Predicts 2022: Connecting the Digital Enterprise

Published 2 December 2021 - ID G00757926 - 15 min read
By Analyst(s): Andrew Lerner, John Watts, Joe Skorupa

Initiatives: Cloud and Edge Infrastructure

For digital enterprises, the percentage of network traffic that rides the physical corporate network is decreasing. This is dramatically shifting traffic patterns, which requires I&O leaders to explore new approaches to provide secure network connectivity.

Overview

Key Findings

- The combination of work from anywhere (WFA) and cloud-based services means that enterprise users increasingly connect to their applications without ever physically traversing corporate-owned network devices.

- Perimeter-based approaches to securing anywhere, anytime access has resulted in a patchwork of vendors, policies and consoles, creating complexity for security administrators and users.

- Secure access service edge (SASE) converges networking and network security, and aligns with the requirements of digital enterprises. There is both high client interest (demand) and vendor investment/hype (supply) driving adoption.

Recommendations

I&O leaders responsible for cloud and edge infrastructure should:

- Enable flexibility to address changing needs (and a dynamic vendor landscape) by making shorter-term one- to three-year investments for zero trust network access (ZTNA), SASE and cloud networking offerings.

- Optimize cloud networking software investments by preferring lightweight, “cloud aware” products that are offered via consumption-based pricing, with robust and well-documented APIs.

- Favor vendors that support open interoperable networking and security policy definitions and distribution by using standard tokens and payload formats.
Strategic Planning Assumptions

By 2025, 35% of companies that use multiple public cloud providers will use a single network stack, an increase of more than 10 times from 2021.

By 2025, 40% of enterprises will adopt software-defined WAN (SD-WAN) and cloud-delivered secure web gateway (SWG) from the same vendor, up from less than 5% in August 2021.

By year-end 2024, 10% of enterprises will replace network access control (NAC) and/or embedded switching security features with ZTNA on corporate-owned campus LANs, up from near 0% in 2021.

By 2025, 40% of newly written composite applications will use standard tokens to communicate security and network requirements.
Analysis

What You Need to Know

The predictions in this research relate to increasing cloud adoption and the need to drive efficient ways to deliver networking and security for digital enterprises. I&O leaders responsible for networking must aim to deliver the right amount of networking, at the right time and at the right cost to support their digital businesses. This is in contrast to many long-standing network practices of building out “rock solid” infrastructure to last five to 10 years, with security at the perimeter. In order to support the dynamic needs of the digital enterprise, network security must be better “baked in” (i.e., integrated) into network architectures versus being a separate silo or “bolt on.” This is one of the main reasons we predict that enterprises will increase their investments in SASE dramatically over the next three years (see Figure 1).

Figure 1: SASE Revenue Forecast

**SASE Forecast, 2019-2024**

Source: Gartner

Note: Five-Year Market Growth = $9.045 Billion (CAGR 41.8%)

Gartner
Strategic Planning Assumptions

Strategic Planning Assumption: By 2025, 40% of enterprises will adopt SD-WAN and cloud-delivered SWG from the same vendor, up from less than 5% in August 2021.

Analysis by: Andrew Lerner

Key Findings:

- Most client inquiries discussing SD-WAN now also include discussion of secure web gateway.

- Organizations with a majority of applications in the public cloud and/or SaaS increasingly prefer using cloud-delivered security, instead of backhauling traffic or deploying local appliances.

- Most SD-WAN vendors are building out broader security offerings to include SWG, including Cisco, Palo Alto Networks, Cato, Citrix, Fortinet, Versa and VMware.

Market Implications:

While many organizations are comfortable integrating their SD-WAN vendor with a separate SWG vendor such as Zscaler, there is a strong desire to source the solution from a single provider. The rationale is that a single supplier will better enable integrated management, policy, visibility, commercial support and billing between SWG and SD-WAN. The combination of SD-WAN with cloud-based SWG is now available from several established SD-WAN vendors including Versa, Cisco, Palo Alto, Citrix and Fortinet. In practice, they're not all mature and/or fully integrated today, but we expect enterprise interest (demand) and vendor investment (supply) to drive dramatic increase in adoption of SASE implementations.

Recommendations:

- Involve both networking and security teams when selecting or refreshing SD-WAN and SWG solutions. Avoid making strategic SD-WAN or SWG decisions in isolation.

- Aim to consolidate SD-WAN and SWG offerings to a single vendor, a managed service provider (MSP), or via vendors that have built deep turnkey integration (which entails embedded automation, shared policy and shared visibility between management platforms).
Related Research:

2021 Strategic Roadmap for SASE Convergence

Critical Capabilities for WAN Edge Infrastructure

Strategic Planning Assumption: By year-end 2024, 10% of enterprises will replace NAC and/or embedded switching security features with ZTNA on corporate-owned campus LANs, up from near 0% in 2021.

Analysis by: John Watts

Key Findings:

- Today, most enterprises use different products to secure access in their campus network (often NAC or switching features) versus remote users (often VPN or ZTNA).

- A small (but growing) number of forward-leaning enterprises are looking to use the same security product for all users, regardless of whether they’re working in a corporate office or at home. This was also attempted by advanced clients to varying degrees of success in the early 2000s using VPN technology.

- Today, most ZTNA vendors target remote access/VPN replacements with cloud-delivered ZTNA services. Some ZTNA vendors support LAN-based use cases for enterprises, but adoption is limited.

- We believe demand will explode for ZTNA on campus when offices fully reopen and as more commercial offerings emerge.

- Existing security for campus, including software from switching vendors and NAC products, often does not offer the granularity of user-to-application segmentation that ZTNA products provide. Further, these existing products can be prohibitively expensive and complex, requiring lengthy deployments.

- Zero trust strategies and the hybrid workforce demand user-to-application segmentation regardless of physical location to reduce the risk of malware propagating across the network.

Market Implications:
Many organizations are pursuing zero trust strategies to increase security posture. A common starting point is implementing ZTNA to replace traditional VPNs. As these enterprises achieve success implementing ZTNA, the question a few forward-leaning organizations are now asking is, “Can we extend this same security model to the campus/corporate LAN?”

Local Gateways and Hostile Networks

Most ZTNA operates as cloud services, sending application authentication and authorization requests to public cloud points of presence (POPs). This introduces latency for local application access, which is undesirable as it can decrease app availability and performance (e.g., user-to-user voice calls would need to be routed to a POP, reliant on an internet connection), and increase internet bandwidth usage. However, local gateways can address this issue. Vendors such as Zscaler, Appgate and Fortinet offer an option for local security gateways, typically in the form of a virtual appliance to enable ZTNA closer to the users and applications hosted on-premises. Once implemented, more granular security and segmentation result in significant security benefits, but require a shift in how these networks are designed and managed. In a zero trust model, all endpoint networks are treated as hostile networks. In essence, the enterprise network team deploys switching and Wi-Fi to provide basic IP connectivity, but without embedded security functionality. It simplifies the switching and Wi-Fi stack, as things like profiling, filtering and end-to-end segmentation are no longer necessary in the network switching/management feature sets.

Challenges

Prior to NAC being widely available, some organizations tried a similar approach using VPN concentrators, but found issues with end-user experience and scale. ZTNA promises to improve on these issues, but may need to overcome a number of other obstacles. These include the need to support and secure headless Internet of Things (IoT) and OT devices such as printers, security cameras, building controls, sensors and other devices on the LAN. However, in environments where the bulk of connectivity is by traditional endpoints, which can support a ZTNA agent, it is feasible. Moving to ZTNA for all application access security policies promises to simplify security, reduce risk and lower costs. Perhaps most importantly, users will have the same experience for getting “on net” regardless of the network to which they are connected.

Recommendations:
Test the feasibility of replacing existing NAC or LAN-based switching security via a functional pilot of ZTNA on the campus or branch network if you have already deployed ZTNA for remote users. This is particularly important before making strategic NAC or switching investments.

Collaborate with endpoint administrators to move all internal IT management systems, such as endpoint management, patching, voice over IP (VoIP) services and IoT device management (e.g., printer management and print queues) to the cloud.

Partner with security teams to choose a ZTNA provider that offers paths to remote and on-premises access controls for the extended workforce (e.g., employees, contractors, vendors and suppliers) using both agent and agentless methods if you do not already have ZTNA.

Related Research:

Market Guide for Zero Trust Network Access

Market Guide for Network Access Control

Magic Quadrant for WAN Edge Infrastructure

Strategic Planning Assumption: By 2025, 40% of newly written composite applications will use tokens to communicate security and network requirements.

Analysis by: Joe Skorupa

Key Findings:

- Adoption of composite applications is being fueled by the need for greater business agility and shorter time to value.
- Composite applications consume APIs from multiple internal and external sources.
- A standard, multivendor interoperable mechanism to describe and enforce secure end-to-end connectivity between application components is needed to ensure performance and compliance.
Market Implications:

Composite applications, built for digital transformation, time to value and adaptability, are built with in-house and third-party business components, typically APIs. The components these applications use are hosted in geographically distributed cloud and data centers often using the internet as network transport. The shift toward the use of third-party components will make it difficult to ensure consistent network and network security requirements between the components. Additionally, communications between components will traverse a mix of private and public networks that will use products from multiple vendors. Intermediaries such as API gateways and service mesh play an important role by issuing and validating tokens, which can extend to tokens used in a cross-mesh and/or heterogeneous API gateway environment.

Some cloud providers may push a walled garden of partners to deliver interoperability, but this approach will significantly limit software development capabilities. As a result, most organizations will leverage many suppliers, which requires an interoperable multivendor solution.

Recommendations:

- Work with application teams to avoid hard-coding network and security policies into applications.
- Adopt a common policy repository to separate policy definition and storage from enforcement.
- Favor vendors that support open interoperable networking and security policy definitions and distribution via standard tokens and payload.
- Use a cross-functional team including networking, security, application owners, and application security and governance personnel to determine the appropriate governance policies, as well as user requirements for performance, availability and cost.
Related Research:

Emerging Technologies: Applying SASE’s Architectural Model to Secure Distributed Composite Apps

Innovation Insight for Comprehensive Secure Connectivity for Composite Applications

Replay Prediction

*The replay prediction is a prediction from a previously published report that is so significant that it is being republished here.*

Strategic Planning Assumption: By 2025, 35% of companies that use multiple public cloud providers will use a single network stack, an increase of more than 10 times from 2021.

Analysis by: Andrew Lerner, Joe Skorupa

Key Findings:

- More than 75% of organizations use multiple public cloud services today, and have plans to expand.
- The native networking capabilities of public cloud providers are insufficient for some enterprises, particularly when scaling beyond a few dozen virtual private clouds (VPCs)/virtual networks (V Nets).
- Networking capabilities vary widely across public cloud providers, which creates management challenges, particularly in multicloud deployments.
- Client interest in public cloud networking and multicloud networking has increased dramatically in the past 15 months.

Market Implications:
Many organizations are finding they need networking functionality within a public cloud provider that is not natively offered and/or they need consistent networking across multiple public cloud environments. Virtual routers and virtual appliances offered by established networking vendors (with large on-premises installed bases) often don’t meet the requirements of cloud and DevOps teams, particularly around programmability, cloud integration or licensing. As a result, a new market has emerged to address “inside the cloud” and multicloud networking challenges.

This market — cloud networking software — enables the design, deployment and operation of a network within multiple cloud environments. These products enable consistent networking policy, network security, governance and network visibility across multiple cloud environments via a single point of management. There is ample investment and innovation occurring in this market, led by venture-funded startups such as Aviatrix, Alkira and Prosimo. We expect the market to be dynamic, with new entrants and a high level of change and innovation.

Recommendations:

- Exploit the benefits of public cloud providers by preferring their native capabilities when starting out or when there is a single public cloud provider strategy.
- Enable advanced networking features and/or network consistency within multicloud deployments by using third-party cloud networking software.
- Optimize cloud networking software investments by preferring lightweight, “cloud aware” products that are offered via consumption-based pricing, with robust and well-documented APIs.
- Enable flexibility to address changing needs by making short-term investments with a one- to three-year time horizon. This is a departure from typical network planning cycles, which are often three to five years.

Related Research:

- Market Guide for Cloud Networking Software
- Technology Insight for Multicloud Networking
A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2019 Prediction — By year-end 2021, network teams will spend three times more time working in public cloud infrastructure than they do today.

In May 2019, Gartner estimated that network teams were spending 5% to 10% of their time focused inside the public cloud. Seven months later at the Gartner IT Infrastructure, Operations & Cloud Strategies Conference in North America in December 2019, audience polling indicated that 8.4% of network teams’ time was spent inside the public cloud.

Since 2019, end-user interest in this topic has skyrocketed, including:

- The amount of Gartner end-user calls on cloud networking has increased by more than five times since July 2019.
- Searches on gartner.com on the topic of cloud networking have increased by more than two times since as recently as November 2020 through September 2021.

As enterprise network teams spent more time in the public cloud, demand for better networking software became apparent. As a result, there has been more than $350 million in venture funding pumped into public cloud networking startups since October 2020 including Aviatrix ($275 million in February 2021 and September 2021), Alkira ($54 million in October 2020) and Prosimo ($25 million in April 2021).

As of 1 December 2021, we now estimate that network teams spend 15% to 30% of their time on networking inside the public cloud. (See Best Networking Practices Inside the Public Cloud.)

Missed: 2017 Prediction — By 2020, only 30% of network operations teams will use the command line interface (CLI) as their primary interface, down from 85% at year-end 2016.

In early 2017, we estimated that 85% of network teams identified the CLI as their primary network operations interface. At that time, most enterprise switches and routers were operated via CLI. Since this time, several drivers reduced reliance on traditional CLI, including:
- SD-WAN appliances (which are not typically operated via CLI) have replaced routers at more than 25,000 enterprises.

- The percentage of workloads in the public cloud has doubled since 2017, and public cloud networks are much less likely to be operated via CLI.

- Organizations have incrementally increased adoption of data center fabric managers and commercial automation tools for switching management (compared to box-by-box CLI).

However, as of December 2021, we estimate that more than half of enterprises still associate the CLI as their primary operational network interface. This falls short of the prediction of only 30% by 2020. Thus, this prediction was wrong, although directionally correct. (See Market Guide for Network Automation and Orchestration Tools.)

### Acronym Key and Glossary Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>MSP</td>
<td>Managed service provider</td>
</tr>
<tr>
<td>NAC</td>
<td>Network access control</td>
</tr>
<tr>
<td>POP</td>
<td>Point of presence</td>
</tr>
<tr>
<td>SASE</td>
<td>Secure access service edge</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Software-defined wide-area network</td>
</tr>
<tr>
<td>SWG</td>
<td>Secure web gateway</td>
</tr>
<tr>
<td>WFA</td>
<td>Work from anywhere</td>
</tr>
<tr>
<td>ZTNA</td>
<td>Zero trust network access</td>
</tr>
</tbody>
</table>

### Evidence

Gartner’s Public Cloud Networking Poll (2020) was conducted online from 28 September through 8 October 2020 with 202 members of Gartner’s ITL Research Circle — a Gartner-managed panel of IT leaders. Participants are IT leaders focused on enterprise architecture and/or infrastructure and operations from a range of regions, industries and revenue sizes. The results of this study are representative of the respondent base and not necessarily the market as a whole.
Gartner’s 2020 Cloud End-User Buying Behavior Study was conducted to understand how technology leaders approach buying, renewing and using cloud technology. The survey was conducted online in July and August 2020 with respondents from the U.S., Canada, the U.K., Germany, Australia and India. The study surveyed 850 respondents, of whom 724 respondents reported that their organization was using the public cloud, hybrid cloud or multicloud infrastructure. Of these 724 respondents, 24% use one provider only, 13% use multiple providers with no primary and 63% use multiple providers with one as the primary provider. This study was developed by the Gartner Primary Research Team. Results of this study do not represent global findings, or the market as a whole, but are a simple average of results for the targeted countries covered in this survey.

Gartner analysts have had more than 10,000 interactions on the topic of networking with clients from 1 January 2021 through 14 September 2021, including more than 2,000 on SASE, more than 500 on SD-WAN and more than 100 on network automation.

Audience Polling at Gartner’s Data Center and Cloud Summit conferences 2017 (n = 64), 2018 (n = 43) and 2019 (n = 97).

Recommended by the Authors

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

Market Guide for Cloud Networking Software

2021 Strategic Roadmap for SASE Convergence