Hype Cycle for Endpoint Security, 2023

Published 1 August 2023 - ID G00793050 - 85 min read

By Analyst(s): Franz Hinner, Satarupa Patnaik, Eric Grenier, Nikul Patel

Initiatives: Infrastructure Security; Meet Daily Cybersecurity Needs

Businesses need cutting-edge solutions to defend endpoints against attacks and breaches. While EDR has become standard, XDR has become the next evolutionary step. UES, DaaS, ASCA, EASM, BAS, EM, ITDR, EAI and AMTD are cutting-edge technologies that provide new XDR views and approaches.

Analysis

What You Need to Know

This Hype Cycle illustrates the most relevant innovations in the endpoint security space to assist security leaders in planning adoption and implementation of emerging technologies. Endpoint security innovations focus on faster, automated detection and prevention, and remediation of threats powering integrated, extended detection and response (XDR) to correlate data points and telemetry from solutions such as endpoint, network, web, email and identity. Methods to provide lightweight, secure remote access remain in demand driving desktop as a service (DaaS) and endpoint and browser isolation for increased control and security posture. We see continued adoption of zero-trust network access (ZTNA), increasingly as a part of security service edge (SSE) or a wider secure access service edge (SASE). This enables application access from any device over any network, with minimal impact on user experience.

The Hype Cycle

The Hype Cycle for Endpoint Security tracks developments that help security executives defend their companies. Two tendencies occur when technology evolves:

- New endpoint technologies include endpoint access isolation, endpoint-agnostic workspace security, and endpoint protection toolset integrations and upgrades.
- Net new security investments may focus on new technologies and suppliers since most purchasers consolidate vendors.

The operational burden of deploying internal people for threat hunting demands greater signal correlation and automation of reaction to counter sophisticated, targeted attacks. This Hype Cycle shows XDR spreading again.

Unified endpoint security (UES), which integrates endpoint protection platform (EPP) and MTD security assets, is rising in this Hype Cycle. While usage is limited, endpoint operations solutions that configure devices for consistency of control and speedy remedial activities are anticipated to grow.

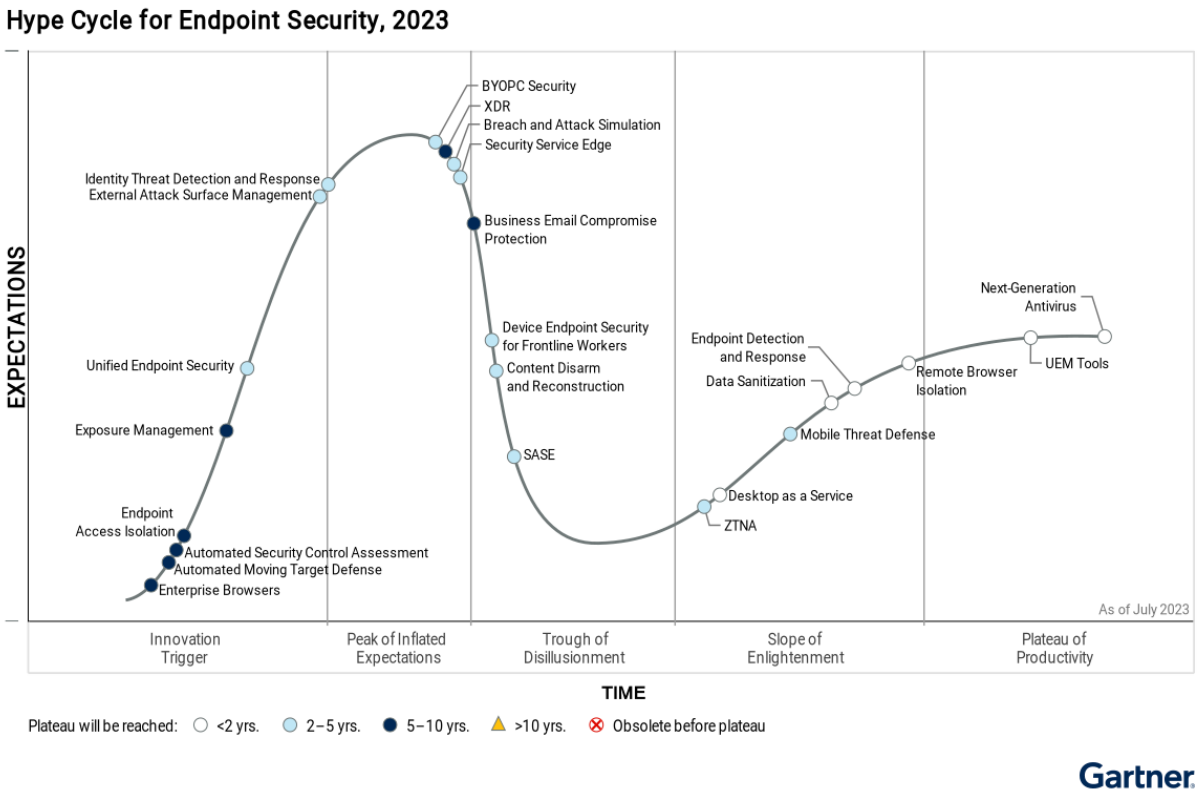
Endpoint detection and response (EDR) adoption continues as EPP matures. This year, business email compromise (BEC) security will detect compromised accounts to prevent phishing. Network-based secure web gateways (SWGs) also prevent endpoint attacks, especially cloud-based ones. SSE is absorbing SWG capabilities.

Technology supports distant and hybrid work. New skills mature and spread.

Bring your own PC (BYOPC), unified endpoint management (UEM) and DaaS are mature in tackling access and endpoint isolation issues, but they are rigid, encouraging technologies like enterprise application integration (EAI) to ascend the hill. SSE empowers ZTNA to let any device access any app over any network. ZTNA alone exposes endpoints to online attacks and loses control of SaaS programs. ZTNA, SASE and new zero-trust philosophy implementations like automated moving target defense (AMTD) are being embraced at different paces.

Edge security services are touted. Buyers want platformwide security tools. UES products encompass phones, tablets and PCs. Attack surface management (ASM) and breach simulation provide unique adversary engagement and understanding. XDR uses several domains and data to identify threats faster. Gartner’s February 2023 Security Vendor Consolidation report shows security and risk managers prefer vendor consolidation as technology improves.

Figure 1: Hype Cycle for Endpoint Security, 2023



The Priority Matrix

Transformational Technology

Gartner has seen SASE defend any application, network and endpoint. Security executives should use SASE to combine network security point solutions like SWG, cloud access security broker (CASB) and ZTNA with SD-WAN transformations and couple with other endpoint security to secure endpoints regardless of location.

Key Technologies

As XDR grows, Gartner expects commercial and technological application cases. These applications simulate bogus assaults to identify hazards quickly. Endpoint detection and response, UEM, and DaaS solutions will become essential for BYOPC security, UES and XDR. Endpoint malware protection needs improvement. As generative AI advances, corporations will prioritize BEC. Attack surface assessment (ASA) and breach attack simulation (BAS) are part of a complete endpoint strategy. Attack surface management (ASM) uses XDR telemetry to catalog attack surfaces without using ASA or BAS, or creating new deceptive technological use cases. These technologies and exposure management (EM) let defenders cross-correlate detection and attack behavior, and teach machine learning and deep learning algorithms new methods through behavior pattern improvement.

Table 1: Priority Matrix for Endpoint Security, 2023

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		SASE Security Service Edge	Exposure Management	
High	Desktop as a Service Endpoint Detection and Response UEM Tools	Breach and Attack Simulation BYOPC Security Content Disarm and Reconstruction Identity Threat Detection and Response Unified Endpoint Security	Automated Moving Target Defense Business Email Compromise Protection XDR	
Moderate	Data Sanitization Next-Generation Antivirus	Device Endpoint Security for Frontline Workers External Attack Surface Management Mobile Threat Defense ZTNA	Automated Security Control Assessment Endpoint Access Isolation Enterprise Browsers	
Low	Remote Browser Isolation			

Source: Gartner (August 2023)

Off the Hype Cycle

Secure Corporate Data Transmissions: Virtual private network (VPN) architecture has matured into a well-understood and reliable solution for remote access problems. The growing importance of ZTNA ideas and SASE tools means that VPN-based secure business data transfers are exiting the Hype Cycle. Contextual, dynamic access restrictions for a wide range of remote employees enabled by deploying these solutions in addition to or in substitute of current VPN infrastructure.

On the Rise

Enterprise Browsers

Analysis By: Dan Ayoub

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Enterprise browsers and extensions deliver security services for policy enforcement, visibility, and productivity through a managed web browser or plug-in extensions. Many products in this category provide lightweight features and benefits similar to those found in SWG, CASB, ZTNA, RBI, VDI, and VPN products. Enterprise browsers are complementary to existing security solutions, and have seen early success providing access and posture assessment security to unmanaged devices.

Why This Is Important

Enterprise browsers represent a new way of delivering security services and receiving real-time intelligence from existing security agents layered into the OS. Today, many of these products are able to deliver some important features and benefits of other security products; however, trade-offs still remain. This gap is expected to close over time as the category becomes more mature and more partners enter the ecosystem.

Business Impact

Existing security products will continue to provide enterprises with increasingly sophisticated levels of protection, access control and reporting analytics. However, many of these products will extend functionality to support browsers via strategic partnerships, integrations or browser extensions. Enterprise browsers are not likely to replace existing security controls throughout the enterprise, but rather extend the reach of these tools for additional use-case coverage.

Drivers

- Enterprise browsers are embracing the new remote-work paradigm to consolidate secure remote access for contractors, suppliers and branch locations relying on nonstandardized equipment.

- Existing security solutions often struggle to support unmanaged devices. This is an area where enterprise browsers have found early traction in the market, by providing an acceptable level of secure remote access that is able to maintain a mostly familiar end-user experience.
- Small and midsize organizations are also expected to be early adopters of this technology. Organizations with simpler environments and requirements may see early opportunities to displace existing or add new security controls with an enterprise browser as a cheaper, centrally managed option that immediately raises their maturity level.
- Many security vendors already offer integration with browsers via extensions, while others have sought strategic partnerships and integrations with browser manufacturers. Enterprise browsers represent a new way of delivering security services to an organization, which extend the edge of traditional network security solutions.
- Enterprise browser vendors are increasing integration with security controls, such as data loss prevention (DLP), configuration management, logging and integration with security information and event management (SIEM)/extended detection and response (XDR) platforms, identity protection, phishing protection, security service edge (SSE) functions, and monitoring for malicious activity across downloads and extensions.

Obstacles

- Free browsers are ubiquitous, to the point that organizations must have specific use cases to justify the purchase of a separate browser. These justifications will become easier to identify as enterprises begin to realize the extensible and flexible enterprise security and management potential of the browser. However, it is unlikely most companies will dedicate budget to an enterprise browser without the ability to offset that spend elsewhere.
- Larger organizations with mature cybersecurity and infrastructure operations may find it impractical to reduce the complexity of their existing environments with enterprise browsers, though specific use cases may exist to justify a relatively small purchase (such as providing Day 1 access for new organizations gained through mergers and acquisitions, contractor access management, or as layered security controls on top of fragile critical infrastructure).

User Recommendations

- Recognize that placing all security controls at the endpoint (or in this case, browser) is a flawed strategy. Browser-based integrations may make sense in some circumstances, but having multiple points of integration will be required.
- Focus on hybrid offerings that are able to leverage browsers to securely deliver access to workforce productivity tools.
- Exercise caution when reviewing messaging and promises from vendors in this space, as specialized infrastructure (proxy, gateway, etc.) may still be required to address certain use cases.
- Expect an increasing number of security and productivity tool capabilities to be incorporated over time. However, the technology is still in the early stages of adoption, so individual vendor roadmaps will be driven by early market success.

Sample Vendors

Check Point Software Technologies; Ermes Cyber Security; Google; Island; Microsoft; Perception Point; Seraphic Security; SlashNext; SURF Security; Talon Cyber Security

Gartner Recommended Reading

Emerging Tech: Security — The Future of Enterprise Browsers

Automated Moving Target Defense

Analysis By: Lawrence Pingree

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Automated moving target defense (AMTD) is a set of technologies that combine deception techniques with unpredictable automated changes to an endpoint, it's configuration or via memory morphing, software-defined networks, containerization, cryptography or other modifications to runtime elements, making it much harder for attackers to identify and exploit vulnerabilities.

Why This Is Important

- AMTD shifts from “detect and respond” to “proactive deception and unpredictable change” to make it tougher for attackers to exploit vulnerabilities in a targeted IT environment.
- AMTD on endpoints disrupts attackers automatically without extensive threat modeling, threat detection logic, or threat intelligence.
- AMTD can prevent attackers from pattern-analyzing networks and services.
- Security operations personnel are overworked and spend a lot of time investigating false alarms.

Business Impact

The business impacts include:

- Organizations with a heavy focus on security continue to face advanced attacks and must move beyond failing detection and response.
- AMTD helps average companies combat emerging AI threats. AMTD is an alternative for organizations when they do not have the budget, staff or time for using AI.
- AMTD promises to reduce security operations staffing requirements by reducing the false positive rates of detection and response technologies, reducing impact breadth and enhancing the detection of advanced attacks.

Drivers

- AMTD technologies and academic research have emerged, creating new ways to implement proactive defensive strategies needed to modernize proactive instead of reactive prevention.
- AMTD technologies have emerged that are capable of delivering new value in defending against the backdrop of an overemphasis on detection and response strategies that are failing to prevent breaches.
- Work-from-home systems are a growing source of data breaches for enterprises and breached credential reuse.

Obstacles

- Buyers wrongly perceive that techniques in moving target defense are disruptive in nature, too simple or have a misunderstanding of the benefits of obfuscation for defense against threats on endpoint systems.
- Work-from-home endpoints suffer from personal resistance to the behavioral recording due to concerns about privacy and management.
- Organizations face a sunk-cost fallacy when considering adoption of AMTD given the extensive investments in existing security controls (such as NGAV, EPP, EDR) designed to be reactive in nature. AMTD introduces proactive controls for identifying threats early and may not replace existing investments.
- Legacy technology may not be in scope for AMTD, including older endpoints, reducing the value of AMTD for the organization.
- AMTD vendors are just now developing the technology and face scalability challenges for larger implementations, particularly for network-focused AMTD.
- Timing. Customers are in “consolidation vs. expansion” mode in many security programs.

User Recommendations

Users evaluating automated moving target defense should:

- Seek to leverage AMTD with mature security operations teams who have a risk appetite for leading edge technology.
- Prioritize AMTD as an optional defensive strategy and technology portfolio augmentation if they are in certain verticals that have a high criticality of defense.
- Evaluate which AMTD solutions are a fit for their environment and allow them to achieve defense-in-depth and maximize deception effectiveness.
- Move away from reactive endpoint protection and toward proactive defense, proof-of-concept studies should be conducted on the potential addition of AMTD-enabled solutions throughout the security stack.
- Enhance current tools like EPP and EDR at the application layer in workloads with AMTD.

- Cover testing workstations and workload endpoints first as these are easy candidates for malware and hacking.
- Require security providers to enhance their product roadmaps with automated moving target defense technologies and strategies to address evolving threats.

Sample Vendors

Agita Labs; ARMS Cyber Defense; Cisco; Dispel; Dispersive; Hopr.co; Morphisec; NexiTech; R6 Security; RunSafe Security

Gartner Recommended Reading

Emerging Tech: Security — The Future of Cyber Is Automated Moving Target DefenseEmerging Tech: Security — Emergence Cycle for Automated Moving Target DefenseEmerging Tech: Security — Tech Innovators in Automated Moving Target Defense

Automated Security Control Assessment

Analysis By: Evgeny Mirolyubov, Jeremy D'Hoinne

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

ASCA processes and technologies focus on the analysis and remediation of misconfigurations in security controls (e.g., endpoint protection, network firewall, identity, email security, and security information and event management), which improves enterprise security posture. ASCA can be a stand-alone tool or a capability of other security products, such as firewalls, identity threat detection and response, network security policy management, and cloud infrastructure entitlement management.

Why This Is Important

Automated security control assessment (ASCA) technologies reduce an organization's attack surface caused by security configuration drift, poor defaults, exessive tuning to reduce false positive rates, and high administration staff turnover. ASCA improves the security posture by verifying the proper, consistent configuration of security controls, rather than simply verifying the existence of controls.

Business Impact

Organizations implementing ASCA processes and technologies enhance staff efficiency, minimize the impact of human errors and improve resilience in the face of organizational churn. ASCA reduces security control configuration gaps that unnecessarily expose the organization to otherwise preventable attacks.

Drivers

- The volume of misconfigurations in security controls continues to grow with the increased complexity of environments, emerging threat vectors, the proliferation of new security tools and the high turnover of administration staff, leading to a more exposed attack surface.
- Specific organizational use cases and objectives require the preservation of complex heterogeneous infrastructure and security architectures, instead of pursuing simplification through vendor consolidation.
- The optimization of configurations of enterprise security controls cannot rely exclusively on manual periodic configuration reviews; siloed, tool-centric approaches; or occasional penetration tests.
- Continuously assessing and remediating security controls configurations in accordance with the highest-risk exposures is an effective risk mitigation strategy, ultimately reducing the attack surface.

Obstacles

- Lack of support for niche vendor and security control assessments makes ASCA tools less valuable for large, complex organizations with specialized point solutions.
- Overlaps with existing tools and vendors that are looking to accomplish similar goals in individual silos, such as tools for network firewall or cloud configuration assessments.
- The slow pace of remediation, paired with continuous assessments, may cause findings to pile up without proper automation and a triage process that considers business context.
- Lack of mature processes to optimize security controls configurations end to end.
- Budget increases to invest in people, technologies and, possibly, managed services needed to respond to an accelerated list of configuration issues discovered by ASCA tools.

User Recommendations

- Reduce complexity by pursuing security vendor consolidation or considering alternatives, such as “policy as code” to manage security configurations.
- Establish processes to evaluate enterprise security controls, including planning, assessing, remediating and validating expected configurations.
- Evaluate incumbent security providers for ASCA capabilities, including continuous configuration monitoring and alerting about the impact of configuration changes on security protection, operations and productivity.
- Assess ASCA providers’ capabilities, including the breadth of coverage for your enterprise security controls, cross-control configuration analysis quality and integration of input from cybersecurity validation tools, such as BAS and VA.

Sample Vendors

Absolute Software; CardinalOps; Veriti; XM Cyber

Endpoint Access Isolation

Analysis By: Chris Silva, Stuart Downes

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Endpoint access isolation (formerly VDI/DaaS endpoint security) facilitates secure access to applications, VDI/DaaS environments, and data using local apps that isolate the session data from the device. Deployed as an agent, browser-based app or extension, the technology extends access to external PCs where a traditional VPN or virtualization client software can’t be used. Local controls include session-hijacking protection, keylogging and screen-capture prevention, and local user verification.

Why This Is Important

Endpoint access isolation is client-side software that can offer use-case-specific isolation of the client device when interacting with workplace apps and data. The technology can be delivered as a dedicated secure access agent, browser-based-app or extension isolating the systems being accessed from local vulnerabilities. Endpoint access isolation tools differ from traditional access clients by adding active prevention and detection features to posturing and profiling.

Business Impact

Traditional remote access tools like classic VPN can profile a device but can't actively neutralize local threats. As organizations rethink allowing access to SaaS apps via any browser, from any device, this technology can offer a more secure way to reach these apps. This technology allows organizations to simplify both the standard IT "stack" and its deployment to end users for remote access. This is particularly important as hybrid working remains a day-to-day reality for most organizations.

Drivers

- Trading physical hardware for virtual desktop infrastructure (VDI) and desktop as a service (DaaS) sessions for contractors and partners won't address the underlying security issues of the local machine — a viable vector for credential and IP theft.
- There has been strong investment in enterprise browser solutions — one manifestation of endpoint access isolation.
- There is a trend of adding a layer of security through enforcing consistent browser configuration and control for any user accessing productivity apps and company data from an unmanaged PC.
- Methods to better secure these sessions relied on proxy- or private-network-based tools. These impact performance and users may not be authorized or equipped to install or configure them.
- There is a need for detailed session monitoring, including the ability to monitor users in front of a device camera or to use camera data to validate that users require these tools.

Obstacles

- Despite their low user appeal and complexity, extending the life of traditional, VPN-based access is a low-cost option in comparison to adding endpoint access isolation technology.
- A mix of endpoint access isolation methods may be required to meet all use cases, such as a browser-based app for employees and a secure access client for contractors.
- Some browser-centric tools may face competition from security service edge (SSE) vendors touting similar capabilities, or from browser vendors that are building or incorporating similar functionality.
- Labor and privacy regulations render the most obtrusive functions of some tools untenable — for example, 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

- Specify control gaps that app-level security or VDI/DaaS tools cannot solve natively (for example, copy/paste restrictions). This will help identify the class of solution needed.
- 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 physical identity of specific users.
- When considering point-solutions, compare their efficacy and their cost to traditional alternatives like VPN.
- Coordinate with legal and human capital teams to examine regulatory privacy obligations when using biometric authentication or camera-based user monitoring.

Sample Vendors

Citrix Systems; Island; Rapid7 (Minerva Labs); SessionGuardian; SentryBay; Talon; ThinScale

Gartner Recommended Reading

Emerging Tech: Security — The Future of Enterprise Browsers

Cool Vendors in Hybrid Work Security

Exposure Management

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

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Exposure management (EM) encompasses a set of processes and technologies that allow enterprises to continually and consistently evaluate the visibility, and validate the accessibility and vulnerability of an enterprise's digital assets. EM is governed by an effective continuous threat exposure management (CTEM) program.

Why This Is Important

EM reduces the challenges organizations face inventorying, prioritizing and validating threat exposure that exist due to a rapidly expanding attack surface where traditional vulnerability management isn't enough. 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 governs and prioritizes risk reduction for the modern enterprise and requires assessments of all systems, applications and subscriptions used.

- Likelihood of exploitation (visibility of the organizations attack surface).
- Inventory and prioritize (vulnerability, threat intel-based, digital assets).

- Validate the potential success of any attack and if security controls can assist with detecting or preventing them.
- CTEM is a program, not the outcome of a specific tool.

Drivers

- Most commonly, organizations are siloing exposure activities such as penetration testing, threat intelligence management and vulnerability scanning. These siloed views provide 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 scope 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 and repeatable approach to answer the question “how exposed are we?” is necessary for organizations. This must have the aim of allowing reprioritisation of priority as environments change in a rapidly changeable IT landscape.
- Organizations must reorient their priorities, and segregate these priorities into three distinct questions: “what does my organization look like from an attacker’s point of view?,” “what configuration has my organization set that will make it vulnerable to attack?”; “how would our defensive controls cope and how would response processes perform?”

Obstacles

- The increased scope of CTEM programs over traditional VM introduces a number of new complexities often not previously considered or budgeted for.
- The concept of evaluating your attack surface is well-understood, continued security tool consolidation in this space, such as EASM with VA is beginning to simplify day-to-day operational processes, but formal integration of other technologies such as CAASM and CSPM technologies is still 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.
- The complex way an attack may manifest itself requires certain skill sets to understand, new markets such as BAS make it more simple to test the out-of-the-box scenarios. But to be more effective at using these technologies/services and develop custom-made simulations, new skills and understanding are required.

User Recommendations

- Embrace broader CTEM programs as security and risk management professionals, rather than simply processing vulnerabilities with VA tools.
- Mobilize various organizational stakeholders as success is dependent on it. Automated remediation from tools is unlikely to have a significant impact.
- Focus on visibility, end users must have an awareness of where risks are, and plan to respond to threats even if the organization has no way to reduce exposure to 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 your organization doesn't directly own, 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

Implement a Continuous Threat Exposure Management (CTEM) Program

Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

Top Trends in Cybersecurity 2023

Unified Endpoint Security

Analysis By: Chris Silva, Franz Hinner

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Unified endpoint security (UES) is a strategic architecture that integrates endpoint operations and endpoint security workflows and tools, which helps to create a complete risk identification, analysis and remediation cycle. UES results from the integration of selected capabilities from unified endpoint management (UEM) tools and endpoint protection (EPP) including endpoint detection (EDR) and mobile threat defense (MTD) tools.

Why This Is Important

Endpoint protection tools can thwart exploits before the device vulnerability is even remediated, but many cannot resolve the underlying misconfiguration, missing patch or update.

UES architecture is the lining of unified endpoint management and EPP tools and workflows, incorporating live, contextual threat intelligence to prioritize patches and remediations for managed endpoints. EPP protects vulnerable systems and informs UEM, which repairs the underlying issues via scheduled maintenance.

Business Impact

Integration of EPP threat intelligence into the endpoint operations process improves:

- Risk-based patching by the UEM and configuration prioritization.
- Consistency of endpoint configuration and patch compliance, though the integration of endpoint protection and unified endpoint management tools.

- Proactive, accurate risk calculation through integrating UEM and EPP tools to continually vet endpoint configuration.

Drivers

The 2022 Gartner Security Vendor Consolidation XDR and SASE Trends Survey, found that 75% of organizations are actively pursuing a security vendor consolidation strategy, an integration that helps create:

- Norms for when and whether things like automatic risk remediation — in the form of a patch or update — should be undertaken.
- Automated, risk-aware endpoint posture protection that follows the user, in contrast to network-based controls and restrictions, often moot for workers accessing SaaS applications off-network.
- Defensible patch metrics centered on risk, not completeness, to actively reduce endpoint attack surface.

Obstacles

- A multivendor environment that requires manual integration of tools. These integrations increase maintenance and support complexities.
- Choosing a consolidated set of tools from a single vendor will raise dependence on this vendor and may lengthen the process of seeking replacements if pricing or other engagement details change.
- Gartner estimates it will take two or three years before this technology crests the peak of the Hype Cycle, with ownership of the operations and security domains separated in many organizations, making unified planning difficult.

User Recommendations

- Assess the potential for integration between EPP and UEM and seek to achieve a one-way integration between the two to improve prioritization of patching.
- Investigate organizational capabilities to implement near-real-time endpoint patch or configuration change remediations are possible; if not, modernizing endpoint management is the first step to take.
- Consider the use of UES architecture to drive other dynamic security outcomes such as integration of UES risk data to be used in dynamic SSE/ZTNA access decisions.

Sample Vendors

BlackBerry; IBM; Ivanti; Microsoft; Sophos; Syxsense; Tanium; VMware

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Guide to Endpoint Security Concepts

External Attack Surface Management

Analysis By: Ruggero Contu, Elizabeth Kim, Mitchell Schneider, Franz Hinner

Benefit Rating: Moderate

Market Penetration: 5% to 20% 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 exposures. Examples include exposed servers, public cloud service misconfigurations and third-party partner software code vulnerabilities that could be exploited by adversaries.

Why This Is Important

Digital transformation initiatives have accelerated the expansion of enterprises' external attack surfaces. Cloud adoption, remote/hybrid working and IT/OT/IoT convergence are some key changes increasing exposure to external threats. EASM helps identify internet-facing assets while also prioritizing discovered vulnerabilities and related threats. It aims to provide risk information relevant to digital assets in the public domain, exposed to threat actors.

Business Impact

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

- Asset discovery/inventory for external-facing assets and systems.
- Monitoring for internet-facing enterprise exposures (cloud services, IPs, domains, certificates and IoT devices).
- Analysis to assess and prioritize the risks and vulnerabilities discovered.
- Indirect remediation, mitigation and incident response through prebuilt integrations with ticketing systems and SOAR tools.

Drivers

- Interest in understanding what organizations are exposed to from an attacker's point of view.
- Digital business initiatives such as cloud adoption, application development, hybrid working and IT/OT/IoT convergence present new enterprise risks.
- Demand to quantify third-party risks arising from activities such as merger and acquisition (M&A) and integration of supply chain infrastructure.
- EASM's adoption across different security platforms, offering EASM capabilities as part of a broader solution set to support better actionability.

Obstacles

- Low-value perception, with EASM leveraged for single-use cases rather than multiple areas.
- Confusion with the availability of EASM as a feature from various platforms, such as DRPS and VA.
- Already overburdened vulnerability management (VM) capabilities and teams concerned about adding to workloads.

User Recommendations

- Review available EASM capabilities arising from converging markets, in areas such as threat intelligence (TI), security testing/validation, vulnerability assessment or providers with broader platforms, such as Palo Alto Networks and Microsoft. 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, prioritization efficacy 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, TI, threat hunting and/or security testing/validation use cases.
- Ensure your EASM investment fits into the larger ASM strategy where external and internal exposure management is combined together.
- Consider EASM a key capability if primary business revenue is driven by externally facing web services.

Sample Vendors

Bishop Fox; Censys; CrowdStrike; CyCognito; FireCompass Technologies; IBM; Palo Alto Networks; Pentera; SOCRadar; ZeroFox

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Competitive Landscape: External Attack Surface Management

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

Innovation Insight for Attack Surface Management

Identity Threat Detection and Response

Analysis By: Mary Ruddy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Identity threat detection and response (ITDR) is a discipline that includes tools and best practices that protect identity infrastructure itself from attacks. ITDR can block and detect threats, confirm administrator posture, respond to various types of attacks and restore normal operation as needed.

Why This Is Important

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

Business Impact

Securing your identity infrastructure is mission-critical for security operations. If your accounts are compromised, permissions set incorrectly or your identity infrastructure itself is compromised, attackers can take control of your systems. Protecting your identity 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 actively targeting the IAM infrastructure itself. For instance:

- Administrator credential misuse is now a primary vector for attacks against the identity infrastructure.
- Attackers can use 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.
- Modern attacks have shown that conventional identity hygiene is not enough. There is no such thing as perfect prevention. Multifactor authentication and entitlement management processes can be circumvented, and these tools generally lack mechanisms for detection and response if something goes wrong.
- ITDR is needed in addition to IGA, PAM, a security information and event management (SIEM) solution and an in-house security operations center (SOC) or outsourced managed detection solution. There are major detection gaps between IAM and infrastructure security controls. IAM is traditionally used as a preventive control, whereas infrastructure security is used broadly but has limited depth when detecting identity-specific threats. ITDR mechanisms are more specific and operate with lower latency than general purpose configuration management, detection and response systems.

Obstacles

- ITDR requires coordination between IAM and security teams, which some organizations find difficult to establish.
- Lack of awareness of IAM administrator hygiene, detection and response best practices means that many organizations are not adequately protecting their identity infrastructure. More is needed than just traditional AD TDR.
- IAM teams often spend too much effort protecting other group's digital assets and not enough protecting their own IAM infrastructure.
- Multiple capabilities are required to fully protect identity infrastructure, including more closely monitoring configuration changes to root IAM administrator accounts, detecting when identity tools are compromised, enabling rapid investigations and efficient remediation and the ability to quickly revert to a known good state.
- The "R" part of ITDR is still nascent. Automated responses are still relatively basic.
- Even though there are many different ITDR capabilities, specific vendors provide only some of them.

User Recommendations

- Include ITDR strategy in your formal IAM program. ITDR requires a sponsor who can identify stakeholders and spearhead this collaborative initiative.
- 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 attack scenarios to ensure that at least well-known attack vectors are addressed.
- Combine foundational IAM infrastructure hygiene, such as PAM and IGA, with ITDR. Manage security posture and configuration of user directories and token generators. This will help to achieve identity fabric immunity.
- 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

Authomize; CrowdStrike; Gurucul; Microsoft; Netwrix; Oort; Proofpoint (Illusive); Semperis; SentinelOne (Attivo Networks); Silverfort

Gartner Recommended Reading

Top Trends in Cybersecurity 2022

Implement IAM Best Practices for Your Active Directory

At the Peak

BYOPC Security

Analysis By: Eric Grenier

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Bring your own PC (BYOPC) programs allow personally selected/purchased client devices to access enterprise applications and company data. These initiatives typically support Apple macOS and Microsoft Windows devices, and less commonly, ChromeOS and Linux. A lack of security controls or standardization in hardware and OS can represent significant risk if not addressed with a defined BYOPC security strategy that is implemented on a use-case-by-use-case basis.

Why This Is Important

Bring your own (BYO) programs have been expanded from primarily mobile devices to include macOS and Windows PCs, but the security of these devices will involve trade-offs for security over functionality. These programs should not be applied to all users, but rather should be applied on a use-case-by-use-case basis.

Maintaining a robust security posture in environments where user-owned/unmanaged devices access corporate applications and data requires a dedicated BYOPC security initiative.

Business Impact

Organizations implementing a BYOPC program need to minimize the security risks arising from the use of user-owned devices for business purposes. Structured BYOPC programs help achieve employee enablement while protecting company data and applications.

Drivers

- Hybrid work has expanded the number of devices from which users access company apps and data, with personal PCs making up an increasing 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. These attacks are increasing and more security will be needed on a personal device.
- Capabilities to establish suitable levels of control on a BYOPC — whether through the use of application controls, isolation of data, conditional access or a combination of all three — 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 more nuanced solutions than standard device management.
- 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.
- BYO is not a fit for every user. The inability to monitor personal devices and remediate BYO systems to an acceptable level limits the use cases that can be covered by BYO.
- Shared use of devices, common for personal hardware, may violate fair and acceptable use policies or other compliance mandates, regardless of security controls.
- The complexity and time needed for proper data classification presents a hurdle that organizations will need to overcome in order to adopt BYOPC on a large scale.
- BYO programmes shift a lot of IT problems to HR problems when devices are unavailable due to security or technical incidents.

User Recommendations

- Establish isolation-based controls for BYOPC; this can pay dividends by creating support models that can adapt for contractors and temporary employees as well.

- Implement BYOPC policies on a use-case-by-use-case basis. Do not use it as a cover-all, as there will be users that are not a good fit for BYOPC. Offer detailed, documented descriptions of the models of access supported from a BYOPC device, the support entitlements and any inherent restrictions for each access model.
- Isolate local device risks and restrict data loss by combining data protection and conditional access policies for all BYO users and utilize VDI/DaaS to access sensitive apps and data.
- Consult with legal and HR teams to understand what technical controls are tenable on users' personal devices and what privacy concerns must be addressed.

Sample Vendors

Amazon Web Services; BlackBerry; Citrix; Microsoft; Okta; Venn Software; VMware

Gartner Recommended Reading

Enable BYOPC for Select Use Cases While Managing Risk

Research Connection: Tech Talk — Best Practices for Securing BYOD/BYOPC

Market Guide for Desktop as a Service

Breach and Attack Simulation

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

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Breach and attack simulation (BAS) technologies allow enterprises to gain better visibility on their security posture weak spots by automating the continuous testing of threat vectors such as 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. Many BAS products have innovated to include external attack surface capabilities to maintain an up-to-date assessment list, and cover more of the attack kill chain. Frequent automated BAS assessments also enable organizations to detect gaps in their security posture due to configuration errors, or reevaluate priorities of upcoming security investments.

Business Impact

BAS allows organizations to validate the impact of what attack surface assessments and security posture management tools indicate as potential exposure to a specific threat. Organizations can continuously execute these assessments to gain more frequent visibility on a larger percentage of their assets. They can evaluate the efficacy of their security controls and discover attack paths leading to their most critical assets, allowing them to prioritize remediation.

Drivers

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

- Threat exposure confirmation: Organizations with establishing cybersecurity validation programs use BAS technology primarily to ensure consistent, yet improved, security posture over time and across multiple locations.
- Security control validation: BAS tools might integrate with security control technologies, through management APIs or by reading alert logs, enabling security configuration management and improving the visibility of defense gaps.
- Compliance optimization: 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 also supports continuous threat exposure management (CTEM) programs by enabling deeper automation of the "validation" step.

Obstacles

- Only higher maturity organizations are successfully implementing an exposure management initiative, or try to go beyond what the minimal compliance requirements are.
- BAS vendors need extensive internal sponsorship, not only from the security team, but from other infrastructure teams, such as networks or applications. Issues that BAS tools discover create complex remediation pathways.
- BAS tools need to expand beyond the diagnostic and basic remediation guidance through standard frameworks.
- The skill set required to deploy, maintain and operate a BAS tool is extensive and includes technical competences; threat actor and technique understanding as well as infrastructure and application architecture insights.
- BAS technology suffers from increased competition with more adjacent tools adding attack simulation, and need to expand and cover more environments, such as cloud infrastructure and SaaS.

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, such as EASM, but also highlighting changes in the security posture and providing reports in a form that minimizes diagnostic fatigue.
- Integrate BAS in a cybersecurity validation roadmap, as part of a continuous threat exposure management (CTEM) program. Don't run BAS in isolation.
- Evaluate the number of threat vectors and attack scenarios BAS tools can deliver and the frequency to which these simulations are updated to reflect real-world attacks.
- Understand the benefits and challenges resulting from the deployment options for BAS technologies. BAS products might leverage software agents, virtual machines and SaaS components.
- 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 products are actionable.

Sample Vendors

AttackIQ; Cymulate; Google; Keysight; Pentera; Picus Security; Ridge Security; SafeBreach; SCYTHE

Gartner Recommended Reading

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

Implement a Continuous Threat Exposure Management (CTEM) Program

Top Trends in Cybersecurity 2023

Using Security Testing to Grow and Evolve Your Security Operations

Security Service Edge

Analysis By: Charlie Winckless, John Watts

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 adaptive access control, data security, visibility and control. Further capabilities include an advanced threat defense and acceptable use control enforced by network-based and API-based integrations. 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 the usage of web and cloud services, and remote work. SSE offerings are the convergence of security functions (at least, secure web gateways [SWGs], cloud access security brokers [CASBs] and zero trust network access [ZTNA]) to reduce complexity and improve user experience. They are delivered from the cloud. When organizations are pursuing a secure access service edge (SASE) architecture, SSE is paired with software-defined WAN (SD-WAN) to simplify networking and security operations.

Business Impact

Hybrid work is continuing to drive the adoption of public cloud services, especially of SaaS applications. Both hybrid work and the adoption of public cloud services remain business enablers for most Gartner clients. SSE allows the organization to support anytime-anywhere workers by using a cloud-centric approach to enforce a security policy when accessing the web, cloud services and private applications. Simultaneously, SSE reduces the administrative complexity of running multiple products.

Drivers

- Organizations need to secure user, application and enterprise data that is distributed, decentralized and requires secure remote access.
- For many enterprises, a significant amount of critical data is now hosted in SaaS. Therefore, there is a need to perform data loss prevention (DLP) on data that is located in, going to, and leaving these SaaS platforms.
- SSE enables flexible and primarily cloud-based security for users and devices without being tied to on-premises network infrastructure and connectivity. The same security outcome is delivered to users regardless of their location or connectivity.
- Administrators can have enhanced visibility on user traffic and a single configuration and monitoring location for this traffic.
- SSE allows organizations to implement a posture based on identity and context at the edge.
- By consolidating vendors, organizations reduce complexity, costs and the number of vendors used to enforce security policy. Using a single SSE platform rather than multiple point offerings, they can both reduce complexity and reduce gaps in security coverage.
- Sensitive data inspection and malware inspection can be done in parallel across all channels of access. SSE allows doing both inspections in parallel, leading to a better performance and more consistent configuration than doing them separately.
- An adaptive access can take into account more input signals and be more consistently enforced, regardless of the application location or type.
- 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.
- Tight integrations that exist between discrete SD-WAN and SSE vendors allow interoperability without requiring a single-vendor approach.

Obstacles

- As the market is being formed by the convergence of capabilities, vendors may be strong in certain capabilities and weak in others. Vendors may also lack overall tight integration between SSE capabilities or with SD-WAN vendors.
- Not all vendors provide sufficiently sensitive data identification and protection to manage business risks.
- Some vendors have focused less on SaaS security and integrations. However, businesses increasingly need this visibility and protection.
- Being cloud-centric, SSE typically doesn't address every need supported by on-premises controls such as internal firewalling.
- Organizations are concerned about uptime or availability of services that they depend on for their business. This is compounded by weak SLAs from some vendors.
- Not all vendors provide all features locally in all geographies, resulting in performance or availability issues.
- Switching costs from incumbent vendors or timing of contract expirations prohibit near-term consolidation.
- Migrating from a VPN will increase costs.

User Recommendations

- Exploit the converged market, consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs by replacing them with a ZTNA approach.
- Approach SSE consolidation identifying which elements you may already have in place (for example, existing cloud-based CASB or SWG). Develop a shortlist of vendors based on your use cases regarding secure end-user requirements, the cloud services you use, and the data you need to protect.
- Inventory your equipment and contracts to implement a multiyear phaseout of on-premises perimeter and branch security hardware in favor of the cloud-based delivery of SSE.
- Global enterprises should validate that remote offices have acceptable performance and features with selected vendors. Vendor point of presence (POP) locations and service support are key.
- 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; Cisco; Cloudflare; Forcepoint; iboss; Lookout; Netskope; Palo Alto Networks; Skyhigh Security; Zscaler

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products

XDR

Analysis By: Eric Ahlm, Thomas Lintemuth, Franz Hinner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Extended detection and response (XDR) delivers unified security incident detection and automated response capabilities. XDRs integrate threat intelligence and telemetry data from multiple sources, with security analytics to provide contextualization and correlation of security alerts. XDR must include native sensors. XDR can be delivered on-premises or as a SaaS offering, and is typically deployed by organizations with smaller security teams.

Why This Is Important

XDR offers a less complex approach for threat detection and response by using a systematic, rather than an integration, approach to building a detection stack. XDR vendors can include a variety of security controls, usually natively integrated by the vendor via APIs. The vendor provides prebuilt playbooks that enable collaboration in their stack, and coherence in the detection of common threats.

Business Impact

The simplicity of XDR to detect common threats reduces the need for internal skill sets and could reduce the staff needed to operate a more complex solution, such as security information and event management (SIEM). XDR can also help reduce the time and complexity associated with security operations tasks through a single centralized investigation and response system.

Drivers

- XDR platforms appeal to organizations with modest maturity needs due to the detection logic, mostly vendor-provided, that generally requires less customization and maintenance.
- XDRs appeal to organizations looking for improved visibility across the security stack, as well as those looking to lower the administration requirements of more complex incident response (IR) solutions.
- Midsize organizations that struggle to correlate and respond to alerts generated from disparate security controls appreciate the productivity gain from centralized XDR interfaces.
- Staff with the required skills to maintain and operate an extensible detection stack are hard to recruit and retrain.
- Purchasing a systemic detection stack in the form of XDR can simplify product selection and acquisition.

Obstacles

- Single-vendor systemic XDR solutions may take years to replace in the case of effectiveness or efficiency issues.
- XDR's lack of extensibility for custom detections and other use cases could cause some clients to need both an XDR and a classic SIEM solution to meet multiple needs.
- Expanding an XDR detection stack's capabilities through the addition or replacement of security controls may be limited by the vendor.
- An XDR product 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. XDR may also be a poor choice for a forensically sound system of record for things such as access data.

User Recommendations

- Work with security operations stakeholders to determine if the 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

CrowdStrike; Fortinet; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Stellar Cyber; Trend Micro; Trellix

Gartner Recommended Reading

Market Guide for Security Orchestration, Automation and Response Solutions

Sliding into the Trough

Business Email Compromise Protection

Analysis By: Satarupa Patnaik, Craig Porter, Franz Hinner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Business email compromise (BEC) protection detects and filters malicious emails that fraudulently impersonate trusted entities such as banks or credit card companies to misdirect funds or data. BEC attacks do not include URLs or attachments and typically have a good sender reputation, which makes detecting them with traditional anti-phishing tools harder. Detecting BEC attacks requires machine learning to perform a deep inspection of the email content in context with the communications history.

Why This Is Important

- BEC does not include malicious links or attachments. BEC emails sent from legitimate servers are difficult to detect. Attacks are socially engineered through publicly available information like LinkedIn, Crunchbase or Wallmine.
- BEC attacks commonly use fraudulent invoices and external links to harvest credentials for future attacks.
- BEC attacks have surged in the last 2 years and almost 40% of ransomware attacks also originate through email.

Business Impact

BEC attacks pose a significant risk to all industries and leads to different kinds of damages, including:

- Reputation/trust damage.
- Loss of funds.
- Loss of confidential or private information.

- Access to systems.

Drivers

Adoption of BEC protection technology is increasing because:

- Traditional techniques for detecting malicious attachments or links are ineffective against BEC attacks.
- Sensitive data still lives in email, as in the case of Uber.
- Losses from BEC attacks can be significant. According to the FBI's 2022 IC3 Annual Report, around 22,000 complaints were registered for BEC attacks in 2022 and the total loss incurred was around $2.7 billion.
- All ad hoc 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 (ATO) attacks are virtually indistinguishable from legitimate emails.
- BEC attacks frequently go unnoticed. Often, fraud is only detected when the intended recipients are notified of a payment made but they don't receive the funds.

Obstacles

- Many organizations may choose to explore lower-cost and less effective alternatives to BEC protection such as user education, only minimally reducing the risk of BEC and delaying its adoption.
- Even the most effective solutions are less than 100% effective. As attackers' techniques evolve to utilize generative AI platforms such as ChatGPT, solutions focused on BEC may lose sight of the latest practices used.
- API-based solutions aren't sufficient to protect against all email-related attacks on their own.
- A key issue to address and mitigate is that account takeover attacks are almost impossible to detect, especially when attackers have credentialed access. This can increase the risk of attackers' knowledge of organizational behavior and the ability to hide their tracks.

- BEC capabilities are likely to be absorbed into comprehensive email security solutions in the future. Therefore, leaders will need to determine if it is wise to invest in BEC protection tools now.

User Recommendations

- Educate users about BEC phishing techniques and the limitations of email as an authentication factor and move high-risk transactions to better authenticated applications.
- Establish standard operating procedures for all financial or data transaction requests to eliminate requests for ad hoc transaction risks.
- Enforce the use of multifactor authentication (MFA) for accessing email to protect all users against account takeover.
- Upgrade or supplement email security solutions with advanced phishing protection specifically designed for BEC attacks.
- Seek solutions that use natural language processing, natural language understanding, computer vision and machine-learning-based social graph analysis.
- Utilize domain-based message authentication, reporting and conformance (DMARC) implementations to authenticate and minimize domain abuse.

Sample Vendors

Abnormal Security; Armorblox; Check Point Software Technologies; Egress; Microsoft; Mimecast; IRONSCALES; Proofpoint; Perception Point; SlashNext

Gartner Recommended Reading

Market Guide for Email Security

Guidance Framework for Building Email Security Architecture

Avoid the Top 9 Pitfalls of Implementing MFA

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:

Organizations should employ frontline worker-specific endpoint security technology to secure purpose-built devices and their users. Devices must be physically locked to permanent stations, tracked and checked out for shift duty, or set up for numerous users in low-connectivity locations, depending on the industry and use case.

Why This Is Important

Hardware availability and authentication techniques like biometrics are essential in harsh field conditions. Frontline workers need durable, monitored, locked-down, secure devices and a robust UEM system to keep them updated and patched. Using personal devices can cause data separation and performance issues, so proper control is crucial.

Business Impact

Users access enterprise systems and data in frontline use cases. Frontline situations necessitate more security. Off-site frontline equipment is vulnerable to manipulation and attack. To secure critical systems and data from customers, workers and contractors, they must be ruggedized. All security risks require many solutions. Some solutions are created for traditional mobile management, not frontline personnel, and require custom development to meet security standards.

Drivers

- More and more businesses are giving their frontline employees access, which exposes both the organizations and the workers to extra cloud-based security concerns.
- Due to the potential for data leakage or other types of malicious attacks, security teams have been forced to reconsider the strategy and architectures behind their frontline endpoint security.
- As BYOD becomes more common, enterprises require new mobile application management (MAM) and mobile threat defense (MTD) solutions, which lead to application-level container solutions.

Obstacles

- Specialized hardware and cloud functions are needed for multilayered security, resulting in unexpected expenses to enterprises.
- Frontline employees may require additional physical security solutions, including cameras, check-in/check-out protocols, user and device identity management, shift-based devices that require data clearance after usage, and geographic/location type protection.

User Recommendations

For managed devices requiring specialized solutions:

- Leverage purpose-built mobile security solutions.
- Manage and lock down the devices with EPP, UEM, or MAM.
- Ensure that OS security settings, updates, and patches are applied.
- Enable secure kiosks with cables, geofencing, and check-in/check-out operations.

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

- Focus on application-level controls for data leakage and identity-level controls for enforcing dynamic access policies.
- 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 to safeguard your organization's data and infrastructure from potential dangers.

- Use AAC for frontline users and devices that access third-party SaaS providers.

Sample Vendors

CommuniTake Technologies; Imprivata (GroundControl); Lookout; Microsoft; Samsung Electronics; SOTI; Veracode; VMware, 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

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Content disarm and reconstruction (CDR), sometimes known as "content sanitization," is the process of parsing a file into its constituent parts and removing any data that doesn't adhere to the file format's original specification/ISO standard. In addition, it isolates macros, links and embedded objects from the content before regenerating a cleaned version.

Why This Is Important

CDR protects against exploits and material that has been changed to be used as a weapon, without the need for time-consuming dynamic analysis or standard content inspection methods (like signatures) to find harmful content. This is especially helpful in situations when files are moving across organizational boundaries, such as when using email, web downloads or content-sharing websites for files.

Business Impact

CDR is a security technology that helps protect businesses from malicious content. CDR works by scanning files and emails for known malicious content. CDR can disarm it or remove the malicious code. It can:

- Enable requirements for files to be delivered safely without active malicious content, rather than relying on endpoint antivirus to detect and block malware.
- Reduce the risk of data breaches. CDR helps prevent data breaches by stopping malware from being run and the spread of malicious files.

Drivers

- Enterprises of all types shuffle documents across boundaries by the minute, including uploading email attachments, downloading web downloads, uploading content such as application forms and resumes, and sharing or receiving documents from untrusted sources.
- It is helpful to boost adoption because certain secure email and security service edge (SSE) platforms, in addition to content collaboration platforms, already offer such capabilities. These features may have been created in-house, repacked or acquired at an additional cost via a license from a third party.
- Existing solutions, such as dynamic analysis in sandboxes and even some antivirus solutions, are notoriously sluggish. CDR solutions reduce processing time, so users can view a sanitized attachment right away.

Obstacles

- CDR removes active code, potentially reducing the functionality of documents. Some systems quarantine the original file if it's broken, and give more detailed control over what's deleted, but this reduces CDR's utility.
- 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 vital for threat intelligence functions.
- CDR solutions have lower investment priority, limiting broader adoption. CDR is useful only for specific file types.

User Recommendations

- Use CDR when you need to eliminate the threat of active malware contained within files, and organizational leadership supports an environment where security is prioritized over potential end-user impacts.
- Use CDR to sanitize file uploads when integrated with web application and API protection platforms or as part of application file upload functions of web applications to protect the organization from files uploaded with embedded malware.
- Use CDR to augment or replace existing sandboxing and multi-AV scanning solutions. Utilize CDR to sanitize content in high-security environments, to ensure tracked changes, internal comments and others are removed before sharing.
- Use CDR with sandboxing solutions to enable sanitized documents to be available immediately, while the sandbox analysis completes.

Sample Vendors

Check Point Software Technologies; Forcepoint; Fortinet; Fortra; Glasswall; JiranSecurity; odix; OPSWAT; Sasa Software; Votiro

Gartner Recommended Reading

Market Guide for Email SecurityQuick Answer: How to Protect Web Applications Against Malicious File Uploads

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 capabilities, including SD-WAN, SWG, CASB, firewall 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, performance, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and security services mainly via a cloud-delivered model. SASE reduces the number of vendors required for secure access to one or two explicitly partnered vendors.

Business Impact

SASE enables:

- 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

- Digital business transformation including the adoption of cloud-based services by mobile workforces, edge computing and business continuity plans that must include a flexible, anywhere, anytime, secure, identity-based logical perimeter model of SASE.
- 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.
- For IT, SASE can reduce the deployment time for new users, locations, applications and devices.
- For information security, SASE enables a single way to set policy enforcement consistently across all types of access — internet, web applications and private applications, reducing the attack surface and shortening remediation times.
- Enterprise desire to simplify network and network security deployments via the reduction of policy engines and management consoles.

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 security architect and network architect when evaluating offerings and roadmaps from the 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.
- Explore single-vendor SASE, dual-vendor SASE and managed SASE options when investing, but avoid deploying SASE with more than two vendors, regardless of vendor marketing for all core services to minimize complexity and improve performance.
- Use vendor combinations — when selecting a dual-vendor solution — that have explicit integration including turnkey automation and visibility, and ideally management and data plane integration.
- 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.

Sample Vendors

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

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Market Guide for Single-Vendor SASE

The Future of Network Security Is in the Cloud

Magic Quadrant for SD-WAN

Magic Quadrant for Security Service Edge

Climbing the Slope

Desktop as a Service

Analysis By: Stuart Downes, Mark Margevicius, Tony Harvey, Craig Fisler, Sunil Kumar, Eri Hariu

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Desktop as a service (DaaS) is the provision of virtual desktops by a public cloud or service provider. DaaS is bought by IT leaders seeking to provide desktop or application experiences from virtual machines accessed using a remote display protocol. DaaS vendors incorporate a fully managed control plane service into their offerings, which facilitates user connections and provides a management interface. DaaS can be delivered preconfigured as a service or can be delivered as a DaaS platform.

Why This Is Important

With DaaS, no data resides on the endpoint, offering a solution that can increase security, resilience and application responsiveness for remote workers. DaaS offers scalable services without adding infrastructure, allowing clients to appropriately size and consume their environments hour by hour, day by day, and month by month; however, not all DaaS solutions offer such granular billing options.

Business Impact

With DaaS, IT leaders can increase security for desktops and applications. Other benefits of DaaS, compared to traditional VDI, include:

- Flexible procurement options that allow scalable deployments.
- Simplified rollout of services to new geographic regions.
- Applicability to a broader range of industries and use cases.
- Lesser skills required for IT operations teams to deploy and operate virtual desktops and applications.
- More rapid expansion or contraction of workloads.

Drivers

DaaS will continue to mature and witness increased adoption through 2026. The technology has moved through the Trough of Disillusionment onto the Slope of Enlightenment due to the following factors:

- DaaS enables business continuity and remote work, with no data residing on the endpoint.
- The technology securely extends services to external contractors and third parties.
- Endpoint computing models allow device-independence and bring your own PC (BYOPC) endpoints.
- On-demand desktops enable a financial model that allows scaling of cloud resources and an operating expenditure (opex) model.
- DaaS can be purchased for short periods, enabling use cases such as seasonal workers or short-term contracts.
- DaaS enables rapid access to systems during mergers, acquisitions and divestitures.
- Rich graphics use cases like engineering, games development, video editing and geographic information systems (GIS) benefit from GPU-enabled workstation-class virtual desktops and applications.
- DaaS can be delivered to users in hours. The supply of a physical device, on the other hand, can take weeks, incur shipping costs and retrieval is not always guaranteed.
- The technology eliminates the need for complex and static VDI implementations.

Obstacles

- Usually, the business case turns positive only when security and user cost impacts are included.
- Organizations struggle when there is a change in financial models from capex to opex.
- GPU use cases can be extremely expensive and often need advanced protocols, which increases complexity.

- Multimedia streaming, web meetings and video call performance in DaaS are not equivalent to that of a physical endpoint.
- Performance issues may occur in DaaS because application architectures introduce network-related issues (i.e., latency and hairpinning).
- Some DaaS solutions require self-assembly, which, although simpler than VDI, can still be too complex for some clients.
- The full range of desktop management requirements may not be completely fulfilled by DaaS providers.
- Microsoft product terms that prevent the installation of Microsoft 365 applications on "Listed Providers" (see 3 Compliance Questions to Ask When Licensing Microsoft Windows and Office for VDI and DaaS).

User Recommendations

- Get familiar with the three DaaS market segments — self-assembled DaaS, vendor-assembled DaaS and vendor-managed DaaS — and select a vendor from the appropriate segment (see Market Guide for Desktop as a Service).
- Ensure your operational teams have the necessary skills if you select self-assembled DaaS solutions.
- Select a vendor-defined DaaS or vendor-managed DaaS solution if you do not have the operational skills.
- 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 the billing granularity you require.

Sample Vendors

Alibaba; Amazon; Anunta; ATSG; Citrix Systems; Microsoft; Nutanix; oneclick; VMware; Workspot

Gartner Recommended Reading

Market Guide for Desktop as a Service

How to Choose a Desktop Delivery Model for the Digital Workplace

Video: PCs, Virtual Desktops or DaaS: What's the Best Fit for Midsize Enterprises

3 Compliance Questions to Ask When Licensing Microsoft Windows and Office for VDI and DaaS

ZTNA

Analysis By: John Watts, Thomas Lintemuth

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines zero trust network access (ZTNA) as products and services that create an identity- and context-based, logical-access boundary that encompasses an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities, limiting 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 logically separates the source user/device from the destination application to mitigate full network access and reduce the attack surface within the organization. This improves user experience (UX) and remote access flexibility while enabling dynamic, granular user-to-application segmentation through simplified policy management. Cloud-based ZTNA offerings improved scalability and ease of adoption for secure remote access.

Drivers

- The rise of zero trust initiatives within organizations has led to the need for more precise access and session control in on-premises and cloud applications.
- There is an increasing 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 an enterprise.
- Cloud-based ZTNA services are needed to augment on-premises remote access methods to offload hardware-based solutions when hybrid work demand exceeds hardware capacity.
- Some organizations need to acquire the ability to observe application access patterns before enforcing granular controls.
- Some organizations have a need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing their entire networks over VPNs, or to connect the applications to the internet for access.
- Organizations that undergo mergers and acquisitions need to be able to extend application access to acquired companies without deploying endpoints or interconnecting their corporate networks.

Obstacles

- **Cost:** ZTNA is typically licensed per named user on a per-user/per-year basis at a price roughly twice or three times that of traditional VPNs.
- **Limited support:** Not all products support all applications. For example, some client-based ZTNA solutions do not support UDP applications, and clientless ZTNA solutions typically only support web, Remote Desktop Protocol (RDP) and Secure Shell (SSH) protocols. Some vendors market VPN as a service (VPNaaS) as ZTNA, but lack support for some zero trust posture capabilities.
- **Adoption limited to VPN replacement:** Cloud-based trust brokers may not extend policy enforcement points on-premises, limiting use cases compared to universal ZTNA offerings.
- **Granularity of access policy:** Organizations must map application access for users, but many lack this understanding and end up with access rules which are either too granular or not granular enough.

User Recommendations

- Enable application and service specific access with clientless ZTNA rather than full tunnel network access intended for extended workforce, “bring your own device” (BYOD) users, mergers and acquisitions, and B2B end users.
- Align ZTNA vendor choice with security service edge (SSE) vendor choice to support unified security controls for hybrid workers and remote branches and ZTNA policies with the organization’s zero trust strategy. Measure risk reduction using outcome-driven metrics.
- Demand universal ZTNA capabilities from vendors offering secure remote access to unify access control policies both on- and off-premises with added Internet of Things (IoT) support to replace legacy network access control (NAC) or software-defined network (SDN) implementations.
- Cloak systems, such as traditional VPN concentrators and collaboration systems exposed to the internet, from scan-and-exploit threats, and permit users to only interact with limited applications and data to reduce risk.

Sample Vendors

Appgate; Cisco; Fortinet; Google; Microsoft; Netskope; Palo Alto Networks; Zscaler

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

How to Select the Right ZTNA Offering

7 Effective Steps for Implementing Zero Trust Network Access

2023 Strategic Roadmap for Zero Trust Security Program Implementation

2022 Strategic Roadmap for SASE Convergence

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 targeting 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 detection based on 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 into mobile device behavior that can indicate malicious activity, which can be correlated with other observables and threat intelligence 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

- MTD can integrate with an existing UEM deployment for streamlined remediation or can be deployed 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

- Many enterprises deploy MTD to counter advanced and targeted attacks. In practice, MTD provides more traditional security hygiene, such as app vetting and device vulnerability management.
- Protection from mobile phishing is a major driver for adoption. Phishing attacks on mobile devices can circumvent traditional enterprise measures such as email security via SMS and instant messaging applications such as WhatsApp.
- Emerging use cases envisage MTD as a component of zero trust architecture and of an extended detection and response (XDR) system. This is in addition to the use of MTD for mobile phishing protection.
- For unmanaged iOS and Android devices, MTD provides 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 has gained popularity to enable Outlook and other Microsoft applications on unmanaged devices.
- Endpoint security vendors are expanding their EPP offerings to include support for 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 (especially iOS and iPadOS) 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 using UEM before investing in MTD products. Use MTD for app vetting and device vulnerability management 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 to extend zero trust principles onto mobile devices. 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; CrowdStrike; Jamf; Lookout; Microsoft; Samoby; Sophos; Tehtris; Zimperium

Gartner Recommended Reading

Market Guide for Mobile Threat Defense

Data Sanitization

Analysis By: Rob Schafer

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

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

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

- **Data security compliance:** 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.

- **Sustainability and the circular economy:** The rapidly growing focus on sustainability, and specifically the circular economy, is driving a shift away from physical destruction to the sanitization/wiping of data-bearing devices. This, in turn, can extend the useful life span of IT assets by 50% to 100%, mitigating up to half their total greenhouse gas emissions.

- **Data sanitization standards and encryption:** 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 will instead enforce data encryption on all data-bearing devices to minimize chain-of-custody security risks.

- **Holistic, pervasive data sanitization:** 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).

- **Remote data sanitization:** For mobile devices, a remote data-wiping capability is commonly implemented via a mobile device manager. 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 may not be 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 that 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., mobile assets, USB drives, IoT devices).
- For externally provisioned services (e.g., SaaS, IaaS, 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: Franz Hinner, Satarupa Patnaik, Eric Grenier

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Endpoint detection and response (EDR) analyzes system, process, and user activity to detect security threats. It provides remedial guidance for threats that bypass prevention controls and enables endpoint threat investigations. EDR capabilities are often included in endpoint protection platforms and delivered as software agents connected to centralized cloud-based security analytics and management software.

Why This Is Important

EDR is an essential defense component for most enterprise endpoints. It requires the installation of an agent to assist in the discovery and reporting of suspicious and malicious behaviors, visualization of attack propagation, and remediation guidance. EDR can stop known malware and ransomware families, and it can also help discover and remediate more stealthy and unknown threats.

Business Impact

- All devices and servers that connect to corporate networks or handle data need EDR protection.
- New threats and covert exploits require early identification and quick reaction.
- Cyber insurers and regulators demand EDR, and some EDR solutions provide low-cost ransomware insurance.

Drivers

- The nature of threats has changed. It is no longer practical to achieve 100% prevention, and older endpoint protection platform (EPP) tools should be updated to also contain 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 bases and most new deployments.
- 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 are increasingly needed to ensure systems are not misconfigured and have no unpatched vulnerabilities.
- The collection of logs and events from EDR agents forms the basis for retrospective threat detection and threat hunting.
- 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

- Many businesses lack and underestimate the knowledge and resources to install and employ EDR tools successfully. EDR adoption requires responder training, including “range” training that mimics assaults.
- Traditional endpoint security technologies and agents don’t function with cloud-hosted workloads’ “agile” deployment pipelines. This splits agile deployed workloads from containers or serverless computing.
- Non-Microsoft-Windows systems may lack feature parity. Endpoint security solutions for these systems lack EDR detection and response capabilities.
- In hybrid and remote working models, older on-premises technologies are difficult to adopt and maintain.

User Recommendations

- Choose solutions with a single unified agent and fast remote deployment.
- Prioritize technologies with ease of use and prebuilt automated playbooks.
- Favor cloud-hosted solutions with flexible deployment options.
- Assess the organization’s ability to monitor and manage detection and response services to identify gaps and determine if a managed service is required for your organization. Ensure appropriate data retention and fulfill regulatory compliance.

Sample Vendors

Cisco; CrowdStrike; Cybereason; Fortinet; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Trellix; Trend Micro

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

Remote Browser Isolation

Analysis By: John Watts, Neil MacDonald

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Remote browser isolation (RBI) separates the rendering of untrusted content (typically from the internet) from users and their devices, or 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 the risk of malware and data loss. When an endpoint is accessing web content, RBI prevents web-delivered malware from being delivered directly to the endpoint. RBI also works in the reverse direction. In use cases such as SaaS access via a cloud access security broker (CASB) or internal application access via zero-trust network access (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, either through exploits delivered by web browsing or via emailed links that trick users into visiting malicious sites. Connecting the browser from the end user's desktop to another browser running in a separate location improves the efficacy of existing security tools. RBI protection can also extend to protect private and SaaS applications accessed from unmanaged devices, thus reducing the threat of data exfiltration.

Drivers

- Many organizations desire to establish an adaptive zero-trust posture by using isolation as a policy action within security service edge (SSE) for forward proxy, reverse proxy and private applications.
- There is often a need to apply malware protection and data protection to both managed and unmanaged devices.
- Isolation of websites is a more efficient means of improving security than relying on slow, static blocklists to stop targeted attacks.
- Allowing isolated access to uncategorized sites, rather than blocking them, can reduce user friction.
- Email-based URLs that resolve externally can be isolated to prevent phishing attacks on employees.

Obstacles

- End users often cite a poor experience when RBI is deployed for all sites, leading some organizations to limit RBI to only certain categories of sites.
- Few stand-alone RBI vendors remain in the market, which limits choices, as most RBI options are now included as features of secure access service edge (SASE) and SSE platforms.
- Localizing the browsing experience for cloud-based, multitenant RBI requires IP address assignments to be regionally combined with either VPN exit points or local points of presence.
- RBI is an additional layer of defense at additional cost, as it rarely fully replaces other security controls.
- Most RBI offerings are software-based and cloud-delivered, limiting options for organizations looking for an on-premises, hardware-based isolation option.
- RBI does not protect against infected content that is permitted to download to the endpoint. Mechanisms like file antivirus and sandboxing, conversion to PDF, remote viewers and content disarm and reconstruction (CDR) are required.

User Recommendations

- Evaluate and pilot an RBI 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.
- Evaluate RBI as a feature of your existing SASE/SSE provider and determine how it can be used to improve the efficacy of the solution. 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, DOM reconstruction or graphics rendering) 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.

Sample Vendors

Authentic8; Broadcom; Cloudflare; Forcepoint; Garrison; Menlo Security; Netskope; Proofpoint; Skyhigh Security; Zscaler

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Market Guide for Single-Vendor SASE

Entering the Plateau

UEM Tools

Analysis By: Tom Cipolla, Dan Wilson, Craig Fisler, Sunil Kumar

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, Chrome OS, Linux, 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

UEM tools can streamline and improve endpoint management. Specific impacts include:

- Location-agnostic endpoint management and patching.
- 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.
- User-centric management across their corporate-managed and bring-your-own-device (BYOD) endpoints.

Drivers

- Supporting hybrid workers requires tools that extend beyond a single platform or requires 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 offer this through broader use of analytics and automation.
- Consolidation of disparate endpoint support teams, tools, processes and definitions of success into a centralized endpoint management framework supports 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.
- Insufficient skills or resources 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 have an endpoint management tool.
- Organizations with many Active Directory Group Policy Objects (GPOs) that have little awareness of what each does will struggle to rationalize and 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 toward the Plateau of Productivity as the tools mature and adoption has become mainstream. Most organizations have successfully adapted processes and refocused IT staff on simplifying and modernizing endpoint management. I&O leaders should:

- Improve endpoint posture and 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 mobile device management (MDM), client management tools (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

How to Maximize the Benefits of Windows Modern Management

Accelerate Windows and Third-Party Application Patching

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

Consolidate Endpoint Management Teams, Tools and Strategies to Reduce Cost and Optimize Operations

Next-Generation Antivirus

Analysis By: Franz Hinner, Jon Amato

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Next-generation antivirus (NGAV) solutions enable preventative security controls such as attack surface reduction, static file analysis, and behavioral analysis to tackle known and new security threats during pre- and postexecution attack phases. NGAVs are a common component of endpoint protection platforms (EPPs). They work in tandem with endpoint detection and response (EDR) capabilities to provide a complete set of endpoint prevention, detection, and response capabilities.

Why This Is Important

Enterprise endpoint attacks are becoming more complex as time goes on. In the case of ransomware, the threat has progressed from basic automated tactics to highly orchestrated human-driven operations, with the latter's objective being to extort between 1% and 2% of business income. Endpoint detection and response (EDR) capabilities are being integrated into NGAVs as a means of protection against more sophisticated threats.

Business Impact

All businesses should completely install NGAV, since it is now deemed essential security hygiene and is used by 99% of business endpoints to strengthen the protection and prevention stack. The importance of EDR's detect-and-respond capabilities has increased because businesses find it impossible to develop security against all potential future attack strategies in advance. However, adopting EDR requires more money for licenses, more work for administrators, and more training for employees.

Drivers

- NGAVs now battle stealthier attackers and sophisticated threats. Organizations prioritize preventing unusual, long-running, targeted and fileless assaults. Static file analysis using machine learning and cloud-based hash lookups can replace or complement signature-based malware identification. Resource consumption and maintenance must be easy. Agent tampering prevention is crucial.
- Cloud-native solutions that are easy to deploy and administer and behavior-based detection and analytics that identify unknown risks advance NGAV.
- OS security has downplayed NGAV by safeguarding credentials, limiting kernel assaults, and isolating important security services. Virtualized browsers and programs lessen OS compromise.
- Firewall management, device control, threat- and risk-based vulnerability management, and patching are being integrated into NGAV platforms to improve security and appeal. Some toolsets restrict applications and encrypt storage.
- NGAVs are table stakes in an EPP solution and continue to evolve to further integrate other security disciplines, which in conclusion means that NGAV as a separate category may be subsumed by EDR.

Obstacles

- As NGAV enables real-time monitoring and other advanced capabilities, it is critical to overall security operations.
- NGAVs 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 NGAV 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.
- As the core OS becomes more secure, attackers will likely target application vulnerabilities and BIOS or firmware attacks leaving NGAVs blind to these threats.
- EDR is essential to detect and respond to stealthier attacks that would bypass NGAV systems that only prohibit. These methods fail to identify stealthy approaches using trusted tools.

User Recommendations

- Assess the strategic fit of the NGAV solution 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 NGAV solutions.
- Favor solutions that have a strong track record of using machine learning for static file analysis and a 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

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

Gartner Recommended Reading

Critical Capabilities for Endpoint Protection Platforms

Competitive Landscape: Endpoint Protection Platforms

Magic Quadrant for Endpoint Protection Platforms

Appendixes

See the previous Hype Cycle: Hype Cycle for Endpoint Security, 2022

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 (August 2023)

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 (August 2023)

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 (August 2023)

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, 2022 - 19 December 2022

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 Authors

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

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

Table 1: Priority Matrix for Endpoint Security, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		SASE Security Service Edge	Exposure Management	
High	Desktop as a Service Endpoint Detection and Response UEM Tools	Breach and Attack Simulation BYOPC Security Content Disarm and Reconstruction Identity Threat Detection and Response Unified Endpoint Security	Automated Moving Target Defense Business Email Compromise Protection XDR	
Moderate	Data Sanitization Next-Generation Antivirus	Device Endpoint Security for Frontline Workers External Attack Surface Management Mobile Threat Defense ZTNA	Automated Security Control Assessment Endpoint Access Isolation Enterprise Browsers	
Low	Remote Browser Isolation			

Source: Gartner (August 2023)

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 (August 2023)

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 (August 2023)

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 (August 2023)