Hype Cycle for Endpoint Security, 2022

Published 19 December 2022 - ID G00771607 - 84 min read

By Analyst(s): Franz Hinner

Initiatives: Infrastructure Security

> Security and risk leaders must prepare to select next-wave technology to continue to protect endpoints from attacks and breaches. EDR remains a mainstream technology, while XDR advances adoption of new use cases and technologies such as UES, DaaS, ASA/ASM, BAS, EM and ITDR.

Analysis

What You Need to Know

This Hype Cycle illustrates the most relevant innovations in the endpoint security space for security leaders to adopt and put in place to address these challenges. Endpoint security innovators have focused on better and more automated prevention, detection and remediation of threats, moving toward extended detection and response (XDR) to correlate data points and telemetry from solutions such as endpoint, network, web, email and identity. With the transition from remote to hybrid work, secure remote access continues to be a priority. Devices not company-owned still drive desktop as a service and secure enterprise browser adoption for increased control and security posture. We see continued adoption of zero trust network access (ZTNA) to opt for security service edge (SSE) and secure access service edge (SASE), enabling application access from any device over any network, with minimal impact on user experience.

The Hype Cycle

The Endpoint Security Hype Cycles' goal is to track the innovations that aid security leaders in protecting their enterprise from attacks and breaches. With evolving techniques and technologies, two trends emerge:

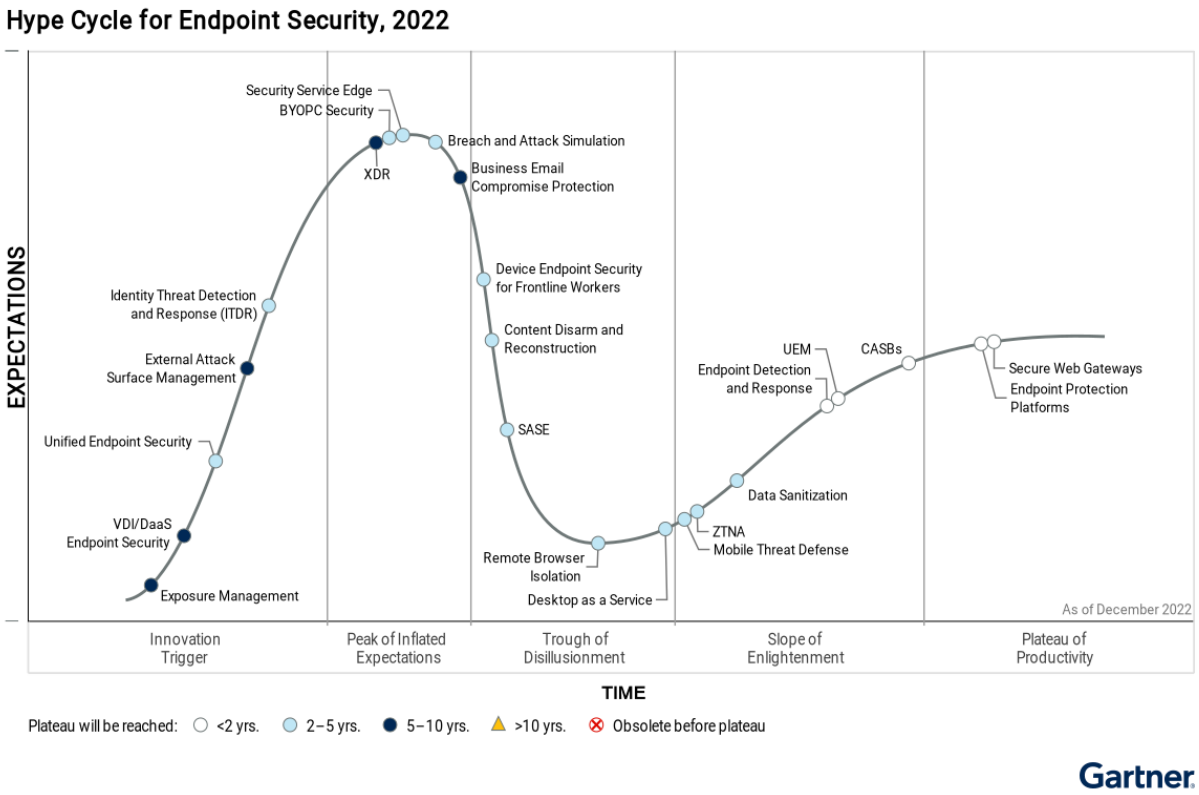
- An increase in the complexity and number of endpoint attacks
- A continuation of remote working becoming mainstream

Ransomware is still top of mind, while fileless and phishing attacks emerge as favorite attack vectors. To counter advanced targeted attacks, it becomes crucial to correlate data from the endpoint and elsewhere when threat hunting. For a second time, XDR emerges in the Hype Cycle with signs of becoming mainstream. The more recent concept of unified endpoint security (UES) is advancing in the Hype Cycle; it combines elements of endpoint detection and response (EDR), endpoint protection platforms (EPP) and mobile threat defense (MTD). While EPP has reached full maturity, EDR continues to grow in adoption. Business email compromise (BEC) continues to be a significant threat, and BEC protection capabilities are continuing to innovate to detect compromised accounts this year to counter phishing attacks. In addition, a secure web gateway (SWG), a network-based technology, is central to preventing attacks on endpoints and is being increasingly adopted by organizations, especially in its cloud-based implementation.

With remote work morphing into hybrid, practices and technologies enable and secure the remote and hybrid workforce. Many new capabilities have reached their full maturity and adoption becoming mainstream.

Many tactical solutions transform into leading-edge services, these include cloud access security broker (CASB), bring your own PC (BYOPC), unified endpoint management (UEM) and desktop as a service (DaaS). A significant portion of that remote work will continue long-term, and much of it already leads to continuous strategic solutions. For example ZTNA and its role in empowering SSE, facilitating access from any device to any application over any network. ZTNA and SASE are gaining adoption as they mature, though at different rates for each.

Figure 1: Hype Cycle for Endpoint Security, 2022



Source: Gartner (December 2022)

The Priority Matrix

Wave of Technology

The Hype Cycle has seen a new wave of zero-trust edge solutions appearing. Most innovations heading toward the peak involve security for multiple channels or systems. For example, UES secures workstations, smartphones and tablets with a single product. Similarly, XDR's scope goes beyond the endpoint to combine information from multiple sources, such as the network, to detect threats. Security and risk managers are meeting the technology convergence trend with increased interest; in vendor consolidation, based on Gartner's Security Vendor Consolidation survey of April 2022.

Transformations Technology

Transformational innovation in the Hype Cycle shows new technologies and techniques that are yet to reach maturity. Gartner has seen the comprehensive implementation of SASE to allow access to any application across any network for any endpoint in a protected manner. Security leaders should start strategizing to align ZTNA and CASB to build a SASE foundation.

High-Impact and Relevant Technologies

With XDR's emergence, Gartner sees multiple business and technology use cases becoming more relevant to XDR endpoint concerns. These target use cases have the goal of detecting threats earlier through simulation of attacks that feature deceptive techniques. They advance attack scenarios by mapping attack surface assessment (ASA) and breach attack simulation (BAS), and they produce results linking detection, protection and response. They are proceeding to inventory them using attack surface management (ASM), without consuming all ASA, BAS, innovating new deceptive technology use cases, but only correlating the essential data to XDR telemetry. These technologies, combined with exposure management (EM), enable defenders to cross-correlate existing detection and attack behavior and teach machine learning and deep learning algorithms new techniques through constant behavior pattern improvement.

Table 1: Priority Matrix for Endpoint Security, 2022

(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	BYOPC Security SASE Security Service Edge		
High	Endpoint Detection and Response Secure Web Gateways UEM	Breach and Attack Simulation Content Disarm and Reconstruction Desktop as a Service Identity Threat Detection and Response (ITDR) Unified Endpoint Security	Business Email Compromise Protection Exposure Management XDR	
Moderate	Endpoint Protection Platforms	Data Sanitization Device Endpoint Security for Frontline Workers Mobile Threat Defense Remote Browser Isolation ZTNA	External Attack Surface Management VDI/DaaS Endpoint Security	
Low				

Source: Gartner (December 2022)

Off the Hype Cycle

- Secure Enterprise Data Communications: Solving remote access challenges solely with VPN infrastructure is a mature method for remote access and is well-understood. Secure enterprise data communications centered on VPN are moving off the Hype Cycle to indicate the rising role of ZTNA concepts and SASE tools. Implementation of these tools alongside — and often, in place of — existing VPN infrastructure to provide contextual, dynamic access controls for an increasingly diverse set of remote workers.

On the Rise

Exposure Management

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

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Exposure management (EM) is a set of processes and capabilities that allow enterprises to continually and consistently evaluate the visibility, accessibility and vulnerability of an enterprise's digital assets. EM is delivered using five stages: scoping, discovery, prioritization, validation and mobilization. Organizations building an EM program leverage tools to inventory assets and vulnerabilities, simulate or test attacks, as well as other forms of posture assessment process and technologies.

Why This Is Important

Security professionals that have responsibility for managing organizational risk have traditionally looked at vulnerability scanning and security controls to identify the level of exposure that infrastructure is subject to. The volume of effort required and the diversity of potential issues lead to conflicting priorities and "dashboard fatigue." SRM leaders struggle to prioritize risk reduction actions, leaving gaps where they feel they have less control, such as SaaS platforms and social media.

Business Impact

Exposure management is necessary to govern and prioritize risk reduction for the enterprise.

It requires to conduct three type of activities:

- Identify likelihood of exploitation (based on visibility on the attack surface),
- Inventory and categorize the exposure (vulnerability, threat intel-based, digital assets).
- Validate as to whether attacks will be successful and security controls can assist with detecting or preventing them.

Exposure management is a program, not the outcome of a specific tool.

Drivers

- Most commonly, organizations are siloing exposure activities such as penetration testing and vulnerability scanning. This siloed view provides little or no awareness of the complete situation regarding the effective risks the organization has.
- The volume of discovered vulnerabilities and issues that testing surfaces continues to grow with the complexity of environments, the increased volumes of applications used and the increased use of cloud services.
- Lack of classification and understanding of prioritization and risk, in line with high volumes of findings is leaving organizations with far too much to do regarding their exposure and little guidance on what to action first.
- A programmatic approach to a set of questions that in their entirety begin to answer the question “how exposed are we?” is necessary. Organizations are beginning to reorient their priorities, end users are beginning to segregate these priorities into three distinct areas and ask: “what does my organization look like from an attacker’s point of view, and how should it find and prioritize the issues attackers will see first?”; “what software is present and what configuration has my organization set that will make it vulnerable to attack?”; “what would happen if an attacker carried out a campaign against my organization’s infrastructure, how would its defenses cope and how would processes perform?”

Obstacles

- The complexity of exposure management programs introduces a number of new areas often not previously considered by organizations.
- The concept of evaluating your attack surface is well understood, only recently have technologies in this space, such as EASM and CAASM gained momentum. The current integration into other technologies such as VA technologies is low.
- Processes to manage end-to-end awareness (from visibility of possible attack vectors to response to breaches) is virtually nonexistent in most organizations who often simply scan and test their networks for compliance reasons with low integration of the findings.

- The complexity of how an attack may manifest itself requires certain skill sets to understand, those that are early adopters of BAS are able to test the out-of-the-box scenarios and develop a limited number of new simulations. To be effective at consuming these technologies, new skills and understanding are required either through internal staff or service partners.

User Recommendations

- Security and risk management professionals must design programs for managing exposure in its entirety, rather than simply managing or processing vulnerabilities.
- Exposure management is dependent on the ability to mobilize various stakeholders. Automated remediation from tools is unlikely to have the level of expected impact, except for a limited number of runtime virtual patches.
- Visibility is key, end users must have an awareness of where risks are, even if the organization has no way to reduce them.
- Prepare response and reaction plans. Monitoring and responding to issues and risks identified as a critical part of managing exposure, validating that exposures exist and controls are functioning is useful, but it is essential that organizations also prepare to react.
- Be sure to include assets that infrastructure has less control over, such as social media accounts, SaaS applications and data held by supply chain partners, in your exposure management program.

Gartner Recommended Reading

Innovation Insight for Attack Surface Management

Emerging Technologies: Critical Insights for External Attack Surface Management

Quick Answer: What Is the Difference Between EASM, DRPS and SRS?

VDI/DaaS Endpoint Security

Analysis By: Chris Silva, Stuart Downes

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

VDI/DaaS endpoint security covers security software that underpins or integrates directly with virtual desktop infrastructure (VDI) and desktop as a service (DaaS) solutions, providing additional security between the underlying device and the VDI or DaaS session. These controls can include basic device posturing, session-hijacking protection, keylogging prevention and screen-capturing prevention. They can also enforce multifactor user authentication.

Why This Is Important

The increased use of VDI and DaaS to deliver access to company apps and data from unmanaged devices demands additional controls. Less control of the local machine introduces the risk of keyloggers, screen-scrapers and credential or session hijacking due to incomplete or outdated device security posture. VDI and DaaS security tools add user validation and session auditing. This technology helps prevent and counteract these security shortcomings on managed and unmanaged devices.

Business Impact

VDI and DaaS security tools act as access agents on the local machine used to access VDI or DaaS sessions manifesting as a secure browser or remote desktop application. These tools can act as security-focused agents to ensure device configuration and behavior are not introducing new risk. They can also serve as a means to validate and monitor users accessing these sessions — for audit and compliance purposes, when needed.

Drivers

Factors driving the popularity of this technology include:

- Endpoint security policy and data sovereignty regulations that require the prevention of data leakage from virtual connections.
- Requirements for validating local user presence and identity along with the ability to capture user actions for later auditing.
- The use of personal, unmanaged local devices introduces vulnerabilities, including the potential for undetectable keylogging or screen mirroring and recordings.

- Increased use of VDI and DaaS for business continuity or to enable remote employees, suppliers and contractors to access corporate apps and data from unmanaged devices. This is common in organizations operating bring your own PC (BYOPC) initiatives. Another driver is increased use of devices with limited management capability (such as Chromebooks).

Obstacles

Obstacles to adoption of this technology include:

- Lack of awareness around potential endpoint security issues when using VDI and DaaS.
- There are only a few vendors focused on VDI and DaaS endpoint security.
- VDI and DaaS endpoint security solutions are often provided by a third-party vendor and not the virtualization vendor. This can potentially cause malfunctions if the virtualization vendor performs an update.
- Vendors in this space risk becoming a feature of virtualization vendors and not a separate product category.
- Labor and privacy regulations render the most obtrusive functions of some tools untenable, such as camera surveillance in the home.
- Organizations may be put off by the cost of adding VDI- and DaaS-specific security tools, in addition to the cost of the underlying infrastructure. This is exacerbated by an environment in which the trend is toward consolidating security tools.

User Recommendations

- Focus investments on solutions with documented support to help meet relevant data compliance laws.
- Pursue a baseline of controls from within the virtualization software to block data transfer to and from other endpoints using cut/copy/paste controls and limitations on data capture
- Faithfully replicate existing security posture used on physical endpoints in the VDI or DaaS environment before considering an additional VDI or DaaS endpoint security tool.
- In addition to these baseline controls, identify where to apply use-case-specific controls such as biometric identity verification, and when you need to validate the identity of specific users.
- Evaluate the vendor's ability to integrate with the planned or existing virtualization solutions and not degrade performance or experience.
- Coordinate with legal and human capital teams to examine regulatory privacy obligations when using biometric authentication or camera-based user monitoring.

Sample Vendors

Citrix; Minerva Labs; SessionGuardian; SentryBay; Talon; ThinScale

Gartner Recommended Reading

Market Guide for Desktop as a Service

Guidance Framework for Selecting Virtual Desktop Use Cases

2022 Planning Guide for Security and Risk Management

Unified Endpoint Security

Analysis By: Chris Silva

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Unified endpoint security (UES) is an IT architecture strategy that integrates endpoint operations and endpoint security workflows and tools, providing improved visibility, earlier threat detection and faster remediation, with increased automation. UES results from the integration of modern, co-management UEM tools with endpoint security tooling, such as endpoint protection/endpoint detection and response (EPP/EDR) for PCs and mobile threat defense (MTD).

Why This Is Important

The growth in hybrid work demands the use of modern tools to manage user-facing endpoints. As the adoption of UEM tools to manage PC and mobile devices in one platform has grown, so too has the adoption of EPP/EDR tools. In tandem, when sharing data, these tools reinforce and augment each other in a UES architecture. UES is the process of integrating endpoint operational tools and endpoint security tools to help close gaps in the early detection and remediation of security threats.

Business Impact

- Combined tools may offer staffing, operational and cost efficiencies.
- The unification of endpoint security and management workflows into a single console supports rapid cybersecurity event response.
- Tight integration enables complex, posture-based policy application, along with supporting technology, such as secure remote access.

Drivers

Drivers for UES adoption include:

- The need to consolidate to fewer security systems by offering a single console with capabilities from EPP, EDR and MTD, providing a better overview and simpler management.
- The requirement to secure any end-user device, no matter the device type, with a parity of control and visibility.
- Zero trust access (ZTA) uses context to drive access decisions and outcomes that adapt to risk based on that context; UES workflows and tool integrations provide the richer context to underpin ZTA.

Obstacles

- No single tool or philosophy provides total protection for each endpoint, and the ideal technology to secure a Windows PC differs from its mobile counterpart.
- A possible drawback of UES is that combined systems don't provide best-of-breed solutions; instead, they're best-of-breed in specific functionality. UES can be a single best-of-breed solution for all endpoint security, provided the unified product's cross-device data analytics is strong. This requires vendors that understand traditional client and mobile security to build a single threat detection framework — regardless of device type.
- Not all enterprises can adopt UES, especially short term. UES will not suit organizations with large fleets of legacy devices, or organizations that don't plan to modernize their remote access and prefer to address device management with traditional, siloed client management — rather than a UEM fashion.
- UES doesn't solve conditional access for unmanaged devices that don't accept corporate software.

User Recommendations

- Adopt a UES strategy to consolidate all endpoint security to a single console that lowers support costs, while improving threat prevention, detection and incident response.
- Prioritize evaluation of endpoint security and management tools that are focused on their ability to use prebuilt integrations with one another.
- Combine UES with ZTNA/secure access service edge (SASE) to provide conditional access control.

Sample Vendors

BlackBerry; Cybereason; Deep Instinct; McAfee; Microsoft; Sophos; Symantec; Tanium; Tehtris

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Innovation Insight for Unified Endpoint Security

External Attack Surface Management

Analysis By: Ruggero Contu, Mitchell Schneider, Elizabeth Kim

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Early mainstream

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 exposed servers, credentials, public cloud service misconfigurations, deep dark web disclosures and third-party partner software code vulnerabilities that could be exploited by adversaries.

Why This Is Important

Digital transformation initiatives have expanded the attack surface enterprises are exposing to malicious actors. Cloud adoption, remote working and IT/OT/IoT convergence are some key changes exposing enterprise assets to external threats. EASM helps identify exposed known and unknown assets. It also helps prioritize discovered vulnerabilities and risks, providing information about systems, cloud services and applications available and visible in the public domain to an attacker/adversary.

Business Impact

EASM provides valuable risk context and actionable information to SRM leaders. EASM delivers visibility through five primary capabilities:

- **Monitoring** (continuously) for exposed assets (cloud services, IPs, domains, certificates and IoT devices)
- **Asset discovery** for external-facing assets and systems
- **Analysis** to assess and prioritize the risks and vulnerabilities discovered
- **Remediation,** mitigation and incident response through prebuilt integrations with ticketing systems and SOAR tools

Drivers

- Digital business initiatives such as cloud adoption, remote working and IT/OT/IoT convergence
- Interest in understanding what organizations expose from an attacker's point of view
- EASM's accelerated adoption, with capabilities available as part of a broader solution set

Obstacles

- With short- and medium-term M&As, there will be a potential impact on investments made into startups in this space.
- Low value perception, with EASM leveraged for single use cases rather than multiple areas
- Confusion with nearby markets inhibiting adoption

User Recommendations

- Review available EASM capabilities from technology and service providers in areas such as threat intelligence, DRPS, security testing/validation or vulnerability assessment. You may have an existing commercial relationship in place with a provider, and its functionalities may be good enough.
- Review providers' capabilities such 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 technology or service provider based on the recognized use-case priority, but also plan for longer-term requirements potentially stretching into DRPS and/or security testing/validation 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; LookingGlass: Pentera; Palo Alto Networks; Randori; SOCRadar

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Emerging Technologies: Critical Insights for External Attack Surface Management

Competitive Landscape: Digital Risk Protection Services

Quick Answer: What Is the Difference Between EASM, DRPS and SRS?

Innovation Insight for Attack Surface Management

Identity Threat Detection and Response (ITDR)

Analysis By: Mary Ruddy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Identity threat detection and response encompasses the tools and processes that protect the identity infrastructure from malicious attacks. They can discover and detect threats, evaluate policies, respond to threats, investigate potential attacks and restore normal operation as needed.

Why This Is Important

Identity is now foundational for security operations (identity-first security). Only authorized end users, devices and services should have access to your systems. ITDR adds an additional layer of security to even mature identity and access management (IAM) deployments. As identity becomes more important, threat actors are increasingly targeting the identity infrastructure itself. Organizations must focus more on protecting their IAM infrastructure.

Business Impact

Securing your IAM infrastructure is mission-critical for security operations. If your user directories are compromised, then your identity infrastructure is compromised and attackers can take control of your systems. Protecting your IAM infrastructure must be a top priority. “Business-as-usual” processes that seemed adequate before attackers began targeting identity tools directly are no longer sufficient.

Drivers

More sophisticated attackers are now actively targeting the IAM infrastructure itself. For instance:

- The attackers behind the SolarWinds breach used administrative permissions to gain access to the organization’s global administrator account or trusted Security Assertion Markup Language (SAML) token signing certificate to forge SAML tokens for lateral movement.
- More recently, a threat actor used a custom backdoor malware to compromise Active Directory Federation Services.
- Credential misuse is now a primary attack vector.
- Modern attacks have shown that identity hygiene is not enough to prevent breaches. Multifactor authentication and entitlement management can be circumvented, and they lack mechanisms for detection and response if something goes wrong.
- A security information and event management (SIEM) solution and an in-house security operations center or outsourced managed detection solution do not replace more specialized threat detection and response processes designed specifically to ensure the integrity of the identity infrastructure itself.

Obstacles

- Lack of awareness of IAM hygiene and ITDR best practices mean that many organizations are not adequately protecting their IAM tools.
- IAM teams often spend too much effort protecting other group's digital assets, and not enough protecting their own IAM infrastructure.
- Although organizations have put significant effort into improving their IAM capabilities, much of that effort has focused on technology to improve user authentication, such as rolling out single sign-on to more applications. Although this represents an important security advance, it has also increased the attack surface of a foundational part of cybersecurity infrastructure.
- More needs to be done to protect identity systems themselves, detect when they are compromised, and enable rapid investigations and efficient remediation. The need for better prevention and detection is clear. Ensuring the highest levels of IAM resilience also requires the ability to quickly revert to a known good state.

User Recommendations

Security and risk management leaders responsible for security operations should:

- Prioritize securing identity infrastructure with tools to monitor identity attack techniques, protect identity and access controls, detect when attacks are occurring and enable fast remediation.
- Use the MITRE ATT&CK framework to correlate ITDR techniques with common attack scenarios to ensure that all the relevant attack vectors are addressed.
- Invest in foundational IAM infrastructure hygiene security best practices for user directories, including credential management, privileged access management and identity governance and administration to limit exposure if a credential is compromised. This helps to restrict lateral movement.
- Prevent administrator accounts from being compromised, e.g., by forcing proper termination of RDP sessions.
- Modernize IAM infrastructure using current and emerging standards (e.g., OAuth 2.0, CAEP).

Sample Vendors

CrowdStrike; Illusive; Microsoft; Netwrix; Quest; Semperis; SentinelOne (Attivo Networks); Silverfort; SpecterOps; Tenable

Gartner Recommended Reading

Top Trends in Cybersecurity 2022

Implement IAM Best Practices for Your Active Directory

At the Peak

XDR

Analysis By: Franz Hinner, Peter Firstbrook

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Extended detection and response (XDR) products are threat detection and incident response offerings that combine multiple security tools to meet more security operations needs. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

Why This Is Important

XDR products can be seen as evolutions and amalgamations of some security operations tools that preceded them. However, XDR products have higher levels of integration, automation, ease of use, and focus on threat detection and incident response. They also include security controls for, among other things, endpoint detection and response (EDR), cloud access security brokers (CASBs), firewalls, identity and access management, and intrusion detection systems.

Business Impact

XDR products reduce the total cost of managing security incidents, improve incident response teams' efficiency and improve an organization's risk posture. Effective XDR deployments enable faster, automated detection of threats and shorter response times via automated actions. XDR tools offer deep integrations with other security tools and can coordinate response actions across them.

Fully cloud-native XDR platforms should cost less to host and manage than the tools they replace or consolidate.

Drivers

- XDR platforms appeal to resource-constrained organizations of all sizes in all industry sectors, due to their ability to automate time-consuming processes, shorten detection and response times, and generally require less maintenance.

- Midsize organizations that struggle to address the alerts generated from disparate security components appreciate the ability to operate XDR tools with less skilled resources.
- Although some earlier security operations tools provide similar functions, their cost, complexity, and ongoing maintenance requirements are too high for midsize enterprises.
- The number of people and skills required to integrate and maintain a best-of-breed portfolio of disparate security tools is too high. Staff with the required skills are hard to recruit and retrain.
- XDR tools are often delivered by security solution providers that also have a portfolio of infrastructure protection products including, among other things, EDR, CASB, secure web gateway, secure email gateway, and network detection and response offerings.
- More advanced XDR tools are integrating with identity, data protection and application access technologies.

Obstacles

- Although the list of vendors that offer a holistic XDR product on their own is short, committing to a single-vendor XDR approach could lead to tie-in.
- Large vendors of XDR products typically execute much more slowly than best-of-breed startups when it comes to addressing new threats.
- All XDR tools require some integration with security products from other vendors, but deep integration with other vendors' solutions is still rare.
- The efficacy of security products is important, but some solutions in a portfolio may be less effective than best-of-breed tools.
- There is potential for dependency on a single source of threat intelligence and detection content provided by an XDR vendor. XDR tools reduce but do not eliminate the need for knowledgeable operators and 24/7 monitoring.
- An XDR solution alone does not always meet all needs for long-term log storage for use cases other than incident response, such as compliance, application monitoring and performance monitoring.

User Recommendations

- Work with security operations stakeholders to determine what XDR strategy is right for your organization.
- Base decision criteria on staffing and productivity levels, level of IT federation, risk tolerance and security budget, as well as consolidation aims and the presence of existing XDR component tools.
- Develop an internal architecture and purchasing policy that is in line with your XDR strategy, one that explains when and why exceptions might be permissible.
- Plan security purchases and technology retirements in relation to a long-term XDR architecture strategy.
- Favor security products that provide APIs for information sharing and that allow automated actions to be sent from an XDR solution.

Sample Vendors

Bitdefender; Cisco; Fortinet; Microsoft; Palo Alto Networks; Secureworks; SentinelOne; Sophos; TEHTRIS; Trend Micro

Gartner Recommended Reading

Innovation Insight for Extended Detection and Response

Market Guide for Security Orchestration, Automation and Response Solutions

BYOPC Security

Analysis By: Chris Silva

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Bring your own PC (BYOPC) programs allow personally selected and purchased client devices to execute enterprise applications and access company data. These programs typically span Apple macOS, Google Chrome and Microsoft Windows devices. A lack of control or standardization in hardware and OS can represent significant risk if not addressed with a defined BYOPC security strategy.

Why This Is Important

Personal device or bring your own (BYO) programs have been expanded to include macOS and Windows PCs, but the security of these devices, in contrast to their Android and iOS counterparts, will involve trade-offs for security over functionality.

Gartner always recommends providing the user with a device that is managed and secure over a BYOPC device, but in circumstances where non-company-owned devices are in use, defenses and controls can be adapted to maintain a valid security posture.

Business Impact

Local controls on personal devices present risks of increased support and license costs, liability for loss of users' data, and privacy compliance. Instead, isolate the local device risks and stem data loss by combining data isolation and zero-trust access policy to yield dynamic outcomes like web-only access via secure browser from unmanaged BYO devices, and prompt for VDI or app virtualization session for sensitive apps and data.

Drivers

- Hybrid work has expanded the number of devices from which users access company apps and data, with personal PCs making up a significant proportion of BYO devices in use.
- Increased access for more users, from more devices improves business continuity, and gives users more flexibility at nominal cost, but requires new and adaptive security controls.
- Increased rigor in authenticating users and devices is warranted as the use of harvested user credentials by bad actors increases.
- Capabilities to establish rightsized control on a BYOPC, whether through some local controls, isolation of data or a combination of both, allow for flexible options to suit multiple use cases.

Obstacles

- More rigorous privacy regulations, paired with the potential risk of configuring and establishing local controls on users' personal PCs, require solutions beyond device management and local agents.
- In attempting to eliminate data loss and isolate company systems from local malware, VDI and DaaS are often employed for BYOPC, but remain costly for IT and complex for users.
- The increased support cost and license burden to establish a consistent posture for BYOPC devices will be compounded by technical limitations of users' local systems.
- Shared use of devices, common for personal hardware, may violate fair and acceptable use policies or other compliance mandates, regardless of security controls.

User Recommendations

- Avoid risk exposure by offering alternative device and control options. BYOPC cannot be required in most cases, nor can the enforcement of onerous controls on users' devices.
- Establish flexible controls for BYOPC; this can pay dividends by creating support models that can adapt for contractor and temporary employees as well.
- Limit use of personally owned macOS and Windows devices to where local control, data isolation or a mix of both can be enabled to protect data leakage, user credentials and company systems.
- Insulate against unexpected costs due to the unknowns of users' devices by modeling costs assuming that all users will require the most costly combination of licenses and support. Actual costs are likely to be lower.
- Define support levels and entitlements with explicit detail on scope, coverage and escalation process.
- Consult with legal and HR teams to understand what technical controls are tenable on users' personal devices and what privacy concerns must be addressed.
- Evaluate virtualization technology for loosely defined BYOPC use cases that span many apps and data types.

Sample Vendors

Amazon Web Services; BlackBerry; Cisco; Citrix; Microsoft; Okta; VMware

Gartner Recommended Reading

Enable BYOPC for Business Continuity While Managing Risk

Quick Answer: How to Securely Enable Access for Unmanaged Devices

Market Guide for Desktop as a Service

Security Service Edge

Analysis By: John Watts, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include access control, threat protection, data security, security monitoring and acceptable use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

Why This Is Important

SSE improves organizational flexibility to secure usage of cloud services and remote work. SSE offerings are the convergence of security functions (secure web gateways [SWGs], cloud access security brokers [CASBs] and zero trust network access [ZTNA]) to reduce complexity and improve user experience, delivered from the cloud. SSE stands alone, but when organizations are pursuing a SASE architecture, it is paired with SD-WAN to simplify networking and security operations.

Business Impact

The trend of hybrid work and the adoption of public cloud services accelerated in the past few years. SSE allows the organization to support the anywhere, anytime workers using a cloud-centric approach for the enforcement of security policy when accessing the web, cloud services and private applications.

Drivers

- Organizations need to secure users, applications and enterprise data that are now everywhere.
- SSE enables flexible cloud-based security for users and devices without tying it to on-premises network infrastructure.
- Organizations look for deeper security capabilities when building a SASE architecture compared to vendors that may have a minimal set of security features as part of their SD-WAN offering.
- SSE allows organizations to implement a zero-trust posture based on identity and context at the edge.
- By consolidating vendors, organizations reduce complexity, costs and the number of vendors used to define security policy. It simplifies complexity or gaps in coverage with the use of multiple offerings.
- Sensitive data inspection and malware inspection can be done in parallel across all channels of access with better performance than doing this separately.
- Improve user experience by unifying the same security outcomes regardless of location.

Obstacles

- Some organizations want to strategically combine their SD-WAN and SSE from a single vendor, but networking requirements or discrete buying centers prohibit them from adopting a best-of-breed SSE.
- Because the market is being formed by convergence of capabilities, vendors may be strong in certain capabilities while weak in others, or lack overall tight integration of SSE capabilities or with SD-WAN providers.
- Some vendors are weak in sensitive data identification and protection, and this capability is critical for risk- and context-based access decisions.
- Being cloud-centric, SSE typically doesn't address every need for on-premises functionality.
- Not all vendors will commit to performance SLAs on all services or may have inconsistent SLAs across services.
- Switching costs for incumbent vendors or timing of contract expirations prohibit near-term consolidation.

User Recommendations

- Consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs (replacing with a ZTNA approach). Leverage a converged market that emerges by combining these services.
- Approach SSE consolidation identifying which elements you may already have in place (e.g., existing cloud-based CASB). Then, create a detailed understanding of the use cases applicable to secure end users remotely and on-premises, the cloud services you use, and the data you need to protect to develop a shortlist of vendors.
- Inventory equipment and contracts to implement a multiyear phaseout of on-premises perimeter and branch security hardware in favor of cloud-based delivery of SSE. Target consolidation of on-premises equipment ideally to a single appliance.
- Actively engage with initiatives for branch office transformation, SD-WAN and Multiprotocol Label Switching (MPLS) offload to integrate cloud-based SSE into the scope of project planning.

Sample Vendors

Broadcom (Symantec); Cisco; Forcepoint; iboss; Lookout; Netskope; Palo Alto Networks; SkyHigh Security; Versa; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Market Guide for Zero Trust Network Access

Breach and Attack Simulation

Analysis By: Jeremy D'Hoinne, Mitchell Schneider, Pete Shoard, Eric Ahlm

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Breach and attack simulation (BAS) technologies allow enterprises to gain better visibility on their security posture weak spots by automating the test of threat vectors such as external and insider, lateral movement, and data exfiltration. BAS complements, but cannot fully replace, red teaming or penetration testing. BAS validates the security posture of organizations by testing its ability to detect a portfolio of simulated attacks run from SaaS platforms, software agents and virtual machines.

Why This Is Important

The key advantage of BAS technology is to provide automated and consistent assessment of an enterprise's threat vectors. BAS also evaluates the ability for its security controls to detect and block the simulated attacks. BAS reports align with industry frameworks such as MITRE, to help prioritize remediation.

Frequent automated BAS assessments also enable organizations to detect gaps in their security posture due to configuration errors, or reevaluate priorities of upcoming security investment.

Business Impact

BAS allows organizations to verify their security posture, and review the configuration and limits of their security controls. The organizations automate these assessments to gain more frequent visibility on a larger percentage of their assets, or discover attack paths leading to critical assets.

BAS vendors continually add new threats vectors to test and expand the scope and depth of their capabilities by adding support for complex and custom scenarios.

Drivers

BAS is relevant for multiple exposure assessment use cases, including, but not limited to:

- **Security posture assessment:** Organizations with mature security programs use these technologies primarily to ensure consistent security posture over time and across multiple locations.
- **Security control assessment:** Some BAS tools integrate with security control technologies, through management APIs or by reading alert logs, enabling security configuration management and improving the visibility of defense gaps.
- **Penetration testing supplement:** BAS provides “safer” and more automated assessments that organizations value to prepare for mandatory penetration testing, or to refocus red team activity on more advanced scenarios.

IT and business stakeholders often sponsor deployment of BAS technologies as they perceive it as a safer way to assess the competency of current security controls, their configuration and the incident response processes for the organization. BAS vendors expand their use cases by adding adjacent capabilities, such as external attack surface management (EASM) or advanced custom scenario engines, to become a key component of enterprise exposure management programs.

Obstacles

- 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 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, for example, 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

- Prioritize your company's use case(s) and then assess the BAS vendors' capabilities to deliver value continually by regularly adding new capabilities, highlighting changes in the security posture and providing reports in a form that minimizes diagnostic fatigue.
- Evaluate the number of threat vectors and attack scenarios the BAS tool can deliver 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; Keysight; Mandiant; Picus Security; SafeBreach; XM Cyber

Gartner Recommended Reading

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

Using Security Testing to Grow and Evolve Your Security Operation

Business Email Compromise Protection

Analysis By: Franz Hinner, Craig Porter

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Business email compromise (BEC) protection detects and filters malicious emails that fraudulently impersonate business associates to misdirect funds or data. Stopping BEC attacks requires deep inspection of personalized email content in context. Correlating subject line intent with statements creating urgency and attempting to extract money or data can be explicit identifiers of business email compromise.

Why This Is Important

BEC typically does not include malicious links or attachments. Because these emails are often sent from legitimate mail servers, they are challenging to detect. Attacks are socially engineered through publicly available information, like LinkedIn, Crunchbase or Wallmine, to increase their effectiveness.

Proofpoint 2022 State of the Phish reports:

- BEC was up 18% in 2021 over 2020.

The impact of BEC in 2020, according to the FBI's 2020 Internet Crime Report:

- There were 20,000 complaints of BEC.
- Losses related to BEC totaled $1.86 billion.
- BEC increased 110% from 2019.

Business Impact

BEC attacks pose a significant risk to all industries. They accounted for 43% of cybercrime losses in 2020. Attacks are relatively low tech, targeting valuable individuals in the organization, such as the C-suite, by tricking accounts payable. BEC attacks use EAC to launch attacks like fraudulent invoices and undermine trust in a relationship, while causing financial loss.

Drivers

Adoption of BEC protection technology is increasing because:

- Traditional techniques for detecting malicious attachments or links are ineffective against BEC attacks.
- Reputation-based detection techniques are relatively ineffective because these attacks often come from legitimate email accounts with good reputations.
- Spoofed emails to customers are challenging to detect because they do not involve the corporate email system.
- Loss of goodwill and trust, as in the case of Uber/Podesta. Sensitive data still lives in email.
- Losses from BEC attacks can be significant — they sometimes amount to millions of dollars.
- All financial transactions, including requests to change payroll details, are at risk.
- Compromised email accounts enable attackers to use email conversations to redirect funds. These account takeover attacks are indistinguishable from legitimate emails.
- BEC attacks frequently go unnoticed; only when the intended recipient notices a made payment, is fraud detected.
- Leading email security vendors are consolidating their service portfolio to include data loss prevention (DLP), user awareness training and BEC as attacks become more targeted and complex.

Obstacles

- BEC protection involves not just the use of BEC solutions, but also user education, of both staff within an organization and external suppliers (and others), to identify BEC attacks; and the move away from means of email to processing high-risk financial transactions. Changes to other processes and procedures, or the introduction of procure-to-pay solutions, can also help.
- Even the most effective solutions are not 100% effective, and as attackers' techniques evolve, solutions focused on BEC may lose sight of the latest practices used.

- Solutions that rely on APIs by cloud email providers are limited to what those APIs allow, as well as continued support by Microsoft and Google.
- Dwell time, or the time attacks have credentialed access, is another key issue to address and mitigate so that the risk of increased attacker knowledge of organizational behavior and ability to hide their tracks is eliminated.
- Before reaching the plateau, BEC capabilities likely are absorbed into comprehensive email security solutions.

User Recommendations

- Educate users about BEC phishing techniques and the limitations of email as an authentication factor in high-risk transactions. Intelligent and dynamic banners are a specific example of this.
- Follow a predefined operation procedure of authenticated email for all financial or data transaction requests to eliminate requests for ad hoc transaction risks.
- Upgrade or supplement email security solutions with advanced phishing protection, including natural language processing, natural language understanding, computer vision and machine-learning-based social graph analysis.
- Leverage domain-based message authentication, reporting and conformance (DMARC) implementations to authenticate and minimize domain abuse. While adoption is high, implementation management is more complex and often neglected. While SPF/DKIM implementation is easy, the reject mode is much more complex, requiring constant updates to achieve the highest degree of efficiency.
- Implement multifactor authentication for an email to protect against account takeover.
- Embrace adaptive trust by segmenting different requirements for more privileged users.

Sample Vendors

Abnormal Security; Armorblox; Avanan; Cellopoint; Cyren; Material Security; Microsoft; Mimecast; IRONSCALES; Proofpoint

Gartner Recommended Reading

Protecting Against Business Email Compromise Phishing

Market Guide for Email Security

Guidance Framework for Building Email Security Architecture

Avoid the Top 9 Pitfalls of Implementing MFA

Sliding into the Trough

Device Endpoint Security for Frontline Workers

Analysis By: Franz Hinner, Patrick Hevesi

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Device endpoint security for frontline workers includes a set of technologies that protect purpose-built devices and their users. Depending on the industry and use case, devices must be physically secured to permanent stations, tracked and checked out for shift duty, or set up for use by multiple users in areas where connectivity can be an issue.

Why This Is Important

Frontline workers must operate from managed, purpose-built, locked down, ruggedized mobile devices tailored to their job. These devices come at a premium and are hard to update and patch to maintain security. Because of this, some organizations and vendors turned to personal devices with protection around mobile applications. However, such devices provide less control than a fully managed device and can open the organization to loss of productivity, data leakage or malicious attacks.

Business Impact

Frontline scenarios involve access to sensitive and critical systems, which raises the risk and the need for precautions. Often, frontline devices are off-premises and handled by customers, contractors, temporary staff and employees. A combination of solutions may be necessary to mitigate all possible security risks. Some solutions are built for traditional mobile management scenarios, not for frontline workers, and may need custom development work to meet security requirements.

Drivers

- More companies are enabling frontline workers to access cloud SaaS applications, which exposes organizations and workers to additional cloud security risks.
- The risk of data leakage or other malicious attacks has caused security teams to reevaluate their frontline endpoint security strategy and architectures.

- In line with the BYOD trend, organizations are increasingly allowing the use of personal devices, driving the need for new solutions around mobile application management (MAM) and mobile threat defense (MTD), resulting in deployments of application-level container solutions.

Obstacles

- Covering all security fronts requires multiple defense layers, encompassing specialized hardware and additional cloud functionality. These security requirements lead to additional costs for which organizations may not have planned.
- Endpoint security for frontline workers must include physical security solutions such as cameras, check-in/check-out processes, user and device identity management, shift-based devices where data needs clearance after each use, and geographic/location type protection. These requirements further elevate the cost and difficulty of deploying device endpoint security solutions for frontline workers.

User Recommendations

For managed devices requiring specialized solutions:

- Leverage purpose-built mobile security solutions.
- Fully manage and lock down the devices with EPP, UEM, or MAM.
- Ensure that OS security settings, updates, and patches are applied.
- Ensure that physical security is in place, such as cables for kiosks, geofencing/geolocation and check-in/check-out processes.

For unmanaged devices, where LOB and other collaboration apps are allowed to run:

- Use UEM tools to apply MAM policies adding security such as encryption, MFA and time-based app lockout.
- Evaluate MTD vendors for device-based risk attestation using MA management.

For custom-built worker apps:

- Ensure that LOB apps are engineered with secure design principles and multiuser authentication.

- Use app-shielding, app-wrapping and in-app MTD to protect IPs in runtime on a device.

For cloud-based apps:

- Use CASB for threat and data protection.
- Use adaptive access control for frontline users and devices consuming external SaaS services.

Sample Vendors

CommuniTake Technologies; Imprivata (GroundControl); Lookout; Microsoft; Samsung Electronics; SOTI; Symantec; Veracode; Zebra Technologies; Zimperium

Gartner Recommended Reading

Guide to Endpoint Security Concepts

Market Guide for Mobile Threat Defense

Advance and Improve Your Mobile Security Strategy

Content Disarm and Reconstruction

Analysis By: Franz Hinner, Neil MacDonald

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Content disarm and reconstruction (CDR), which is also referred to as "content sanitization," breaks down files into their discrete components, and strips away anything that doesn't conform to that file type's original specification/ISO standard. It also removes any content that could be malicious — separating macros, links, embedded objects from content — and it rebuilds a sanitized version.

Why This Is Important

CDR protects against exploits and weaponized content without the need for lengthy dynamic analysis or traditional content inspection techniques (such as signatures) for identifying malicious content. This is particularly useful where files are crossing organizational boundaries, such as email, web, and file content sharing sites.

Business Impact

CDR is an important layer in any organizations defense-in-depth and content protection strategies. It:

- Significantly reduces the risk of malicious content entering an organization (e.g., via email) by removing active content such as macros, which are one of the most common infection vectors, and are hard to deal with in other ways.
- Is much faster than sandboxing; therefore, it makes a good complementary solution.

Drivers

- Remote working has increased the need to ensure that files and documents are sanitized before being shared internally, driving adoption of CDR.
- CDR sanitizes content when files are crossing data boundaries. Some examples include users uploading email attachments; downloading web downloads; uploading content such as application forms, resumes, or CVs; and sharing or receiving documents from untrusted sources.
- Some secure email and web gateways, as well as content collaboration platforms, already include such capabilities, either built in-house, OEM'ed or at additional cost via a third-party license, which is helping to drive adoption.
- The speed of CDR complements dynamic analysis in sandboxes, which is notoriously slow. As a result, users can see a sanitized attachment immediately and can request the original after an integrated sandbox has finished its processing.
- CDR neutralizes all potentially malicious content, without requiring multiple rounds of antivirus scanning or sandboxing.
- CDR serves as a strong and low-latency alternative to sandboxing and multi-AV in malware prevention scenarios in which files (typically Office, PDF and multimedia) move from an untrusted to a trusted environment.

Obstacles

- The use of CDR can decrease document usability by stripping out active code that is intended for legitimate purposes. Some solutions hold the original file in quarantine if its functionality is broken, in addition to more granular control over what is removed; however, this can decrease the value CDR provides.
- Because CDR does not rely on detection, it can be challenging to demonstrate effectiveness without additional, retrospective analysis of content.
- Most CDRs do not identify malicious actors or malicious intent. Such information can be useful in understanding the organizational risk posture.
- Awareness of CDR technology remains low, inhibiting broader adoption.
- CDR is useful only for specific file types.

User Recommendations

- Protect against inbound threats from malicious documents by considering CDR as part of your email and web security strategy.
- Use CDR as an alternative to sandboxing and multi-AV scanning, to ensure that files and documents shared or received from untrusted sources are free of malware.
- Use CDR with sandboxing solutions to enable sanitized documents to be available immediately, while the sandbox analysis completes.
- Utilize CDR to sanitize content in high-security environments, to ensure tracked changes, internal comments, etc., are removed before sharing.

Sample Vendors

Check Point Software Technologies; Fortinet; Glasswall; HelpSystems; OPSWAT; Sasa Software; Votiro

Gartner Recommended Reading

Market Guide for Email Security5 Core Security Patterns to Protect Against Highly Evasive AttacksMagic Quadrant for Secure Web Gateways

SASE

Analysis By: Neil MacDonald, Andrew Lerner

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Secure access service edge (SASE) delivers converged network and security as a service capabilities, including SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

Why This Is Important

SASE is a key enabler of modern digital business transformation, including work from anywhere and the adoption of edge computing and cloud-delivered applications. It increases visibility, agility, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and security services mainly via a cloud-delivered model. SASE can reduce the number of vendors required for secure access to one to two over the next several years.

Business Impact

SASE enables:

- New digital business use cases (such as branch office transformation and hybrid workforce enablement) with increased ease of use, while reducing costs and complexity via vendor consolidation and dedicated circuit offload.
- Infrastructure, and operations and security teams to deliver a rich set of networking and network security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and work from anywhere.

Drivers

- SASE is driven by enterprise digital business transformation including the adoption of cloud-based services by mobile workforces, edge computing and business continuity plans that must include flexible, anywhere, anytime, secure access, and use of the internet and cloud services.
- The need to flexibly support digital business transformation efforts with a zero trust security architecture while managing complexity is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service (see 2021 Strategic Roadmap for SASE Convergence). The rapid shift to hybrid work models accelerated these trends.
- For IT, SASE can reduce the deployment time for new users, locations, applications and devices as well as reduce the attack surface and shorten remediation times.
- Network security models based on data center perimeter security are ill-suited to address the dynamic needs of a modern digital business and its distributed digital workforce. This is forcing a transformation of the legacy perimeter into a set of cloud-based, converged capabilities created when and where an enterprise needs them — that is, a dynamically created, policy-based SASE.

Obstacles

- **Organizational silos, existing investments and skills gaps:** A full SASE implementation requires a coordinated and cohesive approach across security and networking teams, which is challenging given refresh/renewal cycles, silos, and existing staff expertise.
- **Organizational bias and regulatory requirements for on-premises deployment:** Some customers have an aversion to the cloud and want to maintain control.
- **Global coverage:** SASE depends upon cloud delivery, and a vendor's cloud footprint may prevent deployments in certain geographies, such as China, Africa, South America and the Middle East.
- **SASE maturity:** SASE capabilities vary widely. Sensitive-data visibility and control is often a high-priority capability, but it is difficult for many SASE vendors to address. While your preferred single vendor may lack the capabilities you require, two-vendor partnerships can be a viable approach.

User Recommendations

- Involve the chief information security officer (CISO) and network architect when evaluating offerings and roadmaps from incumbent and emerging vendors to ensure an integrated approach.
- Leverage WAN, firewall, VPN hardware refresh cycles or software-defined WAN (SD-WAN) deployments to update network and network security architectures.
- Strive for no more than two vendors for all core services to minimize complexity and improve performance.
- Identify required capabilities for networking and security, including latency, throughput, geographic presence, and endpoint types to develop evaluation criteria.
- Focus on vendors who invest significantly in sensitive data discovery and protection capabilities for their SASE covering multiple data exfiltration vectors and serving verticals with highly advanced requirements for data security.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the number of vendors required.
- Leverage branch office transformation and dedicated circuit offload projects to adopt SASE for security services.

Sample Vendors

Cato Networks; Cisco; Forcepoint; Fortinet; Juniper; Netskope; Palo Alto Networks; Versa Networks; VMware; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Quick Answer: Does SSE Replace SASE?

The Future of Network Security Is in the Cloud

Magic Quadrant for WAN Edge Infrastructure

Magic Quadrant for Security Service Edge

Remote Browser Isolation

Analysis By: John Watts, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Remote browser isolation (RBI) separates the rendering of untrusted content (typically from the internet) from users and their devices, or it separates sensitive applications and data from an untrusted device. When used to protect from untrusted content, RBI significantly reduces the chance of a breach, as a large number of attacks have shifted to users and endpoints. When used to protect sensitive data and applications from unmanaged devices, RBI helps to reduce risks associated with BYOD.

Why This Is Important

Browser isolation keeps the session between an endpoint and the web services it is accessing segregated, reducing risk of malware and data loss. When an endpoint is accessing web content, RBI prevents web-delivered malware from getting onto it. RBI also works in the reverse direction. In use cases such as SaaS access via a CASB or internal application access via ZTNA, it protects sensitive data and applications from attack by an unmanaged and potentially infected device.

Business Impact

Today, most attacks are delivered via the public internet, through either web browsing or emailed links that trick users into visiting malicious sites. Simply removing (or, more strongly, isolating) the browser from the end user's desktop significantly improves enterprise security posture, including protection from malware attacks. RBI protection can also extend to internal private applications and SaaS applications accessed from unmanaged devices, thus reducing the threat of data exfiltration.

Drivers

- Static blocklists of bad sites can fail and are too slow to stop targeted attacks.
- Blocking uncategorized sites can hurt the end-user experience.
- Remote work continues to bring unmanaged devices into the mix. RBI can serve as a control point for unmanaged devices to support sensitive-data protection. Cloud access security brokers (CASBs) and zero trust network access (ZTNA) offerings are now employing RBI for this use case.
- Email-based URLs that resolve externally are often used to phish employees. Isolating these can reduce successful phishing attacks.
- Security service edge (SSE) has combined a set of access capabilities from the cloud, including secure web gateway (SWG), CASB and ZTNA. RBI adds value in multiple use cases and is becoming a common feature of these products.
- RBI is cheaper than using virtual desktop infrastructure (VDI) for isolation, if the applications being isolated are browser-based.

Obstacles

- User experience (UX) is a huge obstacle to adoption. Standardizing on Chromium as the rendering engine helps with most issues; however, concerns remain about latency and bandwidth impacts on UX.
- RBI incurs greater administrative overhead for exception handling and troubleshooting than traditional SWG solutions.
- Localizing the browsing experience requires IP address assignments to be regionally combined with either VPN exit points or local POPs.
- RBI is potentially expensive and additional to existing SWG or firewall per-user licensing.
- Most RBI offerings are software-based and cloud-delivered, limiting options for companies that prefer to run solutions in-house and for defense and intelligence scenarios that require the stronger isolation of hardware-based RBI.
- RBI does not protect against infected content that is permitted to download to the endpoint. Mechanisms like malware scanning, network sandboxing, conversion to PDF, or content disarm and reconstruction (CDR) are required.

User Recommendations

- Evaluate and pilot a browser isolation solution for specific high-risk users (such as finance teams) or use cases (such as rendering email-based URLs), particularly if your organization is risk-averse.
- Pressure your SSE or stand-alone SWG, CASB, ZTNA and/or SEG vendor to provide RBI as an optional defense-in-depth protection option.
- Roll out RBI incrementally for threat protection. Start by deploying to a limited number of high-value target users and by selectively isolating a limited number of URLs. Then, expand the use cases.
- Evaluate different vendor approaches for rendering (e.g., pixel streaming, vector-based), based on performance, latency and bandwidth requirements.
- Use RBI to isolate files for read-only viewing. However, when downloads are required, use CDR or best-in-class file scanning to prevent malware.
- Sign one- to two-year contracts only; the market is in flux, with downward pricing pressure.

Sample Vendors

Authentic8; Broadcom; Cloudflare; Ericom Software; Forcepoint; Garrison; Menlo Security; Netskope; Skyhigh Security; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Quick Answer: How to Securely Enable Access for Unmanaged Devices

Desktop as a Service

Analysis By: Stuart Downes, Mark Margevicius, Tony Harvey, Craig Fisler

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Desktop as a service (DaaS) solutions provide a virtualized desktop experience to workers, entirely from the public cloud. DaaS eliminates the need for businesses to purchase the physical infrastructure associated with virtual desktop infrastructure (VDI), instead of functioning through subscription- and usage-based payment structures. DaaS includes provisioning, patching, and maintenance of the management plane and resources to host workloads.

Why This Is Important

DaaS provides secure remote access to applications and desktops using a persistent network connection. No data resides on the endpoint, offering a solution that can increase security, redundancy and performance for remote workers. DaaS offers scalable services, allowing clients to appropriately size and consume their environments hour by hour, day by day, and month by month; however, not all have such granular billing options.

Business Impact

DaaS increased its ability to deliver secure desktop and application experiences to users in any location:

- Revenue grew by 68% in 2021, compared to 2020, and 98% in 2020, compared to 2019 as clients adopted DaaS to secure distributed work.
- DaaS enables business continuity and anywhere operations for home-based and hybrid home-office operations.
- DaaS enhances security for bring your own PC (BYOPC) use cases, hence reducing risks for businesses.
- DaaS enables business expansion to new regions without the need to deploy data centers.

Drivers

- Security and compliance.
- Enabling remote work with no data residing on the endpoint.
- Extending services to external contractors and third parties.
- Endpoint computing models that allow device independence and BYOPC endpoints.
- Business continuity.
- On-demand desktops with a financial model that allows scaling of cloud resources and an operating expenditure (opex) model.
- Short-term employees, such as seasonal workers.
- Enabling rapid access to systems during mergers, acquisitions and divestitures.
- Rich graphics use cases like engineering, games development, fashion and geographic information systems (GIS) benefit from GPU-enabled workstation-class virtual desktops and applications.
- DaaS can be delivered to users in hours where the supply of a physical device could take weeks.
- Eliminating the need for complex VDI implementations.
- Ability to take advantage of improved broadband network availability.

Obstacles

- Cost — usually the business case turns positive only when security, business and user costs are included.
- Organizations struggling with changes to move financial models from capex to opex.
- GPU use cases can be extremely expensive, preventing migration of some workloads that are highly graphical.
- Multimedia streaming, web meetings and video call performance in DaaS are not equivalent to that of a physical endpoint.
- Performance issues that occur in DaaS because application architectures introduce network-related issues (i.e., latency and hairpinning).
- Some DaaS solutions require complex configuration, which, although simpler than VDI, can in some cases require careful configuration and selection of appropriate storage services to ensure a performant DaaS experience.
- Complex desktop management requirements may not be completely fulfilled by DaaS providers.
- Microsoft license terms that prevent the installation of Microsoft 365 applications on DaaS running on Alibaba, Amazon or Google clouds.

User Recommendations

DaaS will continue to mature and increase in adoption through 2025. DaaS is yet to move through the Trough of Disillusionment onto the Slope of Enlightenment. Clients should:

- Familiarize yourself with the three DaaS market segments and select a vendor from the appropriate segment (see Market Guide for Desktop as a Service).
- Ensure your teams have the necessary operational skills while selecting a vendor that offers client defined DaaS solutions.
- Select a vendor-defined DaaS or managed DaaS solutions if you do not have the operational skills required.
- Choose a DaaS vendor whose services best align with your requirements; even within each segment, there are differences between the services vendors offer.

- Optimize multimedia streaming, web meetings and video calls.
- Select a DaaS vendor that offers billing granularity that you require; some are granular hour by hour, others day by day or month by month.

Sample Vendors

Amazon; Anunta; Citrix; Dizzion; Microsoft; Nutanix; oneclick; Tehama; VMware; Workspot

Gartner Recommended Reading

Market Guide for Desktop as a Service

Microsoft's Restrictions for Licensing Windows and Office 365 for VDI/DaaS on AWS and Other Hyperscale Clouds Require Attention

How to Avoid Surprise Costs With Desktop as a Service

Windows 365, Microsoft's Newest DaaS Solution, Demands a Careful Assessment of Costs and Use Cases

How to Successfully Justify Your Desktop Virtualization Initiative

Climbing the Slope

Mobile Threat Defense

Analysis By: Dionisio Zumerle

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Mobile threat defense (MTD) protects organizations from threats against iOS and Android mobile devices. It provides prevention, detection and remediation for the device, its network connections and its applications. To prevent and detect enterprise threats, such as malware, MTD products use a variety of techniques, including machine learning and behavioral analysis. Offerings come from a variety of vendors, including endpoint protection platform (EPP) vendors and stand-alone MTD providers.

Why This Is Important

MTD improves mobile security hygiene by identifying vulnerable devices, malicious apps and networks. It also provides visibility on mobile device behavior that can indicate malicious activity, and that can be correlated with other endpoint or enterprise data, to improve enterprisewide detection and response capabilities. Among other threats, MTD can counter mobile phishing. Financial services and other high-security and regulated industries are the primary adopters of this technology.

Business Impact

IT leaders responsible for mobile security can use MTD to counter mobile threats:

- MTD can work as a threat-focused integration with an existing UEM deployment or as a stand-alone tool.
- MTD can provide security assurance for regulated industries, enterprises that need to use a varied and fragmented set of mobile operating system versions, and organizations that choose not to manage the mobile devices to which they provide enterprise access.

Drivers

- Enterprises that derive value from MTD do so by implementing security hygiene using proactive measures, such as app vetting and device vulnerability management, rather than the ability to detect and counter advanced attacks.
- Emerging use cases envisage MTD as a component of zero trust architecture and of an extended detection and response (XDR) system for detection and response, which can serve as a pilot for unified endpoint security. This is in addition to the use of MTD for mobile phishing protection.
- For unmanaged iOS and Android devices, MTD can provide security assurance suitable for BYOD and work-from-home scenarios. When a user launches a work application on a device, the application allows access only when MTD is running on the device. In particular, Microsoft's MAM-WE implementation of this option is gaining popularity to enable Outlook and other Microsoft applications on unmanaged devices.
- EPP vendors are approaching the space, extending support of their EPP products to iOS and Android.

Obstacles

- MTD adoption has been slower than what the mobile security hype purported. The lack of evidence of mobile security issues that have led to major enterprise breaches does not make MTD a priority for enterprises.
- Regulated industries and enterprises with high-security requirements adopt MTD solutions. Among mainstream organizations, MTD product adoption is largely limited to those wanting to improve their overall security hygiene or provide device posture information for bring your own device (BYOD) equipment, rather than those aiming to counter malicious mobile threats.
- Mobile operating systems limit the visibility and remediation actions that security tools can take on these platforms.

User Recommendations

- Prioritize MTD adoption in high-security and regulated sectors, and in organizations with large or fragmented Android device fleets. Prioritize devices of users that handle sensitive data and those that are frequently mobile.

- Establish a security baseline for mobile devices before investing in MTD products, and use these products' app vetting and device vulnerability management features to demonstrate immediate benefits, rather than expect them to counter advanced malicious threats or uncover major breaches.
- Integrate MTD with incumbent unified endpoint management (UEM) tools. Favor the app-based option and leave proxy-based deployment for high-security and business-only scenarios.
- Use MTD products to protect enterprise infrastructure where BYOD policies are in operation and for other use cases in which devices must stay unmanaged. Emphasize strategic vendor fit over product differentiation, except for high-security contexts and situations with specific mobile security needs.

Sample Vendors

BETTER; BlackBerry; Broadcom (Symantec); CrowdStrike; Lookout; Microsoft; Samoby; Sophos; Wandera; Zimperium

Gartner Recommended Reading

Market Guide for Mobile Threat Defense

ZTNA

Analysis By: John Watts, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Zero trust network access (ZTNA) makes possible an identity- and context-based access boundary between any user and device to applications. Applications are hidden from discovery and access is restricted via a trust broker to a set of named entities. The broker dynamically verifies identity — context for policy adherence of specified participants and devices before allowing access — and limits lateral movement in the network.

Why This Is Important

ZTNA is a key technology for enabling dynamic user-to-application segmentation through a trust broker, to enforce a security policy that allows organizations to hide private applications and services and enforce a least-privilege access model for applications. It reduces the surface area for attack by creating individualized “virtual perimeters” that encompass only the user, the device and the application.

Business Impact

ZTNA removes full network access to reduce an organization’s attack surface, improves user experience (UX) and remote access flexibility. It enables dynamic, granular user-to-application segmentation through simplified policy management. Cloud-based zero trust network access (ZTNA) offerings improve scalability and ease of adoption for secure remote access.

Drivers

- The need to modernize and simplify traditional VPN deployments that were optimized for static user locations connecting to data center environments rather than applications, services and data located outside the enterprise.
- The need for augmenting remote access methods with cloud-based ZTNA services to offload hardware-based solutions when hybrid work demand exceeds hardware capacity constraints.
- The rise of zero trust initiatives within organizations, which resulted in the need for more precise access and session control in on-premises and cloud applications.
- A need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing the entire network over VPN, or to connect the application to the internet for access.
- Mergers and acquisitions enabled by the ability to extend application access to acquired companies preclosure without needing to deploy endpoints or interconnect the corporate networks.
- The emergence of the security service edge (SSE) market, including ZTNA components, as organizations increasingly seek to secure private applications, web and cloud-services using a single platform and endpoint agent.

Obstacles

- **Cost:** ZTNA is typically licensed per named user on a per-user/per-year basis at roughly two to three times more than traditional VPNs.
- **Limited support:** Not all products support all applications. For example, some only support web, Remote Desk Protocol (RDP) and Secure Shell (SSH) protocols.
- **Weak identity management:** Organizations with no federated identity support in the cloud find limitations with applicable use cases.
- **No on-premises trust brokers:** Cloud-based trust brokers may not be preferred when extending remote access policies on-premises. Some providers offer both cloud-based and on-premises gateways.
- **Complex policies:** Organizations must map the correct application accesses upfront to get the full benefit of ZTNA, but mapping individuals to resources may be too complex to model, implement and manage operationally at scale.
- **Marketing confusion:** Vendors who market VPN as a service (VPNaaS) (or SSL VPN) as ZTNA confuse buyers as they typically lack some zero trust posture capabilities.

User Recommendations

- Enable applications and services intended for extended workforce and B2B end users to be accessed with ZTNA.
- Normalize the UX for application access both on and off the corporate network.
- Implement application-specific access as an alternative to VPN-based access.
- Extend access to systems prior to a merger, without having to configure site-to-site VPN and firewall rules.
- Allow access on personal devices by reducing full bring your own device (BYOD) management requirements and enabling more secure direct application access.
- Cloak systems from hostile networks, such as traditional VPN concentrators and collaboration systems exposed to the internet.
- Permit users in potentially dangerous areas of the world to interact with limited applications and data to reduce or eliminate risk.
- Secure access to enclaves of Internet of Things (IoT) devices if the device can support a lightweight agent or a virtual appliance-based connector on the IoT network segment.

Sample Vendors

Akamai; Appgate; Banyan Security; Cisco; Cloudflare; Cyolo; Google; Microsoft; Netskope; Zscaler

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

How to Select the Right ZTNA Offering

Best Practices for Implementing Zero Trust Network Access

Quick Answer: How to Securely Enable Access for Unmanaged Devices

2021 Strategic Roadmap for SASE Convergence

Data Sanitization

Analysis By: Rob Schafer, Christopher Dixon

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Data sanitization is the disciplined process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will never be recovered.

Why This Is Important

Growing concerns about data privacy and security, leakage, regulatory compliance, and the ever-expanding capacity of storage media and volume of edge computing and Internet of Things (IoT) devices make robust, consistent and pervasive data sanitization a core C-level requirement for all IT organizations. Remember: It only takes one data-bearing device falling through a crack in what is otherwise a robust process to find your data for sale on the internet.

Business Impact

While data sanitization will not necessarily result in increased revenue or cost savings, it will minimize the risk of significant monetary and brand damage that can result from serious IT asset disposition (ITAD)-related data breaches. The benefit rating is moderate, because data sanitization has become an increasingly accepted process to minimize the material business risks of data security.

Drivers

- Regardless of the targeted end state of deinstalled IT hardware, data sanitization or physical hard-drive destruction/shredding are critical activities to ensure compliance with both internal and external privacy and security requirements. These processes are often most effectively and reliably executed by an experienced ITAD vendor. Given the critical risk to your brand that less-than-robust data sanitization processes represent, certification is required that the data was sanitized to common industry standards.
- The rapidly growing focus on sustainability and specifically the circular economy is driving a shift away from physical destruction to the sanitization/wiping (and consequent reuse) of data-bearing devices.
- Companies are leveraging international standards such as the U.S.-based NIST 800-88 or the U.K.'s ADISA, and requiring NAID's AAA Certification (not just NAID membership) of ITAD service providers. To minimize chain-of-custody security risks (such as loss in transit to the ITAD vendor's facility), many ITAD managers (especially in the financial and healthcare sectors) require that some form of data sanitization be performed on-site. Some that do not require on-site data sanitization instead enforce data encryption on all data-bearing devices to minimize chain-of-custody security risks.
- Comprehensive data sanitization is being applied to all devices with storage components (e.g., enterprise storage and servers, PCs, mobile devices, and increasingly, edge computing and some IoT devices). Lack of robust data sanitization competency is often due to handling asset life cycle stages as isolated events, with little coordination between business boundaries (such as finance, security, procurement and IT).
- For mobile devices, a remote data-wiping capability is commonly implemented via a mobile device manager (MDM). Although this should not be considered a fail-safe mechanism, its reliability should be adequate for most lost or stolen mobile devices.

Obstacles

- **Complacency:** The "business-as-usual" syndrome: "We've always done it this way and never had a problem." The rapid increase in data security requirements (e.g., General Data Protection Regulation [GDPR], Health Insurance Portability and Accountability Act [HIPAA], and the California Consumer Privacy Act [CCPA]) dictate a thorough (annual) review of data security and sanitization processes.
- **Cost:** Robust data sanitization is costly compared to the many lower-cost "trust me" alternatives (e.g., the "friend" who promises his processes are robust). Remember: This is about the integrity of your brand in the market.
- **Lack of executive awareness and focus:** Too often, C-level executives confidently say they have world-class data sanitization processes in place, yet haven't had a thorough review/audit of those processes in several years. Large organizations may well have a robust, disciplined data sanitization process in place, but in certain remote locations those processes are not consistently enforced.

User Recommendations

- Follow an IT risk management life cycle approach that includes explicit, documented decisions about data archiving, sanitization, and device reuse and retirement.
- Collaborate with data sanitization stakeholders (e.g., IT, security, privacy, compliance, legal, IT asset managers) to create appropriate end-to-end data sanitization standards and processes, based on data sensitivity, for all data bearing devices.
- As different media require different sanitizing methods, ensure your internal IT organization or external ITAD vendor provides a certificate of data destruction to your security standards (e.g., NIST 800-88).
- Assess and minimize the security risks of portable data-bearing devices (e.g., USB drives, IoT devices).
- For externally provisioned services (e.g., SaaS, infrastructure as a service [IaaS], platform as a service [PaaS]), analyze end-of-contract implications and data-exit processes, and request that providers supply their data destruction, storage reuse and recycling practices and certifications.

Sample Vendors

Blancco; Iron Mountain (ITRenew)

Gartner Recommended Reading

Market Guide for IT Asset Disposition

Market Guide for Mobile Threat Defense

Endpoint Detection and Response

Analysis By: Paul Webber, Jon Amato

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Endpoint detection and response (EDR) solutions facilitate detection and investigation of security events, identify attacks and produce remediation guidance. They must analyze all user, process and system activity, and report device configuration. Detection of threats is combined with remote remediation. Automation of response actions is usually provided and tight integration with other tools is key. Cloud services are prevalent and some vendors provide on-premises options as well.

Why This Is Important

All systems exposed to the internet, or hosted in internal networks, are potentially at risk from attacks that target vulnerable or unprotected systems. EDR is an essential part of any layered defense. It must be deployed to all systems in order to report configuration and telemetry, identify anomalous or malicious activity, reveal the tactics and techniques of advanced attacks and provide a response facility. EDR prevents known malware and ransomware and can identify advanced threats.

Business Impact

- EDR is a must-have protection layer for all sectors and must be applied to all devices and servers that connect to corporate systems or handle data.
- Early detection and rapid response are critical for dealing with the latest threats and stealthy exploits that can evade traditional detection.
- EDR is a mandatory security control required by cyber insurers and regulatory bodies, and some EDRs provide basic cost-effective ransomware insurance.

Drivers

- The nature of threats has changed. It is no longer practical to achieve 100% prevention and protection, and older endpoint protection platform (EPP) tools should be updated with EDR functionality. Stealthy malware and ransomware campaigns, state-sponsored adversaries and supply chain attacks use advanced techniques to remain undetected and to bypass older security controls.
- Remote work has accelerated the adoption of cloud-managed solutions, which now represent 80% of the installed base and most new deployments.
- Fileless attacks are now a common component of all malware types, making the behavioral detection of EDR tools critical to combatting both advanced threats and ever-changing human-operated ransomware campaigns.
- Advanced adversaries targeting an organization have shown that they can disable protection solutions, making antitamper protection critical. Comprehensive alerting and telemetry to facilitate early detection and fast response are also needed.
- Detection of user- and machine-identity-related exploits and credential misuse is an emerging must-have feature.
- Rapid real-time response, as incidents unfold, is critical to contain a threat and stop 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.
- Sophisticated attacks require a new breed of EDR tools that work holistically together with other security tools as a composable security ecosystem to maximize protection and minimize exposure.

Obstacles

- Adding sophisticated detection and response features is now considered mainstream, though many organizations still lack the skills and resources to effectively configure and use them.
- EDR adoption must be accompanied by investment in training responders, including “range” training that simulates real attacks.
- Cloud-hosted workloads often have radically different “agile” deployment pipelines that preclude the use of traditional endpoint security tools and agents. This results in a split environment, using separate tools for agile deployed workloads and containers or serverless compute.
- 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.
- Older on-premises solutions present deployment and maintenance issues when combined with current hybrid and remote working models where devices do not connect to campus networks.

User Recommendations

- Select solutions with a single lightweight agent, simple and rapid remote deployment, and low maintenance needs.
- Search for tools with automated playbooks and response actions if in-house resources are scant.
- Favor cloud-hosted solutions with fast time-to-value and vendors that provide flexibly hosted cloud-native deployment including multi- and hybrid-cloud or private cloud.
- Target vendors that provide managed services themselves, including alerting, monitoring, incident response, and managed detection and response.
- Favor vendors that can identify vulnerabilities and correct misconfigurations to harden the endpoint against attack.
- Identify EDR tools that provide direct access to endpoints to rapidly respond to issues.
- Specify tools with antitamper measures to ensure that agents are not disabled by attackers.
- Ensure data retention is adequate, uses archiving or low-cost long-term storage, and meets regulatory and regional compliance requirements (including for logging and monitoring needs).

Sample Vendors

Bitdefender; Cisco; CrowdStrike; Cybereason; Microsoft; SentinelOne; Sophos; Trellix; Trend Micro; VMware Carbon Black

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

UEM

Analysis By: Tom Cipolla, Dan Wilson, Craig Fisler, Chris Silva

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Unified endpoint management (UEM) tools provide agent-based and agentless management of endpoint devices running Windows, Google Android and Chrome OS, Apple macOS, iPadOS, and iOS. UEM tools apply data protection, device configuration and usage policies using telemetry from identities, apps, connectivity and devices. They also integrate with identity, security and remote access tools to support zero trust.

Why This Is Important

UEM simplifies endpoint management by consolidating disparate tools and streamlining processes across devices and operating systems. UEM has expanded beyond management to offer deeper integration with identity, security and remote access VPN tooling to support a zero-trust security model. Leading UEM tools also use intelligence to drive automation, reduce IT overhead and improve the digital employee experience (DEX) through rich data collection and insights.

Business Impact

By adopting UEM, it is possible to streamline and improve endpoint management. Specific impacts include:

- Location-agnostic endpoint management and patching, enabling the distributed enterprise.
- Reduced total cost of ownership (TCO) by simplifying device management and support processes.
- Better security hygiene through consistent application of configuration and data security across all platforms

Drivers

- Supporting hybrid and remote workers requires tools that extend beyond a single platform or require devices to be on a specific network to function.
- IT looks to simplify and streamline endpoint deployment, management and patching to enable provisioning of new devices for remote employees and reduce security risk through consistent controls and configuration management.
- Increasing emphasis on improving DEX requires greater visibility into endpoint performance, reliability and consistency. Advanced UEM tools are doing this through broader use of analytics, ML and automation.
- Consolidation of disparate endpoint support teams, tools, processes and definitions of success into a centralized endpoint management framework to support efficiency efforts and the transition to higher business-valued work.
- Increased cyberattacks demand faster patch deployment and improved configuration management control and compliance.

Obstacles

- Legacy organization models where the responsibility for mobile and PC management, remote access, and security is distributed across several IT teams.
- Lack of skills or resource availability to adopt new tools or practices.
- Heavy reliance on antiquated and ineffective high-touch practices of the past, such as monolithic imaging.
- Cost concerns for the small number of organizations that do not yet use mobile device management or client management tools.
- Organizations with many GPOs with little awareness of what each does will struggle to rationalize them in order to migrate to configuration service provider (CSP) profiles.
- Highly complex environments with multiple Active Directory forests or domains and/or autonomous subsidiaries or business units may struggle with the centralized nature of UEM tools.
- Fragile environments with a significant amount of technical debt, including legacy operating systems or applications that depend on unsupported browsers, runtime environments or plug-ins.

User Recommendations

UEM has advanced within the Slope of Enlightenment and is approaching the Plateau of Productivity as UEM tools have matured and adoption has increased. Many organizations have successfully completed the human change management that is required to adapt processes and have started to refocus IT staff on simplifying and modernizing endpoint management.

- Improve endpoint posture, security and ease operations by consolidating PC, macOS, and mobile management into a single UEM.
- Review IT policies and procedures to identify and eliminate unnecessary references to or dependence on MDM, CMT or location-specific technologies. This will help avoid common inertia, limitations and excuses related to something being against policy.
- Upskill or replace IT engineers and support staff to increase the use of UEM, modern management and automation capabilities.

Gartner Recommended Reading

Magic Quadrant for Unified Endpoint Management Tools

Critical Capabilities for Unified Endpoint Management Tools

Embrace Windows 10 Modern Management to Enable a Highly Distributed Digital Workplace

Modernize Windows and Third-Party Application Patching

How to Implement Continuous Endpoint Engineering: An Agile Approach for the Digital Workplace

CASBs

Analysis By: Craig Lawson, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud access security brokers (CASBs) provide critical controls to allow for the secure use of cloud services, with key features being visibility, compliance, data security and threat protection. They consolidate multiple types of security enforcement into one place that can span SaaS, IaaS and PaaS.

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 use of CASBs.

Business Impact

CASBs enable the secure use of cloud services, are suitable for organizations of all sizes in all industries and can demonstrate that organizational cloud usage is well-governed. With continued feature expansion, ongoing convergence with secure web gateway (SWG) and zero trust network access (ZTNA) into security service edge (SSE), and relative ease of switching providers, we recommend preferencing an SSE solution when renewing or selecting CASB features. One year contract terms are still recommended for this evolving market unless substantial discounts can be obtained and you are satisfied with that vendor's roadmap execution.

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 CASB vendors enabling secure use of business-critical cloud applications and infrastructure, and SWG 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 past few years have seen 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

- Unclear and often distributed organizational ownership of cloud services can lead to a CASB implementation that fails to secure these services adequately.
- Overlapping CASB functionality from a number of vendors leads to duplication and confusion. Lack of an effective data security policy can lead to frustration, with a CASB trying to enforce an ineffective policy resulting in issues like false positives and risk of data loss.
- A subset of controls are offered by some cloud service providers themselves. For example, Microsoft 365's native security features and Salesforce Shield continue to see interest from users.
- Some cloud workload protection platform (CWPP)/cloud native application protection platform (CNAPP) offerings also overlap in the area of IaaS security.

User Recommendations

The CASB market has now converged into the security service edge (SSE) market and, as such, Gartner has depreciated the stand-alone CASB and SWG Magic Quadrants. Therefore, we recommend you:

- Move to a consolidated SSE offering during upcoming refresh cycles.
- Read the Magic Quadrant for Security Service Edge for a more detailed analysis of the SSE market where we have detailed evaluations of vendors that can help you secure access to the web, cloud services and private applications.
- 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 a CASB.

Sample Vendors

Broadcom; Cisco; iboss; Lookout; Microsoft; Netskope; Palo Alto Networks; Skyhigh Security; Versa; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Market Guide for Zero Trust Network Access

Entering the Plateau

Endpoint Protection Platforms

Analysis By: Franz Hinner, Jon Amato

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Endpoint protection platforms (EPPs) protect against existing and emerging unknown threats against endpoints. Primarily safeguarding against malware, file-based and fileless exploits, EPPs continue to embrace technologies and practices against the growth of stealth attacks and ransomware. They also support the continuation of remote and hybrid working while growing investigative and remediation capabilities.

Why This Is Important

Attackers use increasingly sophisticated techniques against enterprise endpoints. Ransomware, in particular, has evolved from relatively simple automated methods to highly organized human-operated attacks with the goal to extract between 1% and 2% of corporate revenue as ransom. Defending against evolving attacks, EPPs are evolving to include endpoint detection and response (EDR) capabilities

Business Impact

EPP is considered fundamental security hygiene for all organizations and is fully deployed on 99% of enterprise endpoints. It is impossible to predevelop protection for all possible future attack techniques, increasing the emphasis on effective detect-and-respond capabilities of EDR. However, expansion into EDR increases the license cost, administration workload and training requirements.

Drivers

- EPPs have adapted to address more advanced threats and combat stealthier attackers. Organizations currently place a premium on preventing rare, long-running targeted, and fileless attacks. Machine learning and cloud-based look-up capabilities are alternatives to local, signature-based identification. Ease of use, low resource utilization and reduced maintenance are must haves. Agent tampering protection mechanisms are essential.

- Principal EPP innovations are cloud-native solutions that are easier to deploy and manage, as well as advances in behavior-based detection and analytics that allow the identification of unseen threats.
- OS security has further marginalized the scope for EPP by improving prevention of previously unseen attacks, protecting credentials, preventing kernel attacks, and isolating critical security services from being compromised. Additionally, virtualized browsers and applications reduce the risk of OS compromise.
- EPP vendors are consolidating multiple capabilities into a single platform to widen the appeal and extend security protection to IT disciplines like firewall management, device control, threat- and risk-based vulnerability management, and patching. Some providers even include application control and storage encryption management in their toolsets.

Obstacles

- As EPP enables real-time monitoring and other advanced capabilities, it is critical to overall security operations.
- EPPs are often anchor products in more extensive portfolios of security infrastructure (such as firewalls, email security, security service edge, and other core products) for buyers seeking more out-of-the-box integration.
- Dedicated EPP vendors are assessing how they can fit into broader security operations and eliminate blind spots and information silos to make incident response and alert management more efficient.
- Improved security in the core OS will likely shift the focus of attackers toward application weaknesses and BIOS or firmware exploits outside of the OS.
- More stealthy attacks mean that EDR features are required to detect and respond to threats that would bypass EPP tools that are reliant on prevention alone. These mechanisms are not optimal for identifying stealthy techniques that already exploit trusted and existing utilities.

User Recommendations

- Assess the strategic fit with the security operations incident response.
- Seek solution providers that fit with existing security staffing levels and those that can supplement staff with an extensive support and services menu and training.

- Assess whether vendors can provide managed service offerings where the organization lacks internal resources or skills to operate advanced EPP solutions.
- Favor solutions that have a cloud look-up of unknown items and good anti-tamper protection.
- Seek a solution provider that can consolidate numerous endpoint security functions into tightly managed solutions.
- Seek solutions that can help harden and reduce the attack surface.
- Focus on solutions that can remediate systems remotely, with manual and automatable actions.

Sample Vendors

Broadcom (Symantec); Bitdefender; CrowdStrike; Cisco; Cybereason; Deep Instinct; Trellix; Microsoft; SentinelOne; Sophos; Trend Micro; VMware Carbon Black

Gartner Recommended Reading

Secure Web Gateways

Analysis By: John Watts

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Secure web gateways (SWGs) use URL filtering and a range of advanced threat defense (ATD) methods to protect organizations and enforce internet use and compliance with acceptable use policies. SWGs are delivered as cloud-based services, hybrid (cloud and on-premises), or on-premises solutions only.

Why This Is Important

Because SWGs are positioned between the user and the internet, they offer valuable protection from internet-born threats. Also, the SWG dashboards and reporting tools provide visibility into users' behavior on the internet. This functionality is important to detect and investigate whether an employee has violated the organization's internet usage policy.

Business Impact

SWGs provide an additional layer of protection against destructive attacks, and enable safer, more-efficient adoption of cloud-based services. Cloud-delivered SWGs can reduce branch office networking costs by using commodity internet access for outbound web security, instead of backhauling web traffic over MPLS links to appliances in a centralized data center. Cloud SWG services are increasingly part of security service edge (SSE) offerings to provide protection regardless of the location.

Drivers

- Rapid adoption of SaaS and hybird work is driving enterprises to migrate from on-premises, appliance-based SWGs to cloud-delivered SWG services. They are increasingly delivered with cloud access security broker (CASB) and zero trust network access (ZTNA) components from a converged SSE offering.
- Improve the end-user experience through a reduction in latency by routing internet-bound traffic directly to a cloud SWG, rather than using a WAN backhaul to a centralized data center where physical security appliances are positioned.
- Cloud-based SWGs continue to add security services, including firewall as a service (to apply policies to all ports and protocols), data loss prevention (DLP), sandboxing and remote browser isolation. Cloud-based SWGs form the foundation for platforms that can decrypt once and inspect with multiple security services to improve latency.

Obstacles

- Cloud-based recursive DNS solutions have become popular solutions with midmarket customers, because they offer cost-effective security protection. Some of the Domain Name System (DNS) services use selective proxying — i.e., they proxy traffic destined for suspicious websites (typically, about 10% to 15% of the traffic is proxied).
- Some industry verticals that are cloud-averse have resisted migrating their on-premises SWGs to the cloud. This is particularly true in the financial services and healthcare verticals.
- Appliance-based SWG options in the market are dwindling, forcing organizations that require on-premises appliances to consider alternatives, such as higher-end, hardware-based firewalls on the edge to decrypt and inspect web traffic.

User Recommendations

- Take a fresh look at the emerging SSE market, rather than the stand-alone SWG market, when renewing existing appliance or cloud SWG contracts.
- Replace SWG appliances with cloud-based SWG offerings as part of a larger SSE service to improve the end-user experience and flexibility to apply a single web security policy for hybrid workers.
- Replace branch office firewalls with a secure access service edge (SASE) architecture that includes cloud-based SWG to secure web traffic integrated with a software-defined wide-area network (SD-WAN) device at the branch.

Sample Vendors

Broadcom; Cisco; ContentKeeper; Forcepoint; iboss; SkyHigh Security; Menlo Security; Netskope; Sangfor Technologies; Zscaler

Gartner Recommended Reading

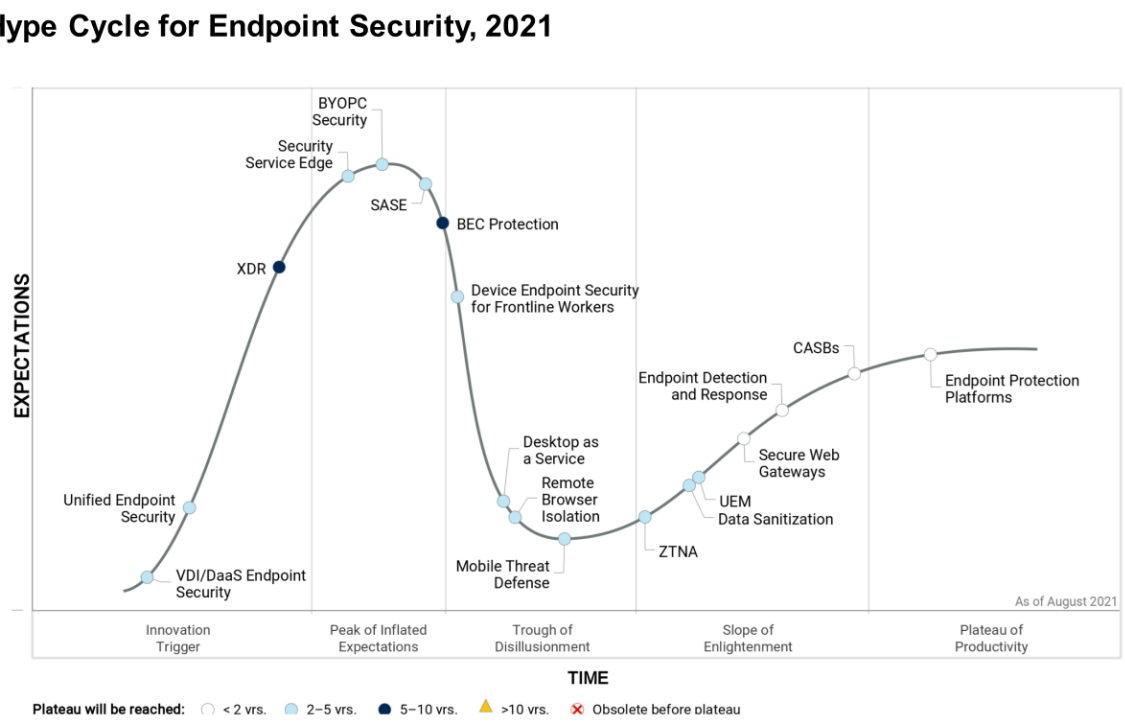
Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Using Secure Web Gateway Technologies to Protect Users and Endpoints

Appendixes

Figure 2. Hype Cycle for Endpoint Security, 2021



Source: Gartner (August 2021)

747412

Gartner

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 (December 2022)

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 (December 2022)

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 (December 2022)

Acronym Key and Glossary Terms

ASA	attack surface assessment
ASM	attack surface management
BEC	business email compromise
BYOPC	bring your own personal computer
CASB	cloud access security broker
DaaS	desktop as a service
EDR	endpoint detection and response
EPP	endpoint protection platform
SASE	secure access service edge
SSE	security service edge
SWG	secure web gateway
UEM	unified endpoint management
UES	unified endpoint security
VDI	virtual desktop infrastructure
VMI	virtual mobile infrastructure
VPN	virtual private network
XDR	extended detection and response
ZTNA	zero trust network access

Document Revision History

Hype Cycle for Endpoint Security, 2021 - 11 August 2021

Hype Cycle for Endpoint Security, 2020 - 15 July 2020

Hype Cycle for Endpoint Security, 2019 - 31 July 2019

Hype Cycle for Endpoint and Mobile Security, 2018 - 25 July 2018

Hype Cycle for Mobile Security, 2017 - 20 July 2017

Hype Cycle for Mobile Security, 2016 - 14 July 2016

Hype Cycle for Enterprise Mobile Security, 2015 - 22 July 2015

Hype Cycle for Enterprise Mobile Security, 2014 - 24 July 2014

Recommended by the Author

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

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

Innovation Insight for Extended Detection and Response

Innovation Insight for Unified Endpoint Security

Table 1: Priority Matrix for Endpoint Security, 2022

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	CASBs	BYOPC Security SASE Security Service Edge		
High	Endpoint Detection and Response Secure Web Gateways UEM	Breach and Attack Simulation Content Disarm and Reconstruction Desktop as a Service Identity Threat Detection and Response (ITDR) Unified Endpoint Security	Business Email Compromise Protection Exposure Management XDR	
Moderate	Endpoint Protection Platforms	Data Sanitization Device Endpoint Security for Frontline Workers Mobile Threat Defense Remote Browser Isolation ZTNA	External Attack Surface Management VDI/DaaS Endpoint Security	
Low				

Source: Gartner (December 2022)

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 (December 2022)

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 (December 2022)

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 (December 2022)