Network Sourcing Decision Matrix Benchmark
Final Report

Prepared for Shared Services Canada (SSC)
04 February 2021 330068737

Gartner®

SSC requested Gartner's assistance to benchmark its network strategy, review current and past network sourcing use cases, and develop a repeatable sourcing decision framework for future network procurements modelled on best practices

Our Understanding of the Current Situation

- SSC currently selects vendor(s) to support the installation of Data Centre Networks (DCN) at SSC's data centres.
- As part of future vendor selection, SSC needs to determine critical decision criteria regarding the risks and value associated with data center network conditions.
- SSC requires a review of network requirements to establish conditions when continuing with an incumbent vendor for a follow-on procurement is the only viable option, and conditions when an open competition for procurement is possible.

Gartner's Approach

- SSC sought the support of an independent and objective partner to create a Data Centre Network and Security sourcing decision matrix through the following steps:
  - Assess/benchmark 3-4 specific examples of network and security procurements as use cases
  - Engage in workshops with stakeholders (including procurement, business, operations, project delivery) to establish optimal business, technical and procurement outcomes, constraints, etc.
  - Leverage Gartner benchmark data, best practices/Analyst insights
- The outcome of this engagement will include the following:
  - A benchmark review of SSC's existing **Network & Sourcing Strategy**
  - An analysis of past and current **Network sourcing use cases**
  - A **Decision Guide** for future network procurements based on identified business, technical, security and procurement risks and imperatives, and informed by SSC's Network & Security Strategy, studied use cases and Gartner benchmark data and industry best practices
  - **Recommendations** on potential approaches to help balance business, technical, security and procurement risks in order to optimize overall outcome
  - Executive briefing presentation

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

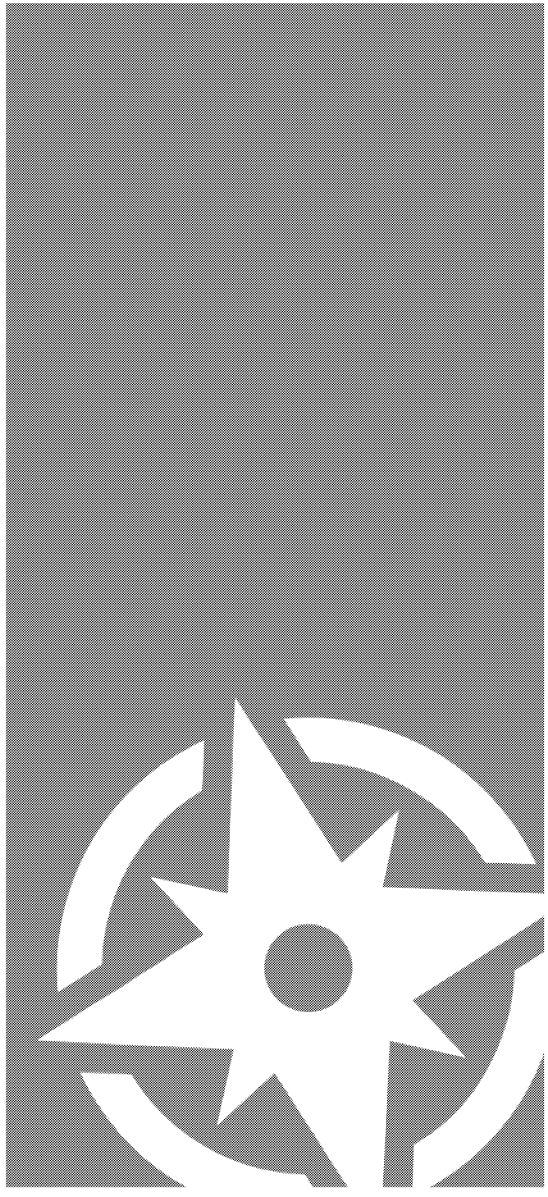
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix**



Gartner

Executive Summary — Network Strategy Review

The Request

Review SSC's Network & Security Strategy draft documentation to ensure alignment with best practices and that a descriptive future state was well documented so that it could be shared with the Industry

Gartner's approach

- Benchmark SSC's Network Strategy against Gartner's published best practices
- Conduct an in-depth review and analysis of the document to assess its effectiveness in communicating the Network Strategy
- Provide recommendations toward improving the document

Key Takeaways

- Gartner has identified that the **objectives** outlined in the Network Strategy document are **aligned** with other governments objectives and goals but that the **links** to current context, business strategy and other IT strategies **could be strengthened**
- SSC has identified upcoming **technologies that align with current Gartner research** however this document **does not provide sufficient guidance** to elaborate a plan on how these solutions will be deployed in relation to other service line strategies
- SSC's strategy document structure, based on the three "pillars" creates overlapping repetitive text and gaps that **could be avoided by following an industry standard strategy framework**

Gartner

Executive Summary — Network Sourcing Decision Aid

The Request

Gartner was tasked with developing a Network Sourcing Decision Matrix Benchmark for future network equipment sourcing decisions

Gartner's approach

- Conduct stakeholder workshops to understand the goals and constraints of Network Sourcing stakeholders
- Utilize Gartner's published research to build a decision aid that aligns with industry best practices
- Provide vendor landscape insight based on Gartner Research

Key Takeaways

- Gartner has created a **Network Sourcing Decision Aid** to help with future sourcing of Network related initiatives
- In all three Network areas (LAN, WAN, DCN), Gartner recommended the establishment **of technology standards through open, competitive procurements** and provided boundaries for these standards that encourage competition while keeping operational burden in check
- Gartner proposed two DCN technology standards and a single WAN standard across its EDCs, and a LAN standard for each facility
- For existing environments where there is an established vendor (de facto standard) but not an established technology standard, Gartner recommended that **OEM-specific procurement exceptions** be reviewed in cases when the upgrade is urgent and necessary

Gartner

Executive Summary — Use Case Analysis

The Request

Gartner was provided 3 Use Cases to find insights into current LAN, WAN, and DCN sourcing decisions at SSC

1) EDC [redacted] – WAN upgrade and DCN spine

2) CCM/DCSL Data Centre [redacted] — Workload Migration to EDC

3) Lester B. Pearson- Building LAN, Phase 1

Gartner's approach

- Map networking sourcing stakeholders goals and constraints
- Conduct an in-depth benchmark review and analysis of the use cases
- Utilize and validate the Network Sourcing Decision aid that Gartner developed for SSC leveraging best practices
- Assess business impact of following decision aid for in-flight projects
- Document findings

Key Takeaways

- Gartner developed a network sourcing decision aid for use cases and future network sourcing based on identified stakeholder's goals and constraints
- Gartner assessed the use of the decision aid against the three use cases; while **use cases 1 and 3 fully aligned** with the network sourcing decision aid, **use case 2** (CCM) only **partially aligned**, with the sourcing decision for DCN components deviating from guidance
- In consultation with stakeholders, Gartner documented the **business impacts** that would arise from following the network sourcing decision aid for DCN components in use case 2, thereby **providing decision-making insight** to SSC leadership to determine the procurement path

Gartner

NOTES : 2021-03-03 GagnonP: Releasing information about modification to any datacenter could jeopardize security.

Short-term Recommendations

1. Update and enhance the Network Strategy to include key missing elements so that it can be used as a reference for short/midterm planning as well as a communication tool.
2. Formalize the adoption of a sourcing decision approach for Network equipment procurement, including technology domains and boundaries for technology standards. Consider expanding the practice to other technology areas.
3. Create review mechanisms and approval processes for deviating from the established sourcing decision approach. This process should include consultations with relevant stakeholders and documentation of constraints as well as business impacts that led to the decision.

Documenting, formalizing and communicating SSC's network strategy will foster accountability and transparency

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

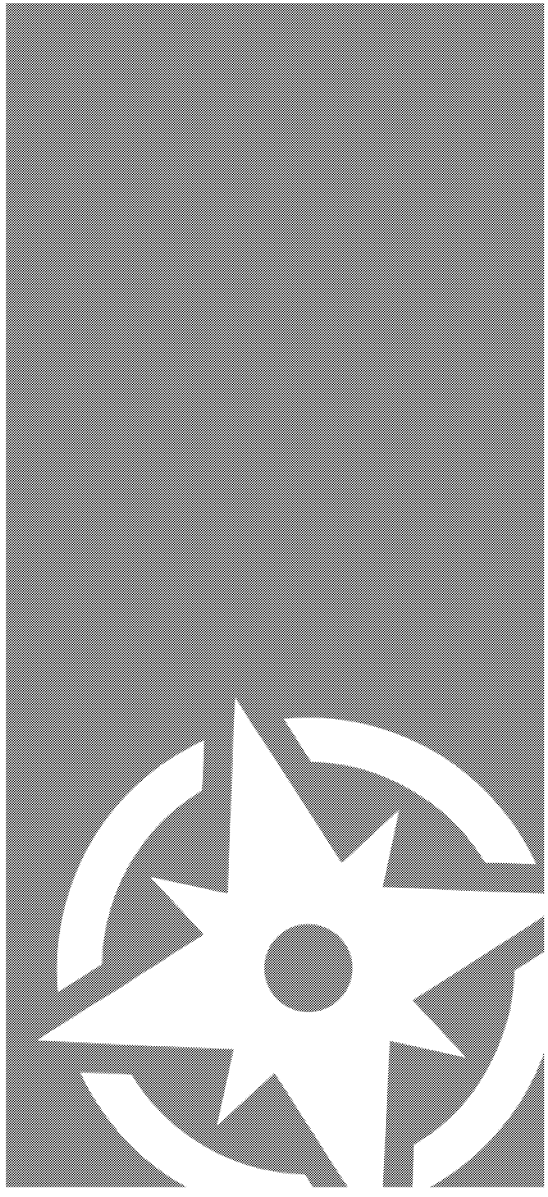
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix**

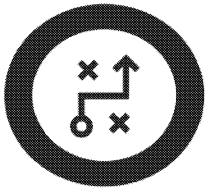


Gartner

Gartner Research has identified key components of a successful Network Strategy

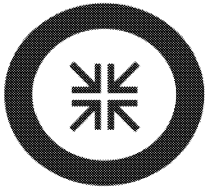
Strategic Network planning is essential to meet the challenges associated with initiatives like cloud, mobility, sourcing, and IoT while maintaining security and reducing costs

Effective Network strategies have several core foundational factors



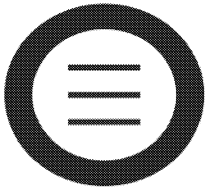
Business Strategy

Use business strategy — not technology — to drive network strategy



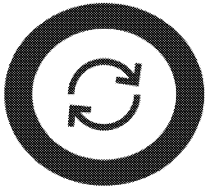
Inner-workings of strategy

Build a network strategy that includes current state, future state, gap analysis and action plan



Prioritization/Risks

Prioritize networking projects based on investment required, criticality to business success and risk



Update strategy yearly

Keep the network strategy updated on a yearly basis, and/or as business priorities change

Gartner

Gartner's review aligns with current Gartner Research and past dialogue with SSC team members over recent years

Gartner has performed the following actions and has provided general insights and recommendations on the following slides

Review of "SSC Network and Security Strategy"

- Originally drafted in May 2020
- Version: 1.8, updated November 2020, with inputs from SSC, CSE, CCCS, and TBS

Review of SSC Current Initiatives and Future Activities

- Gartner highlighted the need to integrate Current Initiates and Future Activities into one coherent structure

Identified Potential improvements to text

- Gartner highlighted potential improvements that can be made to the Strategy document text to communicate SSC's needs more effectively

Review SSC Network Modernization Discussion

- This discussion document should be better linked to the SSC Network and Security Strategy

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

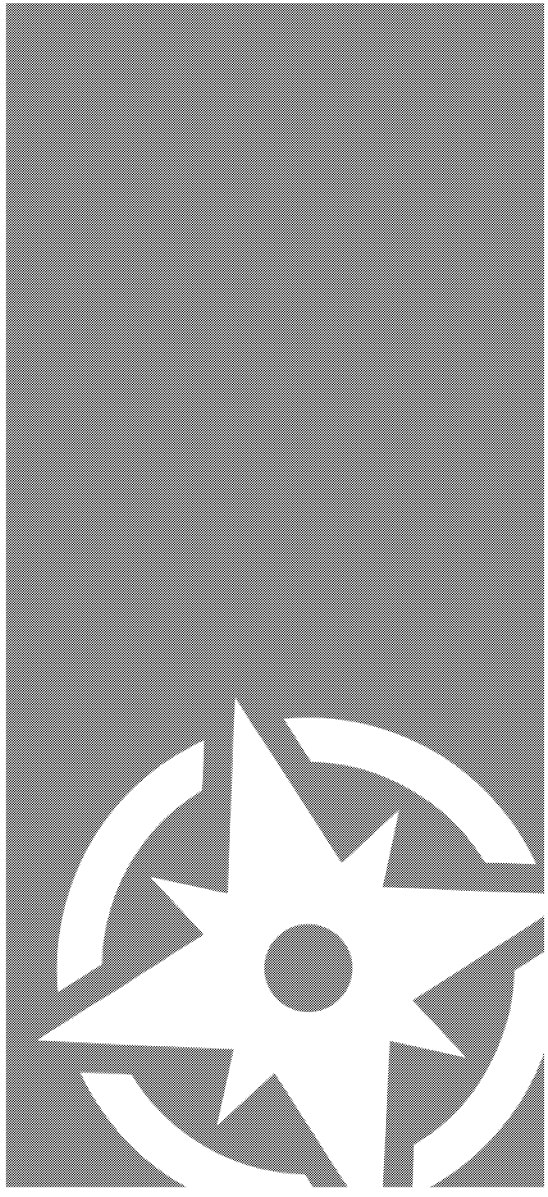
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix**



Gartner

Gartner compared SSC Network and Security Strategy to Gartner Research best practices

- The SSC Network and Security Strategy (SSC Strategy) is designed to improve end-user experience while protecting government information
  - Gartner sees that SSC objectives are aligned with other governments and large enterprise clients

- The SSC Strategy reviews the advantages of emerging network and security solutions
  - The emerging solutions discussed in the SSC Strategy are aligned with technologies discussed by Gartner Research
  - The SSC Strategy does not provide a full plan on how these solutions would be deployed

- SSC has designed a new strategy document structure of "Pillars" and "Rows" to communicate to its stakeholders.
  - Gartner believes that this new strategy document structure creates overlapping repetitive text, including references to Zero Trust in both Towers and Rows, and creates gaps, including gaps in reference to Service Management. (Specific examples are included in this section)
  - Gartner recommends that the SSC Strategy should follow an industry-standard strategy documentation approach.* Current State and Future State should be holistic and not siloed into "Pillars" (Gartner recommended structure on Page 36)
  - The SSC Strategy Executive Summary should provide an outline of all components of the strategy including direct reference to current state, future state, and planned Activities.

In the following slides, Gartner comments on how SSC Network Strategies align with Gartner Research

Gartner

*See notes section for further details

Gartner compared SSC Network Strategy Document to the Gartner Research

Pillar 1 Connectivity	SSC Network and Security Strategy	Gartner Research + Comments
Intra Building Network	▪ The GC has adopted a wireless-first strategy for end user and IoT devices. ▪ In the medium-term, devices will continue to rely on Wi-Fi and cellular (3G/4G) connectivity as 5G reaches maturity. ▪ Ability to confidently identify devices and users accessing GC Network resources.	▪ Aligns with Gartner Research — In "Top 10 Trends for the Communications Service Provider Industry in 2021, published 9 March 2021. ▪ Gartner identifies "5G as a platform for Enterprise Solutions." ▪ SSC activities for wireless are not defined.
Inter Building Network	▪ The dependence on traditional building infrastructure will lessen. ▪ Inter-building backbone services will likely remain the same within the National Capital Region.	▪ Specific initiatives for inter-building networks are not included in this section.
Data Centre Networks (Software Defined Network)	▪ Data centre networks will move to SDN to enable rapid provisioning of new network services and changes. ▪ SD-WAN will act as the new transport layer for internet access at small — medium size data centres. ▪ AIOps will automate changes for threat remediation, performance management.	▪ Gartner sees SDN as a generic vendor marketing term that has lost any specific meaning. ▪ Gartner recommends that SSC define its specific expectations of SDN value, and align the strategy to those requirements. ▪ Gartner recommends a Solution Path to AIOps in Appendix – Gartner Research
External Network Connectivity	▪ Protected B data will be accessed leveraging the Secure Cloud Enablement for Defense (SCED) connectivity solution. ▪ More clients leverage SD-WAN solutions to enable access to internet and Cloud SaaS services. ▪ Direct access to SaaS applications such as Microsoft O365, without VPN, will be enacted to optimize the traffic and reduce the latency, ultimately enhancing user experience.	▪ Gartner notes that SSC has defined a specific initiative (SCED) to support secure access to cloud services. ▪ SSC needs to build an integrated internet access strategy to access public cloud services, including use of SD-WAN and SASE solutions.

Gartner

Gartner compared SSC Network Strategy Document to the Gartner Research

Pillar 2 Identity and Access Control	SSC Network and Security Strategy	Gartner Research + Comments
Virtual Perimeter	▪ Move from a traditional perimeter security approach to a "virtual perimeter"; relying on the concept of "Zero Trust" (ZT) and micro-segmentation. ▪ Traditional perimeter security may still serve as the first line of defense, but both device and user will be continuously verified, authenticated and authorized.	▪ Aligns with Gartner Research on the deployment of Zero Trust Architecture. ▪ SSC should set-out some expectations for the deployment of ZTA, e.g., "Within X years…". ▪ Gartner Research summary of Zero Trust in Appendix
Active Directory	▪ Re-establish control over a compromised Active Directory environment by maintaining a separate bastion environment that is known to be unaffected by malicious attacks.	▪ Aligns with best practice
Privileged Accounts	▪ Isolate the use of privileged accounts to reduce the risk of those credentials being stolen.	▪ Aligns with best practice
Secrets Management	▪ A Secrets Management service must be provided to enable automation and orchestration and be tightly coupled with access control mechanisms.	▪ Only reference to Secrets Management in Strategy
Smart Risk Engines	▪ Smart" risk engines will result in additional capacity requirements to enable collection and processing of end user and device metadata.	▪ Gartner defines the Access Management market as technologies that use access control engines. (identity providers, authorization servers, policy servers, etc.) to provide core capabilities.
Data Management	▪ Establish proper data governance, master data management and data leakage protections.	▪ Data governance has become more challenging as data straddles edge, on-premises and multiple cloud environments. Also, new regulations are driving demand for effective data governance.

Gartner

Gartner compared SSC Network Strategy Document to the Gartner Research

Pillar 3 Monitoring	SSC Network & Security Strategy	Gartner Research + Comments
Monitoring Tools	▪ SSC will need to move from stand-alone monitoring tools and processes to an integrated set of technologies that is supported by a centralized data repository here on in referred to as "SSC Data Lake", and provides improved visibility.	▪ SSC should define gaps in current tools. ▪ SSC Strategy is not specific on what types of monitoring tools that it plans to deploy.
Artificial Intelligence (AI)	▪ SSC will need to implement AI, automation, and orchestration to improve the efficiency with which it secures the IT infrastructure. There is an initiative underway in SSC to address AI for Operations ("AIOps").	▪ AI promises to revolutionize IT operations, but most teams struggle to see through the hype to pragmatic use cases and the right tools. I&O technical professionals should use this Solution Path to clarify their approach to AIOps adoption by layering AIOps tools, platforms and features.
Data Centre Consolidation	▪ Data centre consolidation will be key in facilitating the consolidation of monitoring tools and the SSC Data Lake. This will include the establishment of a centralized monitoring solution within Enterprise Data Centres (EDCs) that will form the foundation of a centralized monitoring capability for the GC.	▪ SSC should explain the dependency between Data Centre Consolidation and Monitoring tools and Data Lakes.
Next Generation SIEM	▪ Maturing the SIEM capability will be critical to gaining situational awareness across the GC environments and enabling more rapid and coordinated incident response capabilities. This should include an integrated, next generation SIEM solution.	▪ SSC should provide its definition of "next generation SIEM solution", including reference to the use of Data Lakes.

Gartner

Gartner compared SSC Network Strategy Document to the Gartner Research

Provisioning	SSC Network & Security Strategy	Gartner Research + Comments
SDN/SDI	▪ Implement Software-Defined Networking and Infrastructure (SDN/SDI), integrated with on-premises network and security platforms.	▪ ***While true SDN solutions have not had any significant market adoption***, the development of SDN and the threat to established market players had a profound, positive effect on subsequent market developments. ▪ In 2021, we are seeing SDI move to vendor-specific silo technology (not heterogeneous service drive) and, hence, obsolete as multivendor interoperable standards. **Note: Detailed in following slide**
Hyper-converged infrastructure	▪ Implement SDN/SDI, integrated with on-premises infrastructure, such as hyper-converged infrastructure.	▪ This is the only reference to "hyper-converged infrastructure" in the Strategy. ▪ SSC should add context, and reference to actions.
Cloud Provisioning	▪ Off-premises Cloud computing will enable rapid provisioning of network, security and compute services.	▪ SSC should explain how they will benefit from "Cloud Provisioning".
Operating Model	▪ SSC will need to undertake a fundamental change to its operating model as it moves to Cloud and new network and security capabilities. This will require changes in the: Organizational structure of SSC, Skills required, Operational processes, Vendor management capabilities.	▪ SSC Strategy does not describe a new operating model. ▪ SSC has not identified any initiative to change its organization structure.
New Roles	▪ Software-Defined Architect ▪ ZTA Architect ▪ Vendor Management ▪ Additional partner relationship management focus in all roles	▪ SSC should define roles in broader terms, including Network Architecture and Security Architecture. ▪ SSC Strategy should address how it will improve its partner and vendor collaboration.

Gartner

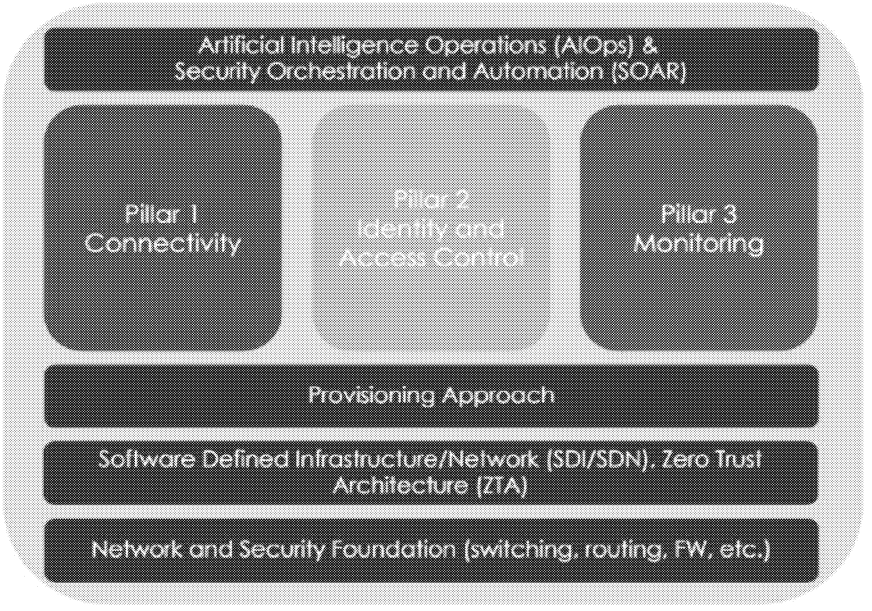
Gartner compared SSC Network Strategy Document to the Gartner Research

	SSC Network & Security Strategy	Gartner Research + Comments
SDN	▪ Implementation of enabling technologies, such as Software-Defined Networking and Infrastructure (SDN/SDI), integrated with on-premises network and security platforms	▪ While SDN is clearly obsolete in the enterprise market there are still many organizations that site SDN as a cornerstone of their future strategy and architecture. What is critical for enterprises is to understand what they are trying to accomplish when they think "SDN." We recommend the following: ▪ Don't get caught up in the hype and vendor claims that commercial products are SDN or engage in any discussions or planning to deploy SDN. SDN is not the answer to any enterprise networking challenge today. ▪ Focus on the desired outcomes you are trying to achieve such as increased automation, virtual segmentation, external orchestration, control and programmability of the network or decoupling physical hardware from software switch operating systems. ▪ Select an operational/automation framework first — then decide on networking vendors and products. Decoupled hardware and software and independent network overlays provide a way of establishing long-term operational models that are independent of underlying hardware if that is a desired outcome. ▪ Evaluate both hardware infrastructure and software overlays approaches. Evaluate not only vendor promises but the operational requirements to actually achieve a stated benefit. Hold any considered or deployed vendor accountable to deliver your desired outcomes and don't believe marketing hype surrounding SDN-related claims. Evaluate reference accounts and pay particular attention to implementation and ongoing operational costs and investments to ensure that benefits can be realistically achieved. ▪ Develop cross-functional collaboration and investigate methodologies to better integrate server, virtualization, network, security and application teams. These teams can help identify key use cases — both short-term, such as self-service development environments and micro segmentation; and long-term, integrating networking more broadly into data center orchestration. ▪ Allocate time and resources to evaluate technologies and a shortlist of relevant vendors — both incumbent and nonincumbent — in order to arrive at a solution that best meets the needs of the cross-functional organization.

Gartner

SSC Strategy Document Structure

- The SSC Strategy document structure includes overlapping concepts and a number of specific gaps. If the "Pillars" are defined more broadly they could cover all aspects of the strategy
- Pillar 1 — Connectivity
  - Overlaps with Network Foundation (in row 3), and include elements of Layers 1-3 of the OSI stack including wired (copper, fiber) and wireless (4G, 5G, Wi-Fi 6, Satellite) switching, routing, and associated protocols (IP, MPLS, etc.)
- Pillar 2 — Identity and Access Control
  - A component of Security, and overlaps with Zero Trust Architecture, in row 2
  - This second Pillar should be defined as "Security" and should cover all aspects of Network Security
- Pillar 3 — Monitoring
  - A component of Service Management, as is Provisioning (a row), and AIOps (in row 0), Configuration Management (CMDB)
  - This third Pillar should be defined as Service Management, and address all components, as defined by ITIL



Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

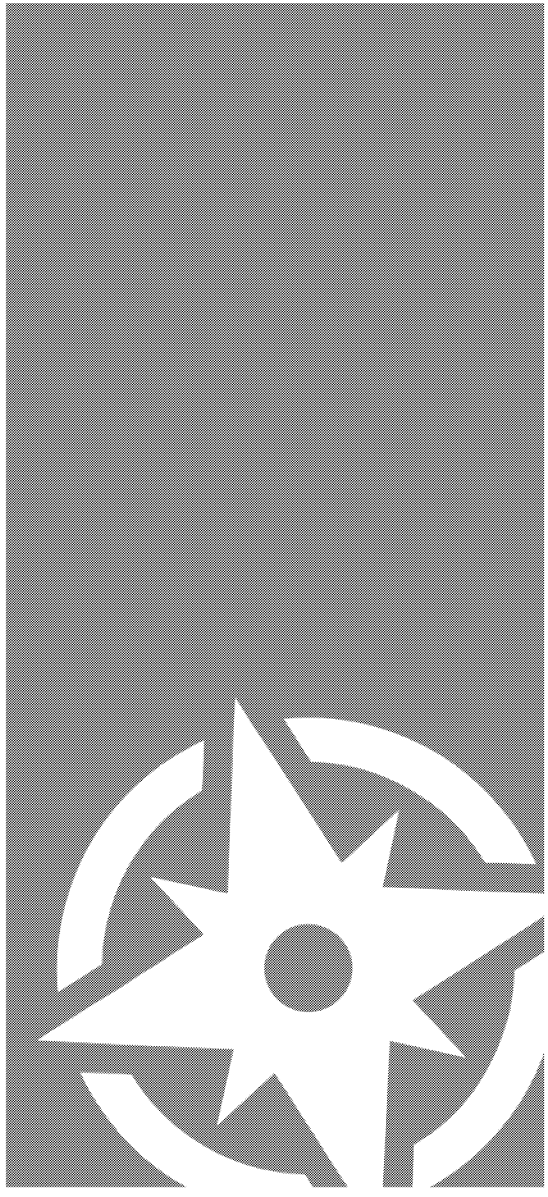
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

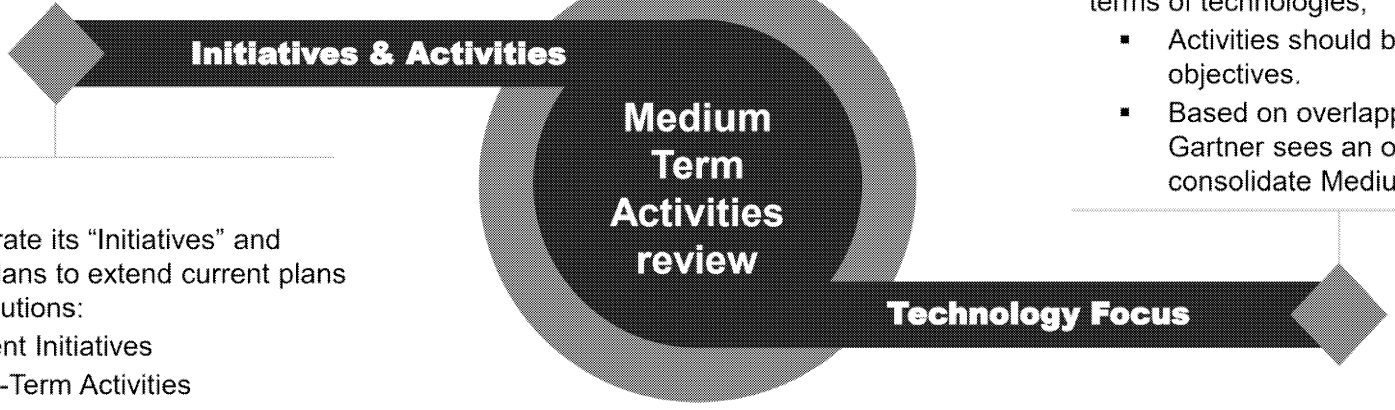
04 **Use Case Analysis**

05 **Appendix**



Gartner

Gartner has completed a Medium-Term Activities Review of current SSC Network Strategy Documentation



Integration

- SSC should integrate its "Initiatives" and "Activities", with plans to extend current plans to include new solutions:
  - Current Initiatives
  - Short-Term Activities
  - Medium-Term Activities

Definitions

- SSC Activities are typically defined in terms of technologies,
  - Activities should be aligned with objectives.
  - Based on overlapping objectives, Gartner sees an opportunity to consolidate Medium-Term Activities.

In the following slides, Gartner comments on how SSC activity definitions align with Gartner Research

Gartner

SSC Network and Security Strategy — Medium-Term Activities

Activities	SSC Network & Security Strategy	Gartner Research + Comments
1. Automation and Orchestration	• Continual increased automation and orchestration tools — Move past just automation and think about the tools working together.	▪ Gartner recognizes the importance and value or automation and orchestration tools. ▪ The SSC Strategy should provide details on tool selection or deployment plans.
2. Update CMDB	▪ Continue to update CMDB with all SSC infrastructure, however consideration should be made for procurement of autodiscovery tools.	▪ Configuration Management Database defines the inventory of infrastructure assets and is critical to effective service management. ▪ SSC should define completion goals.
3. Determine requirements for SSC Date Lake	▪ Determine requirement of SSC Data Lake for logging of all SSC infrastructure services. Will SSC need more information than what will be provided by traditional SIEM — Central Logging Service (CLS)?	Gartner defines Data Lakes as an important SIEM tool. Successful organizations often utilize SIEM together with their security data lake. • SIEM for near-real-time analysis; a security data lake for extended log management • SIEM for short-term analysis; a security data lake for longer-term, historical analysis • SIEM for real-time detection; a security data lake for testing and refining the rules and data models • SIEM for some security use cases; a security data lake for other use cases calling for collection of data that does not fit into a SIEM
4. Begin Identity Roll-out	▪ Begin Identity strategic roll-out including designs, plans, and implementations.	▪ Identity is core to Zero Trust Architecture ▪ Integrate with Zero Trust Architecture Activity #11

Gartner

SSC Network and Security Strategy — Medium-Term Activities

	SSC Network & Security Strategy	Gartner Research + Comments
5. Evolve SDN, SDI, SDP	▪ Evolve End-State Data Centre (EDC) Software-Defined Networking (SDN) with integrated Security Infrastructure and Software-Defined Perimeter (SDP) and Micro-segmentation.	▪ SSC Strategy should provide basic details on its plans ▪ Re-define and re-structure this activity to align with defined goals, avoiding obsolete terms with no clear definition.
6. Evaluate SDDC	▪ Software-Defined Data Centre (SDDC) proof of service in End-State Data Centres.	▪ SSC Strategy should include a rough process for this evaluation. ▪ Integrate with Activity #5, above
7. Implement Microsoft Office 365	▪ Implementation of commercial internet for M365 and SaaS at office buildings where and if deemed feasible during study.	▪ SSC should redefine this activity to "Internet Access Strategy" to support SaaS Applications.
8. Evaluate SASE	▪ Evaluate SASE (Security Access Service Edge) roadmap and integration with other security and network services.	▪ SASE described as a "Trend" but is not described as a "Strategy", i.e., why it is important, and how it would improve SSC operations. ▪ Integrate with Internet Access Strategy
9. Implement SD-WAN	▪ Design and implement Software-Defined WAN (SD-WAN).	▪ Define link to SASE plans in one strategy ▪ Integrate with Internet Access Strategy
10. Implement SD-LAN	▪ Design and implement Software-Defined LAN (SD-LAN) — building WI-FI and LAN infrastructure based on solutions determined through the ENM project.	▪ Redefine SD-LAN Activity to align with clear objectives of ENM project. ▪ Should this be defined as "In-building Network Initiative" or "LAN Modernization"?

Gartner

SSC Network and Security Strategy — Medium-Term Activities

	SSC Network & Security Strategy	Gartner Research + Comments
11. Evaluate Zero Trust Architecture POS	▪ Design and implement Zero Trust Architecture proof of service.	▪ Zero Trust Architecture will be valuable to SSC and the GoC ▪ Ensure coordination with Internet Access Strategy
12. Build Roadmap for Zero Trust Architecture	▪ Determine detailed roadmap and plan for Zero Trust Architecture based on proof of service.	• Integrate with "Evaluate Zero Trust Architecture POS", above

Gartner

SSC Medium-Term Initiatives should be consolidated with Short-Term Initiatives and

SSC Strategy Medium-Term Sections	Gartner Recommended Structure
1. Automation and Orchestration	Automation and Orchestration
2. Update CMDB	Update CMDB
3. Determine requirements for SSC Date Lake	Determine requirements for SSC Date Lake — Link to SIEM
4. Begin Identity Roll-out	Zero Trust Initiative (Linked to Internet Access)
5. Evolve SDN, SDI, SDP	Initiatives Needs Clearer Definition — Should these be linked?
6. Evaluate SDDC	
7. Implement Microsoft Office 365	Internet and SaaS Access
8. Evaluate SASE	
9. Implement SD-WAN	
10. Implement SD-LAN	Initiatives Needs Clearer Definition
11. Evaluate Zero Trust Architecture POS	Zero Trust Initiative Linked to ICAS and “Internet and SaaS Access” Initiatives
12. Build Roadmap for Zero Trust Architecture	

Gartner

SSC Current Initiatives should integrate with future Activities

Initiative	Definition	Associated Future Activities
SIEM	Security Information and Event Management	Data Lakes
EVAS	Endpoint Visibility Awareness and Security	Integrate with SSC plans for 2021-2024
EVCM	Enterprise Vulnerability and Compliance Management	Integrate with SSC plans for 2021-2024
CMN	Centralized Management Network	Integrate with SSC plans for SD-WAN
DCAM	Directory Credential Account Management	Integrate with SSC plans for 2021-2024
AACS	Administrative Access Controls Service	Link to Zero Trust
NDA (now CLM)	Network Device Authentication/Crypto life cycle Management	Link to Zero Trust
ICAS	Internal Centralized Authentication Service	Link to Zero Trust
GCNAC	Government of Canada — Network Access Control	Link to Zero Trust
ENM	Edge Network Modernization	SD-LAN
EPS	Enterprise Perimeter Security (EPS)	Evolve “Software-defined Perimeter (SDP)”
SRAM	Secure Remote Access Management	Internet and SaaS Access/Zero Trust
RHS	Regional Hub Strategy	Link to other Activities
SCED	Secure Cloud Enablement for Defence	Internet and SaaS Access/Zero Trust

Gartner

SSC Network and Security Strategy — Other References

Solution	SSC Network & Security Strategy	Gartner Research + Comments
5G	▪ 5th Generation Cellular (5G) which is poised to fundamentally change how network services are delivered to consumers and enterprises. ▪ The strategy/approach of wireless first will simplify user connectivity, reduce fit-up costs, and enhance user experience.	▪ SSC Strategy should suggest the potential use of 5G over the next three years. (Medium-Term) ▪ SSC should develop plans to deploy 5G services.
Wi-Fi 6	▪ Technologies such as Wi-Fi 6 and 5G will provide an opportunity to modernize and enhance the user experience.	▪ SSC Strategy should define its expectations for the deployment od Wi-Fi 6. ▪ SSC Strategy should comment on where it would prefer to use Wi-Fi 6 and 5G.
Hyper-converged infrastructure	▪ Implementation of enabling technologies, such as SDN, integrated with on-premises infrastructure, such as hyper-converged infrastructure.	▪ SSC Strategy should define opportunities to use hyper-converged infrastructure. ▪ SSC should establish some "Medium-Term Activity" to achieve specific goals within three years.
Skills	▪ SSC Strategy identifies the need for new skills.	▪ SSC Strategy should set-out any Medium-Term initiatives to address this gap.
Inter-operability	▪ SSC Strategy – "Supports a movement towards open standards with a vendor agnostic mindset." ▪ SSC Strategy has no reference to inter-operability	▪ SSC Strategy should reference steps it will take to ensure inter-operability and use of open standards in the future.

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

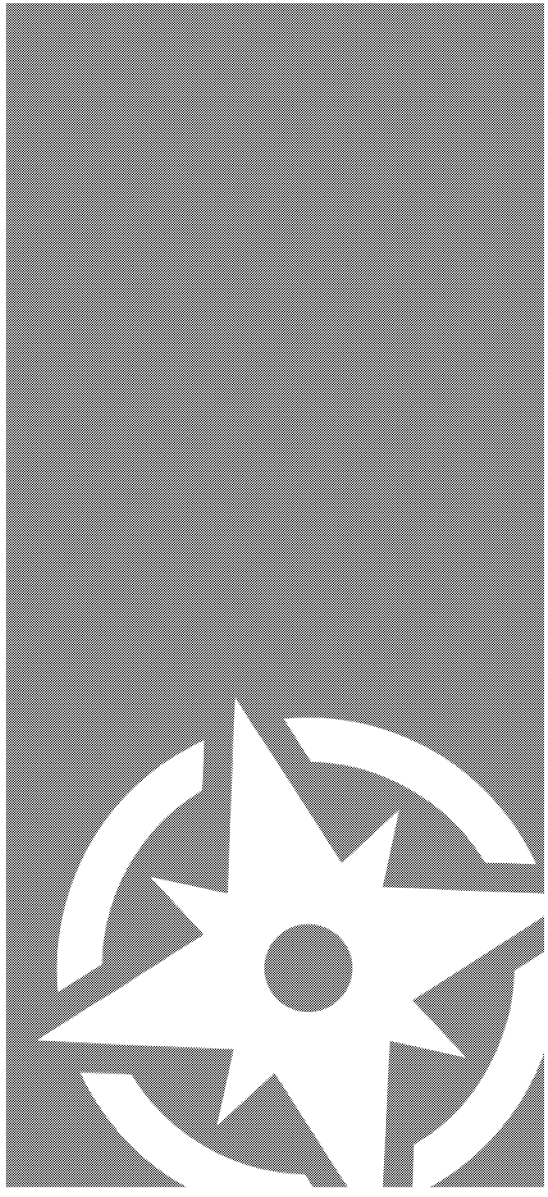
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix**

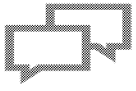


Gartner

Gartner has completed a document Review of the provided SSC Network Strategy and has recommendations for text enhancements

General Overview — Moving the text from passive and negative to active and positive

Focus on “Current State” — Providing a more balanced view of SSC successes and opportunities



Focus on “Requirements” — Areas where SSC should consider additional requirements

Focus on “Service Management” — Using ITIL structure to identify gaps in the Service Strategy

In the following slides, Gartner comments in further detail on SSC documentation writings and how they align with Gartner Research

Gartner

SSC Network and Security Strategy — Document Review
General Overview

SSC Network & Security Strategy Observations	Gartner Recommendations

▪ The SSC Strategy Executive Summary is written in a passive voice, when it could be written as an active strategy based on defined activities.
▪ Examples —
  ▪ "SSC will need to consider how it can create a value proposition that attracts valued skill sets and enables their retention."
  ▪ "Consider investing in automation and orchestration…"
	▪ By writing the SSC Strategy in an active voice would communicate confidence. The Strategy should focus on planned activities.
	▪ Suggestion —
	  ▪ "SSC will create a value proposition that attracts valued skill sets and enables their retention."
	  ▪ "SSC will invest in automation and orchestration…"

▪ SSC Strategy vague negative references to SSC Current State ▪ Example — "Ensure existing and future projects are provided guidance and not done in silos but done with all services in mind toward the Network and Security vision and strategy."	▪ SSC Strategy should focus on how it will improve delivery of services. ▪ Suggestion — "SSC leaders will work with project teams to ensure alignment with the SSC Network and Security Strategy."
▪ Some solutions discussed in the Strategy are not included in Medium-Term Activities, e.g., 5G deployment.	▪ SSC should define Medium-Term Activities associated with these activities.
▪ Some solutions defined as Medium-Term Activities and not included in the Strategy, e.g., CMDB update.	▪ Executive Summary should highlight the actions that will be taken, by aligning with Short-Term and Medium-Term Activities.

Gartner

SSC Network and Security Strategy — Document Review
Focus on Current State

SSC Network & Security Strategy Current State — Observations	Gartner Recommendations
Current State Analysis is written as an indictment of SSC. "There are over 500 individual projects planned or in progress to maintain, refresh or replace these environments with no comprehensive or integrated strategy."	▪ SSC actually does have a strategy, but has poor documentation of the strategy. ▪ SSC should present a balanced view of current state. ▪ SSC should reference metrics that it has improved or hopes to improve. (Examples included in Appendix, Page 102)
"technology evolving too quickly to keep pace"	▪ Hyperbole — Not a useful phrase ▪ Is it clear that SSC is falling behind? How is this being measured/addressed?
"technology advancement is outpacing the available skills required."	▪ Hyperbole — Not a useful phrase ▪ Available skills — in SSC, in GC, in Canada?
"staff cannot respond quickly enough, since they don't have the right information available to them."	▪ Hyperbole — Not a useful phrase ▪ What data is missing? How will this be addressed?
"SSC requires a new approach to managing and operating the SSC network and security environment"	▪ What is that approach? ▪ This approach is not clearly defined in the Strategy?
The Strategy refers to "negative impacts on the provisioning times"	▪ Are there metrics for provisioning times? Are these metrics getting worse? ▪ Use of specific metrics and trends provide important context.
"heightened risks related to the manual effort"	▪ Examples where risks are increasing? Where will manual efforts be replaced?

Gartner

SSC Network and Security Strategy — Document Review
Focus on Requirements

SSC Network & Security Strategy Government of Canada Requirements — Observations	Gartner Recommendations
End-users • Strategy refers to 400,000 end-users	▪ SSC does not address current user experience and associated metrics. ▪ SSC does not address remote access challenges such as latency. ▪ SSC does not address specific needs of employees and citizens.
Applications • Traditional VPN or remote desktop applications, while functional, were typically not scaled for the majority of the workforce to leverage simultaneously. • Efforts are currently underway to realign the external connectivity with the existing and near-future Cloud-based SaaS applications such as SSC Network and Security Strategy Office 365.	▪ SSC does not define "efforts are currently underway to realign the external connectivity." ▪ Gartner expects the GC departments to use more SaaS applications in the future, but the SSC Strategy does not address this growth.
Workload • "workloads that are migrating to the public cloud"	▪ SSC Strategy does not document any assumed metrics associated with changes in workloads, including migration to the cloud.
Impact of COVID • In response to COVID-19, most organizations where forced to adopt work from home (WFH) and a remote access work model . This shift of locale has stressed these services to the breaking point.	▪ Was SSC successful in adapting to work from home? ▪ What was at the breaking point? How was this addressed? ▪ What lessons were learned? ▪ How did this impact SSC Strategy?
Post-COVID-19Plans • How will work from home (WFH) impact SSC Strategy Post-COVID.	▪ What assumptions does SSC make about Post-COVID-19work environment? ▪ Does SSC plan based on more users working from home? ▪ How does this impact SSC plans for Intra-building networks

Gartner

SSC Network and Security Strategy — Document Review Focus on Service Management (1 of 2)

SSC Network & Security Strategy Service Management — Observations	Gartner Recommendations/Comments
Service Management — Only Monitoring and Provisioning are addressed in the first 25 pages of the Strategy.	▪ Reference to Service Management should be included in the Executive Summary, and discussed early in the Strategy.
Configuration Management "Configurations have been primarily done manually, by system engineers and operators within SSC and within other departments, which can lead to inconsistencies in the configurations."	▪ SSC strategy addresses part of Configuration Management on Page 37 — "Establish and update CMDB with all SSC infrastructure."
Provisioning — Implement SDN/SDI, and Cloud Provisioning "SSC will need to undertake a fundamental change to its operating model as it moves to Cloud and new network and security capabilities."	▪ SSC should define current or planned Provisioning metrics in terms or users, applications, infrastructure refresh, etc. ▪ SSC Strategy should include improvement of Provisioning metrics through Medium-Term Activities.
Monitoring — SSC considers Monitoring as a "Pillar" of the Strategy. "SSC will need to move from stand-alone monitoring tools and processes to an integrated set of technologies that is supported by a centralized data repository."	▪ See "Pillar 3 — Monitoring" on page 9 of this Gartner report. (above)
Capacity Management Network on Demand will provide "better capacity planning, but Network on Demand is identified as a "Trend" and not defined as a Strategy.	▪ SSC should define strategy to address Capacity Management
Maintenance Intra-building network infrastructure, equipment and cabling have multiple custodians, leading to complexity of operational models with disparate strategies for technologies, vendors, deployment, maintenance and operations	▪ SSC Strategy should define maintenance programs or any initiatives to improve infrastructure maintenance.

Gartner

SSC Network and Security Strategy — Document Review
Focus on Service Management (2 of 2)

SSC Network & Security Strategy Service Management — Observations	Gartner Recommendations
Change Management • SSC Strategy makes reference to the need for Change Management • "Develop the change management processes to manage the operational change (highly important) following ITSM best practices."	▪ SSC should define specific activities to address Change Management
Incident Management "Artificial Intelligence Operations platforms (AIOps) will enable SSC to derive deep insights and drive automated response to incidents"	▪ SSC should be clear, upfront, about how Incident Management will be improved. The use of metrics would highlight SSC goals.
Problem Management "Inconsistency in device monitoring and support teams working in silos further adds to the layers of complexity that hinder timely and cost-effective problem resolution."	▪ SSC should define strategies to improve Problem Management, beyond improvements in Monitoring.

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

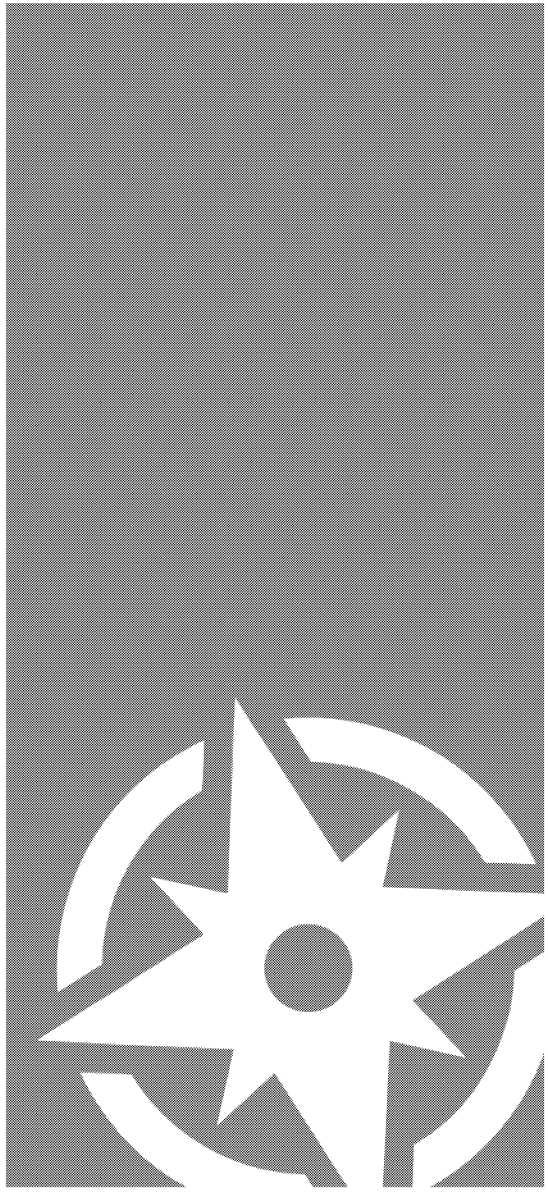
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

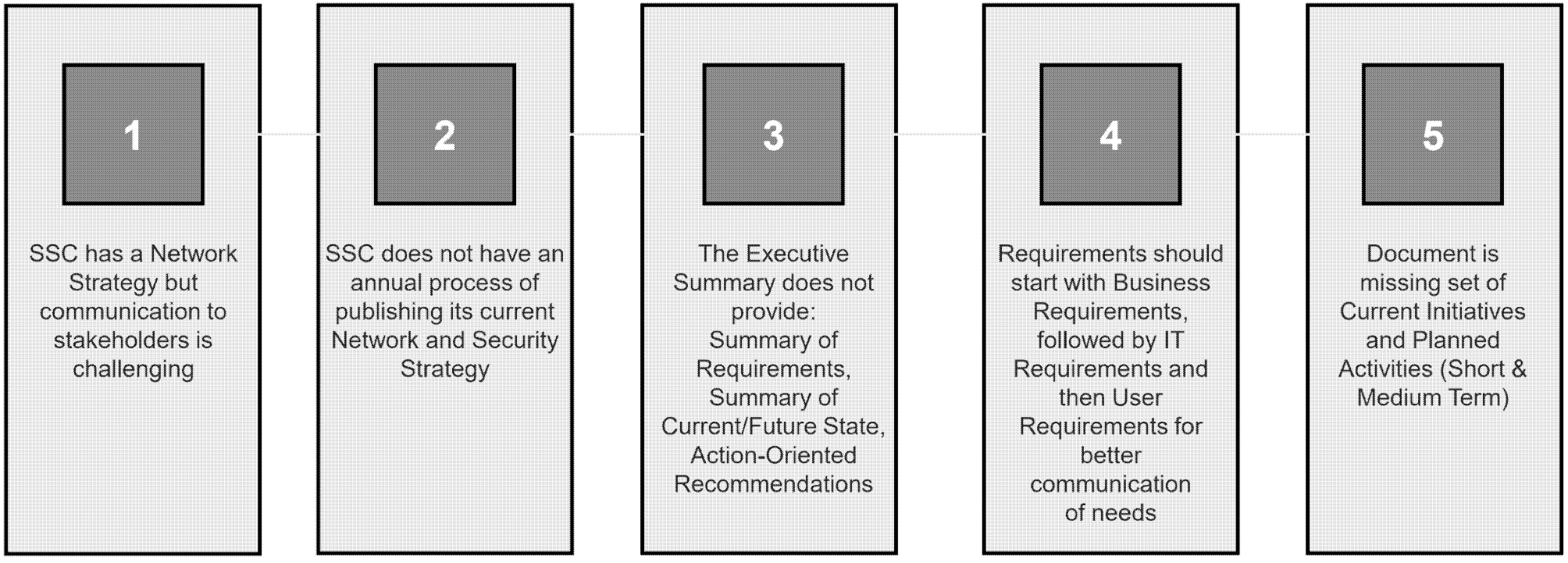
04 **Use Case Analysis**

05 **Appendix**



Gartner

Gartner identified 5 key gaps when comparing the SSC Network Modernization Discussion Document to Gartner's Template for Network Strategy



In the following slides, Gartner comments on how SSC can build its Network Strategy document to incorporate identified gaps

Gartner

Gartner Recommended Strategy Document Structure

Gartner Research: Creating a Business-Relevant Network Strategy, 5 January 2016

Sections	Focus	Description
Executive Summary	▪ Summary of all sections below, in order	▪ Stand-alone summary of key points
Business and IT Drivers	▪ Addresses Known Requirements	▪ Linked to established Business and IT Strategies
IT Environment	▪ Current IT environment	▪ Defining constraints, including legacy solutions
User Environment	▪ User Types and Experience	▪ Address key metrics on user needs and user experience
Current State Assessment	▪ What works well, and what doesn't	▪ What needs to be addressed
Desired Future State	▪ How would service work better	▪ Established goals and objectives over a fixed period
Gap Analysis	▪ Assumptions and Dependencies	▪ What externalities will impact the strategy?
	▪ Risk Assessment	▪ What are risks of alternatives, including doing nothing?
	▪ Constraints	▪ What will restrict the execution of the plan?
Action Plan/ Roadmap	▪ In depth recommendations	▪ What can be done. When? By whom?
	▪ Roadmap(s) for implementation	▪ Specific Initiatives — How will Future State be achieved?

Gartner

Gartner compared the "SSC Network Modernization Discussion Document" to the Gartner Template Network Strategy

Network Strategy	Gartner Network Strategy Template	SSC Network Modernization Document	Gartner Comments
Overview	▪ **Gartner Research —** Creating a Business-Relevant Network Strategy; 5 January 2016, G00294550	▪ SSC "Network Modernization Discussion Paper- December 2020"	▪ Discussion Document should define its audience, and how this document should be used. GoC partners should be identified and solicited for their reaction. ▪ The Discussion Document should take a positive perspective and avoid writing from a defensive posture.
Executive Summary	▪ Summary of Requirements	▪ SSC utilizes a "what the partners are asking for" section to list known requirements."	▪ SSC should identify any requirements that are unique to the Canadian Government and its employees (e.g., network latency)?
	▪ Summary of Current State	▪ Ten years ago, "this infrastructure was aging, costly to maintain and unable to support modern services."	▪ If this infrastructure has not been refreshed since 2011, this would be a major gap in the Current State. ▪ Otherwise, the relevance of this point is unclear.
	▪ Summary of Future State	▪ "SSC is currently designing the future state solution."	▪ Although SSC is still designing its future state, the strategy should document the current initiatives that are in fact defining the SSC future network architecture. ▪ Examples would include the new Data Centre LANs.
	▪ Action-oriented recommendations	▪ This document does not address any specific initiatives.	▪ SSC should communicate their major network initiatives in an annual Network Strategy

Gartner

Gartner compared the "SSC Network Modernization Discussion Document" to the Gartner Template Network Strategy

Network Strategy	Gartner Network Strategy Template	SSC Network Modernization Document	Gartner Recommendations
Business and IT Drivers	▪ Business Priorities ▪ CIO Strategies ▪ HR/Skills Plan	▪ Business Priorities — Includes reference to support working from home. ▪ CIO Strategies — Includes reference to applications moving to Cloud services. ▪ Reference to Security Vision document is helpful ▪ HR/Skills Plan — SSC document lacks clarity on future skills required	▪ Establish a process to solicit Business Priorities on an annual basis. ▪ Reference specific and unique GoC Business Priorities ▪ Reference link from Discussion Document to the SSC Network and Security Strategy and SSC other strategies. ▪ SSC recognizes that new skills will be required, and should provide examples
IT Environment	▪ Architecture ▪ Infrastructure/Governance ▪ Sourcing ▪ Metrics used	▪ Architecture — High-level network architecture diagram ▪ Governance — No clearly defined and scheduled decision-making process ▪ Sourcing — SSC recognizes need to update its existing procurement strategy ▪ Metrics not included	▪ Architecture — High-level network architecture diagram should be supported by descriptive text. ▪ Sourcing — Procurement processes will improve transparency, accountability and efficiency. ▪ Metrics — Add reference to using metrics to track improvements
User Environment	▪ Workforce plan ▪ Desired Capabilities ▪ Facilities Plan	▪ Workforce Plan — Mentions impact of COVID-19 but does not define associated gaps. ▪ Desired Capabilities — Defined in generic terms without reference to any specific GoC requirements ▪ Facilities Plan — Impact of COVID-19 discussed, with reference to changing work-site utilization	▪ A Network Strategy should set expectations for COVID-19 period and post-COVID-19 work environments. ▪ Facilities Plan should set-out expectations of GoC building network support needs (LAN) ▪ Strategy should include reference to improve processes to define client department user requirements

Gartner

Gartner compared the "SSC Network Modernization Discussion Document" to the Gartner Template Network Strategy

Network Strategy	Gartner Network Strategy Template	SSC Network Modernization Document	Gartner Recommendations
Current State Assessment	▪ Budget and Finance ▪ Service Levels ▪ Technology ▪ Organization and Staffing ▪ Vendor Assessment	▪ Budget — Does not include an analysis of current spend ▪ Service Levels — Does not reference current performance metrics ▪ Vendor Assessment — Not address current highs and lows of vendor relationships ▪ Technology — Includes vendor list for each network category, but no solution details ▪ High-level network architecture diagram is not supported by descriptive text.	▪ Provide metrics for current consumption of services to show trend toward future demand for services. ▪ Show key measurable efficiency metrics aligned with public GoC/SSC budget reporting. ▪ Define performance metrics that are useful and measurable, e.g., uptime, latency, equipment failure, etc. ▪ Technology — Add some measure of planned future use of new technologies — Who? Where? ▪ Organization — How is SSC organized to address GoC network needs? ▪ Vendors — How is vendor performance measured?
Desired Future State	▪ Future Services Offered ▪ Future Technology Trends ▪ Changes to Current State	▪ Future State not yet defined — "SSC is currently designing the future state solution." ▪ Reference to technology trends does not include reference to applicability, or measurable benefits. ▪ SSC document includes a "notional procurement approach", with focus limited to vendor selection. ▪ SSC plans for greater use of Dark Fibre Service and Satellite Services.	▪ Although SSC is still designing its future state, the strategy should document current initiatives that are in fact defining a future. Examples would include the new Data Centre LANs. ▪ SSC should set some level of expectation for the use of Dark Fibre Service and Satellite Services.

Gartner

Gartner compared the "SSC Network Modernization Discussion Document" to the Gartner Template Network Strategy

Network Strategy	Gartner Network Strategy Template	SSC Network Modernization Document	Gartner Comments
Gap Analysis	▪ Assumptions and Dependencies	▪ The Discussion Document assumes that SSC will support the current COVID-based work from home, but does not address any further response efforts. ▪ SSC has not defined Dependencies.	▪ Once SSC defines its network strategy, it will want to define any Assumptions and Dependencies.
	▪ Risk Assessment	▪ Risk statements are unclear. Example: "Standardize on two or more products – …..mitigates the risk that the GC no longer wants to do business with a specific vendor for commercial or security reasons."	▪ SSC should identify Risk that will impact its ability to provide and improve services. ▪ SSC should identify Risk that will impact its ability to provide and improve services.
	▪ Constraints	▪ Constraints — Lack specifics on what causes constraints.	▪ SSC should consider the major constraints that may limit its ability to provide services.
Action Plan/ Roadmap	▪ In depth recommendations ▪ Roadmap(s) for implementation	▪ SSC has not defined clear recommendations. ▪ Roadmap — Project timelines are discussed but there is no clear roadmap for deployments.	▪ The Discussion Document should include specific recommendations from the SSC Network and Security Strategy. ▪ The Discussion Document should include a 5 year roadmap for major initiatives, and reference to resources needed to achieve future state.

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

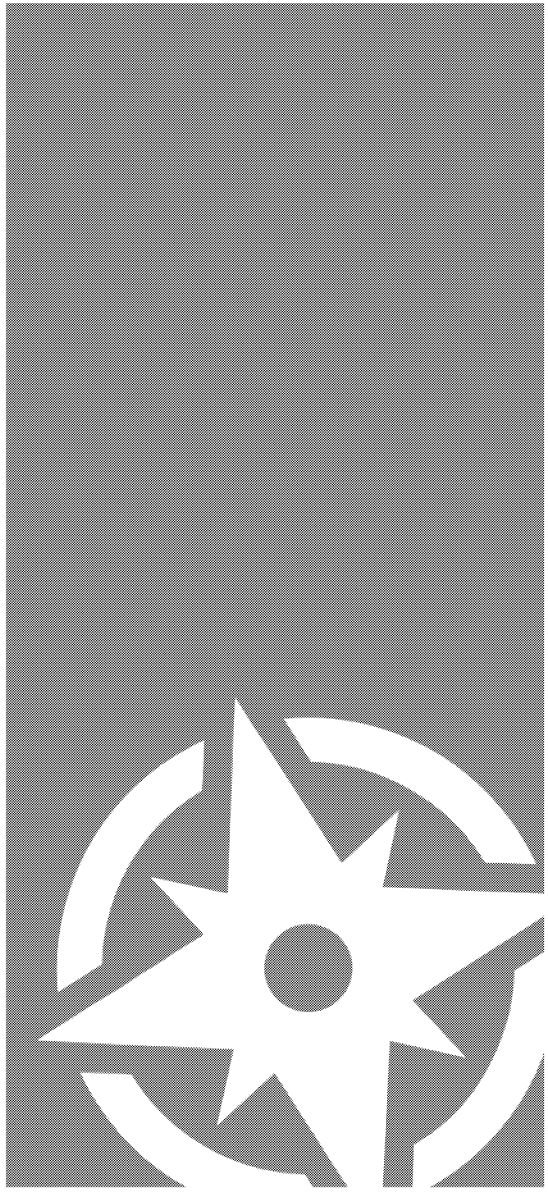
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

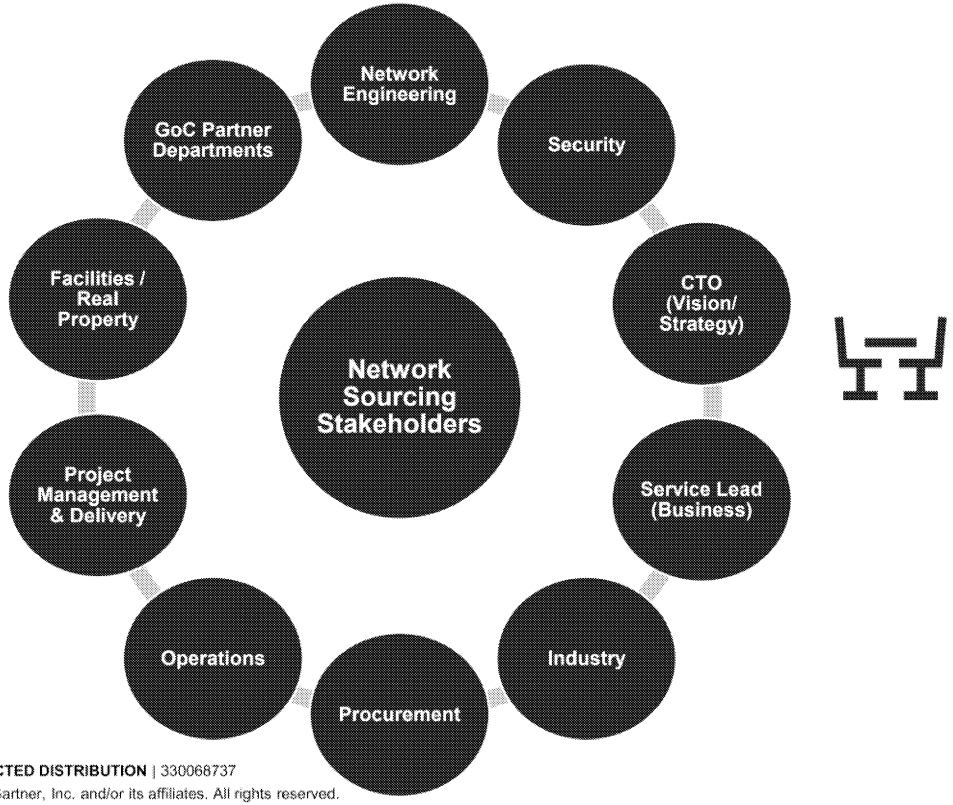
05 **Appendix**



Gartner

Discovery workshops were held to discuss network sourcing stakeholder's Goals/Constraints and informed the sourcing approach

This insight has been used to in formulating a sourcing decision approach that balances often competing stakeholder goals and constraints. As more complex network sourcing decisions or exceptions are made, Gartner recommends considering the position of each stakeholder in order to reach the optimal outcome for SSC as a whole, as well as its GoC partners.



Insights

- Standardization of processes/vendors are key goals for several stakeholders
- Procurement and Legal obligations impose significant constraints
- Budget, skills, and workforce size have surfaced as constraints for many stakeholders
- Both industry and SSC stakeholders have a goal to increase transparency
- Legacy networks exist and persist through the business of SSC
- Security constraints (e.g., certifications, supply chain integrity) are immovable for select sourcing

Gartner

Stakeholder Overview

Network Engineering	Procurement	Security
▪ **Goals:** Standardization, Supportability, Interoperability within existing ecosystem ▪ **Constraints:** Industry and SSC Standards, Capacity (e.g., Interop Test), Existing Capabilities (Skills)	▪ **Goals:** Acceptable Terms & Conditions, Meeting deadlines, budget, and business needs, Openness & Transparency ▪ **Constraints:** SSC Procurement Rules and Regulations, CIIT Rules and Regulations, Legal Considerations, Capacity (Staff), Funding allocations	▪ **Goals:** Meeting security functions ▪ **Constraints:** Industry Certifications (e.g., FIPS, CC), Alignment and compliance with CSEC, Supply chain integrity requirements

Operations	CTO (Vision/Strategy)
▪ **Goals:** Management Simplicity, Maintain/improve service levels ▪ **Constraints:** Existing capabilities (Skills), Operations capacity	▪ **Goals:** Alignment to established Vision & Strategy ▪ **Constraints:** None were identified during Discovery Interview

Gartner

Stakeholder Overview

Project Management & Delivery	Service Lead (Business)	Facilities/Real Property
▪ **Goals:** Budget, Schedule, Scope ▪ **Constraints:** Project Expenditure Authority, Procurement Process	▪ **Goals:** Value for money, maintaining/improving service line, continuous service improvement, service life cycle management, vendor performance management ▪ **Constraints:** Budget, Capacity	▪ **Goals:** Project Management Simplicity ▪ **Constraints:** Cabling Plant, Roles and Responsibilities (SSC vs. PSPC)

Industry	GoC Partner Departments
▪ **Goals:** Profit, Footprint, Visibility into Procurement, Education ▪ **Constraints:** IP, Interoperability, Industry Standards, Access to information	▪ **Goals:** Meet Departmental Objectives ▪ **Constraints:** None were identified during Discovery Interview

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

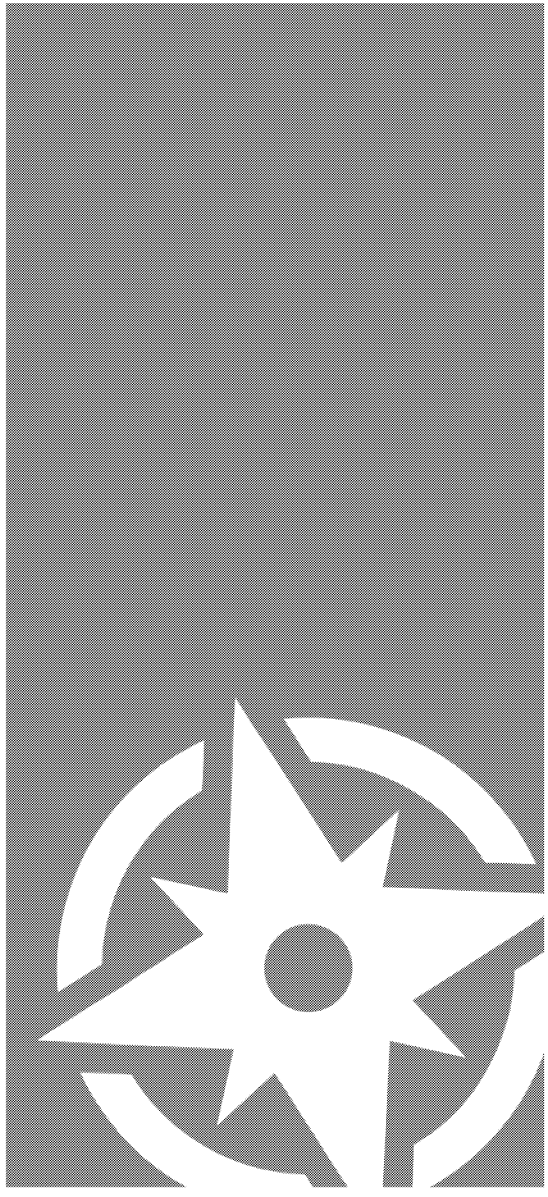
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix**



Gartner

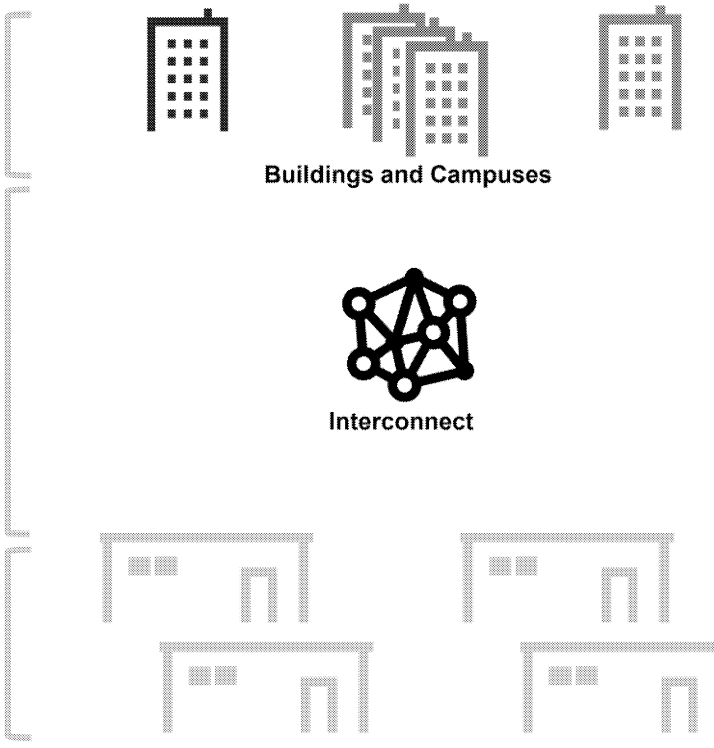
Defining the three areas of SSC's network will help give clarity for future procurement efforts

To best align with the Industry, Gartner proposes that SSC's network be considered as three distinct areas, as depicted below, allowing the establishment of **technology standards** with clearly defined boundaries and scope.

LAN (Local-Area Network)
- In-building wired network
- Wireless (Wi-Fi) networking

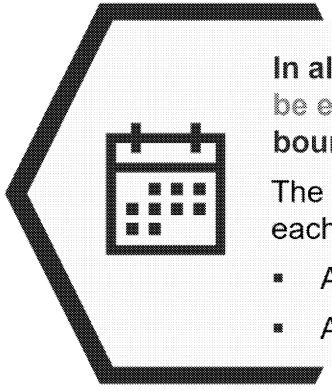
WAN (Wide-Area Network)
- Backbone routers
- Transport (Optical, DWDM)
- Edge Routing and Services Layer

DCN (Data Centre Network)
- Underlay/Physical Network
- Overlay/Virtualized Network



Gartner

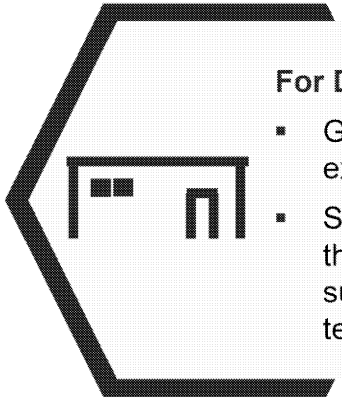
Gartner has developed considerations for establishing technology standards across SSC



In all three Network areas, Gartner recommends that technology standards should be established **in each identified LAN, WAN and DCN domain (within identified boundaries)** through open, competitive procurements

The technology standard should remain in place for the expected life of the equipment in each area, and should be recompeted once they expire:

- Approximately 10 years for LAN
- Approximately 5-7 years for WAN and DCN

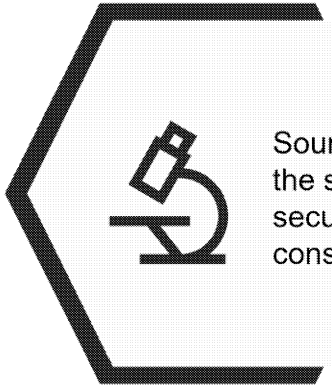


For Data Network Centers Gartner recommends two technology standard domains

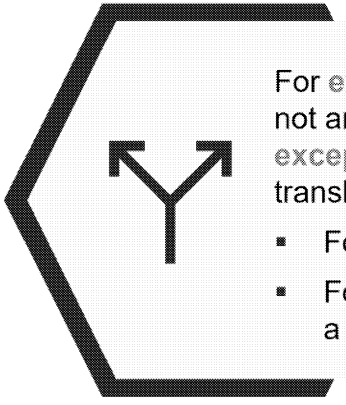
- Gartner recommends staggering the start/end dates of the standards so that they don't expire at the same time
- SSC might consider an initial competition where the first-place successful proposal sets the technology standard for the first "DCN Network" for 7 years and the second-place successful proposal sets the standard for 5 years. Further procurements would set technology standards for 7 years

Gartner

Gartner has provided guardrails for sourcing without established technology standards



Sourcing taking place prior to the establishment of a technology standard, or after the standard has expired should be carefully reviewed to balance business, technical, security, legal, procurement and industry constraints. Such decisions should be made in consultation with stakeholders

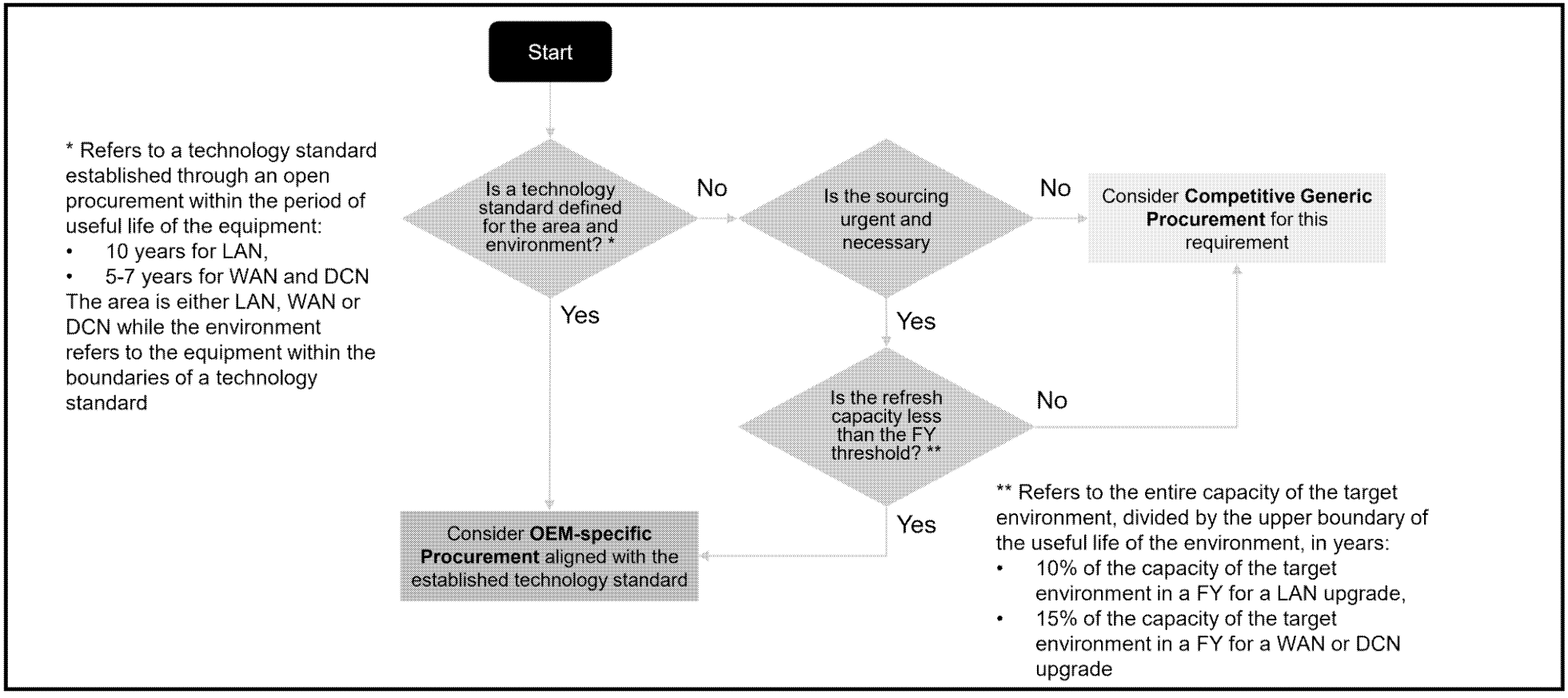


For existing environments where there is an established vendor (de facto standard) but not an established technology standard, Gartner recommends that sole-sourcing exceptions be approved in cases when the upgrade is urgent and necessary. This translates to:

- For the LAN area, less than 10% of the capacity of the target environment in a FY
- For the WAN and DCN area, less than 15% of the capacity of the target environment in a FY

Gartner

The Network Sourcing Decision Aid for SSC's future network procurements is summarized in this decision tree



* Refers to a technology standard established through an open procurement within the period of useful life of the equipment:
- 10 years for LAN,
- 5-7 years for WAN and DCN

The area is either LAN, WAN or DCN while the environment refers to the equipment within the boundaries of a technology standard

** Refers to the entire capacity of the target environment, divided by the upper boundary of the useful life of the environment, in years:
- 10% of the capacity of the target environment in a FY for a LAN upgrade,
- 15% of the capacity of the target environment in a FY for a WAN or DCN upgrade

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

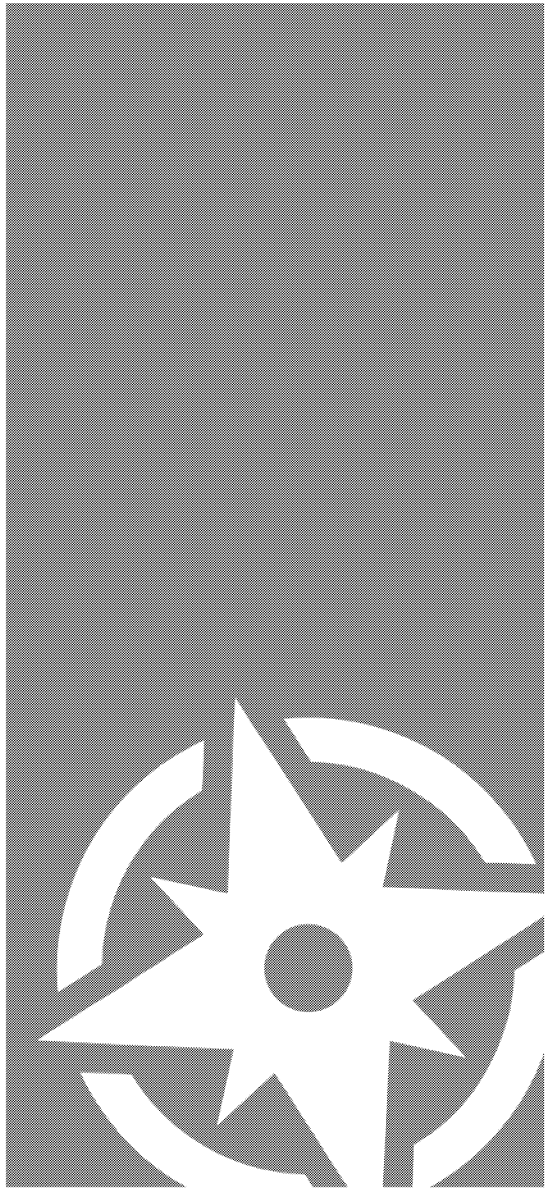
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

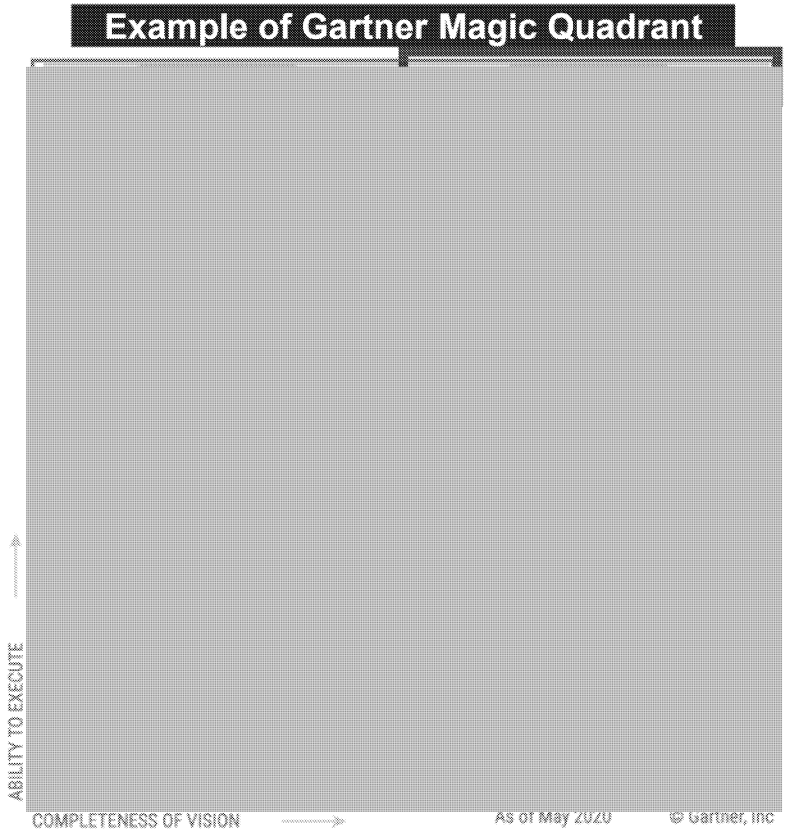
05 **Appendix**



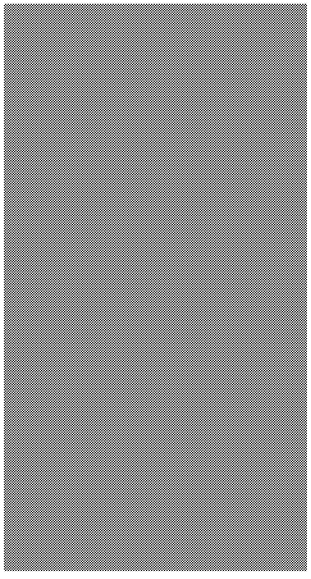
Gartner

SSC should strive to include industry leading vendors in its procurements while balancing GoC context and constraints

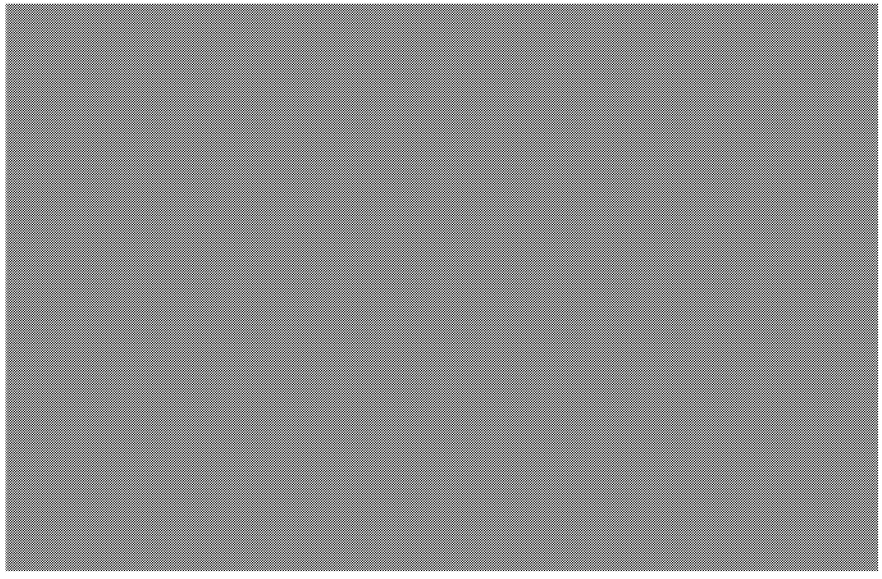
- Gartner has provided in each network area a breakdown of established vendors that SSC should strive to include in its procurement efforts
- A Leader in Gartner's Magic Quadrant showcases both visionary attitudes and actions in their domain and demonstrates a high level of execution in its operations, attributes that are highly desirable
- Challengers, Visionaries and Niche Players can also be included, as appropriate
- While this represents an industry view, SSC should also consider constraints that would warrant excluding specific vendors from open procurements. These constraints include but are not limited to those related to: Supply Chain Integrity, Security, Vendor Management Sanctions, etc.



Gartner



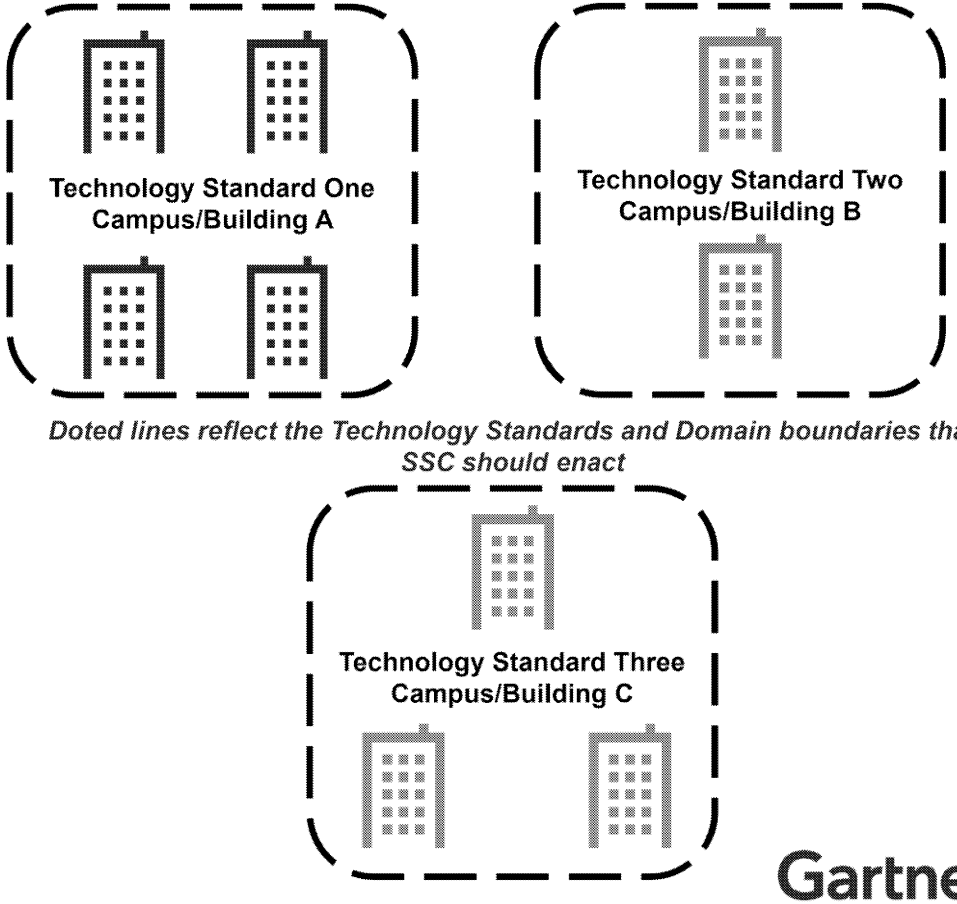
LAN



Gartner

LAN Equipment should have technology standards/boundaries that are associated with each building/campus at SSC

- By enacting standards/boundaries for LAN equipment (including WLAN) SSC can deliver operational efficiency while encouraging competition
- Technology standards set through a competitive procurement rank highly in terms of transparency, fairness and value while minimizing technical interoperability concerns
- By formalizing these boundaries and technology standards at a building/campus level, SSC can incorporate a multi-vendor sourcing approach to its LAN Equipment
- The useful life of equipment in this area is about 10 years, which should align with the life cycle of the technology standards

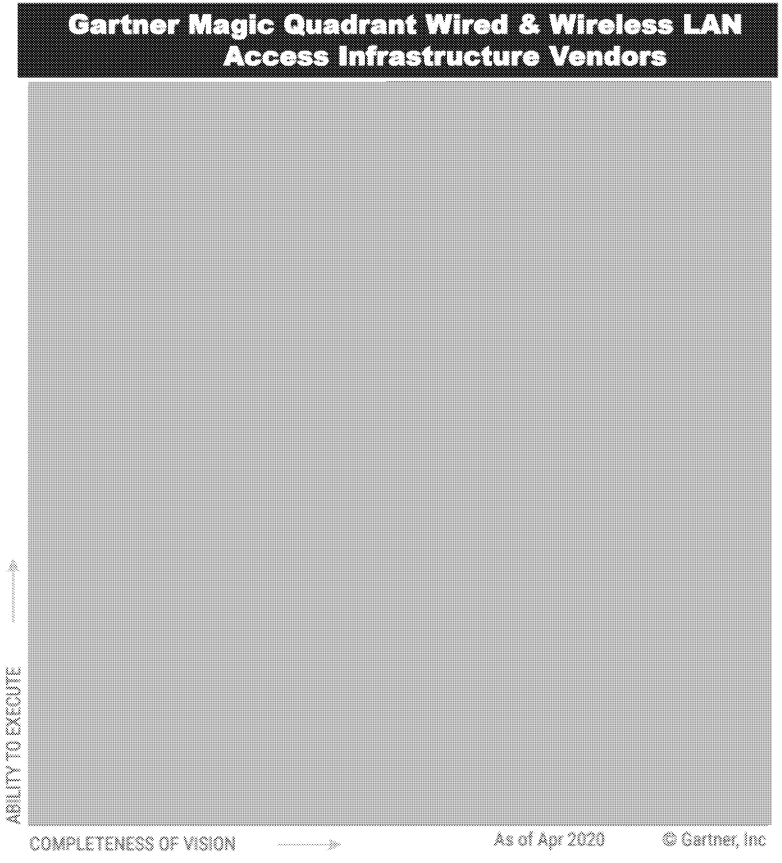


Doted lines reflect the Technology Standards and Domain boundaries that SSC should enact

Gartner

Leading Wired & Wireless LAN Access Infrastructure vendors are presented in this Gartner Research Magic Quadrant

- The primary business outcome is new, refreshed or expanded wired and wireless LAN connectivity. Typically, it is within carpeted enterprise environments, campus buildings, and remote or branch offices, and it is between client devices and applications or other assets residing in corporate data centers, the cloud or the internet. Increasing IoT endpoints or OT devices used for applications such as building automation require WLAN connectivity
- Leaders should have demonstrated the ability to maintain strong relationships with their channels and customers and have no obvious gaps in their portfolios
- Gartner predicts there will be approximately 1.7 billion new devices per year attaching to the enterprise network by 2023, but not all attach the same way or via the same architecture



Company Profiles of each of these vendors have been provided on the next pages

Gartner

Juniper Networks Company Profile

Company Overview

Headquarters:
Sunnyvale, California
United States

Maturity:
Founded: 1996
Headcount: ~9,400 (2019)
Reach: Global
Revenue: ~$4.4B

Relevant Network Background

Its AI-driven enterprise solution delivers a broad portfolio of cloud-based network application and services with a full complement of wired switching and WLAN products. Its operations are geographically diverse, servicing clients in all markets, from SMB to large enterprise. With its Mist Systems acquisition, the vendor continues investing in its AI foundation, utilizing the Marvis AI technology to differentiate as it expands its Mist Assurance and Mist Analytics applications across the entire campus network. The addition of Juniper's wired access layer switching products to the Mist architecture has made the solution a complete, end-to-end offering

Strengths

- [redacted]
-
-

Cautions

-
-
-

HPE (Aruba) Company Profile

Company Overview

Headquarters:
Santa Clara, California
United States

Maturity: (Aruba)
Founded: 2002
Headcount: ~6,000 (2019)
Reach: Global
Revenue: ~$3.0B

Relevant Network Background

As part of HPE's "edge to cloud" strategy, Aruba Edge Services Platform (ESP) delivers a broad portfolio of cloud-based and on-premises managed network applications and services in conjunction with its access wired switching and WLAN products. Its operations are geographically diversified, and Aruba services clients in all markets, from SMB to large enterprise. Aruba has a strong security presence in the campus networking market and continues to evolve its network automation and application visibility capabilities

Strengths

-
-
-

Cautions

-
-
-

Gartner

Cisco Company Profile

Company Overview

Headquarters:
San Jose, California
United States

Maturity:
Founded: 1984
Headcount: ~75,000 (2019)
Reach: Global
Revenue: ~$59.1B

Relevant Network Background

Its Catalyst and Meraki products deliver a broad portfolio of access wired switching, WLAN products, network applications and services. Its operations are geographically diversified, and Cisco services clients in all markets, from small and midsize businesses (SMBs) to large enterprises. Cisco continues to invest in new chips and operating system development that can be leveraged across its entire portfolio

Strengths

-
-
-

Cautions

-
-
-

Extreme Networks Company Profile

Extreme

Company Overview

Headquarters:
San Jose, California
United States

Maturity:
Founded: 1996
Headcount: ~2,750 (2019)
Reach: Global
Revenue: ~$983.1M (2018)

Relevant Network Background

Extreme delivers a broad portfolio of cloud-managed and on-premises managed network applications and services in conjunction with its end-to-end wired switching and WLAN products. Its operations are geographically diversified, and Extreme Networks services clients in all markets, from SMBs to large enterprises. Extreme continues to invest in its containerized microservices architecture — which enables deployment in any cloud platform (Amazon Web Services [AWS], Google Cloud Platform [GCP] and Microsoft Azure) or on-premises — as well as its vertical market solutions

Strengths

-
-
-

Cautions

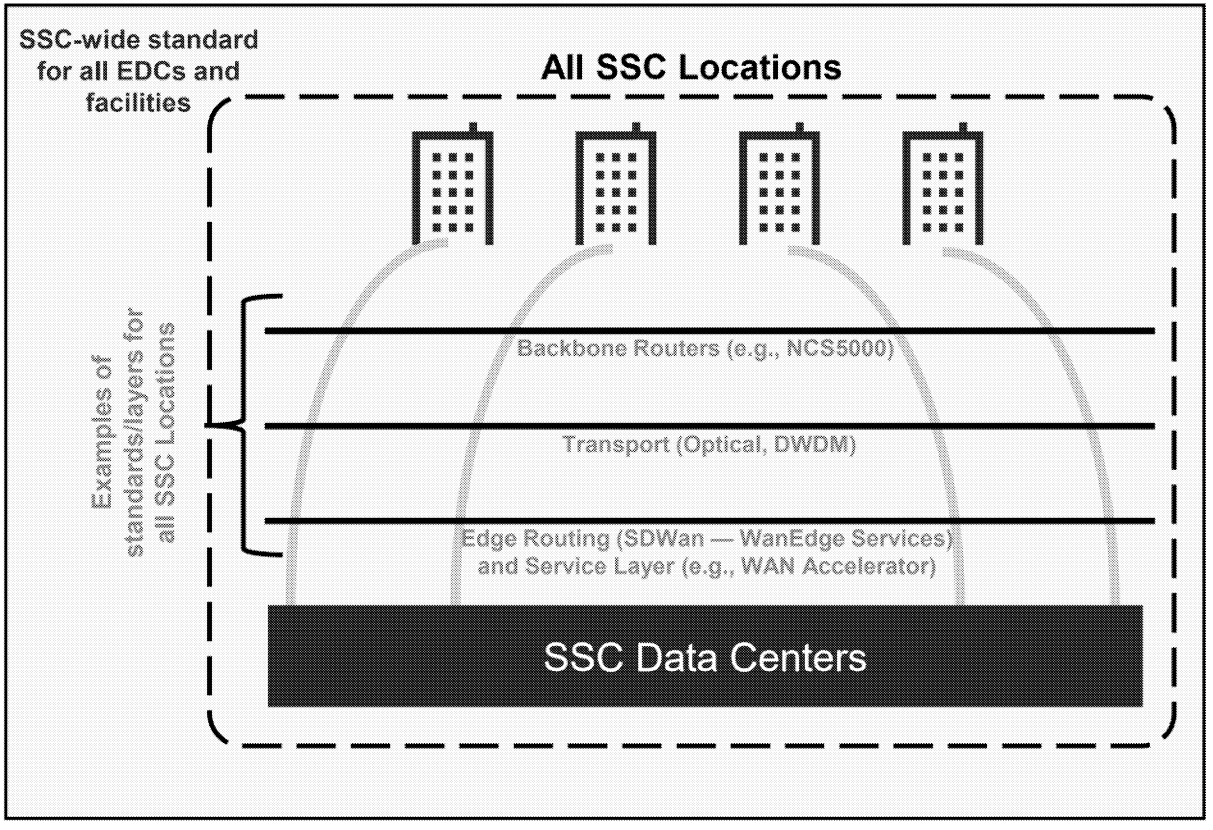
-
-
-

WAN

Gartner

A WAN technology standard should be created across all EDCs and facilities to support any-to-any connectivity

- The WAN domain stretches across all SSC locations and WAN technology standards should follow this boundary to allow for any-to-any connectivity and visibility within SSC
- As the WAN is composed of multiple layers (Backbone, Transport and Edge/Services), SSC-wide technology standards should be established for each layer
- The useful life of equipment in this area is about 5-7 years, which should align with the life cycle of the technology standards

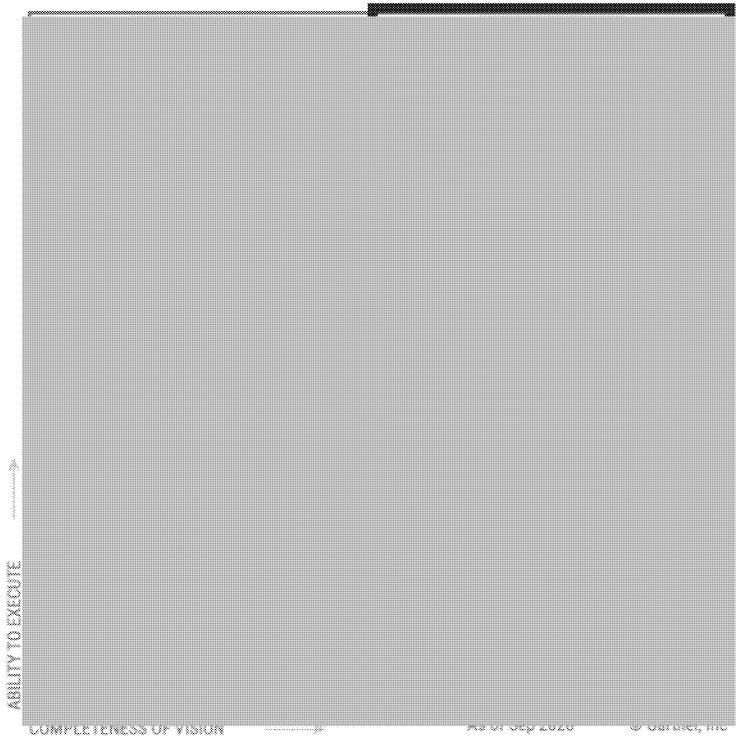


Gartner

Leading WAN Edge Infrastructure vendors are presented in this Gartner Research Magic Quadrant

- The fundamental business outcome is connectivity between enterprise users, applications and services that reside in distributed locations (both on-premises and off-premises). Locations include headquarters, branches, corporate data centers, colocation/hosting facilities, SaaS providers and cloud service providers. Increasingly, buyers require improved agility, automation, orchestration, flexibility and application control
- A Leader has demonstrated a sustained ability to address changing requirements for enterprise WAN edge
- Gartner views SD-WAN and SASE as key technologies to help enterprises transform their networks from fragile to agile. SASE splits functions between on-premises and the cloud, and Gartner expects to see more functions supported in the cloud

Gartner Magic Quadrant WAN Edge Infrastructure Vendors



Company Profiles of each of these vendors have been provided on the next pages

Gartner

VMware Company Profile

vmware

Company Overview

Headquarters:
Palo Alto, California
United States

Maturity:
Founded: 1998
Headcount: ~31,000 (2019)
Reach: Global
Revenue: ~$8.7B

Relevant Network Background

Its product is branded as VMware SD-WAN powered by VeloCloud, which primarily includes SD-WAN edge (VCE) appliances, gateways (VCG) and an SD-WAN orchestrator (VCO). VMware is based in California, U.S., and Gartner estimates it has more than 9,000 SD-WAN customers. We expect VMware to make future investments in enhancing its SASE security capabilities, multicloud onramp, edge compute and AI/ML for improved analytics with the integration of Nyansa

Strengths

-
-
-

Cautions

-
-
-

Gartner

Fortinet Company Profile

Company Overview

Headquarters:
Sunnyvale, California
United States

Maturity:
Founded: 2000
Headcount: ~6,000 (2019)
Reach: Global
Revenue: ~$216B

Relevant Network Background

Its offering is the Fortinet Secure SD-WAN, which includes FortiGate hardware and virtual appliances with accompanying networking and security (FortiGuard) software managed by the orchestrator in FortiManager. We expect Fortinet to make future investments in SASE, AI/ML for troubleshooting SD-branch/SD-WAN, and cloud/multicloud orchestration

Strengths

- [redacted]

Cautions

- [redacted]

Versa Networks Company Profile

Company Overview

Headquarters:
San Jose, California
United States

Maturity:
Founded: 2012
Headcount: ~150 (2019)
Reach: Global
Revenue: ~$30 M

Relevant Network Background

It has two offerings, with the primary one being the full-featured VOS (formerly FlexVNF), which can be delivered on the Versa branch Cloud Services Gateways (CSG) or third-party hardware, along with the Versa Director and Versa Analytics. The second offering is Versa Titan, which is a simpler, cloud-based solution with limited native features. We expect Versa to make future investments in SASE, multicloud fabric and campus SD-LAN

Strengths

-
-
-

Cautions

-
-
-

Cisco Company Profile

Company Overview

Headquarters:
San Jose, California
United States

Maturity:
Founded: 1984
Headcount: ~75,000 (2019)
Reach: Global
Revenue: ~$59.1B

Relevant Network Background

It has one offering branded as Cisco SD-WAN powered by Viptela, which includes Viptela OS or IOS XE software with vManage orchestration. The other is Cisco SD-WAN, powered by Meraki, which includes MX appliances and software with orchestration. Cisco Umbrella can optionally be deployed for enhanced cloud security capabilities. We expect Cisco to make future investments in enhancing security capabilities, improving cloud visibility and using ML to optimize performance

Strengths

-
-
-

Cautions

-
-
-

Palo Alto Networks Company Profile

Company Overview

Headquarters:
Santa Clara, California
United States

Maturity:
Founded: 2005
Headcount: ~7,000 (2019)
Reach: Global
Revenue: ~$3.4 B

Relevant Network Background

Its offering is the CloudGenix SD-WAN with ION edge appliances and optional Prisma Access for integrated advanced security. Palo Alto Networks acquired CloudGenix during the past year. We expect Palo Alto Networks to make future investments in new form factors, SD-branch, SASE, automation and enhanced visibility

Strengths

Cautions

Silver Peak Networks Company Profile

Company Overview

Headquarters:
Santa Clara, California
United States

Maturity:

Founded:	2004
Headcount:	~400 (2020)
Reach:	Global
Revenue:	~$20.2 M for its first quarter of 2019

Relevant Network Background

Its products include the Unity EdgeConnect SD-WAN Edge Platform, which is composed of the Unity Orchestrator, EdgeConnect appliances, and an optional Unity Boost feature that enables WAN optimization. We expect Silver Peak to make future investments in enhancing analytics to improve troubleshooting, visibility and security, as well as orchestrate with third-party security solutions

Note: As of 13 July 2020, HPE announced its intention to acquire Silver Peak. Reflection of this acquisition is excluded from this research, because it occurred after the cutoff date for the analysis. This company has become part of HPE Subsidiary Aruba Networks as of September 2020

Strengths

-
-
-

Cautions

-
-
-

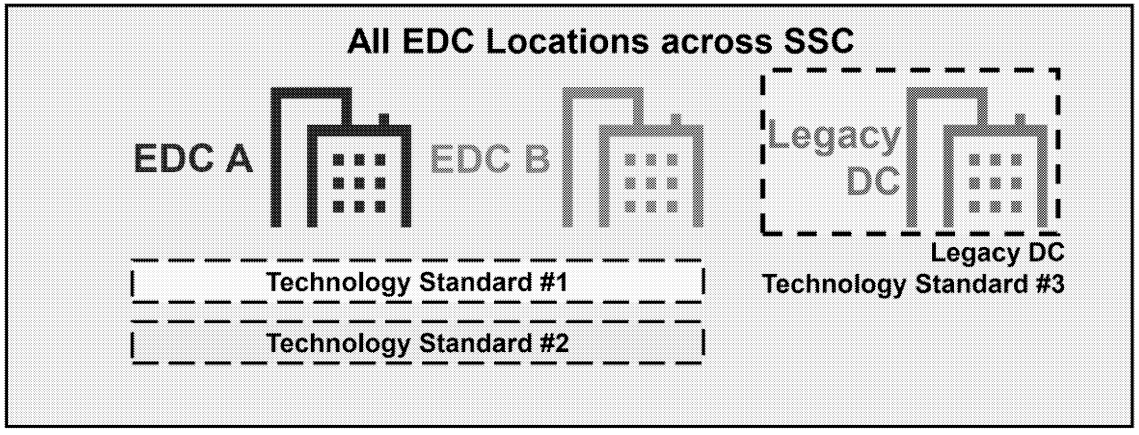
Gartner

Data Center Networking (DCN)

Gartner

SSC should establish dual DCN technology standards across its EDCs to promote competition and innovation

- Given that GoC Partner workloads stretch across 2 or more EDCs and that there is a strong operational, security and supportability requirement for given partner's workload to be hosted on a homogeneous DCN technology standard, SSC should establish technology standards that stretch across all EDCs.
- A dual-vendor strategy is desirable, however, to encourage competitive pricing and innovation. To that end, SSC should consider establishing two "DCN networks" present across all its EDCs, each based on a competitively established technology standard.
- Over time, GoC Partner workloads will be distributed, as evenly as possible, across these two "DCN networks"

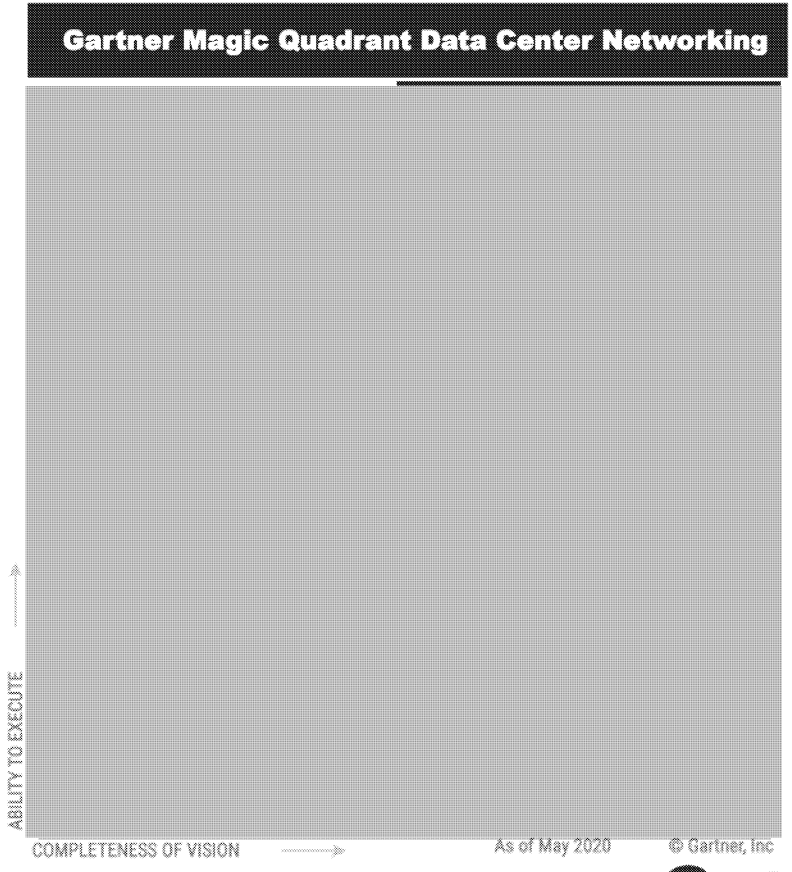


- As the two "DCN networks" technology standards are competed, SSC should consider single-vendor proposals, as well as joint proposals that could include distinct overlay and underlay vendors
- Each Legacy Datacentre has its own technology standard boundary, which may extend to also encompass a secondary datacenters where workload spans across DCs.
- The useful life of equipment in this area is about 5-7 years, which should align with the life cycle of the technology standards

Gartner

Leading Data Center Networking vendors are presented in this Gartner Research Magic Quadrant

- The primary business outcome of utilizing a Network vendor is local network connectivity within enterprise data centers to support cloud and cloud-inspired environments, delivered in an automated fashion with central management. These environments are highly virtualized (typically 80%) and increasingly containerized (often 10% and growing)
- A Leader has demonstrated sustained ability to address changing network requirements for enterprise data centers that underpin cloud and cloud-enabled infrastructures, including a complete product portfolio
- As it relates to future vision states, key areas of interest, include support for: Automation, including alignment with DevOps and infrastructure as code (IaC) principles, Hyperconverged infrastructure, Kubernetes and containers, Multicloud networking



Company Profiles of each of these vendors have been provided on the next pages

Gartner

Cisco Company Profile

Company Overview

Headquarters:
San Jose, California
United States

Maturity:
Founded: 1984
Headcount: ~75,000 (2019)
Reach: Global
Revenue: ~$59.1B

Relevant Network Background

Its offering includes fabric management via Application Policy Infrastructure Controller (APIC) or Data Center Network Manager (DCNM), Nexus switches, and associated tools including Network Assurance Engine (NAE) and Network Insights. We expect Cisco to make continued investments to expand analytics and assurance, and enhance existing multicloud offerings

Strengths

-
-
-

Cautions

-
-
-

Arista Networks Company Profile

ARISTA

Company Overview

Headquarters:
Santa Clara, California
United States

Maturity:
Founded: 2004
Headcount: ~2,300 (2019)
Reach: Global
Revenue: ~$2.41B

Relevant Network Background

Its offering is Universal Cloud Network (UCN), which includes 7000 series switches, Extensible Operating System (EOS), and CloudVision management and visibility platform. We expect Arista to make continued investments focused on as-a-service delivery and security enhancements

Strengths

Cautions

Gartner

Juniper Networks Company Profile

Company Overview

Headquarters:
Sunnyvale, California
United States

Maturity:
Founded: 1996
Headcount: ~9,400 (2019)
Reach: Global
Revenue: ~$4.4B

Relevant Network Background

Its primary offering in this market includes the QFX5000 and QFX10000 series switches, Junos OS and Contrail Enterprise Multicloud. We expect Juniper to make continued investments leveraging Mist to improve network autonomy, cloud-based management and 400 Gbps improvements

Strengths

-
-
-

Cautions

-
-
-

VMware Company Profile

vmware

Company Overview

Headquarters:
Palo Alto, California
United States

Maturity:
Founded: 1998
Headcount: ~31,000 (2019)
Reach: Global
Revenue: ~$8.7B

Relevant Network Background

Its flagship offering in this market includes NSX-T, a software-based network overlay, and vRealize Network Insight (vRNI) for management and troubleshooting. We expect VMware to continue investments in the areas of overlay/underlay management, security and predictive capabilities.

Note: Gartner notes that Vmware is actually in the visionary quadrant of its Magic Quadrant analysis but as it is a leader in WAN that it should be included in this analysis.

Strengths

-
-
-

Cautions

-
-
-

Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

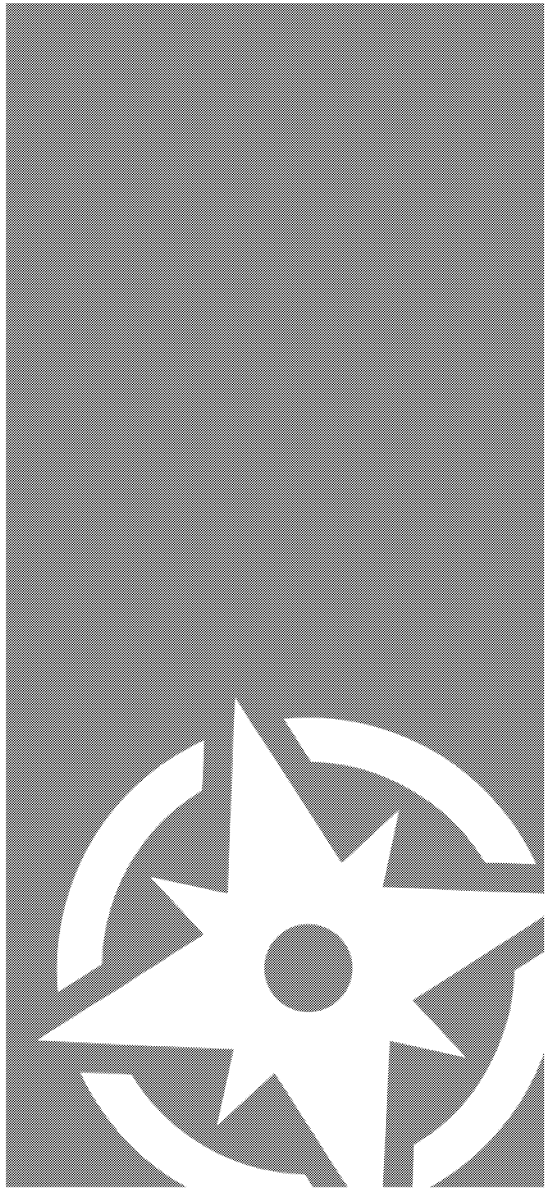
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix**



Gartner

Gartner analyzed Use Cases to better understand the network sourcing approach used by SSC and develop recommendations for improving the process

Selected Cases

Gartner reviewed the following Use Cases to find insights into current LAN, WAN, and DCN sourcing operations

1) — WAN upgrade and DCN spine

2) CCM/DCSL Data Centre — Workload Migration to EDC

3) Lester B. Pearson- Building LAN, Phase 1

Process/Analysis

- Review of documentation
- Understanding Alternatives
- Apply Network Sourcing Decision tree
- Validation with Gartner research
- Documentation of Findings

Outcome

Recommendations for use cases and future network sourcing, based on network sourcing decision tree

Documentation of rationale and supported quantitative impact for situations where the network sourcing decision tree is not followed

Gartner

Executive Summary of Use Cases

	Observations	Recommendations
[redacted] WAN upgrade and DCN spine	▪ The WAN components represent a modest incremental upgrade (less than 15% of SSC's WAN infrastructure within a FY, and addition of line cards in existing footprints) ▪ The DCN components are being procured to create a net new network "spine" at EDC [redacted], where a technology standard for DCN has not yet been established through competition	▪ Based on the decision matrix, Gartner recommends proceeding with the OEM-specific procurement of WAN equipment through the NSSC contracting vehicle * ▪ Based on the decision matrix, Gartner recommends proceeding with the OEM-specific procurement of DCN equipment through the NSSC contracting vehicle *

CCM/DCSL Data Centre [redacted] Workload Migration to EDC	▪ Modest incremental WAN upgrade to system and SSC can leverage existing footprint
	▪ Sizeable DCN requirement and the lack of a competitively established technology standard
		▪ Based on the decision matrix, Gartner recommends proceeding with the OEM-specific procurement of WAN equipment through the NSSC contracting vehicle *
		▪ Based on the decision matrix, Gartner would recommend an open and competitive procurement for the DCN requirement. However, given the significant business impacts of following an open and competitive procurement process for this requirement, it is expected that SSC will proceed with an OEM-Specific procurement through the NSSC instead, in order to avoid:
		  ▪ A financial setback estimated to be between $31.5MM and $51MM,
		  ▪ Significant delays (12-24 months) to these critical projects, and
		  ▪ Potential significant impact to these agencies and their services

Lester B. Pearson Building LAN, Phase 1	▪ This use case relates to a procurement that took place in 2020, for equipment that falls in the LAN area, as defined in the Network Sourcing Decision Aid section ▪ A major refresh of equipment in a building where a technology standard had not been set in recent years	▪ The approach followed by SSC is consistent with Gartner's recommendations found in the Network Sourcing Decision Aid section and sets the technology standard for LAN in this building/campus for the next 10 years

* Evaluate among the qualified vendors under NSSC, which was an open and competitive solicitation that established a procurement vehicle for network equipment and services

Gartner

Quantified impacts that could occur if a competitive RFP is held rather than an OEM-specific procurement through the NSSC for Use Case 2: CCM/DCSL Data Centre [redacted] Workload Migration to

Area	Quantified Impact	Estimated Costs
Team & Skills	▪ Difficulty in finding specialized IT skills in this environment will lead to trouble for SSC when filling required positions for additional workload. Doubling the current team would be required for new technology ▪ Impact on team with COVID-19 related issues and current workload for addressing additional work required for competitive RFP	▪ ~$2MM Full time employees (FTE) ▪ ~$2.5MM Professional Services DCN Operations (x2 Security)
Technical & Architecture	▪ Interoperability issues between current data state and future vendor ▪ Sunk costs — Storage, Computer equipment and software has already been purchased from current vendor and would be left unused for a period of 12-24 months if competitive RFP is required	▪ ~$20MM/year in Sunk cost
[redacted]		
Testing	▪ Diverting resources for testing of new system would mean multiple interruptions in other projects implementation; Multi-domain, multi-service-lines (Mainframe, Midrange, Storage, Facilities, Network, Security/ATO) ▪ Business Impacts of having a restricted change window from December through April ▪ Testing timeline extended by at least ~8 months to verify full and successful network integration	Timeline extension: 8 months
Facilities Carrying Costs	▪ CCM/DCSL costs incurred for power, support, and maintenance. The DCSL lease cannot be extended beyond May 2024 or SSC could face legal action ▪ [redacted] is currently an empty data hall awaiting new operations and would have unused capacity for 12-24 months ▪ EDC [redacted] ncremental cost of power/cooling (2x over E [redacted]. Growth is estimated for this facility at around 10%/yr.	▪ DCSL — $4.5MM/year ▪ Barrie — $2.5MM/year
Risks	▪ Cyber attacks on aging networks ▪ Existing contracting would suffer a cascading impact, as the sourcing plan was laid out at the start of the project with components designed to work together ▪ Inability to support business-driven workload growth	Information unavailable

Source: SSC

Gartner

Detailed Use Case Analysis

Gartner

Use Case 1: EDC [redacted] – WAN upgrade and DCN spine (page 1 of 3)

Description	Documents Reviewed
Network equipment purchase to add 10Gb longwave optical line cards in existing Cisco NCS2000 DWDM footprint, as well as associated software licenses, network encryption licenses, patch panels and fibre cables. The BoM also includes 30-port 100GE and 48-port 10GbE modules for existing Cisco Nexus 7700 data center switches, as well as acquiring new Cisco Nexus 9300 48+6 port switches with associated SFPs and transceivers. This equipment will be installed at EDC [redacted] and EDC [redacted] n order to provide encrypted DC-to-DC links between the two data centres as well as a DCN foundation for EDC [redacted]	▪ Bill Of Materials EDC [redacted] Annex_A_-_LoD_-_R000073858_-_EN.xlsx ▪ IPS_-_Technical_Justification_-_EDC [redacted] _Optical_73858.pdf

Alternative(s)
1. Acquire WAN equipment through an open procurement process. Doing so could result in the selection of an alternative vendor technology that would require new DWDM footprint, foregoing the existing capacity remaining in the Cisco NCS2000 (empty shelves) and introducing new tools and support processes, requiring training, as well as testing.
2. Split procurements with WAN (Cisco NCS2000) and DCN (Cisco Nexus) so that it is acquired separately, following established WAN and DCN standards.

Gartner

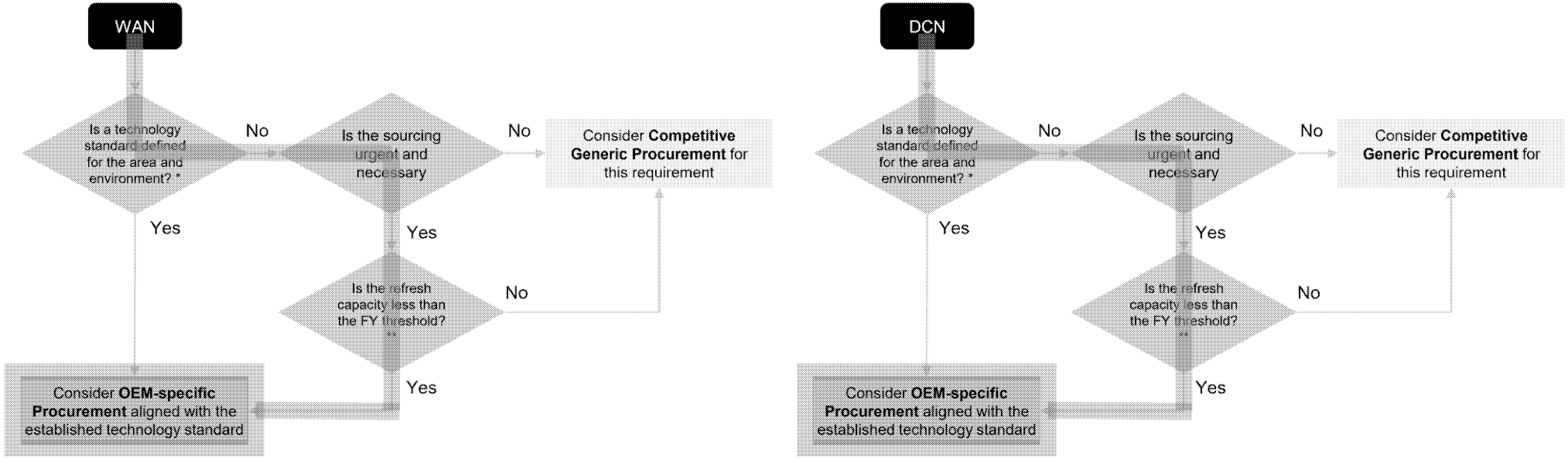
Use Case 1: EDC [redacted] — WAN upgrade and DCN spine (page 2 of 3)

Findings	Recommendations
This purchase mostly builds on existing frames at EDC [redacted] and EDC [redacted] except for the net new Nexus 7000 and 9300	Consider an OEM-specific procurement for both the DC WAN components, based on legacy compatibility, and for the DCN components, based on compatibility and integration with existing EDC [redacted] DCN equipment.
WAN equipment must match at both ends of the link, forcing further sole-source procurement decisions	Consider establishing an SSC-wide WAN standard (all EDCs and large facilities) through an open procurement process
Overall Comments	
Using untapped capacity by populating empty shelves/slots in existing equipment is the most cost-effective and viable way to address this requirement. Given that the DCN components acquired through this procurement represent a modest upgrade (amounting to about 5% of the DCN capacity established prior to FY20-21), an OEM-specific procurement is an efficient and effective way to address the requirement.	

Gartner

Use Case 1: EDC [redacted] — WAN upgrade and DCN spine (page 3 of 3)

Below are the paths and recommendations for this use case, using the network sourcing decision tree.



Gartner

Use Case 2: CCM/DCSL Data Centre (Workload Migration to EDC (page 1 of 3)

Description	Documents Reviewed
SSC has begun consolidating its 800 data centres to 7 new Enterprise Data Centres. As part of this effort, workload currently hosted at the legacy DCSL data center will be migrated to Enterprise Data Centers (EDC) located in and To this end, new infrastructure must be acquired at the target EDCs, including WAN (inter-data centre links and data optimization technology) and Data Center Networking (DCN) equipment. SSC has stated that this new infrastructure will need to be compatible with the existing solutions deployed at EDC and EDC Requirements include single point provisioning, central firmware deployment, multitenancy and virtualization automation, automatic fabric deployment, detailed role-based access control (RBAC), and multi-site compatibility. SSC selected Cisco and Riverbed products based on compatibility with legacy infrastructure.	▪ Bill Of Materials WLM CCM Riverbed_P2P 71968.xlsx ▪ Bill Of Materials WLM CCM WAN CIsco_R000073361_-EN.xlsx ▪ WLM CCM (DCSL) Legacy DC Closure — DCN P2P 70268.xlsx ▪ IPS_-_Technical Justification_-_Encryption P2P 73361 WLM CCM WAN Cisco.pdf ▪ technical-justification_for_Riverbed_Data_ Centres WLM CCM P2P 71968.pdf ▪ WLM CCM (DCSL) Legacy DC Closure DCN Tech JUSTIFICATION P2P 70268.pdf

Alternative(s)
1. Acquire equipment through an open procurement process could result in the selection of another solution. The selection of an alternate solution would result in additional training, testing and operating costs and would introduce greater operational risks. 2. Split procurements with WAN (Cisco and Riverbed) and DCN (Cisco) so that it is acquired separately, following established WAN and DCN standards.

Gartner

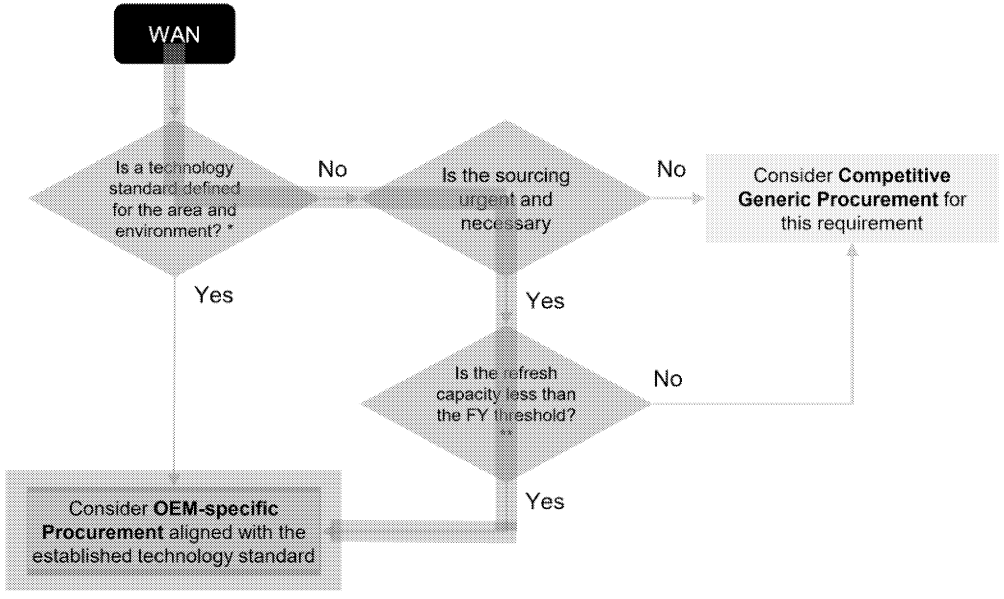
Use Case 2: CCM/DCSL Data Centre ( ) Workload Migration to EDC (page 2 of 3)

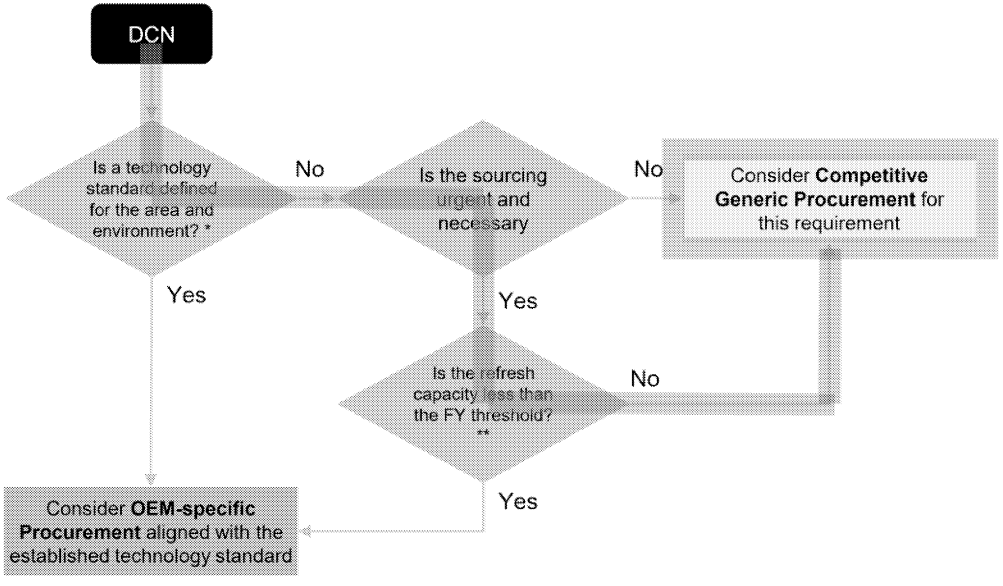
Findings	Recommendations
WAN components including Riverbed devices must integrate with legacy WAN infrastructure at other GoC sites.	• Consider an OEM-specific procurement of the WAN components based on legacy compatibility. • Consider soliciting bids for DCN components of this order.
In this large DC LAN footprint with over 50 switches, more than 90% of network connections are internal and there is limited connection to external legacy infrastructure. Based on the scale of this order, SSC could establish a separate solution support team. An open solicitation should recognize the operational value of continuing the use of legacy vendor technology, but a single vendor solution may not be a hard requirement.	Establish an SSC-wide standard for all EDCs and large facilities that sets out the rules for sole-sourcing components based on the relative cost of maintenance and the need to integrate with legacy solutions.
Overall Comments	
SSC must define a clear, transparent and detailed process to justify sole-sourcing of solutions, beyond this procurement.	

Gartner

Use Case 2: CCM/DCSL Data Centre ( ) Workload Migration to EDC (page 3 of 3)

Below are the paths and recommendations for this use case, using the network sourcing decision tree.





Gartner

Use Case 3: Lester B. Pearson Building LAN, Phase 1 (page 1 of 2)

Description	Documents Reviewed
Global Affairs Canada (GAC) headquarters at 125 Sussex Drive in Ottawa, is known as the Lester B. Pearson (LBP) Building. The building is undergoing a multi-year retrofit project, starting with Tower D in 2020. Shared Services Canada (SSC) will be implementing new LAN infrastructure as part of this retrofit project. SSC set-out a solicitation based on technical requirements with no specific bias toward one vendor's technology.	▪ Annex A — SOW — Generic R000070124.docx ▪ ANNEX B GENERIC BOM — LoD — Generic R000070124.xlsx ▪ Annex C — SoR — Generic R000070124.xlsx ▪ Annex D — ITP — Generic R000070124.xlsx ▪ Annex E — Test Results — Generic R000070124.xlsx

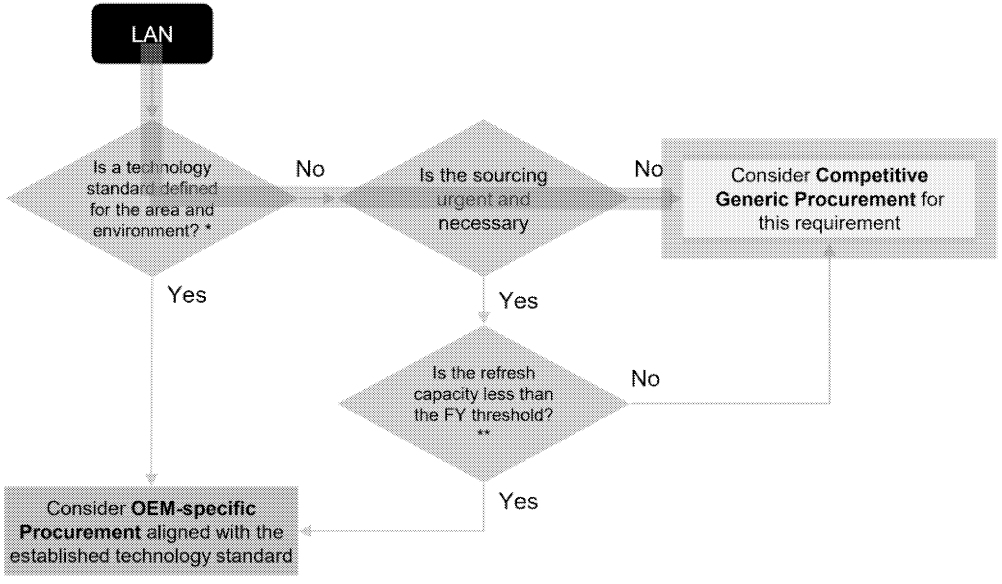
Alternative(s)
1. SSC could have defined Cisco equipment as a requirement based on compatibility with other similar GoC sites. This approach would have limited the diversity of bids, reduced the quality of the options, and by reducing competition could have resulted in a higher cost of the total solution.

Findings	Recommendations
SSC has created a competitive solicitation process which allowed direct comparison of vendor solutions, including use of OEM equipment.	The process used for the Lester B. Pearson Building should be applied to other stand-alone building LAN projects.

Overall Comments
Establishing an open solicitation process helps SSC to review competitive solutions and select the best solution at the best price. A building-by-building (or campus-by-campus) technology standard set through a competitive procurement rank highly in terms of transparency, fairness and value while minimizing technical interoperability concerns.

Use Case 3: Lester B. Pearson Building LAN, Phase 1 (page 2 of 2)

Below is the paths and recommendation for this use case, using the network sourcing decision tree.



Gartner

01 **Executive Overview**

02 **SSC Network and Security Strategy Benchmark Review**

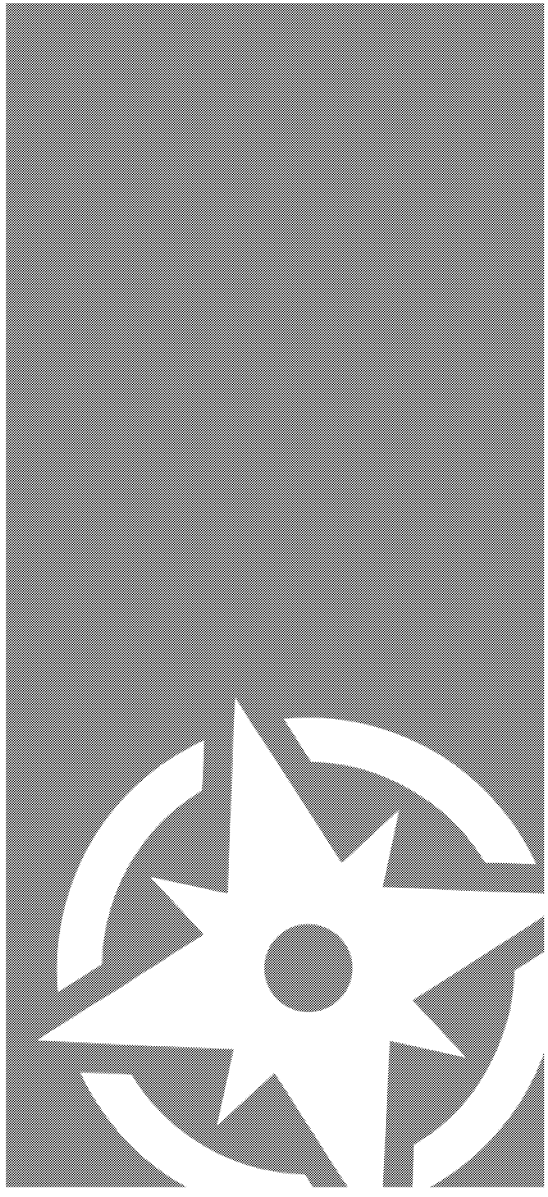
- Overall Content
- Activities
- Communication Concepts
- Discussion Document

03 **Network Sourcing Decision Aid**

- Stakeholder Insight
- Defining the LAN, WAN and DCN areas
- Technology Standards and Vendors

04 **Use Case Analysis**

05 **Appendix 1**



Gartner

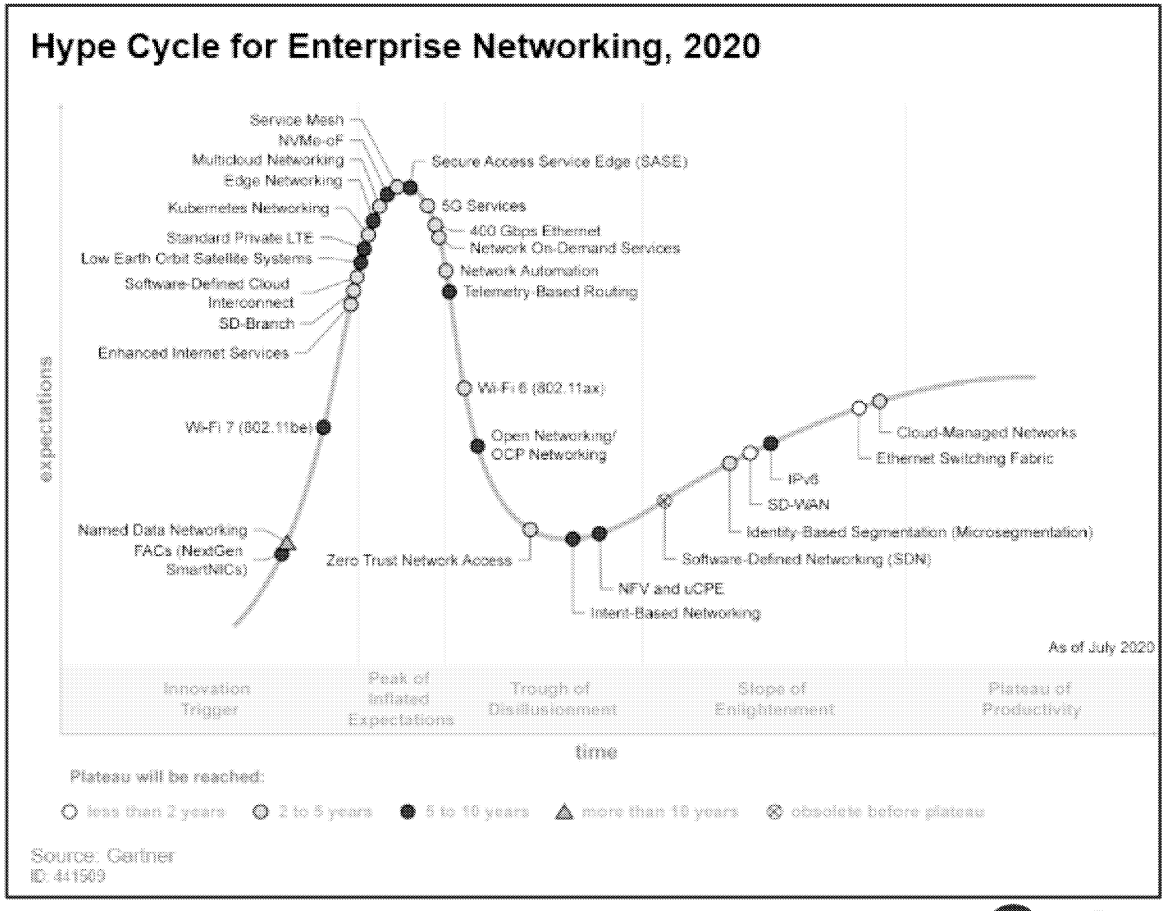
Gartner Research

Perspectives on emerging solutions

Gartner

Gartner Research — Hype Cycle for Enterprise Networking

- SSC Network and Security Strategy includes technologies discussed by Gartner;
  - SASE
  - 5G Services
  - Wi-Fi 6 (IEEE 802.11ax)
  - Zero Trust Network Access
  - Software-defined Networking (SDN)
  - Identity-based Segmentation
  - Software-defined WAN (SD-WAN)



Gartner

SSC Network and Security Strategy — Gartner Research of Technologies

Solution	Gartner Research
SASE	▪ By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.
5G	▪ Identify opportunities to pilot 5G networks and services to deliver innovation, based on current 5G capabilities
Wi-Fi 6	▪ Wi-Fi 6 (802.11ax) represents an opportunity to significantly improve performance for special use cases.
Zero Trust Network Access	▪ The benefits of ZTNA are immediate. Similar to a traditional VPN, services brought within the ZTNA environment are no longer visible on the public internet and, thus, are shielded from attackers
Software Defined Network (SDN)	▪ True SDN solutions have not had any significant market adoption. See Gartner recommendation details on Slide X
Software Defined Wide-area Network	▪ Refresh branch WAN equipment by implementing SD-WAN when migrating apps to the public cloud, building hybrid WANs; also when equipment is at end of life, or managed network service/MPLS contracts are up for renewal.
Identity-based Segmentation	▪ Identity-based segmentation is a form of zero trust networking and is used to reduce the "blast radius" if and when an attacker breaches the enterprise network by reducing the ability of the attacker to spread laterally. It also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads.

Gartner

Gartner Research — SASE

- **Definition:** Secure access service edge (SASE, pronounced "sassy") delivers multiple capabilities such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA).
  - SASE supports branch office and remote worker access. SASE is delivered as a service, and based upon the identity of the device/entity, combined with real-time context and security/compliance policies. Identities can be associated with people, devices, IoT or edge computing locations.
- **Position and Adoption Speed Justification:** SASE is driven by enterprise digital business transformation: the adoption of cloud-based services by distributed and mobile workforces; edge computing and business continuity plans that must include flexible, anywhere, anytime, secure remote access. While the term originated in 2019, the architecture has been deployed by early adopters as early as 2017. By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.
  - By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor, up from less than 5% in 2019. However, today most implementations involve two vendors (SD-WAN + Network Security), although single vendor solutions are appearing. Dual-vendor deployments that have deep cross-vendor integration are highly functional and largely eliminate the need to deploy anything more than a L4 stateful firewall in the branch office. This will drive a new wave of consolidation as vendors struggle to invest to compete in this highly disruptive, rapidly evolving landscape.
  - SASE is in the early stages of market development but is being actively marketed and developed by the vendor community. Although the term is relatively new, the architectural approach (cloud if you can, on-premises if you must) has been deployed for at least two years. The inversion of networking and network security patterns as users, devices and services leave the traditional enterprise perimeter will transform the competitive landscape for network and network security as a service over the next decade, although the winners and losers will be apparent by 2022. True SASE services are cloud-native — dynamically scalable, globally accessible, typically microservices-based and multitenant.

Gartner Research — 5G

- **Definition:** 5G services comprise local or wide-area cellular data connectivity based on 3GPP Release 15 or later, providing the next generation of cellular communications networking to follow 4G LTE. Providers will base services, such as new or enhanced end-user or IoT applications, on key 5G performance requirements of up to multigigabit mobile data throughput. Services will also be based on low-latency data transmission and support for massive deployment of machine-to-machine communications that are supported by Release 16 and later.
- **Position and Adoption Speed Justification:** 5G is the most-searched term among networking technologies considered for Gartner Hype Cycles, based on a composite metric comprising Gartner search, Gartner inquiry, and Google trends. As of 2Q20, more than 70 service providers globally had launched commercial fixed or mobile wireless services using 3GPP-compliant 5G technology, according to the Global mobile Suppliers Association (GSA). Expanding network availability will keep 5G services moving rapidly through the emerging state. However, coverage will grow slowly in some regions and service providers have identified few use cases requiring 5G performance capabilities instead of widespread alternatives such as Wi-Fi or 4G LTE. Ratification of the next two 5G technology specifications, Releases 16 and 17, expected in 2020 and 2022, respectively, will bring significant performance improvements beyond data throughput. These will support ultra-low latency, massive coverage density for low-powered IoT endpoints and network slicing.
- **User Advice**: 5G continues to suffer from immaturity, substantial hype and unrealistic expectations about features and availability sets, caused by infrastructure and service provider marketing. Enterprises must incorporate realistic networking assumptions for business plans by working with business leaders and network service providers to identify the availability of 5G at specific locations. Optimal 5G performance will require use of low- and midband cellular spectrum plus millimeter wave spectrum. We do not expect 5G using millimeter wave spectrum to become readily available outside of dense urban areas. Further, identify locations where available millimeter wave signals may encounter signal propagation challenges from obstacles such as building walls, window glass and heavy foliage.
  - Identify opportunities to pilot 5G networks and services to deliver innovation, based on current 5G capabilities, such as high-speed data. At the same time, identify applications where currently available service provider technologies (such as LTE-A) will support usage scenarios requiring up to 1 Gbps data speeds and latency up to 30 milliseconds.

Gartner

Gartner Research — Wi-Fi 6 (IEEE 802.11ax)

- **Definition:** Wi-Fi 6 (802.11ax) is the latest iteration of the IEEE 802.11 WLAN family. Its main enhancements are allowing the network to control device connectivity for the first time and to improve the efficiency of existing 2.4GHz and 5GHz spectrum, thereby increasing throughput in densely populated areas. As such, its goal is to support a larger number of devices including IoT that are properly connected to the network.
- **Position and Adoption Speed Justification**: IEEE, the standards body of 802.11-based technologies, started the High Efficiency WLAN (HEW) Study Group in May 2013 to examine the most pressing needs for the next-generation Wi-Fi technology. Ratification of the new Wi-Fi 6 (802.11ax) standard was expected in late 2019 but was delayed until 2020 and perhaps longer due to COVID-19. Prestandards-based networking equipment has already been released by a majority of the key/leading vendors. Successive Wi-Fi technologies have increased per-device throughput at an impressive rate through the years (from 802.11b's 11 Mbps to 10 Gbps expected from the new standard).
  - The number of IoT devices and the convergence of building automation and line of business devices onto the enterprise communication infrastructure continues to contribute to congestion. 802.11ax will be able to more intelligently use network resources instead of letting the device make connectivity decision as previous versions of the standard allowed. Advancements allow differing streams to communicate to multiple devices simultaneously as well as cutting latency by as much as 75%.
- ***User Advice**:* We advise clients not to pay a premium for any adoption of Wi-Fi 6 (802.11ax) unless existing wireless solution do not provide the performance and functionality needed to meet defined end-user requirements.
  - For IT leaders, Wi-Fi 6 (802.11ax) represents an opportunity to significantly improve performance for special use cases such as dense device deployments, they are advised to monitor the standardization timeline and product availability to find the right entry point for future infrastructure upgrades as well as availability of client devices that will support the new standard.
  - We advise clients that "Wi-Fi 6 certification" currently does not mean 802.11ax compliant since the standard is not ratified. Any organization that purchases prestandard products should have the ability to upgrade or update their product at no cost to be standards compliant.

Gartner

Gartner Research — Zero Trust Network Access (ZTNA) (1 of 2)

- **Definition:** Zero trust network access (ZTNA) creates an identity- and context-based, logical-access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access, and prohibits lateral movement elsewhere in the network. This removes the application assets from public visibility and significantly reduces the surface area for attack.
- **Position and Adoption Speed Justification:** ZTNA is a synthesis of concepts promulgated by the Cloud Security Alliance's software-defined perimeters (SDP) project, by Google's BeyondCorp vision, and in O'Reilly's *Zero Trust Networks* book. Early products on the market tended to focus on use cases involving access to web applications. Newer, more complete products work with a wider range of applications and protocols.
- As more organizations suddenly find themselves transitioning to much more remote work, hardware-based VPNs exhibit limitations. ZTNA has piqued the interest of those seeking a more flexible alternative to VPNs and those seeking more precise access and session control to applications located on-premises and in the cloud. ZTNA vendors continue to attract venture capital funding. This, in turn, encourages new startups to enter an increasingly crowded market and seek ways to differentiate. Merger and acquisition (M&A) activity in this market is underway, with several startup vendors now having been acquired by larger networking, telecommunications and security vendors.
- **User Advice:** Organizations should evaluate ZTNA for any of these use cases:
  - Opening up applications and services to collaborative ecosystem applications, such as distribution channels, suppliers, contractors or retail outlets without requiring the use of a VPN or DMZ.
  - Normalizing the user experience for application access — ZTNA eliminates the distinction between being on and off the corporate network.
  - Application-specific access for IT contractors and remote or mobile employees as an alternative to VPN-based access.
  - Extending access to an acquired organization during M&A activities, without having to configure site-to-site VPN and firewall rules. The merged companies can quickly and easily share applications without requiring the underlying networks and/or identity systems to be integrated.

Gartner Research — Zero Trust Network Access (ZTNA) (2 of 2)

  - Enabling users on personal devices — ZTNA can improve security and simplify bring your own device (BYOD) programs by reducing full management requirements and enabling more-secure direct application access.
  - Cloaking systems on hostile networks, such as systems facing the public internet used for collaboration.
  - Carrying encryption all the way to the endpoints for scenarios where you don't trust the carrier or cloud provider.
  - Permitting users in potentially dangerous areas of the world to interact with applications and data in ways that reduce or eliminate risk prone to originate in those areas.
  - Securing access to enclaves of IoT devices if the device can support lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.
- **Business Impact:** The benefits of ZTNA are immediate. Similar to a traditional VPN, services brought within the ZTNA environment are no longer visible on the public internet and, thus, are shielded from attackers. In addition, ZTNA brings significant benefits in user experience, agility, adaptability and ease of policy management. For cloud-based ZTNA offerings, scalability and ease of adoption are additional benefits. ZTNA enables digital business transformation scenarios that are ill-suited to legacy access approaches. As a result of digital transformation efforts, most enterprises will have more applications, services and data outside their enterprises than inside. Cloud-based ZTNA services place the security controls where the users and applications are — in the cloud. Some of the larger ZTNA vendors have invested in dozens of points of presence worldwide for low-latency access.
- Benefit Rating: Moderate
- Market Penetration: 5% to 20% of target audience
- Maturity: Adolescent
- Sample Vendors: Akamai; AppGate; Cato Networks; Cisco; Netskope; Perimeter 81; Proofpoint; Pulse Secure; SAIFE; Zscaler

Gartner Research — Software-defined Networking (SDN) (1 of 2)

- **Definition**: Software-defined networking (SDN) is an architectural approach to designing, building and operating networks that promised increased agility and extensibility by abstracting the network topology and control plane. However, SDN products never made it to mainstream enterprise adoption. Rather, SDN spawned innovations in automation, orchestration, segmentation and the disaggregation of network hardware and software.
- Position and Adoption Speed Justification: SDN remains a major topic of discussion across multiple network markets and in many vendor marketing efforts. However, true SDN technologies have not achieved any significant enterprise market traction and should not be considered by any enterprise networking organization. The hope that SDN would allow for the decoupling of the control plane from network hardware and foster independent software innovation never came to fruition and there are effectively no SDN technologies available in the mainstream marketplace today.
  - While true SDN solutions have not had any significant market adoption, the development of SDN and the threat to established market players had a profound, positive effect on subsequent market developments. SDN clearly influenced the increasing use of white-box switches, the open-source hardware and software movement (supported by the Open Compute Project) and the development of independent network switch software providers. More important to the enterprise market was a shift in focus of traditional network vendors innovation around operations and management. This has led to improvements in agility and automation, simplified operational requirements and a general adoption of function-wide configuration (i.e., management that spans devices in a data center, campus or WAN environments). Without the threat of SDN it is unlikely the operational advances from traditional vendors would have occurred.
- **User Advice:** While SDN is clearly obsolete in the enterprise market there are still many organizations that site SDN as a cornerstone of their future strategy and architecture. What is critical for enterprises is to understand what they are trying to accomplish when they think "SDN."

Gartner

Gartner Research — Software-defined Networking (SDN) (2 of 2)

- **User Advice (continued):**
  - Don't get caught up in the hype and vendor claims that commercial products are SDN or engage in any planning to deploy SDN.
  - Focus on the desired outcomes you are trying to achieve such as increased automation, virtual segmentation, external orchestration.
  - Select an operational/automation framework first — then decide on networking vendors and products.
  - Evaluate both hardware infrastructure and software overlays approaches.
  - Develop cross-functional collaboration and investigate methodologies to better integrate server, virtualization, network, security and application teams.
- **Business Impact**: There is no direct commercial impact of full SDN solutions. However, downstream innovation can increase network agility, simplify management, improve security and lead to reductions in operational and capital costs while fostering cross-functional collaboration. New network solutions should focus on reducing or eliminating the "human middleware" problem that has plagued traditional network solutions for the past two decades. By bringing network operations into more streamlined and automated operational process that have been architected in the virtual compute environment, user organizations can bring application deployments in line with the increasing speed of business. Available network overlay technology can create new competitive environments shifting the focus from physical infrastructure to software and operational features.
- **Benefit Rating:** Low
- **Market Penetration:** Less than 1% of target audience
- **Maturity**: Obsolete
- **Sample Vendors:** NEC
- **Recommended Reading**: "State of SDN: If You Think SDN Is the Answer, You're Asking the Wrong Question"

Gartner

Gartner — Identity-Based Segmentation (Microsegmentation)

- **Definition:** Identity-based segmentation (also referred to as microsegmentation, zero trust network segmentation or logical segmentation) uses policy- and workload-identity-driven firewalling (typically software-based) or differentially encrypted network communications to isolate workloads, applications and processes in data centers, public cloud IaaS and containers. This includes workloads that span on-premises and multiple public cloud IaaS providers.
- **Position and Adoption Speed Justification:** With more servers being virtualized or moving to infrastructure as a service, traditional firewall, intrusion prevention, and antivirus rarely 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 further segmentation and zero trust networking based approaches for east-west traffic between applications, servers and services in modern data centers. The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies complex, if not impossible, to apply. Further, the shift to microservices container architectures for applications has also increased the amount of east-west traffic and further complicated the ability of network-centric firewalls to provide this segmentation. The extension of data centers into public cloud also has placed a focus on software-based approaches for segmentation, in many cases, using the built-in segmentation capabilities of the cloud providers.
- **User Advice**: Security and risk management leaders should use the following guidelines when implementing identity-based segmentation:
  - Don't oversegment. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.
  - Don't use IP addresses or network location as the foundation for segmentation policies.
  - Start with a network flow mapping project to understand application and server flows before undertaking the segmentation project.
  - Apply continuous adaptive segmentation. Start with new assets, then close existing gaps.
  - Adopt a risk-based approach and look beyond technical considerations when segmenting.
  - Architect for consistent segmentation policies across on-premises and public cloud IaaS.

Gartner

Gartner Research — Software-defined WAN (SD-WAN)

- **Definition:** Software-defined wide-area network (SD-WAN) products replace traditional branch routers. They provide several features: dynamic path selection, based on business or application policy; centralized policy and management of WAN edge devices; and zero-touch configuration. SD-WAN products are WAN transport/carrier-agnostic, and can create secure paths across multiple WAN connections. SD-WAN products can be hardware- or software-based, and managed directly by enterprises or embedded in a managed service offering.
- **Position and Adoption Speed** Justification: Rampant client interest in SD-WAN products continues, and we estimate that more than 25,000 customers have deployed SD-WAN products in production networks, which is over 600,000 branch locations. We expect continued rapid growth of SD-WAN deployments, and forecast vendor revenue to grow at a more than 23% compound annual growth rate (CAGR) for the next three years. In conjunction with a hybrid WAN topology, SD-WAN improves availability, cost and performance for enterprise WANs. Organizations moving to hybrid or internet-only WAN transport are driven toward SD-WAN products, because of their improved path selection functionality and manageability. Large numbers of vendors (several dozen) are competing in the market, including incumbent network and security vendors, startup vendors and smaller vendors with regional or vertical focus.
- **User Advice:** Networking leaders should refresh their branch WAN equipment by implementing SD-WAN when they're migrating apps to the public cloud, building hybrid WANs, equipment is at end of life, or managed network service/MPLS contracts are up for renewal. Follow a comprehensive SD-WAN selection process by evaluating a diverse set of vendors and running a pilot. This is particularly important now, because not all offerings on the market are stable and scalable. Include network security teams in the design, planning and implementation, because SD-WAN-enabled hybrid WANs directly affect placement of security controls, such as firewalls and secure web gateways (SWGs).

Gartner

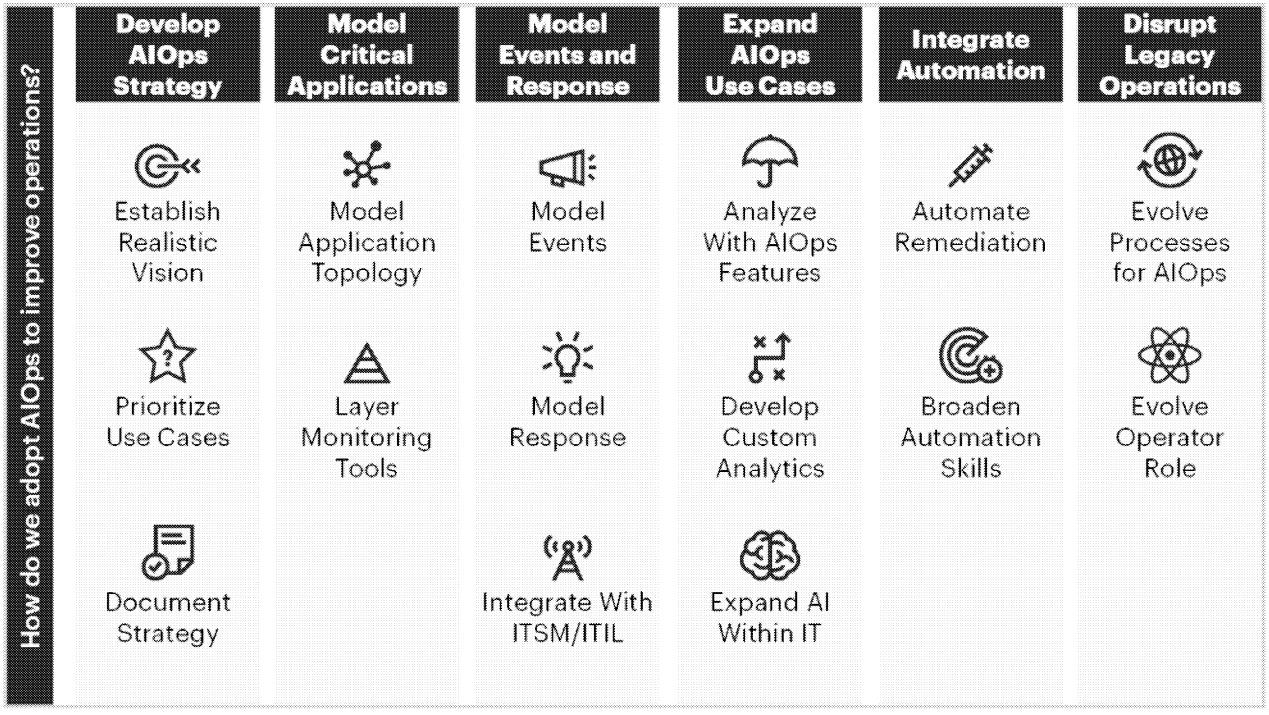
Gartner Research – Solution Path for Adopting AIOps, 1 Dec 2020

- AI promises to revolutionize IT operations, but most teams struggle to see through the hype to pragmatic use cases and the right tools. I&O technical professionals should use this Solution Path to clarify their approach to AIOps adoption by layering AIOps tools, platforms and features
- **Key Findings**
  - Ambiguity and hype around the term "AIOps" is the biggest obstacle in establishing an impactful vision and successful strategy for AI in IT operations.
  - The countless potential applications of AI in IT operations require prioritization and focus on high-value use cases.
  - Maximizing the impact of AIOps will require multiple, often overlapping, tools and technologies. There is not one unifying product, platform or approach currently in the market — and there probably never will be.
  - Practical applications of "intelligent automation" are far less intelligent than the term implies.
  - Most AIOps practices are built around traditional operations. The truly transformational impact of AI on IT operations is still in the future.
- **Recommendations**
  - Technical professionals seeking to leverage AI to improve IT operations should:
  - Develop an AIOps strategy that maps the prioritized use cases and the layered set of tools that solves the individual challenges of each use case.
  - Integrate traditional monitoring, modern observability and advanced analytics to establish an operational model that manages applications and services, rather than components and resources.
  - Expand the automation portfolio to create more intersections between AIOps and automation.
  - Maximize AIOps impact by adapting IT processes and operations that cannot be automated.

Gartner

Gartner Research – Solution Path for Adopting AIOps, 1 Dec 2020

Solution Path for AIOps



Source: Gartner
731459_C

Gartner

Service Management Metrics – Examples from list of over 100

Reference: "IT Performance Management Toolkit Tactics and Tools for Improving IT Metrics Maturity" CEB a Gartner Company

Provisioning

- New Employees
- New Sites
- New Workstations
- New Applications
  - New SaaS Services
- Installs – Time to Install
  - Circuits, Switch, Router, Firewall
- On-time delivery (%)

Maintenance

- Time between Failures
- Site Visits
- Maintenance Staffing
- Time between Failures
- Service Availability (%)

Project Management

- Project on time (%)
- Projects on Budget (%)
- Projects meet goals (%)

Change Management

- Number of CAB Changes
- Changes on-time, on-budget
- Changes successful (%)

Incident + Problem

- Incidents/Outages
  - SSC identified (%)
- Incident Response Time
- Mean Time to Repair
- Problems – (e.g., Recurring Incidents)
- Root Cause Analysis – Delivery on-time

Configuration

- Assets in CMDB %
- Time to add Assets to CMDB

Service Desk

- Average Time to Answer
- First Call Resolution
- Self-service resolution

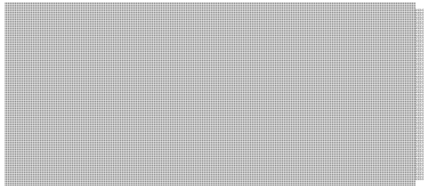
Customer Satisfaction

- Average "Usefulness Score" on Web Portal FAQs
- Average Sentiment Score

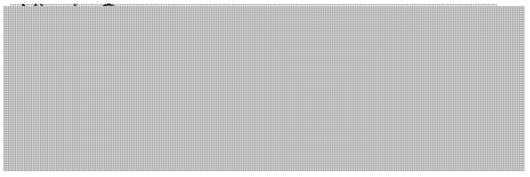
Gartner

Contacts

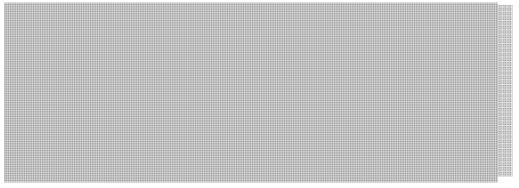
Gartner



Gartner



Gartner



Gartner