GIGAOM

Image credit: gorodenkoff

Chris Grundemann, Ivan McPhee
Jun 4, 2021

Key Criteria for Evaluating Secure Service Access (SSA) v1.0

An Evaluation Guide for Technology Decision Makers

Cloud & Infrastructure, Edge & Networking, Security & Risk

Key Criteria for Evaluating Secure Service Access (SSA)

An Evaluation Guide for Technology Decision Makers

Table of Contents

1. Summary

Since the inception of large-scale computing, enterprises, organizations, and service providers have protected their digital assets by securing the perimeter of their on-premises data centers. With the advent of cloud computing, the perimeter has dissolved, but—in most cases—the legacy approach to security hasn not. Many corporations still manage the expanded enterprise and remote workforce as an extension of the old headquarters office/branch model serviced by LANs and WANs.

Bolting new security products onto their aging networks increased costs and complexity exponentially, while at the same time severely limiting their ability to meet regulatory compliance mandates, scale elastically, or secure the threat surface of the new *any place/any user/any device* perimeter.

The result? Patchwork security ill-suited to the demands of the post-COVID distributed enterprise.

Converging networking and security, secure service access (SSA) represents a significant shift in the way organizations consume network security, enabling them to replace multiple security vendors with a single, integrated platform offering full interoperability and end-to-end redundancy. Encompassing secure access service edge (SASE), zero-trust network access (ZTNA), and extended detection and response (XDR), SSA shifts the focus of security consumption from being either data center or edge-centric to being ubiquitous, with an emphasis on securing services irrespective of user identity or resources accessed.

This *GigaOm Key Criteria* report outlines critical criteria and evaluation metrics for selecting an SSA solution. The corresponding *GigaOm Radar Report* provides an overview of notable SSA vendors and their offerings available today. Together, these reports are designed to help educate decision-makers, making them aware of various approaches and vendors that are meeting the challenges of the distributed enterprise in the post-pandemic era.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Secure Service Access Primer

Digital transformation shifted the focus from the data center to the cloud. Instead of branches and remote users connecting back to the data center to access applications, they began accessing those same applications in the cloud via SaaS solutions. Backhauling traffic introduced latency and impacted performance, so the traditional WAN quickly became obsolete. Centralizing control and providing intelligent routing, its replacement, the application-aware software-defined WAN (SD-WAN) reduced complexity, increased efficiency, and provided a seamless on-ramp to the cloud.

However, SD-WAN comes in various flavors and is designed to connect networks—not users—with numerous third-party products required to secure the network. Operating in silos, today's network and security teams are faced with severe challenges, including:

- **Managing point security products:** The typical enterprise deploys dozens of point security products, with many larger enterprises deploying over 100. The result? Human error, misconfigured and out-of-date tools, gaps in coverage, infrequent network scans, and too many security alerts. Moreover, most security team leaders cannot establish whether the tools deployed are working correctly or not, with many failing to realize the full value of their multimillion-dollar annual security investment.
- **Coverage and visibility gaps:** When remote users connect to the cloud, centralized security policies are practically unenforceable unless traffic is backhauled to the data center. Since doing so adds latency and negatively impacts the user experience, IT administrators often opt to live with coverage and visibility gaps, compromising both compliance and security. The inability of traditional perimeter-based security solutions to detect and stop advanced targeted attacks is a primary barrier to reaching security maturity.
- **Limited budgets and resources:** With IT and security budgets under pressure and a shortage of skilled security personnel, deploying and managing multiple costly point security solutions across multiple locations with limited resources is proving impractical and ineffective. Almost all enterprises have a shortage of skilled staff—resulting in their implementing a reactive and incident-driven security approach—and a general lack of confidence in their staff's and technology's abilities to stop data breaches.

In an attempt to create a roadmap for their customers, vendors are adopting different models and strategies to varying degrees—including Gartner's secure access service edge (SASE) and Forrester's zero trust network access (ZTNA)—each with pros and cons. While frameworks supporting authenticated users—contractors, employees, and partners—extend the perimeter, they fail to address the security needs of either open web applications or authenticated bad actors.

The distributed digital enterprise requires defense-in-depth comprising a secure network mesh with built-in, fully-integrated security for applications, data, and users (application, device, or human). SSA solutions provide easy-to-use, flexible, integrated, and scalable cloud-native, user-centric layered security functions meeting the unique needs of each enterprise, organization, or service provider—irrespective of network architecture, cloud services, or user location and device. An emerging technology, SSA solutions converge networking and security and make it available as-a-service, resulting in an enhanced user experience with seamless, low-latency services. When exploring offerings from both incumbent and new vendors, customers should look for the following critical capabilities that make up an SSA solution:

- **Global Network Mesh:** Traffic must be intelligently routed across private or public points of presence (POPs) to ensure compliance and minimize latency. Despite early reservations regarding using the public cloud as the transport layer, building a proprietary network is prohibitively expensive. While some security vendors and managed service providers have invested hundreds of millions of dollars in their own networks, others are leveraging the existing investments of public cloud operators—such as AWS, Google, and Microsoft Azure—as an economical alternative. Many of the new SSA vendors are taking advantage of the public cloud to deliver secure, low-latency services.
- **Distributed Policy Enforcement:** As users and apps become increasingly distributed, common sense dictates that traffic inspection and policy enforcement should happen at the edge. While control is still centralized to ensure coverage and visibility, SSA solutions shift inspection, detection, and mitigation to the edge. Whether it is called “zero trust” or something else, access is granted based on both identity and behavior, with fine-grained controls enabled for sensitive applications and data. As SSA matures, we expect behavioral analytics to play a crucial role in establishing trust in a distributed environment.
- **Extended Detection and Response (XDR):** Combining the capabilities of endpoint threat detection and response (EDR) with network threat detection and response (NTDR), XDR provides cross-layered detection and response. Collecting and correlating data spanning multiple security layers—cloud, data center, endpoint, and network—XDR accelerates threat detection and mitigation. While XDR simplifies the security landscape in theory, converging two very different technologies is no easy feat. Vendors are investing heavily in this area, and we expect to see rapid innovation over the next 18-36 months.

Over time, we expect the solution landscape to change dramatically as acquisitions and mergers take place and new innovations and new vendors emerge. However, in the interim, creating heightened access security awareness and mapping your path forward is essential for your organization. As SSA evolves and matures, the sooner you explore your choices and start working toward networking and security convergence, the greater your ability to withstand security threats and market forces will become.

3. Report Methodology

A GigaOm Key Criteria report analyzes the most important features of a technology category to help IT professionals understand how solutions may impact an enterprise and its IT organization. These features are grouped into three categories:

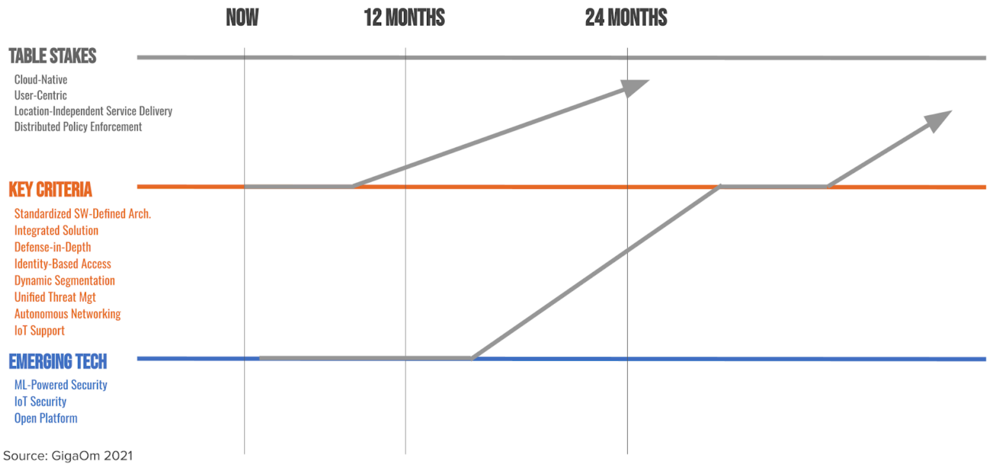
- Table Stakes: Assumed Value
- Key Criteria: Differentiating Value
- Emerging Technologies: Future Value

Table stakes represent features and capabilities that are widely adopted and well implemented in a technology sector. As these implementations are mature, they are not expected to significantly impact the value of solutions relative to each other, and will generally have minimal impact on total cost of ownership (TCO) and return on investment (ROI).

Key criteria are the core differentiating features in a technology sector and play an important role in determining potential value to the organization. Implementation details of key criteria are essential to understanding the impact that a product or service may have on an organization's infrastructure, processes, and business. Over time, the differentiation provided by a feature becomes less relevant and it falls into the table stakes group.

Emerging technologies describe the most compelling and potentially impactful technologies emerging in a product or service sector over the next 12 to 18 months. These emergent features may already be present in niche products or designed to address very specific use cases, however at the time of the report they are not mature enough to be regarded as key criteria. Emerging technologies should be considered mostly for their potential downfield impact.

Over time, advances in technology and tooling enable emerging technologies to evolve into key criteria, and key criteria to become table stakes, as shown in **Figure 1**. This Key Criteria report reflects the dynamic embedded in this evolution, helping IT decision makers track and assess emerging technologies that may significantly impact the organization.



Source: GigaOm 2021

Figure 1. Evolution of Features

Understanding Evaluation Metrics

Table stakes, key criteria, and emerging technologies represent specific features and capabilities of solutions in a sector. Evaluation metrics, by contrast, describe broad, top-line characteristics—things like scalability, interoperability, or cost effectiveness. They are, in essence, strategic considerations, whereas key criteria are tactical ones.

By evaluating how key criteria and other features impact these strategic metrics, we gain insight into the value a solution can have to an organization. For example, a robust API and extensibility features can directly impact technical parameters like flexibility and scalability, while also improving a business parameter like total cost of ownership.

The goal of the GigaOm Key Criteria report is to structure and simplify the decision-making process around key criteria and evaluation metrics, allowing the first to inform the second, and enabling IT professionals to make better decisions.

Characteristics and Infrastructure

For this report, the applicability of the solution will be graded across four target market categories differing in (1) their characteristics, and (2) how they can be integrated with existing infrastructures:

- **Cloud Service Providers (CSPs):** Service providers delivering pay-per-use, on-demand services to customers over the internet, including IaaS, PaaS, and SaaS.
- **Network Service Providers (NSPs):** Service providers selling network services—such as network access and bandwidth—provide access to backbone infrastructure or network access points (NAP). In this report, NSPs include data carriers, ISPs, telcos, and wireless providers.

- **Managed Service Providers (MSPs):** Service providers delivering application, IT infrastructure, and network and security services and support for businesses on customer premises, in the MSP's data center (hosting), or in a third-party data center.
- **Enterprises (Large, Medium, Small):** Enterprises refer to all businesses responsible for planning, building, deploying, and managing their applications, IT infrastructure, networks, and security in either an on-premises data center or a colocation facility.

Also, we recognize four *deployment models* for solutions in this report: private cloud, public cloud, hybrid cloud, and multi-cloud.

- **Private Cloud:** Used exclusively by one enterprise or organization, cloud computing resources are physically located in an on-premises data center or hosted by a third-party colocation service provider. Tailored to meet specific requirements, private clouds offer compliance, control, and flexibility.
- **Public Cloud:** Owned and operated by a third-party cloud service provider and delivered over the internet, public cloud providers offer cost-effective, scalable, and reliable on-demand resources for enterprises and SaaS vendors.
- **Hybrid Cloud:** Enabling data and apps to move seamlessly between two environments, a hybrid cloud combines private, on-premises infrastructure with a public cloud. Hybrid cloud allows compute resources to be brought closer to the edge where data resides—reducing latency and increasing reliability—while still meeting regulatory compliance and data sovereignty requirements.
- **Multi-Cloud:** Comprising multiple public cloud services performing different functions, multi-cloud allows enterprises and organizations to take advantage of different public cloud capabilities or geographies. Multi-cloud deployments may include private clouds, resulting in cloud deployment that is both hybrid and multi-cloud.

4. Decision Criteria Analysis

In this section, we describe the criteria that organizations should use to evaluate available solutions. First, we describe the elements we consider to be “table stakes”—fairly common capabilities but not particularly useful metrics to separate one solution from another. We then focus on the key criteria that differentiate solutions available in the marketplace. Finally, we describe an additional set of evaluation metrics, in each of which different solutions may excel, that can further help evaluate and separate them.

Table Stakes

We consider table stakes to be stable, mature solution features that are relatively common across all vendors. These features form the basis of the platform offerings and usually do most of the heavy lifting. For this discussion, assume all platforms in this report support these table stakes to a reasonable level:

- Cloud-native
- User-centric
- Location-independent service delivery
- Distributed policy enforcement

Cloud-native: Software services are available in the cloud independently of specific hardware requirements. Architected from the ground up to run in the cloud, cloud-native refers to platforms specifically designed to take advantage of a cloud delivery model to increase agility, availability, performance, and scalability.

User-centric: Policies are enforced based on the identity and behavior of the user (application, device, or human) accessing the resource. Well-designed, converged network and security systems should enable the user journey, providing authenticated users with authorized access to resources and services as easily and quickly as possible.

Location-independent service delivery: Services are independent of user location and available to any user on any device anywhere in the world. With the shift toward a distributed workforces and large-scale IoT rollouts, remote users and devices must have the same access to resources and services as they would if they were physically located in a corporate office. In addition, applications should be able to move seamlessly from the data center to the cloud—and between clouds—with the same levels of availability and security.

Distributed policy enforcement: Instead of the enterprise data center being the access gateway to the network, policies are enforced and threats detected and eliminated at multiple data touchpoints.

While still managed centrally, authentication, authorization, decision-making, and policy enforcement are distributed across the network, minimizing latency and increasing availability.

Key Criteria

Providing the basis upon which organizations can make informed decisions about which solutions to adopt for their particular needs, this section outlines *the primary criteria for evaluating solutions*. Attributes and capabilities will vary from one vendor to another and should be evaluated based on each organization's needs and use cases.

- Standardized software-defined architecture
- Integrated solution
- Defense-in-depth
- Identity-based access
- Dynamic segmentation
- Unified threat management
- Autonomous networking
- IoT support

Standardized software-defined architecture: SSA depends on the availability of a ubiquitous, cloud-native software-defined architecture supporting a broad range of use cases and scenarios across a shared infrastructure. Running over existing private, public, or managed networks via global POPs, software-defined applications accelerate time-to-value by eliminating the need to deploy and commission hardware.

Integrated solution: Despite a basic tenet of SSA being the convergence of networking and security, it is unlikely that a single vendor will provide all capabilities required. We're seeing several vendors claiming to have integrated SSA solutions. However, looking under the hood, we find—for the most part—these are loosely cobbled together under a common UI and marketecture. Having said that, some established vendors are planning tighter integration aggressively across their product portfolio to meet the needs of their installed base.

Defense-in-depth: Based on the premise that attacks lose momentum over time, defense-in-depth (DiD) provides layers of security to protect sensitive applications and data. Ideally, defense-in-depth should be implemented within multiple layers of the OSI model, with Layer 3 and 4 firewalls filtering traffic at the packet level and Layer 7 firewalls filtering content for granular protection.

Identity-based access: A simple, coarse-grained digital security method, identity-based access determines whether a user will be permitted or denied access to a resource. In the case of a service, users may be applications, devices, or humans. Authorization at the identity authentication level, however, is just one of many layers. SSA encompasses zero trust—a condition in which nothing inside or outside the network is trusted—requiring granular verification. We expect to see a lot of innovation in this area, with behavioral analytics playing an essential part in establishing trust.

Dynamic segmentation: Blocking east-west traffic to contain breaches, dynamic network segmentation enforces granular identity and context-aware security policies—across the data center, network, and cloud—in real time. Reducing the attack surface and improving breach containment, micro-segmentation creates zones to isolate and secure individual workloads. Micro-segmentation may also be referred to as application segmentation or east-west segmentation.

Unified threat management: Unified threat management (UTM) integrates multiple security features within a single device or service on the network. Simplifying security, UTM performs multiple threat detection, identification, and mitigation services, including anti-virus, anti-spam, anti-phishing, and content and web filtering.

Autonomous Networking: An autonomous network runs with little to no human intervention based on the intent determined by the business. In the context of SSA, the introduction of AIOps creates a shared context encompassing applications, networks, and services. Reducing complexity and increasing efficiency, advanced analytics and machine learning (ML) automate and enhance IT operations, improving the end-user experience and maximizing network investments.

IoT Support: With the rapid deployment of IoT devices increasing network exposure, IoT requires different strategies, focal points, and skill sets. Compromised IoT can lead to data breaches, interrupted operations, and physical damage to facilities and operators. IoT support includes securing connectivity between IoT devices and the cloud, and securing IoT data in the cloud during processing and storage.

Emerging Technologies

While vendors are leveraging existing capabilities and developing new ones to provide a comprehensive SSA solution, there are a few emerging technologies we expect to see integrated to one extent or another over the next 18-36 months. While some of these are available to a limited degree in some vendor solutions, we expect vendors to implement them more broadly as they mature.

- Machine learning-powered security
- IoT security
- Open platform

Machine learning-powered security: As attacks morph and new devices are onboarded, security administrators cannot adapt security policies fast enough to accommodate changes manually. Organizations will look increasingly to SSA solutions that incorporate ML-powered security capabilities to detect and block sophisticated new threats in real-time with behavior-based, signatureless attack prevention and automated policy recommendations.

IoT security: Unmanaged IoT and operational technology (OT) devices make up more than 30% of the devices on enterprise networks, but they cannot be trusted. IoT devices often ship with vulnerabilities and are open to a wide range of threats, increasing the attack surface with unfettered access to the network. Securing IoT devices requires deploying IoT security sensors and appliances, introducing additional operational overhead and costs. SSA solutions will start incorporating IoT security capabilities to strengthen security for both remote locations and workforces.

Open Platform: As customers adopt multiple cloud-based services from different vendors, integrating them becomes increasingly complex. With limited vendor support for manual configuration and complex scripting, organizations are forced to dedicate precious time and resources to perform the most basic integrations. SSA solutions incorporating an open API platform will enable qualified third-party security and infrastructure services to be integrated easily to satisfy specific customer use cases.

5. Evaluation Metrics

Our assessment of the solution space continues with an exploration of the evaluation metrics used here to evaluate *the impact that a solution might have on an organization*. In many cases, these metrics will be consistent across technology sectors, reflecting fundamental aspects like ease of use, interoperability, and total cost of ownership. For this sector, we will consider the following evaluation metrics:

Ease of Use
The speed and ease with which administrators can implement and operate the service, onboard users, and secure and manage the environment. While some solutions can be deployed in a matter of hours, others take time to plan, configure, and deploy. Many vendors are claiming ease of use through a single, unified management interface, but customers need to be aware that in no way does this reduce the complexity of the underlying infrastructure. Also, some solutions have a sophisticated GUI for adding new users and services, updating policies, and responding to threats, while others rely on a CLI requiring additional skills.

Performance
The impact on end users in terms of network latency and application performance when accessed via the SSA solution. Performance depends on several aspects, including network architecture, edge processing, and the level of integration between products. Some vendors have implemented proprietary protocols, with each packet touched only once for networking and security, increasing performance while mitigating security exposure and vulnerabilities.

Interoperability
The depth and ease with which other solutions can be integrated, including security information and event management (SIEM) platforms. With enterprises challenged to protect an expanding IT perimeter blurred by BYOD, cloud, IoT, and mobile, interoperability between networking and security, and among platforms and products and multiple point products must be seamless. Many vendors—and some analysts—are promoting a “best-of-breed platform” approach to alleviate concerns, so customers should consider the long-term implications before committing to a vendor.

Redundancy
The ability of the solution to ensure 24×7 availability with no single point of failure. With more vendors leveraging public cloud provider networks—including AWS, Azure, and GCP—redundancy becomes almost a moot point until the last mile, where enterprises take on the responsibility for ensuring availability using local service providers and operators. However, with north-south firewalls assumed to be the best protection against cyber threats, generally little attention is given to east-west, server-to-server traffic. Network segmentation—or micro-segmentation—isolates workloads and prevents a compromised system from affecting others.

Visibility, Monitoring, and Auditing
The ability to monitor and enforce policies in a decentralized network is based on observability. Shifting visibility to a software-defined approach with traffic routed via a managed cloud

service—instead of an on-premises appliance—reduces complexity and increases visibility. As an integrated system, SSA requires the monitoring, management, tracking, and escalation of alerts as close as possible to the end user, with the ability to audit activities (of user, device, and resource), thereby supporting regulatory compliance.

Total Cost of Ownership

The three-year TCO of the solution irrespective of acquisition model (subscription or perpetual license). With significant differences in architecture, customers should be aware of the various pricing models for different point products within the SSA solution. While we expect vendor pricing to come under the microscope as new entrants disrupt the market with lower-cost solutions, customers need to understand the full TCO impact based on each vendor's architectural and integration approach to SSA.

Support

The ability of the vendor or service provider to support a globally distributed service. With various products, capabilities, and partners comprising an SSA solution, customers must create a strategic partnership with the primary vendor as the "one-throat-to-choke." While some vendors promote an end-to-end "best-of-breed platform" with global support, we anticipate the emergence of managed services providers prepared to take ownership of multi-vendor SSA solutions, filling the gap for customers wary of vendor lock-in.

Vision and Roadmap

The vendor's vision and roadmap in terms of innovation and execution to meet market demand. In an emerging sector like SSA, vendors must have a clear roadmap and vision—especially when the current strategy is based on slideware. As vendors move to protect their installed base, customers need to do their due diligence, establishing what is real and what is not. Levels of integration vary significantly across vendors, and new acquisitions to fill gaps in their portfolios will prolong the wait for a fully integrated platform.

6. Specific Security Capabilities

Specific security capabilities differentiate one solution from another based on specific functionality required to reduce the attack surface, detect threats, and mitigate risk. These capabilities provide a comprehensive—but not exhaustive—list of functions enterprises and organizations require to take advantage of cloud computing. Indicating each vendor's strengths, this metric also identifies converged platforms that can be tailored to meet unique requirements through in-house development or best-of-breed partnerships. For this sector, we will rate each vendor for the following security capabilities:

Domain Name System Security
Blocks requests to malicious and unwanted destinations before a connection is established. Created for users to connect to services over the internet, domain name system (DNS) is often subject to bad actor exploits. Querying external servers and storing all server names and IP addresses for the domain, DNS servers are targeted by hackers to manipulate caches and exfiltrate data.

Secure Web Gateway
Filters content by category, real-time inspection of inbound files, and advanced sandboxing. Sitting between the user and the internet, a secure web gateway (SWG) analyzes inbound and outbound traffic for malicious content and policy compliance. A cloud-delivered or on-premises network security service, SWG enforces consistent internet security and compliance policies for all users irrespective of location or device.

Firewall-as-a-Service or Next-Gen Firewall-as-a-Service
Logs activity and blocks unwanted traffic using global IP, port, and protocol policies. Firewall-as-a-Service (FWaaS) provides perimeter protection without requiring the deployment of dedicated hardware at each business or user location. A cloud-based service delivering advanced, hyperscale Layer 7 and/or next-generation firewall (NGFW) capabilities, FWaaS includes access controls, intrusion prevention, and threat avoidance.

Cloud Access Security Broker
Monitors application usage and traffic volumes with the ability to allow or block specific applications. An on-premises or cloud-based point of policy enforcement, cloud access security brokers (CASBs) provide visibility and control of cloud-related activity to ensure compliance, governance, and security. Combining various types of policy enforcement, they extend on-premises infrastructure controls to the cloud.

Zero-Trust Network Access
Leverages micro-segmentation and fine-grained perimeter enforcement based on identity, location, and other data to determine trust. Designed to enforce an organization's zero-trust policy, ZTNA provides secure remote access to applications and services based on defined access control policies. Reducing exposure to cyber threats, users are only authorized to connect to applications and services if that particular access is required to fulfill their role.

Endpoint Threat Detection and Response (ETDR)

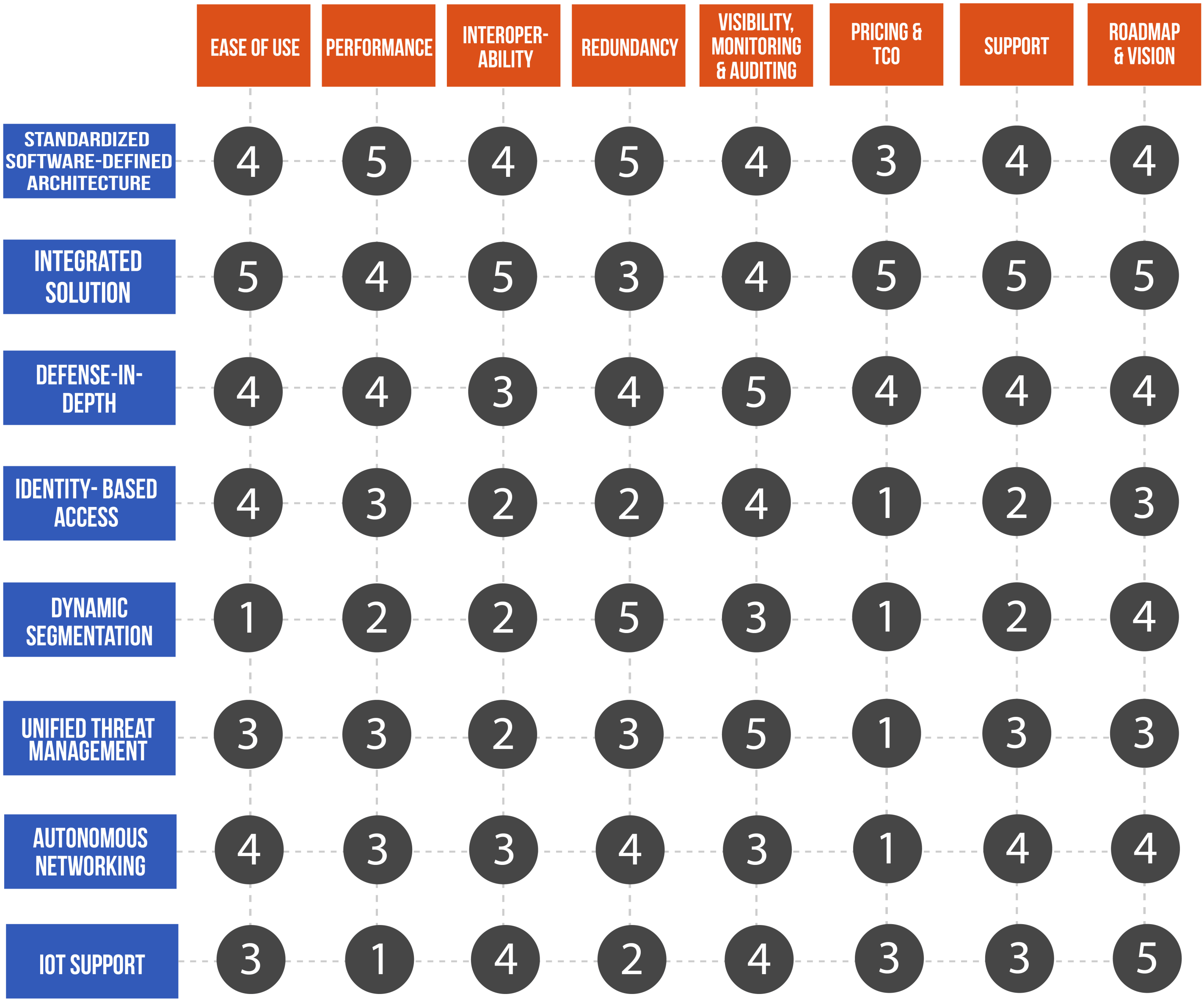
Monitors, collects, and analyzes data from endpoints to identify and eliminate threats in real time. An integrated, layered approach to endpoint protection, ETDR combines the continuous monitoring and collection of endpoint data with real-time rules-based analysis and automated response. ETDR tools provide deep visibility and accelerate threat response, automatically performing remediation based on predefined rules.

Network Threat Detection and Response

Monitors and analyzes network traffic in real time to identify and mitigate malicious activity. Similar to ETDR but with a much larger scope, NDTR solutions monitor network traffic for malicious actors and suspicious behavior, automatically responding to mitigate cyberattacks. NDTR leverages machine learning and behavioral analysis to rate threats faster, accelerating triage and response times.

7. Temporary Report Title

This section provides guidance on how the key criteria impact the evaluation metrics. Table 1 helps the reader understand each feature or capability's impact on each evaluation metric, making it possible to better assess the value a solution may have to an organization.



	EASE OF USE	PERFORMANCE	INTEROPER-ABILITY	REDUNDANCY	VISIBILITY, MONITORING & AUDITING	PRICING & TCO	SUPPORT	ROADMAP & VISION
STANDARDIZED SOFTWARE-DEFINED ARCHITECTURE	4	5	4	5	4	3	4	4
INTEGRATED SOLUTION	5	4	5	3	4	5	5	5
DEFENSE-IN-DEPTH	4	4	3	4	5	4	4	4
IDENTITY- BASED ACCESS	4	3	2	2	4	1	2	3
DYNAMIC SEGMENTATION	1	2	2	5	3	1	2	4
UNIFIED THREAT MANAGEMENT	3	3	2	3	5	1	3	3
AUTONOMOUS NETWORKING	4	3	3	4	3	1	4	4
IOT SUPPORT	3	1	4	2	4	3	3	5

Source: GigaOm 2021

Table 1. Impact of Key Criteria on Evaluation Metrics

Impact on Ease of Use

While a single, seamlessly integrated solution offers the greatest ease of use, we do not expect to see that anytime soon—if ever. However, deploying an SSA solution using a standardized software-defined architecture encompassing autonomous networking, defense-in-depth, identity, and, in the future, behavioral-based access will go a long way toward simplifying operations.

Impact on Performance

With some solutions built from the ground up and others temporarily cobbled together via slideware only, customers should carefully evaluate the impact of SSA architecture on performance. Depending on the vendor's defense-in-depth architecture and level of integration, performance can vary significantly. Leveraging a standardized, software-defined architecture, some vendors claim access to over 150 PoPs providing less than 10ms latency from 80% of the world's population and less than 5ms from all major cloud providers.

Impact on Interoperability

With SSA generally a brownfield deployment, customers need to be aware of any interoperability issues with existing systems, including the level of investment required for integration. While some vendors are consolidating their product portfolios and integrating them as best-of-breed platforms, others provide ultra-secure, high-performance networks with a few key partnerships filling in the gaps. Still others are investing in deep integration with a few carefully selected best-of-breed vendors.

Impact on Redundancy

Many vendors address pathway redundancy through dynamic routing via global PoPs and partnerships with the leading cloud operators. However, customers should be mindful that network redundancy does not equate to security availability. Since the failure of any SSA component interferes with the data flow, each security capability—firewalls and gateways, for example—must include built-in redundancy.

Impact on Visibility, Monitoring and Auditing

Considering the exponential increase in bad actors, the ability to correlate all events across defense-in-depth and unified threat management architectures is critical. With IoT blurring the line between operational technology, and IT and regulatory requirements posing a challenge, SSA solutions must include advanced observability and auditing capabilities with AI-enabled event correlation and alerting. Furthermore, XDR enhances visibility into data across applications, clouds, endpoints, and networks, making it easier to apply analytics and automation for threat hunting and response.

Impact on Pricing and TCO

Nearly all SSA solution pricing is based on an OPEX, per-user subscription model. Despite vendor plans to bundle pricing for SSA solutions—or parts thereof—this is proving to be a relatively slow process. As new, innovative solutions emerge and vendors focus on delivering fully integrated, cloud-native SSA solutions, we expect downward pressure on subscription prices in line with market expectations.

Impact on Support

With support directly proportional to the number of products deployed, integration is key to improving the end-user experience. As vendors focus on "true" network and security convergence and deep integration between point products, the level of support should improve. We also anticipate advances in self-healing, autonomous networks to have a significant impact on reducing support requirements.

Impact on Roadmap & Vision

While some vendors have broad, all-encompassing SSA architectures supporting the “if you want it, we can do it” approach, others are focused on enabling customers with core capabilities complemented by best-of-breed point products. In addition to focusing on key criteria, vendor roadmaps must provide a clear vision for deep integration and the adoption of innovative, next-generation capabilities for achieving network and security convergence.

8. Analyst's Take

As the distributed enterprise becomes the norm, remote users become the *de facto* workforce and cloud (private, public, or hybrid) the default platform. The convergence of cloud-native networking and security gives enterprises what they need to secure their digital assets without compromising performance. Spanning on-premises, hosted, and managed services—all accessed via globally distributed PoPs—converged SSA solutions meet demand by reducing latency, ensuring compliance, and minimizing the attack surface.

Encompassing all of these areas within a single cloud-native solution, secure service access is an emerging sector. We expect the vendor landscape to evolve quickly over the next 18-36 months. While incumbent vendors are repositioning legacy products as SSA platforms or engaging in acquisitions and strategic alliances to fill the gaps in their portfolios, new entrants are emerging with innovative approaches in an increasingly competitive market. Enabling the on-demand deployment of security, SSA delivers the following:

- Globally available converged network-as-a-service (NaaS) and security-as-a-service (SECaaS)
- Comprehensive, end-to-end, distributed protection of resources, services, and users
- Centralized control of services comprising applications, data, devices, and internet access
- Cloud-native agility, availability, scalability, and cost-efficiencies

However, because of the array of approaches and marketecture available, customers need to carefully consider (1) the approach that best meets the needs of their business based on features, functions, and the availability of in-house expertise; and (2) each vendor's ability to deliver it. Depending on your comfort level, the different approaches to be explored include:

- An end-to-end SSA platform from a single vendor
- Multiple best-of-breed point products integrated and delivered by a single provider
- Multiple best-of-breed point products deployed and managed in-house

As you explore SSA, choose a strategy based on your market, deployment model, and use cases. When talking to vendors, verify the level of integration between different point products. Make sure their vision is aligned with yours, and their roadmap includes the features and integration you need.

With the emergence of new entrants and exciting innovations, now is not the time to settle for your incumbent vendor's platform. Allow them to explain their approach and vision, but keep your eyes open for the next big thing in this space.

9 About Chris Grundemann

Chris Grundemann is a passionate, creative technologist and a strong believer in technology's power to aid in the betterment of humankind. He is currently expressing that passion by helping technology businesses grow and by helping any business grow with technology.

Chris has well over a decade of experience as both a network engineer and solution architect designing, building, securing, and operating large IP, Ethernet, and Wireless Ethernet networks. He has direct experience with service provider and enterprise environments, design and implementation projects, for-profit and not-for-profit organizations, big picture strategic thinking and detailed tactical execution, and standards and public policy development bodies. Chris frequently works with C-level executives and senior engineering staff at internet and cloud service providers, media and entertainment companies, financials, healthcare providers, retail businesses, and technology start-ups.

Chris holds eight patents in network technology and is the author of two books, an IETF RFC, a personal weblog, and a multitude of industry papers, articles, and posts. In addition to being the lead research analyst for all networking and security topics at GigaOm, he is the co-host of Utilizing AI, the Enterprise AI podcast. He is also a cofounder and Vice President of IX-Denver and Chair of the Open-IX Marketing committee. Chris has given presentations in 34 countries on 5 continents and is often sought out to speak at conferences, NOGs, and NOFs the world over.

Currently based in West Texas, Chris can be reached via Twitter.

10 About Ivan McPhee

Formerly an enterprise architect and management consultant focused on accelerating time-to-value by implementing emerging technologies and cost optimization strategies, Ivan has over 20 years' experience working with some of the world's leading Fortune 500 high-tech companies crafting strategy, positioning, messaging, and premium content. His client list includes 3D Systems, Accenture, Aruba, AWS, Bespin Global, Capgemini, CSC, Citrix, DXC Technology, Fujitsu, HP, HPE, Infosys, Innso, Intel, Intelligent Waves, Kalray, Microsoft, Oracle, Palette Software, Red Hat, Region Authority Corp, SafetyCulture, SAP, SentinelOne, SUSE, TE Connectivity, and VMware.

An avid researcher with a wide breadth of international expertise and experience, Ivan works closely with technology startups and enterprises across the world to help transform and position great ideas to drive engagement and increase revenue.

11. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

12. Copyright