Hype Cycle for Zero Trust Networking, 2023

Published 18 July 2023 - ID G00790730 - 69 min read

By Analyst(s): Andrew Lerner, John Watts

Initiatives: I&O Platforms; Infrastructure Security

Most organizations have a zero trust strategy for information security, which directly impacts network strategy and design. This Hype Cycle will help infrastructure and operations leaders choose suitable technologies to pragmatically embed zero trust principles in their networks.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Strategic Planning Assumption

By 2026, 10% of large enterprises will have a comprehensive, mature and measurable zero trust program in place, up from less than 1% in 2023.

Analysis

What You Need to Know

Zero trust is a priority for most organizations as they seek to reduce risk in their environments. Consequently, infrastructure and operations (I&O) networking leaders and their teams are increasingly asked to apply zero trust concepts to their infrastructure. Zero trust replaces implicit trust with continuously assessed risk and trust levels, based on identity and context. I&O leaders must work closely with security leaders to incorporate zero trust principles into their networks.

There is plenty of “noise” about zero trust, which makes it difficult to distinguish solid practices from marketing hype. Zero trust is not a single technology, implementation or final destination. Instead, it is fundamentally a mindset or paradigm that leads to a strategy for, and implementation of, specific architectures and technologies.

I&O leaders must invest in people, processes and technologies to improve the zero trust posture of their networking environments. This Hype Cycle focuses on the technologies they should focus on to embed zero trust principles in their networks.

The Hype Cycle

This is a new Hype Cycle that describes the 19 most relevant and hyped zero trust technologies for I&O networking leaders. We define each technology, describe its benefit, identify its market penetration, and indicate drivers and inhibitors of its growth.

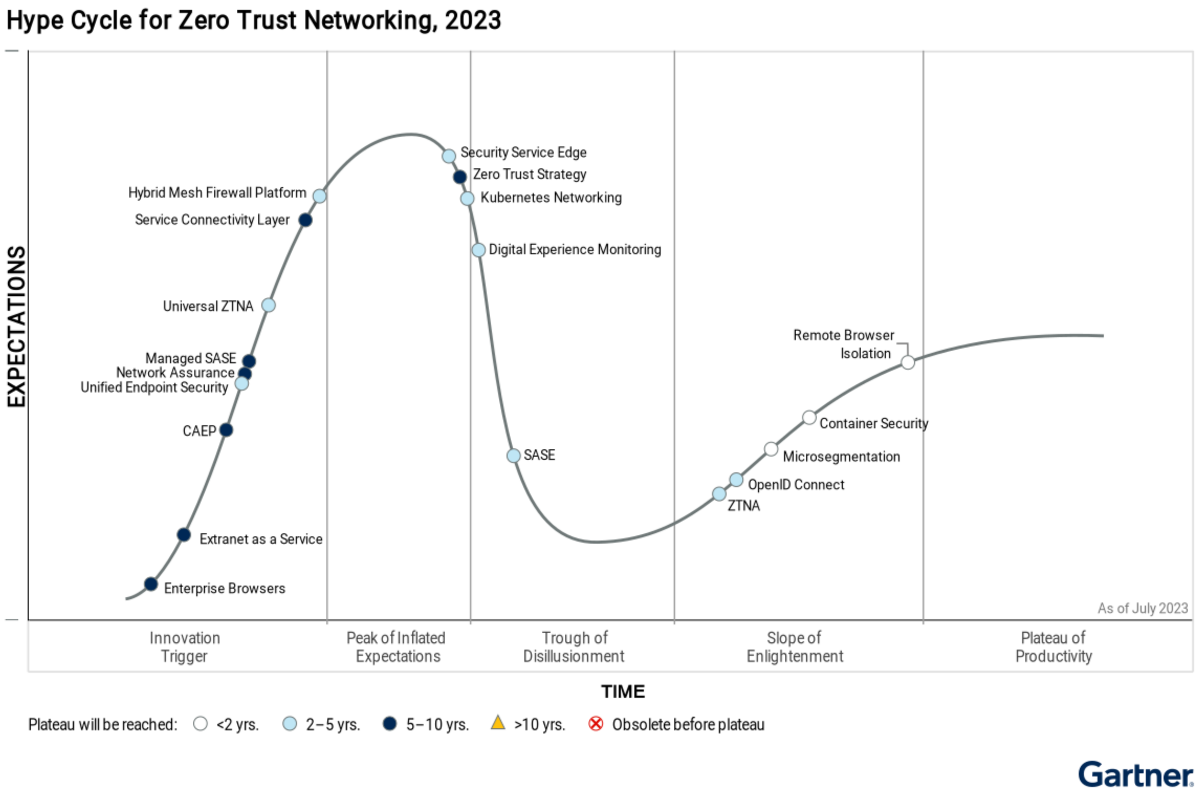
Highlights:

- **At peak hype:** Security service edge (SSE) is at the Peak of Inflated Expectations, due to a shift in the traffic flows associated with public cloud and SaaS services, and organizations’ desire to converge security tools and vendors. Interest in SSE is very high as this technology helps address both these developments by delivering cloud-resident enforcement and converging disparate vendors and operational interfaces.
- **Deep in the trough:** Secure access service edge (SASE) is in the Trough of Disillusionment, due to exaggerated marketing by many technology vendors.

- **Approaching the plateau:** Several technologies are on the Slope of Enlightenment, having achieved a state of maturity in terms of enterprise adoption. They include remote browser isolation (RBI), container security, microsegmentation, OpenID Connect and zero trust network access (ZTNA). These are the technologies subject to the most real-world adoption, and are providing real-world benefits on the journey toward zero trust.

- **Progressing quickly:** RBI is one of the fastest-moving technologies because it is increasingly embedded as a feature of SSE, which is accelerating adoption. Service connectivity layer (SCL) is also moving rapidly along the Hype Cycle as the number and influence of platform teams increases — these teams are looking for software abstraction that simplifies networking and networking security to speed up development.

Figure 1: Hype Cycle for Zero Trust Networking, 2023



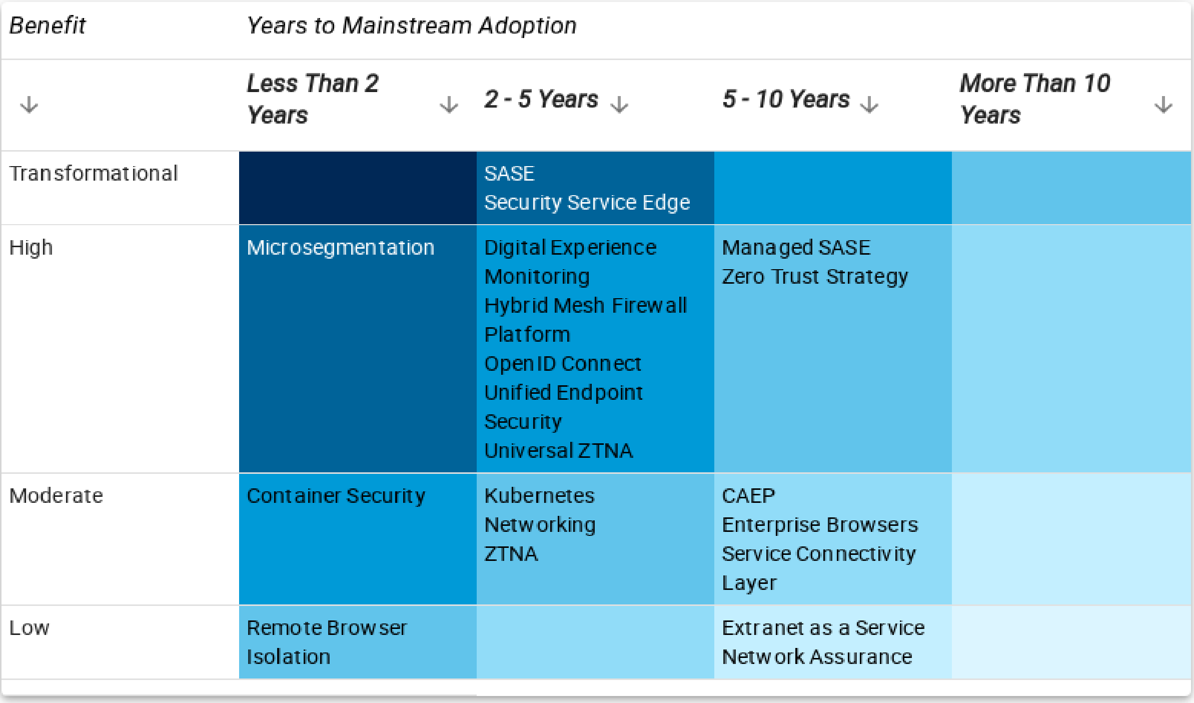
The Priority Matrix

We expect microsegmentation, container security and RBI to achieve mainstream adoption within the next two years, as many enterprises are already showing interest in, and adopting, these technologies.

There are no technologies of transformational benefit that we expect to achieve mainstream enterprise adoption within the next two years. This is because of the criticality of existing enterprise networks and/or the time frame to implement substantial adjustments. We do, however, expect SASE and SSE to achieve mainstream adoption in the next two to five years. This progress will be driven by enterprises' demands for cloud-delivered security and converged capabilities as they move workloads to the cloud, and by healthy emerging supply from commercial vendors.

Table 1: Priority Matrix for Zero Trust Networking, 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		
High	Microsegmentation	Digital Experience Monitoring Hybrid Mesh Firewall Platform OpenID Connect Unified Endpoint Security Universal ZTNA	Managed SASE Zero Trust Strategy	
Moderate	Container Security	Kubernetes Networking ZTNA	CAEP Enterprise Browsers Service Connectivity Layer	
Low	Remote Browser Isolation		Extranet as a Service Network Assurance	

Source: Gartner (July 2023)

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

Extranet as a Service

Analysis By: Andrew Lerner

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

ExtranetaaS is a networking software offering that delivers extranet as a service. An extranet is a logical network zone that connects multiple independent parties together, typically under different administrative domains, often with diverse requirements. These are sometimes also referred to as B2B networks.

Why This Is Important

ExtranetaaS can help accelerate the sharing of information between partners using cloud services. Although extranets have been around since the 1980s (and the term extranet has been in use since 1995), ExtranetaaS simplifies the ability to set up and secure operation of an extranet in the modern era, as enterprises increasingly use public cloud and SaaS services.

Business Impact

Extranets are a way for enterprises, partners, customers and other outside parties to access data and systems resident on a network. It allows these parties to connect and exchange needed information such as application components or financial transactions, and is helpful in connecting independent parties with common interests. An example is within the financial services industry where local connectivity between regulatory agencies, stock exchanges, market data companies and trade clearing is often required.

Drivers

- Traditionally, extranets were established in data centers, nearby applications and data, using dedicated circuits or IPsec VPN. As organizations are migrating applications to the public cloud and SaaS, it is causing them to rethink their existing extranet approaches.
- The native public cloud providers don't offer robust advanced networking configurations to support complex extranet connectivity scenarios, driving enterprises to entertain ExtranetaaS solutions.
- There is a desire to simplify and replace physical infrastructure, including routers, firewalls and VPN appliances, with software with solutions that are more API- and software-oriented.
- There is also a desire to remove expensive dedicated lines such as MPLS or dedicated broadband.
- Smaller and startup network vendors are aggressively targeting enterprises to help them solve the technical and security challenges as organizations migrate their applications to cloud services.

Obstacles

- ExtranetaaS is a new and unknown technology to most enterprises.
- Extranets often support mission-critical environments that lead to a desire for moderate incremental change. This is in contrast to a shift to ExtranetaaS, which entails a software-only aaS delivery from lesser-known vendors.
- The public cloud providers' native capabilities are good enough for some extranet use cases.
- Organizations can use colocation in cloud data centers to address the challenge of getting the services closer to public cloud, SaaS and partner services without using ExtranetaaS.
- Most enterprise network teams take a "set it and forget it" perspective toward extranet deployments, preferring not to rearchitect the entire deployment. This drives moderate incremental modernization of existing extranets versus conversion to ExtranetaaS.
- The ROI of ExtranetaaS is unproven.
- The supply of vendor solutions is immature as many of the vendors focused on this technology are smaller companies that are unproven.

User Recommendations

- Investigate ExtranetaaS if using the native cloud provider constructs doesn't support your B2B networking requirements.
- Look to ExtranetaaS if you're migrating an existing on-premises, hardware-based extranet or B2B network to a public cloud environment.
- Shortlist ExtranetaaS offerings as an option for connecting to a large number of customers' data in a secure fashion.

Sample Vendors

Alkira; Graphiant; Trustgrid

Gartner Recommended Reading

Market Guide for Multicloud Networking Software

CAEP

Analysis By: Erik Wahlstrom

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Continuous Access Evaluation Profile (CAEP) is a standard that enables IAM, security tools and the services they protect to continually share security events to enable session management, mitigate breaches and to reenforce policies in a decentralized environment. CAEP profiles the Shared Signals and Events (SSE) Framework that defines mechanisms to communicate events between trusted parties to enable continuous runtime access decisions.

Why This Is Important

- Applications and services are consumed and deployed in a hybrid and decentralized IT environment. A decentralized environment requires new session management mechanisms.
- The sharing of events between systems requires a standardized event-based protocol.
- CAEP helps resolve challenges with long-token lifetimes, step-up authentication, the continuous assessment of assurance levels and device postures, and provides mechanisms to communicate and respond to identity life cycle events.

Business Impact

CAEP increases security in services that are connected with identity federation, by enabling continuous exchange of security events. This enables higher assurance levels of sessions and a better user experience. CAEP provides a near-real-time mechanism to validate claims, request step-up authentication and to manage sessions. It thus enables centralized security in a hybrid and decentralized IT environment.

Drivers

- The increasing decentralization of applications and services in organizations' hybrid and multicloud environments has made continuous session management hard. For example, the implementation of single logout has historically been impossible to implement at scale.

- Organizations need a way to understand what's going on in applications after users are authenticated. Organizations have therefore been looking at technologies beyond federated identity flows that just protect the "front door" to also understand what goes on "behind the doors" of protected applications. Cloud access security brokers (CASBs) have historically been the only alternative to add this control, due to the lack of an industry standard that allows for the event-based sharing of access signals.

- OAuth 2.0 provides refresh and access tokens to keep sessions up to date, but it's not responsive enough. Keeping assurance levels high throughout a session have required users to be reevaluated at a central identity provider, thereby interrupting user journeys.

- A tightly woven identity fabric, where an organization weaves multiple IAM tools together to solve its identity use cases, requires event-based and runtime communication mechanisms to be established to evaluate and establish trust, and orchestrates the right tools for the use cases. For example, an event saying a claim about a user is no longer valid, or an out-of-compliance security posture of a device must trigger other IAM tools to respond to that event and reevaluate their access decisions in runtime.

- CAEP is a profile of the SSE Framework defined by the acclaimed OpenID Foundation.

- Using CAEP to continuously feed signals into an adaptive access engine enables the engine to have more data and make more accurate access decisions.

- The community is starting to offer CAEP testbeds such as caep.dev to provide education, and also to test CAEP implementations and thereby driving adoption.

Obstacles

- All identity standards take a long time to be commonly implemented. Identity standards have a "chicken and egg" problem before they reach wide deployment. Target applications wait to see if a standard takes off and IAM vendors wait for wide support in their target applications. This is also true for CAEP. The number of deployments is now growing from small numbers. Deployments are within a vendor's own tools or between close partners. For example, Microsoft has implemented CAEP in Azure Active Directory and uses it for Exchange, Teams and SharePoint Online.

- CAEP is still not commonly known and understood by IAM professionals, or by application and service developers. Also, product documentation and education material from IAM vendors about CAEP is still limited.

User Recommendations

- Define an IAM architecture that supports centralized/decentralized systems. CAEP is a protocol next to other modern identity protocols such as JSON Web Tokens (JWTs) and Open Policy Agent (OPA) that enable it.

- Ask IAM vendors about their roadmaps. Gartner expects CAEP and other related standards — like the Risk Incident Sharing and Coordination (RISC) profile of the OpenID SSE Framework Specification to share security and risk events across decentralized systems — to become increasingly important going forward.

- Add CAEP as an optional RFP criterion when procuring new applications, specifically SaaS apps. Support is still emerging, but Gartner expects the adoption of CAEP to grow. Configuring a new application in an IAM tool should, over time, include standardized life cycle management, single sign-on and the sharing of events.

Sample Vendors

Amazon Web Services; Broadcom; Cisco; Google; Microsoft; SGNL

Gartner Recommended Reading

Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

Identity-First Security Maximizes Cybersecurity Effectiveness

Managed SASE

Analysis By: Ted Corbett, Lisa Pierce, Jon Dressel

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Managed secure access service edge (MSASE) delivers the full life cycle of SASE functionality as a managed service. This includes design, migrations, configuration, installation, operations and management. These services cover the core SASE components of SD-WAN, SWG, CASB, firewall, zero trust network access (ZTNA) elements, and security posture and vulnerability assessments.

Why This Is Important

SASE management is often performed by the enterprise, making SASE only suitable for clients with mature security engineering and operations capabilities. Many enterprises lack the expertise to manage and secure networks, indicating that MSASE is a better choice for them. Sixty to 70% of SD-WAN buyers use managed services (e.g., MNS); we expect MSASE to increasingly align the same way. Gartner client interest in SASE is solid, with thousands of inquiries in the last two years.

Business Impact

MSASE can speed time to value for enterprises, and reduces strain on internal resources while reducing operational risk in order to reap SASE benefits. Currently, the vast majority of SASE offerings assume skilled and experienced client networking and security teams in emerging technologies, which many clients lack. MSASE services help these clients to more rapidly adopt SASE and achieve comparable benefits as organizations with solid internal network and security expertise.

Drivers

- There is strong client interest in SASE because it allows them to reduce the number of security vendors they employ, decreasing complexity while supporting key transformation initiatives, including cloud and hybrid work.
- Most enterprises cannot hire and retain enough employees that are skilled enough to support the demands of expanding security operations.
- Enterprise interest in MSASE is robust, as it optimizes their security architecture and reduces investments in internal resources.
- MSASE providers view the high interest in SASE and vendor consolidation as a prime opportunity to capitalize on the trend, resulting in a proliferation of choices for customers.
- The increase in MSASE vendors has resulted in downward pricing pressure, making it a more attractive alternative for customers considering buying SASE without a managed component.
- Enterprises clearly see the efficiency and performance by subscribing to an MSASE service that provides a single platform view of their security posture, due to the market's current lack of a consolidated platform and single portal interface.

Obstacles

- SASE solutions are available from an array of network and security vendors, yet few viable offerings exist in the market with a single management plane, unified data model, data lake and simplified pricing.
- Vendors have yet to fulfill Gartner's full vision of SASE, leaving some clients disillusioned and seeking more capabilities more quickly from their providers.
- Vendors commonly generalize specific enterprise use cases and lead with their solution first.
- Today, few fully deployed MSASE services exist. Vendor offers are expanding, but solution proof points in production environments are limited at this stage of market adoption.
- Client adoption is constrained by current commitments — either a capex commitment with remaining depreciation, or opex commitments constrained by contract terms.
- Client-aligned migration plans are lacking.
- The lack of productized life cycle process (days 0-2) standardization for MSASE will result in fragmented SLA experiences.

User Recommendations

- Evaluate MSASE providers if networking and security labor is the primary constraint to adopting SASE for the organization.
- Invest in MSASE to accelerate deployment, streamline security integrations, enable life cycle management and reduce staffing risk.
- Seek MSASE vendors who align their underlying SASE products with your organization's primary use cases, such as branch transformation, hybrid work support, or best-in-class security capabilities.
- When assessing MSASE services versus SASE offers, set realistic expectations about your organization's needed time and assets for both configuration and operations, since the managed services elements would require internal resources.
- When assessing MSASE offers, prioritize operational simplicity, unified management, ease of procurement and reduced overhead.
- Judge MSASE services by the level of standardization of their key network and security functions and life cycle processes, the maturity of SLAs, and commercial terms.

Gartner Recommended Reading

Forecast Analysis: Secure Access Service Edge, Worldwide

How to Align SD-WAN Projects With SASE Initiatives

2022 Strategic Roadmap for SASE Convergence

Market Guide for Single-Vendor SASE

Quick Answer: How Can Midsize Enterprises Benefit From Security Vendor Consolidation?

Network Assurance

Analysis By: Gregg Siegfried, Simon Richard

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Network assurance tools enable users to verify that a network behaves as intended. These tools are delivered as software, and typically discover and model a network environment.

Why This Is Important

Networks are increasing in complexity, and are changed repeatedly. Changes in configuration, use case or consumption should not degrade or have unintended side effects. Network assurance is of key interest to network and infrastructure leaders responsible for the health and performance of their network. The techniques that network assurance tools use facilitate testing and validation, and can support self-healing.

Business Impact

For network operations, it is not easy to answer the question as to whether the network behaves the way it is expected to. But this is what network assurance addresses by modeling the network and its traffic and running validation tests. Having a model of the network that validates applications and network changes accelerates the delivery of applications and increases reliability. The visibility gained by deploying network assurance will also decrease mean time to resolution (MTTR).

Drivers

- Networks are becoming more dynamic, and network changes are more frequent. Network operations are running out of resources to manually validate current state and upcoming changes.
- Modern applications are increasingly distributed and rely on external services as application workloads span the administration domain, making networks more difficult to assess.
- Network complexity increases the effort in maintaining an awareness of network health.
- The rise of digital experience monitoring exposes application performance issues at the same time, and modern applications are placing greater demands on the network.
- Improved compliance and simplified auditing, due to the algorithmic correctness of configurations, direct mapping to business intent and ongoing, dynamic and real-time validation.
- There are a handful of vendors that are actively investing in and promoting these capabilities in the market.
- Vendors are marketing network "digital twins" as a safe environment to test and validate network activities in support of networking and security use cases.

Obstacles

- Network assurance is an addition to an organization's existing network toolkit, not a replacement. Tool sprawl is already a challenge for most network teams.
- Net assurance needs integration with network discovery and source of truth tooling, which increases complexity and can't be used off the shelf.
- Network assurance tools build a model assuming that network devices, such as switches and router firewalls are bug free and that there are no cable or hardware issues. Unless they ingest and process live data, they only represent a partial state of the network.
- Organizations will need to design, create and deploy custom validation tests fit for their network, and face high costs of operation.

User Recommendations

- Include network assurance tooling to validate proposed network change.
- Integrate network assurance with network discovery and network source of truth.
- Pilot the network assurance solution offered by your network vendor, if any.

Sample Vendors

Cisco; Forward Networks; IP Fabric; Juniper Networks; NetBrain

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

Universal ZTNA

Analysis By: Andrew Lerner, John Watts

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Universal zero trust network access (ZTNA) extends existing ZTNA technologies to use cases beyond remote access, to support local enforcement in campus and branch "on-premises" locations. "Universal ZTNA" is a marketing term, as the original ZTNA definition was not limited to remote access use cases. Universal ZTNA centralizes a user or device zero-trust-access policy to enable a single access policy definition.

Why This Is Important

Extending ZTNA products to campus environments creates several benefits for enterprises, including security gap elimination, unified policy, enhanced visibility, simplified operations and modernized pricing models.

Business Impact

Although remote work surged in recent years, the future of work is hybrid. Hybrid working creates challenges for employees due to inconsistent network access implementations, which can lead to lost productivity and increase the likelihood of security and networking incidents. Universal ZTNA helps to streamline network and security policies across multiple environments.

Drivers

- Organizations that have deployed ZTNA for remote workers and are looking to extend the same technology for users while on-premises.
- Organizations are looking to develop a unified security policy to allow access to resources regardless of the user or device's physical location.
- Vendors are starting to aggressively market universal ZTNA.
- When done in conjunction with retiring duplicate systems for on-premises or remote access security, extending existing ZTNA implementations beyond remote access allows enterprises to achieve lower total cost of ownership (TCO).
- There is a desire for a consistent end-user experience when accessing corporate resources, whether in the office or remote.
- Organizations are looking for simplified administration of campus networks, via reducing the amount of switching configuration (e.g., between VLANs, 802.1X, MACsec, private VLANs, access control lists [ACLs] and microsegmentation) or reducing the need for network access control (NAC).
- Organizations are looking for improved visibility and control of end-user devices both on and off the local network.
- Organizations are looking to enable near-real-time adaptive access controls based on the risk of the user and device, beyond relying on the physical location or IP address of a user or device.

Obstacles

- Siloed network and security teams mean organizations overlook the opportunity to unify remote access and campus security using a single tool — with each silo picking their own product.
- There is a limited number of vendors with robust universal ZTNA offerings. Specifically, shortcomings include unmanaged devices and unauthenticated users, including unmanaged operational technology (OT) and Internet of Things (IoT).
- Steering traffic to enforcement points may require network redesign, or create latency or complexity and impact performance.
- IT management tools for patching and software distribution may need modernization to support reaching isolated endpoints, even in campus locations.
- There is an increased concentration risk of ZTNA failures due to poor policies, vulnerabilities or operational downtime in ZTNA infrastructure. There is increased risk of account takeover attacks applied to both remote and campus workers.
- Organizations have not defined what adaptive signals are important and what actions to take when adaptive signals fall below a certain threshold.

User Recommendations

- Start with secure remote user access use cases before extending to on-premises use cases.
- Pilot universal ZTNA deployments by extending existing remote access ZTNA deployments to campus environments in order to determine feasibility.
- Prefer universal ZTNA vendors who offer both on-premises and cloud-hosted enforcement points, to help avoid suboptimal traffic routing.
- Prefer cloud-based management for universal ZTNA deployments to gain faster access to new capabilities from the vendor, and avoid having to manage the management system.
- Align universal ZTNA with the need for web and SaaS security through secure access service edge (SASE) and security service edge (SSE) products, which, in addition to remote access, enable security and better networking performance on-premises.
- Create and test a resiliency plan for what happens when enforcement points are unavailable and resources are not reachable (for example, local policy caching when cloud resources are not available).

Sample Vendors

Appgate; Elisity; Fortinet; Versa Networks; Zscaler

Gartner Recommended Reading

Emerging Tech: How to Differentiate in the Fast-Growing but Crowded ZTNA Market

Campus Network Security and NAC Are Ripe for Market Disruption

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

Market Guide for Single-Vendor SASE

Service Connectivity Layer

Analysis By: Simon Richard

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

The service connectivity layer (SCL) abstracts the necessary network plumbing and security controls required to connect application services together regardless of location or IP address. The technology simplifies the stitching of services for developers who are not networking experts, and can provide facilities such as discovery and registry, connectivity, authorization, identity and observability.

Why This Is Important

SCL technologies (such as service meshes, cloud private endpoints and service connectivity fabrics) allow developers and application architects to configure their services assuming that the network is flat, and that services are reachable, without having to be concerned about details of the underlying network infrastructure.

Business Impact

Organizations that are building or operating modern distributed applications will benefit from decreased cycle time, increased productivity and operational simplicity. The SCL will help deliver software faster by abstracting services and connectivity between them. Developers can concentrate more on business functionality, and less on networking minutiae.

Drivers

- The increasing use of cloud services benefits from secure, transparent and controlled connectivity. The adoption of mesh app and service architecture (MASA) relies on ubiquitous connectivity between apps and services and between services.
- New offerings such as Amazon VPC Lattice validate the emergence of the SCL.
- Kubernetes service mesh users want to extend the service mesh benefits outside their clusters into more static environments. The SCL can bridge the gap between highly dynamic and static environments.
- Organizations are increasingly leveraging cloud private endpoints to communicate to service in public clouds.
- The SCL establishes some of the foundation for zero trust security architectures by pushing enforcement out to the service endpoints.
- The technology that extends identity to services and processes is gaining traction.
- The SCL is aligned to platform engineering efforts, as it reduces application developers' networking cognitive load.

Obstacles

- Vendor ecosystems are nascent and immature, with some emanating from the service layer and some from the network layer.
- The lack of clear buyer persona between networking, security, platform and developers makes it difficult for vendors to gain customers. Consensus needs to be reached among many teams, including networking, security and application architects for every sale.
- Integration with existing legacy networks' construct, architecture and operational processes makes it difficult to operationalize the SCL.
- The SCL works better for organizations that have a platform operations team and have adopted infrastructure as code. Some developers and infrastructure and operations (I&O) teams are unaware that SCL technologies can address some of their issues.

User Recommendations

- Deploy a service connectivity solution to insulate application development from complex network technologies when necessary.
- Work with I&O and platform operations teams to ensure service connectivity is at the right level of abstraction.
- Include security, platform, development and network teams in the product evaluation and architecture processes.
- Try your public cloud offering's service connectivity before looking at third parties' offerings.

Sample Vendors

Amazon Web Services; Google; greymatter.io; HashiCorp; Solo.io; Tetrate

Gartner Recommended Reading

Using Emerging Service Connectivity Technology to Optimize Microservice Application Networking

Adopt a Mesh App and Service Architecture to Power Your Digital Business

Managing Machine Identities, Secrets, Keys and Certificates

Hybrid Mesh Firewall Platform

Analysis By: Rajpreet Kaur, Adam Hils, Feng Gao

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

A hybrid mesh firewall (HMF) platform is a centralized policy management plane supporting hybrid environments through different firewall enforcement types by integrating with native cloud and on-premises network security controls along with other adjacent security technologies. The management plane is primarily a cloud-delivered service connected to on-premises, cloud and as-a-service firewall enforcement points from a single vendor.

Why This Is Important

Security and risk management leaders are struggling with the need to implement firewall controls in multiple environments leading to a lack of centralized implementation, management and visibility. Hybrid mesh firewall platforms offer multiple firewall enforcement types (e.g., hardware, virtual, cloud-native, firewall as a service [FWaaS]) from the same vendor, which can be deployed and managed from a centralized management interface.

Business Impact

Hybrid mesh firewall platforms help enterprises align with the cybersecurity mesh architecture (CSMA) concept for their firewall requirement. It allows you to consolidate into a firewall platform from a single vendor across multiple environments supporting consolidated policy management. It can support multiple firewall use cases such as data center, cloud, work from home, roaming users, branch offices and enterprise networks.

Drivers

- Cloud-hosted workloads often have radically different “agile” deployment pipelines that preclude the use of traditional firewall controls. This requires firewall controls for agile deployed workloads and containers or serverless compute offering automation and seamless integration to support this evolving use case.

- Growing adoption of zero trust architecture has also changed the firewall selection criteria, as enterprises have moved beyond adding a point firewall solution toward a platform, which can help them use the firewalls across multiple use cases.

- Remote and hybrid working has accelerated the adoption of FWaaS and preference from the same firewall vendor.

- Adoption of Internet of Things (IoT) devices is changing the interconnectivity requirement and the need to secure them.

- There is a need for centralized visibility and control across multiple firewall enforcements.

- Use of best-of-breed firewall players for evolving use cases is leading to added complexity and management overhead.

Obstacles

- The features and automation promised by the vendor don’t always work as advertised.

- On-premises firewalls present deployment and maintenance issues when combined with current hybrid and remote working models. They require different firewall enforcement points without an additional management overhead for the administrators.

- Network security teams lack skills and resources to configure and run the firewalls for emerging use cases such as DevSecOps, distributed connectivity for hybrid environments leading to integration and support challenges.

- Multiple different enforcement types are leading to different pricing models, leading to pricing and licensing complexity as the traditional models are no longer relevant.

- Not all vendors offer mature enforcement types for all the firewall use cases; as a result, teams are bound to adopt best-of-breed stand-alone offerings.

User Recommendations

- Integrate hybrid mesh firewalls with your zero trust strategy, as most existing controls such as hardware-based firewalls will not be fully retired in the mid to long term, driving complexity that HMF helps simplify.
- Always evaluate the automation and integration needs for the specific use case, such as DevSecOps being run in the environment.
- Demand transparent contracts from the reseller/vendor. Refuse to sign a contract that doesn't clearly highlight the part numbers and components involved in it.
- Closely verify the requirement for all the software subscriptions. You might not need all of the subscriptions that the vendors try to sell.

Sample Vendors

Barracuda; Check Point Software Technologies; Cisco; Forcepoint; Fortinet; H3C; Huawei; Juniper; Palo Alto Networks; SonicWall

Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Quick Answer: Demystifying Network Firewall Pricing Models to Build an Effective Sourcing Strategy

Tool: Competitive Evaluation of Network Firewalls

At the Peak

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

Zero Trust Strategy

Analysis By: John Watts, Thomas Lintemuth

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Zero trust strategy constitutes a set of core principles and program-level activities that establish contextual-based adaptive access controls. It replaces implicit trust with explicit adaptive trust aligned with a calculated risk of access to the sensitivity of the asset. Chief information security officers (CISOs) typically define and own a zero trust strategy, and execute zero trust initiatives to achieve a risk-optimized security posture for their organizations.

Why This Is Important

A zero trust strategy reduces the risk of attackers abusing implicit trust in environments that achieve lateral movement, employ available exploits and gain privilege escalation to gain their objectives. It matches the level of security controls to the sensitivity of the resource to improve end-user experience. Also, it limits an attacker’s ability to bypass static controls by establishing continuous trust assessments.

Business Impact

A zero trust strategy establishes strategic objectives based on cybersecurity principles to improve organizations' end-user experience and reduce the risk of certain cybersecurity threats. This is done by replacing legacy perimeter security approaches with fine-grained access controls. A zero trust strategy limits the impact of incidents when they occur and enables the digital transformation of businesses by installing flexible security controls closer to the assets that need protection.

Drivers

- The excessive hype in the information security community about the zero trust strategy is leading to higher sector visibility across organizations, even for nonsecurity leaders.
- The strategic response to security incidents where attackers abuse the excessive trust extended to user accounts, devices and workloads result in ransomware and data-exfiltration incidents.
- The desire to improve end-user experience with more adaptive controls. Also, the need to reduce the burden for access to less critical resources while requiring more context for more sensitive resources.
- The strategy to reduce the attack surface and limit scan and exploit attacks is cloaking existing networks and applications from discovery.
- The desire to deemphasize user and device location as a single, weak proxy for trust.

Obstacles

- The hype from vendors around zero trust often overpromises and underdelivers on their ability to achieve the vision of an organization's zero trust strategy.
- Organizational resistance to zero trust is interpreted as having no trust in employees.
- The isolated strategic development within the CISO group lacks context and conflicts with other organizational goals.
- The required involvement and availability from business-domain stakeholders and technical staff limit the use of outsourced strategy development to overcome skill and resource constraints.
- External constraints, such as technical debt and integration of multiple technologies from different security vendors, limit the strategic scope and require more resources for implementation than organizations can anticipate.
- Misaligned outcome expectations of a zero trust strategy lead organizations to replace existing security controls rather than augment them.

User Recommendations

- Establish an identity-first strategy as part of an identity and access management (IAM) program. Mature identity practices are a prerequisite to a zero trust strategy.
- Make the zero trust strategy part of a wider vision for cybersecurity. Integrate it with other cybersecurity strategies such as data, endpoint, and application security.
- Collaborate with stakeholders from security and nonsecurity functions to avoid confusion from varied interpretations of the term zero trust.
- Align the zero trust strategy to business initiatives, like digital transformation.
- Prioritize and rationalize investments defined by a zero trust strategy using zero-trust architecture development to define the scope and desired future end state.
- Build a set of outcome-driven metrics to measure the current risk and track the progress of risk reduction over time.

Gartner Recommended Reading

2023 Strategic Roadmap for Zero Trust Security Program Implementation

Treat Cybersecurity as a Business Decision to Minimize Cyber Risk

Kubernetes Networking

Analysis By: Simon Richard

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Kubernetes networking addresses three requirements: pod-to-pod communications, external entities to services communications (often called north-south traffic) and pod-to-service traffic communication (often called east-west traffic). Container networking interface (CNI) plug-ins handle pod-to-pod networking and pod-to-service networking; ingress controllers/gateway API handle north-south traffic; and service mesh provides enhanced east-west service traffic control and security.

Why This Is Important

Kubernetes has become the de facto standard system for container orchestration. The native networking capabilities within K8s don’t suffice for most enterprise production workloads at scale. CNI software and ingress controllers bridge this gap.

Business Impact

Many organizations are investing in Kubernetes as a foundational technology to their digital business strategies. To securely scale networking within K8s, a CNI and an ingress controller are needed. K8s’ CNIs enable developers to implement network policies and multitenancy without requiring developers to concern themselves with lower-level network tasks. Some K8s CNI also support network policies, which effectively implement a clusterwide distributed firewall and multitenancy.

Drivers

- The default networking capabilities in K8s do not scale to meet production enterprise requirements and/or fall short from a security/visibility and management-at-scale perspective. Kubernetes ingress controllers provide several benefits, including automatically encrypting traffic and increasing network performance and visibility.

- Open-source options reduce acquisition friction and initial cost (compared with commercial vendors), and align with the culture of many advanced customers who prefer OSS.

- Network virtualization vendors and data center networking vendors have CNI plug-ins that extend their policy model to Kubernetes applications and are supported by commercial Kubernetes platforms.

- For on-premises Kubernetes deployments, third-party CNI plug-ins and ingress controllers are necessary. However, commercial platforms include support for a default CNI plug-ins.

- On the ingress-controller side, most load balancing as well as some API gateway solutions extend their offerings to provide ingress controller functionality.

Obstacles

- Public cloud providers offer their own natively integrated CNI plug-ins and ingress controllers that integrate with their cloud platform and load balancers. Moreover, their Layer 7 load balancers can act as ingress controllers.
- Kubernetes networking vendors are pivoting to become CNAPP or service mesh vendors.
- Many enterprises lack deep K8s expertise. Moreover, many enterprises also lack deep K8s networking expertise.
- Organizations not using K8s don't need networking capabilities for it.
- Commercial vendors offering CNIs have difficulty maintaining pace with the K8s releases, which can limit the value to enterprises.
- With Kubernetes networking, pods do not have fixed IP addresses, which breaks many existing network security processes.
- The technology landscape associated with container networking solutions is fragmented, with many commercial vendors and open-source CNI plug-ins — which can confuse customers — and delay adoption for fear of making a wrong choice.

User Recommendations

- Determine if your requirements include network policies or pod-to-pod encryption. If so, look for an advanced CNI offering.
- Avoid making Kubernetes networking decisions in isolation. When sourcing, designing and deploying container networking solutions, ensure that the networking, cloud and development teams are part of a cross-functional effort.
- Hide network complexity from the application team (e.g., an ingress controller exposing Layer 7 policy rules to the application team but hiding the load balancing minutia).
- Eliminate manual network provisioning in Kubernetes-based environments. The automation and self-service provisioning of network resources are required.
- View first to extend your deployed network virtualization or data center fabric vendors/solutions from the cloud or data center networking during deployment.
- Prefer ingress controllers that extend your existing load balancing or API gateway vendors.Include requirements for turnkey Kubernetes network integration in network RFPs.

Sample Vendors

Amazon; Avesha; Azure; Cisco; F5; HAproxy; Isovalent; Juniper Networks; Tigera; VMware

Gartner Recommended Reading

Solution Path for Cloud-Native Infrastructure With Kubernetes

Using Emerging Service Connectivity Technology to Optimize Microservice Application Networking

Sliding into the Trough

Digital Experience Monitoring

Analysis By: Mrudula Bangera, Padraig Byrne

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Digital experience monitoring (DEM) technologies monitor the availability, performance and quality of experience for an end user or digital agent as they interact with an application and the supporting infrastructure. Users can be external consumers of a service, internal employees accessing corporate tools, or a combination of both. DEM technologies seek to observe and model the behavior of users as a continuous flow of interactions in the form of "user journeys."

Why This Is Important

DEM helps organizations address visibility in two key areas:

- **Remote employees' experience:** Instrumenting the corporate network is relatively easy. Doing the same for a home or coffee shop network ranges from challenging to impossible.
- **Web applications:** Visibility into the performance of as-a-service-based applications (including e-commerce) presents a unique challenge, due to the location of the application and difficulty in instrumenting cloud-based environments.

Business Impact

RUM and STM technologies in DEM allow businesses to understand how the users (customers) are interacting with the brand across mobile and web. The endpoint monitoring technology gives organizations increased flexibility to gain visibility into the endpoint, network and service of the user, irrespective of where workers are located, and without requiring extensive instrumentation of the physical environment.

Drivers

- **User experience:** Organizations are coming to the realization that metrics tell only part of the story. If the user is having a less-than-ideal experience, then whatever the metrics say are meaningless. DEM can help provide visibility into not just the metric-based performance, but also the subjective portion of the user experience.

- **SaaS:** As organizations move from on-premises-based applications to SaaS-based applications, they lose visibility into, and control over, the performance of these applications. A user of a SaaS-based application in one location using a specific endpoint (such as a laptop or mobile) may have a totally different experience from a different user at a different location using a different endpoint. Even the same user at the same endpoint may have very different experiences, depending on where they are located at the time. DEM enables organizations to understand where the performance bottlenecks are, so they can be addressed.

- **Work from anywhere:** The massive changes in workforce location brought on by the COVID-19 pandemic are driving infrastructure and operations (I&O) teams to adopt endpoint monitoring technologies to analyze and optimize remote workers' access to, and use of, applications.

- **"Last mile" in full-stack observability:** Monitoring of applications from the server side is important, but I&O teams need to understand the end-user journey and the corollary experience. Endpoint monitoring through DEM tools allows I&O teams to track performance from the endpoint's connectivity to Wi-Fi through service provider networks and beyond.

- **Commercial off-the-shelf (COTS) and virtual desktop infrastructure:** Organizations often rely on COTS applications for critical business operations. The very nature of these solutions makes them difficult (if not impossible) to instrument from an application perspective. I&O teams rely on the visibility provided by DEM tools to provide information on performance from the end user's perspective.

Obstacles

- There are very few DEM vendors that provide functionality across all three pillars of DEM (synthetic monitoring, endpoint visibility and real-user monitoring), making it difficult to choose a vendor that can provide a complete solution.

- Most DEM visibility comes from an agent installed on the endpoint, which can represent a challenge for organizations that are already running numerous endpoint agents.

- Large organizations may struggle with the management of tens or hundreds of thousands of endpoints via a DEM tool user interface.
- Due to the sheer volume of data generated by DEM tools, organizations without a robust analytics approach may struggle to make sense of all the data. Few vendors use analytics to enable a proactive approach in this space.
- User experience can be enhanced through autorectification of anomalies. However, very few DEM vendors provide the ability to automate remediation.

User Recommendations

- Gain a holistic view of digital experience by choosing and deploying DEM solutions that gather sentiment alongside other data points.
- Minimize endpoint performance impacts by evaluating DEM capabilities from vendors and tools you already own (for example, DEM capabilities from a unified endpoint management , security or remote access vendor).
- Enable insight-driven automation by choosing DEM solutions that provide analytics and remediation functions.
- Measure SaaS application performance by choosing DEM solutions that can perform real-user monitoring and synthetic transaction monitoring.
- Gain transparency into employee experience by monitoring as many endpoints as possible.

Sample Vendors

Apica; Catchpoint; Cisco; Fortinet; Kadiska; Lakeside Software

Gartner Recommended Reading

Market Guide for Digital Experience Monitoring

How to Monitor and Troubleshoot Remote Workers' Application Performance

3 Ways to Optimize Observability and Monitoring of Digital Services in the Cloud

Use DEM to Understand and Enhance Your Employees' Work-From-Home Experience

Use Synthetic Monitoring to Enhance User Experience for Hosted and SaaS Applications

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

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

OpenID Connect

Analysis By: Erik Wahlstrom, Brian Guthrie

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

OpenID Connect (OIDC) is an identity federation protocol built on the OAuth 2.0 framework that enables web services to externalize authentication functions. It enables applications (e.g., web-based, mobile and JavaScript) to authenticate human end users, as well as obtain basic profile information over an API.

Why This Is Important

- OIDC lets application owners and developers authenticate human users across websites and applications without having to create, manage and maintain identities.
- With OIDC, you can provide single sign-on (SSO) and use existing enterprise or social accounts to access applications and thereby improve usability, security and privacy.
- OIDC provides consent management, support for hybrid and multicloud environments, and also support for more client types than previously developed federation protocols.

Business Impact

Built on top of the OAuth 2.0 protocol, OIDC offers a flexible, efficient alternative to SAML. Its main benefits are:

- Improving user experience by providing lightweight authentication and authorization, and fine-grained consent management.
- Reducing the data entry burden during user registration with SSO and federation support.
- Providing better support for key discovery and rotation than SAML.
- Efficiently supporting token and API-centric architectures with mobile and single-page applications.

Drivers

- There is an increased interest in the protocol, which has replaced SAML in terms of preference for new client-facing and enterprise applications. The benefits that OIDC brings to API access controls, privacy regulation, consent management, step-up authentication, compliance and implementation of adaptive access will accelerate its time to plateau and become mainstream.
- Extensions built for OIDC establish a federation of federation services (multilateral federation), which is commonly used in higher education and with select industries such as healthcare, in which a common set of policies is followed.
- OIDC is a way to use a single set of user credentials to access multiple sites.
- OIDC has been proven to allow identity interactions to be conducted more seamlessly and with less friction for developers than XML-based standards, such as SAML, or purely proprietary implementations, and with greater security than preceding protocols.
- Finance, government and healthcare institutions can benefit from its increasing work to profile OIDC specifications to support, and be fine-tuned for use by, industry verticals.
- There is ongoing work to extend OpenID Connect to support more use cases. This includes fast trust establishment between OpenID providers and relying parties, support for verifiable credentials, and the establishment of standards to share risk signals.
- OIDC is mature, well supported and organizations can find certified solutions through the OpenID Connect Foundation that certifies solutions against server conformance profiles of OIDC.

Obstacles

- The list of SaaS applications supporting OIDC continues to grow; however, it still has smaller market penetration than SAML.
- Developers often underestimate the intricacies of the protocol and build homegrown libraries with “cherry-pick” features from the specification, making implementations unsecure. Instead, they should use proven and well-tested, open-source and/or vendor-provided libraries that are up to date and meet the latest security recommendations.

User Recommendations

- Give preference to OIDC over SAML. Use OIDC for modern application “greenfield” developments.Leverage an access management tool that centralizes adaptive access engines, supports multiple protocols and can translate among protocols, especially between SAML and OIDC, and other proprietary security token formats.
- Use OIDC for human user authentication, not for machines (workloads and devices) that instead should rely on the OAuth 2.0 framework to get tokens.
- Use OIDC instead of proprietary authentication methods to avoid vendor lock-in and balance security, privacy, usability and scale when building and deploying applications and services.
- OIDC is often seen as a panacea for API access control, and the ID token issued in an OIDC flow next to an access token is sometimes misused as a credential when calling APIs. Instead of using the ID token, use the access token to access APIs and therefore focus on validation of that token.

Sample Vendors

Cloudentity; Curity; ForgeRock; Gluu; Google; IBM; Microsoft; Okta; Ping Identity; Red Hat

Gartner Recommended Reading

Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

Buyer’s Guide for Access Management

IAM Leaders’ Guide to Access Management

Magic Quadrant for Access Management

Architect a Modern API Access Control Strategy

Microsegmentation

Analysis By: Adam Hils, Rajpreet Kaur, Jeremy D'Hoinne

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Microsegmentation — also referred to as identity-based segmentation or zero trust network segmentation — can create more granular and dynamic access policies than traditional network segmentation, which is limited to internet protocol/virtual LAN (IP/VLAN) circuits.

Why This Is Important

Once a system is breached, attackers move laterally (including in ransomware attacks), which can cause serious damage. Microsegmentation seeks to limit the propagation of such attacks. It can greatly reduce the initial attack surface as well.

Business Impact

Microsegmentation can mitigate the risk and impact of cyberattacks. It is a form of zero trust networking that controls the access between workloads and is used to limit lateral movement, if and when an attacker breaches the enterprise network. Microsegmentation also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including those that host containers.

Drivers

- As servers are being virtualized, containerized or moved to infrastructure as a service (IaaS), existing safeguards such as traditional firewalls, intrusion prevention solutions and antivirus software struggle to follow the fast pace of deployment for new assets. This leaves the enterprise vulnerable to attackers gaining a foothold and then moving laterally within enterprise networks. This has created increased interest in visibility and granular segmentation for east-west traffic between applications, servers and services in modern data centers.

- Zero trust is becoming a requirement in data center design, and microsegmentation is a practical way to accomplish this.

- The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies difficult to manage at scale, if not impossible to apply.

- Some microsegmentation products provide rich application communication mapping and visualization, allowing data center teams to identify which communication paths are valid and secure.

- The shift to microservices container architectures for applications has also increased the amount of east-west traffic and further restricted the ability of network-centric firewalls to provide this segmentation.

- The extension of data centers into IaaS has placed a focus on software-based approaches for segmentation — in many cases, using the built-in segmentation capabilities of cloud providers.

- Growing interest in zero trust networking approaches has also increased interest in using application and service identities as the foundation for adaptive application segmentation policies. This is critical to enforcing segmentation policies in the dynamic networking environments used within container-based environments.

Obstacles

- Complexity — If not planned and scoped correctly, microsegmentation projects can lose organizational support before completion.
- Lack of knowledge — Security and risk leaders don't know which applications should be communicating with others, sowing doubt in automatically generated protection rules.
- Legacy network firewalls — Some data centers have network firewalls for broader east-west traffic segmentation, which is adequate for some organizations. Traditional firewalls can also present operational challenges to some identity-based segmentation solutions when policies overlap or conflict.
- Organizational dynamics — Cloud-centric organizations employing DevOps may value agility more than security, believing that any additional security controls will introduce operational friction.
- Expense — Full microsegmentation can come at a high price. Many organizations consider microsegmentation to be a net new budget item.

User Recommendations

- Select zones to microsegment based on the highest risk. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.
- Seek a solution that maps application communication paths and makes policy recommendations, using AI to make policy recommendations.
- Do not use IP addresses or network location as the foundation for east-west segmentation policies. Use the identities of applications, workloads and services — either via logical tags, labels, fingerprints or stronger identity mechanisms.
- Use the microsegmentation style (network overlay, host-based, cloud-native, API-based) that covers both the location of the workloads (on-premises, hybrid and IaaS) and the type of environment in which workloads are hosted (containers and virtual machines).
- Target the most critical assets and segment them first.
- Plan for coexistence of traditional firewalls and microsegmentation approaches for the next five years, and seek products that can support both.

Sample Vendors

Akamai Technologies; Aqua Security Software; Cisco; ColorTokens; Fortinet; Illumio; Palo Alto Networks; VMware; Zero Networks; Zscaler

Gartner Recommended Reading

2023 Strategic Roadmap for Zero Trust Security Program Implementation

Container Security

Analysis By: Charlie Winckless, Michael Warrilow, Thomas Lintemuth

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Container security refers to the technologies and processes, testing, and controls in container-based environments. Full-life-cycle container security starts in development by assessing the risk or trust of the container's contents, secrets management and configuration of container instances. This extends into production with runtime container segmentation, threat protection and access control.

Why This Is Important

By enabling greater speed and agility to streamline development, container-based applications have become mainstream. Rapid adoption of orchestration platforms, such as Kubernetes, has left traditional vendors and some security teams without appropriate tools to ensure secure application deployment. Container security requires a life cycle approach, starting with scanning of containers in development and protection of containers at runtime.

Business Impact

Containers are not inherently insecure, but they are being deployed insecurely with known vulnerabilities and configuration issues. Without proper controls, developers can introduce vulnerabilities into development and, subsequently, production environments. This can expose organizations to avoidable risk. Furthermore, security has been slow to embrace secure container development practices and tools, leaving organizations unaware of potential risks and unprepared to respond to attacks.

Drivers

- Developer adoption of containers and Kubernetes has shifted threats from traditional environments to containerized ones, forcing security teams to use different tools and approaches to address these new threats.
- Container-as-a-service (CaaS) offerings, such as Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS) and Google Kubernetes Engine (GKE), are on the rise. These require security integrations to provide coverage for the clusters and containers they host.
- With rising adoption of containers, security and risk management leaders need to address container-related security issues around vulnerabilities, visibility, compromise, and compliance. This would help meet the needs of digital business and application modernization.
- Multiple point solutions can now integrate transparently into the continuous integration/continuous delivery pipeline and DevOps practices, to proactively scan containers for security and compliance issues. However, organizations must carefully manage these point solutions to minimize the complexity they introduce.
- Microservices architectures are proliferating and driving container deployments in DevOps processes, which causes some of the responsibility for securing the environment to shift left to developers. DevOps pipeline integrations provide opportunities to secure against supply chain and other development risks in these environments.

Obstacles

- Container security must start in development, yet many security vendors and enterprises treat container security as a runtime-only problem. Worse, some vendors are simply placing an agent on a container, forwarding logs and calling this “container security.”
- If container image governance policies are not introduced early on, applying standards becomes increasingly difficult, as different software product teams start to implement their own processes for building container images.
- Organizations and teams may resist the use of active runtime container security for fear of disrupting applications and business.

User Recommendations

- Create and maintain a minimum set of hardened and immutable container images as the basis for all container workloads. In doing so, prioritize the use of a container-optimized operating system distribution.
- Scan containers in development for configuration and vulnerability issues of all code types, before deploying to production. Integrate with admission controllers to prevent these vulnerable containers being deployed.
- Take advantage of continuous scanning provided by code repositories and cloud providers.
- Use automated tools to analyze the processes expected to run in containers, along with their behaviors. Use this information to replace signature-based deny-listing with allow-listing-based lockdown.
- Require container security solutions to explicitly support and integrate with your container management tooling and/or Kubernetes.
- Design single-purpose containers and clear tagging mechanisms to track data sensitivity.

Sample Vendors

Aqua Security; Lacework; Palo Alto Networks; Red Hat; Snyk; SUSE, Sysdig; Tigera; Trend Micro; Uptycs

Gartner Recommended Reading

Container Supply Chain: 10 Security Vulnerabilities and How to Address Them

Market Guide for Cloud-Native Application 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

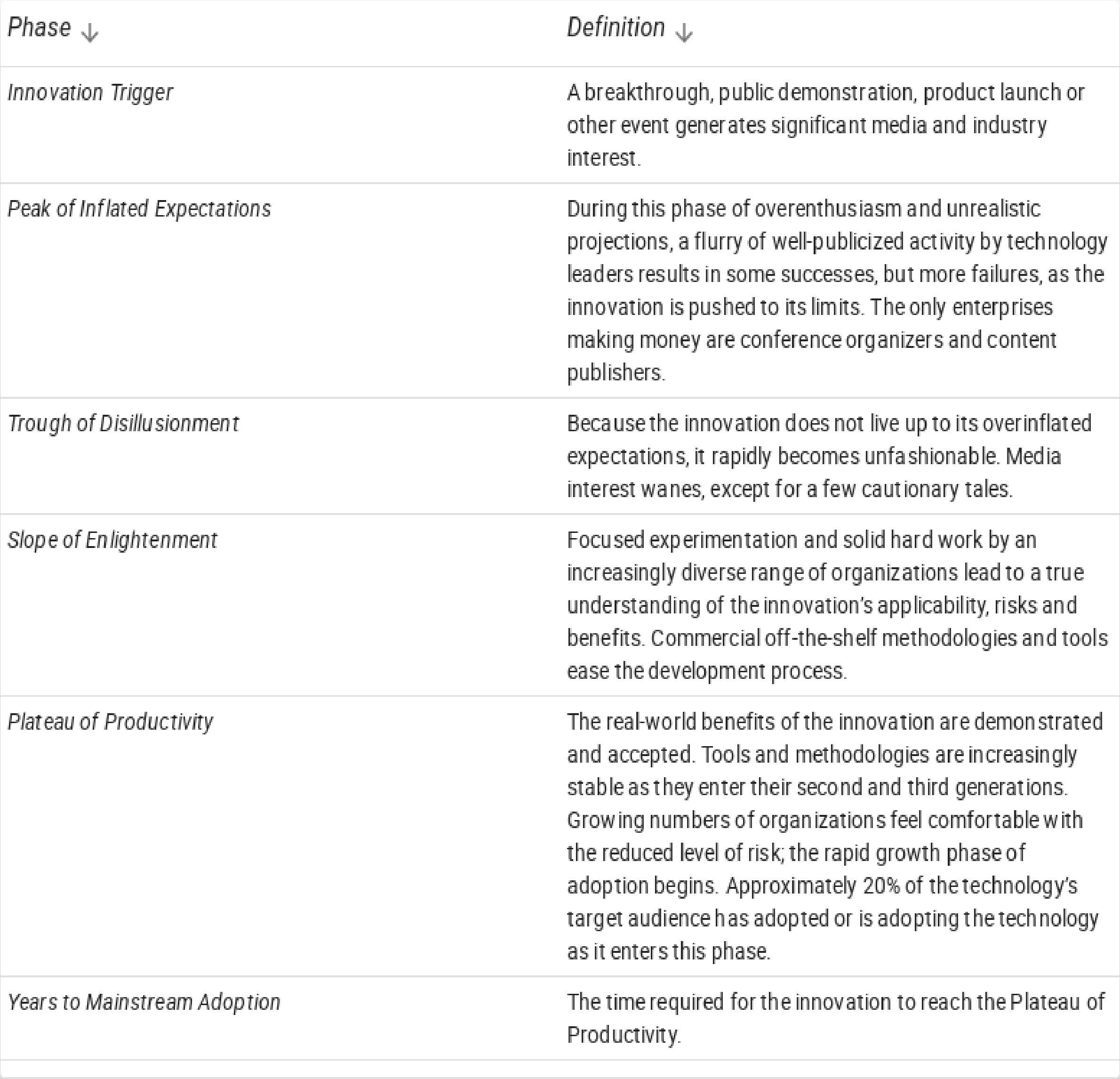
Market Guide for Single-Vendor SASE

Appendixes

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)



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

Source: Gartner (July 2023)

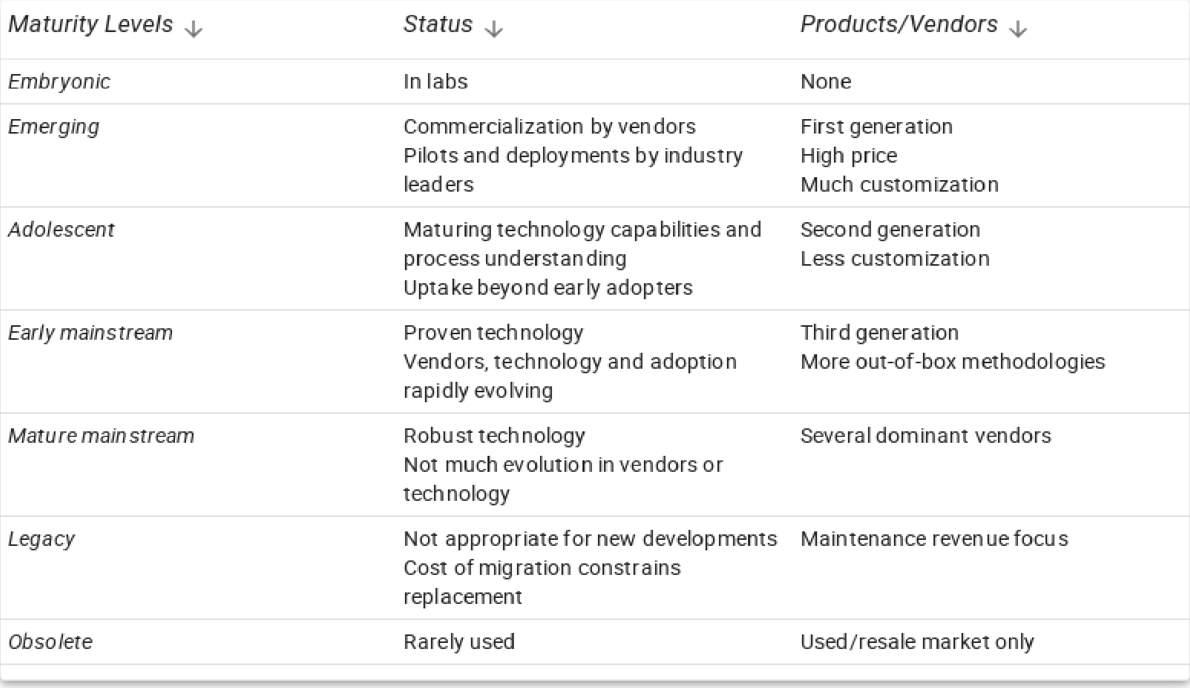
Table 3: Benefit Ratings

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 (July 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 (July 2023)

Evidence

Gartner analysts conducted over 4,000 client interactions from 12 May 2022 through 12 May 2023 on the topics of ZTNA and SASE.

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

Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality

Infographic: 4 Essential Stages on the Journey to Zero Trust

How to Build a Zero Trust Architecture

Table 1: Priority Matrix for Zero Trust Networking, 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		
High	Microsegmentation	Digital Experience Monitoring Hybrid Mesh Firewall Platform OpenID Connect Unified Endpoint Security Universal ZTNA	Managed SASE Zero Trust Strategy	
Moderate	Container Security	Kubernetes Networking ZTNA	CAEP Enterprise Browsers Service Connectivity Layer	
Low	Remote Browser Isolation		Extranet as a Service Network Assurance	

Source: Gartner (July 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 (July 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 (July 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 (July 2023)