as SaaS applications), new ways to generate revenue, operational technology (OT), Internet of Things (IoT), cyber-physical systems (CPS) and supply chain touchpoints pose new threats. Many emerging technologies are aimed at helping organizations manage a growing attack surface due to their technological environments becoming increasingly complex and dispersed, both on-premises and in the cloud.
- Advanced attackers are increasingly attacking and attempting to exploit the identity system. Identity access management (IAM) programs and technologies are evolving not just to focus on authentication, authorization and ensuring rightsize access while enhancing the user experience, but also to secure the identity system itself.

- A cybersecurity mesh architecture (CSMA) creates and leverages interoperable connections between stand-alone security tools to promote composability and a consistent security posture. Emerging technologies such as extended detection and response (XDR), secure access service edge (SASE), composable security, and low-code/no-code security frameworks represent a trend toward security product consolidation and the cybersecurity mesh.
- Not all emerging opportunities come from new technologies. Some opportunities will come from delivering existing technologies in a new way. Examples include deception as a feature and vendor-delivered service wrappers (VDSWs).
- The shortage of skilled security practitioners will continue to drive an increased appetite for automation within the security operations field, and artificial intelligence (AI) will be strongly leveraged across a range of products to deliver enhanced security outcomes at greater speed.

Recommendations

Product leaders seeking to leverage the impact of emerging technologies and trends on products and services:

- Meet evolving customer needs by developing specialized features that align closely to new edge computing, cloud computing and remote working requirements. Here, solutions offering more dynamic deployment models, integrations and product architectures are increasingly preferred over traditional controls.
- Assess your product roadmap, integrations and partnerships, and focus on developing more comprehensive offerings that support continuous threat and exposure management. This can span across threat intelligence, digital risk protection services (DRPS), external attack surface management (EASM) and cyber asset attack surface management (CAASM).
- Bolster your solutions for emerging categories such as XDR, identity threat detection and response (ITDR), endpoint detection and response (EDR), and Active

Directory (AD) audit by developing capabilities spanning AD security requirements, prioritizing monitoring, detection and response.

- Develop modularity of controls by implementing concrete architectural frameworks such as API-first architecture or out-of-the-box integrations that enable integrations with heterogeneous environments.
- Develop cloud-native components as scalable modules to increase your agility and efficiency. Continued innovation and investment by other SASE vendors will require the agility and efficiency that can be delivered only from a cloud-native architecture to remain competitive.
- Comprehensively or progressively embrace AI and machine learning (ML) for security operations technologies by prioritizing the development of risk-based processes for threat detection, investigations and response. Then codify those procedures into automation playbooks for increased efficiency gains.

Analysis

Overview

- This Impact Radar aims to track some of the more impactful emerging technologies and trends driving innovation in the security market. Gartner identified six central themes across the 27 emerging technologies and trends included in this year' s security Impact Radar:
- Securing cloud service usage — Gartner predicts that, by 2023, 70% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 40% in 2020. Therefore, it is not surprising to see that many emerging technologies in security are focused on supporting organizations in their effort to improve the security of their cloud service usage. SaaS security posture management (SSPM), SaaS ecosystem security, cloud infrastructure entitlement management (CIEM), cloud-native application protection platform (CNAPP) are emerging technologies in cloud security.

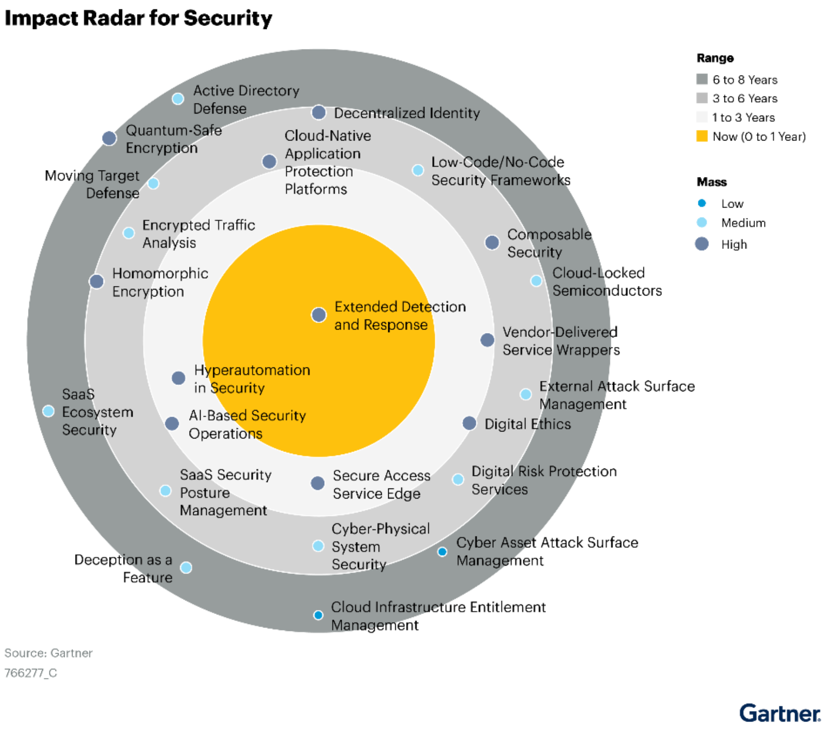
- Attack surface expansion — Organizations are tasked with managing a growing attack surface due to their technological environments becoming increasingly complex and dispersed, both on-premises and in the cloud. New technologies and business initiatives (such as SaaS applications), new ways to generate revenue, OT, IoT, CPS and supply chain touchpoints pose new threats. DRPS, CAASM, EASM and CPS security (CPS-Sec) are emerging technologies that help address the expanding attack surface.
- Identity as a new perimeter — The IAM efforts of organizations have been focused on authentication, authorization and ensuring rightsize access while enhancing the user experience. However, the security of the underlying IAM architecture itself has become a lower security priority in most organizations. Advanced attackers are increasingly attacking and attempting to exploit the identity system. Emerging technologies and trends protecting this “new perimeter” include ITDR, AD defense and decentralized identity (DCI).
- New approaches to security — The cybersecurity mesh architecture concept is evolving and gaining popularity. This is because existing approaches to security and identity architectures are siloed and work in isolation, making zero trust architecture challenging. A CSMA creates and leverages interoperable connections between stand-alone security tools to promote composability and a consistent security posture. Emerging technologies and trends representative of the trend toward security product consolidation and the cybersecurity mesh include XDR, SASE, composable security and low-code/no-code security frameworks.
- Same technology, new delivery model — Some emerging technologies are not necessarily new, but technology providers are delivering them in a new way. Examples include deception as a feature, which integrates deception technology into existing platforms, such as firewalls, network detection and response (NDR), EDR, XDR and ITDR. Other examples are VDSWs and many cloud-delivered technologies.
- Security automation — The shortage of skilled security practitioners will continue to drive an increased appetite for automation within the security operations field. AI will be strongly leveraged across a range of products to deliver enhanced security

outcomes at greater speed. This year’ s security Impact Radar will continue to explore hyperautomation in security and AI-based security operations.

The Impact Radar

Figure 1 shows the highest-impact security-related emerging technologies and trends based on range and mass.

Figure 1: Impact Radar for Security


Impact Radar for Security
Range
▨ 6 to 8 Years
▨ 3 to 6 Years
□ 1 to 3 Years
🟨 Now (0 to 1 Year)
Mass
● Low
● Medium
● High
Active Directory Defense
Decentralized Identity
Quantum-Safe Encryption
Cloud-Native Application Protection Platforms
Low-Code/No-Code Security Frameworks
Moving Target Defense
Encrypted Traffic Analysis
Composable Security
Cloud-Locked Semiconductors
Homomorphic Encryption
Extended Detection and Response
Vendor-Delivered Service Wrappers
Hyperautomation in Security
External Attack Surface Management
SaaS Ecosystem Security
AI-Based Security Operations
Digital Ethics
SaaS Security Posture Management
Secure Access Service Edge
Digital Risk Protection Services
Cyber-Physical System Security
Cyber Asset Attack Surface Management
Deception as a Feature
Cloud Infrastructure Entitlement Management
Gartner

Source: Gartner
766277_C

The objective of this research is to guide product leaders on how emerging technologies and trends are evolving and impacting areas of interest. Providers can leverage this knowledge to determine which technologies or trends are most important to the success of their business and when it makes sense to advance their products and services by investing in them.

Emerging Technologies or Trend Profiles

Table 1 lists emerging technologies and trends in security according to their time to adoption. Click on a technology name in the table to jump to a profile of the technology.

Table 1: Emerging Technologies and Trends in Security Based on Time to Adoption

Now Range	1 to 3 Years	3 to 6 Years	6 to 8 Years
Extended Detection and Response	AI-Based Security Operations	Cloud-Locked Semiconductors	Active Directory Defense
	Digital Ethics	Cloud-Native Application Protection Platforms	Cloud Infrastructure Entitlement Management
	Hyperautomation in Security	Composable Security	Cyber Asset Attack Surface Management
	Secure Access Service Edge	Cyber-Physical System Security	Deception as a Feature
	Vendor-Delivered Service Wrappers	Decentralized Identity	Quantum-Safe Encryption
		Digital Risk Protection Services	SaaS Ecosystem Security
		Encrypted Traffic Analysis	

	External Attack Surface Management
	Homomorphic Encryption
	Low-Code/No-Code Security Frameworks
	Moving Target Defense
	SaaS Security Posture Management

In addition to the technologies in Table 1, there are several longer-range technologies that product leaders should track and be prepared to make early investments in so as to be ready to utilize them when they come to maturity. These include:

- Device Identity (Machine-to-Machine)
- Identity Threat Detection and Response
- Wireless Network Security

Now Range

Extended Detection and Response

Back to Top

Analysis by: Dave Messett and Carl Manion

Description: Extended detection and response (XDR) is a threat detection investigation and response (TDIR) platform that integrates, correlates and contextualizes data and alerts from multiple security prevention, detection and response components. Primary functions include:

- Centralization and normalization of security event telemetry data in a cloud-based repository for analysis
- Orchestration and integration of security alerts, security telemetry and threat intelligence into incidents
- Improved protection, and detection and response efficiency resulting from a converged solution from a simplified configuration, and security product coordination

The TDIR capability should be able to change the state of individual security products as part of the remediation process.
Initially, XDR was often achieved through the vertical integration of an individual vendor's solution portfolio. However, increasingly, the vendors in this space are partnering with third-party vendors to offer a more heterogeneous stack. Their goal is either to supplement the multiple components they have as an "anchor vendor," or in some cases, to provide a significant majority of the overall solution. These vendors leverage API integrations of disparate solutions and an "Open XDR" architecture to ingest alerts and telemetry data from a wide variety of sources for analysis and response. These sources span endpoints, servers, networks and cloud environments. The response can be automated by initiating two-way actions between tools. In most instances, managed detection and response (MDR) services are sold as part of the overall solution either by the technology provider itself or in partnership with managed security service providers (MSSPs). Given the complexity of a typical XDR deployment and the scarcity of skilled resources in many organizations, this is an essential part of solution delivery.

Sample Vendors: Broadcom (Symantec), Cisco, Confluera, CrowdStrike, Cybereason, Cynet, Elastic, Exabeam, Fidelis Cybersecurity, Fortinet, Gurucul, Heimdal Security, Hunters, IBM, Microsoft, Netsurion, Palo Alto Networks, Qualys, Rapid7, Red Piranha, ReliaQuest, Secureworks, Securonix, SentinelOne, Sophos, Splunk, Stellar Cyber, TEHTRIS, Trend Micro, Trellix and Veryx

Range: 0 to 1 Year

Gartner considers XDR to be a short-range technology that will gain rapid adoption and acceptance in the market, enabling lower-maturity organizations to deliver integrated threat detection and response capabilities. Despite overly enthusiastic marketing from some security companies, significant investment in XDR technology is being demonstrated by many major security vendors traditionally known for delivering security platforms, EDR, network detection and control capabilities, and security information and event management (SIEM). In many cases, this investment can be demonstrated by their organic development; however, there have also been multiple acquisitions in this space as vendors seek to build a portfolio of adjacent technologies. Gartner is also seeing significantly increased interest and deployments from early adopters, with many EDR-oriented conversations incorporating XDR as an additional topic of discussion.

The use cases, such as detection of threats in the user workspace and correlation of threat telemetry across multiple domains, which are addressed by XDR align closely to some major challenges faced by customers. As such, XDR delivers against key business criteria demanded by organizations looking to enhance protection and detection efficiency. The increasing volume and sophistication of attacks drive the need to triage alerts faster and with more confidence, identify and consolidate weak signals into strong detections, quickly gather additional contextual data, and take appropriate actions at speed. This in turn demands either additional skilled resources or improved integration and automation of security tools. The lack of skilled resources is a wellknown problem, and organizations are looking for solutions that can automatically contextualize incidents, provide suggested actions and improve productivity of existing resources frequently using automated playbooks. For this reason, XDR is expected to be the solution of choice for smaller, less-sophisticated security teams — ahead of more complex solutions, such as SIEM and security orchestration, automation and response (SOAR), that more sophisticated teams may opt for.

Mass: High

Mass is high because of increasing focus on detection and response capabilities, the desire to improve visibility into attacks across the entire security infrastructure, and a more general trend for vendor consolidation. It is worth noting that reduced spending on detection and response is only rarely an important factor in the decision to use XDR technology.

The vast majority of interest continues to derive from low- to medium-maturity security organizations and in almost all cases is combined with a need to leverage managed security services (MSS) or MDR to deliver XDR functionality. More-mature organizations may also choose to outsource all or part of the XDR implementation and ongoing management but have the additional option of integrating XDR technology into their existing security stack.

Expanding integration capabilities will further drive adoption by opening up the potential of an integrated security stack and enhanced detection and response capability to organizations that:

- Have traditionally adopted a best-of-breed purchasing approach that was poorly integrated
- Wish to consolidate an existing infrastructure made up of solutions from a variety of vendors

XDR is evolving as vendors converge XDR offerings with previously separate point solutions, encompassing everything from single-vendor ecosystems to more open solutions, with components being delivered by a selection of vendors with prebuilt integrations. As such, the ability to deliver the benefits of XDR without the need to overhaul and replace existing solutions removes a significant barrier for adoption and avoids tie-in to a single vendor.
Recommended Actions:

- Drive deep, Blueprint integrations across your portfolio and beyond, including key security solutions from competitors in key areas such as identity, email, network and cloud.
- Work with product marketing managers to effectively articulate the value of moving up the cyber kill chain — identifying, blocking and containing malicious activity earlier in the attack cycle.
- Enhance automation capabilities to support faster, more accurate alert triage and detection, and to enable coordinated response and remediation via automated playbooks.

Recommended Reading:

- Market Guide for Extended Detection and Response
- Hype Cycle for Security Operations, 2022
- Hype Cycle for Endpoint Security, 2022

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