UNCLASSIFIED

Network and Security Strategy

Network and Security Architecture
Digital Enablement
Chief Technology Officer Branch

Version: 1.9

Shared Services Canada
Services partagés Canada

Canada

Document Approvals

Don Messier
Director General, Digital Enablement
Chief Technology Officer Branch
Shared Services Canada

Date

Raj Thuppal
Chief Technology Officer
Chief Technology Officer Branch
Shared Services Canada

Date

Patrice Nadeau
Assistant Deputy Minister, Networks and Security
Networks, Security and Digital Services Branch
Shared Services Canada

Date

Document Change Control

Version	Date of Issue	Author(s)	Description of Change
0.1	May 13, 2020	C Johnson, K Galbraith, Q Walajahi, B McKittrick, C Parsons, Deloitte	Initial Document creation
1.0	May 19, 2020	Chris Johnson	Updates, post internal team review
1.1	May 28, 2020	Chris Johnson	Updates, Dir. review
1.2	Jun 26, 2020	Chris Johnson	Updates/Changes from review input
1.3	July 3, 2020	Chris Johnson	Updates based on Treasury Board of Canada Secretariat (TBS), Communications Security Establishment Canada (CSEC), SSC and internal team feedback. Feedback provided by: - Chris Wharram, NSDS, SSC - Po Tea-Duncan, TBS - Mario Lefebvre, CCCS, CSEC
1.4	July 14, 2020	Chris Johnson	Internal Digital Enablement Revisions
1.5	Sept 1, 2020	Chris Johnson and Brian McKittrick	Updates based on CTO and DG feedback.
1.7	Oct 23, 2020	Chris Johnson	Updates post tech writer review and other stakeholders including: - Michel Fortin, NSDS, SSC - John Bain, EA, CTOB, SSC - Marty Gratton, NSDS, SSC
1.8	Nov 20, 2020	Chris Johnson	Updates post Digital Enablement internal feedback
1.9	Feb 5, 2021	Chris Johnson	Changes and revision from Gartner review

Table of Contents

1. Executive Summary 2

1.1. Connectivity 4

1.2. Identity and Access Control 5

1.3. Monitoring 5

1.4. Provisioning Approach 5

2. Introduction 7

2.1. Purpose 7

2.2. Audience 7

3. Strategy Rationale 8

4. Business Drivers and Other Challenges 9

5. Current State of Networking and Security within the GC 11

6. Emerging Industry Trends 13

6.1. Zero Trust Architecture (ZTA) 13

6.2. Work from Home and Secure Remote Access 14

6.3. Software-Defined Infrastructure 14

6.3.1. SD-LAN - Edge Network - Office / Building LAN Services 15
6.3.2. Remote Access—Software-Designed Perimeter 16
6.3.3. Software-Defined Wide Area Network (SD-WAN) 16
6.3.4. GC Backbone and Cloud/Internet Access –SD-WAN 17
6.3.5. Enterprise Data Centre and Core Network Services (SDDC and SDN) 18

6.3.5.1. Software-Defined Data Centre 18

6.3.5.2. Software-Defined Network (SDN) 19

7. Adoption Roadmap 20

7.1. Strategic Pillars 20

7.2. Pillar 1: Connectivity 21

7.2.1. Overview 21
7.2.2. Current State 21
7.2.3. Future State 23
7.2.4. Implications and Dependencies 25

7.3. Pillar 2: Identity and Access Control 25

7.3.1. Overview 25
7.3.2. Current State 26
7.3.3. Trends 26
7.3.4. Future State 27
7.3.5. Implications and Dependencies 27

7.4. Pillar 3: Monitoring 28
7.4.1. Special Consideration Regarding Security 28
7.4.2. Overview 29
7.4.3. Current State 29
7.4.4. Trends 29
7.4.5. Target State 30
7.4.6. Implications and Dependencies 31
7.5. Provisioning 31
7.5.1. Overview 31
7.5.2. Current State 31
7.5.3. Trends 32
7.5.4. Future State 32
7.5.5. Implications and Dependencies 33
7.6. Considerations 33
7.6.1. Re-skilling and Re-tooling the Organization 33
7.7. Recommended Next Steps 35
7.8. The Principles 35
7.9. Communication Plan 35
7.10. Reference Architectures 36
7.11. Support Existing Initiatives 36
7.12. Required Future Initiatives 39
8. Conclusion 40
9. Acronyms 41
10. References 42
Appendix A—Network and Security Trends 43
Trend #1—Zero Trust Architecture 43
Trend #2—Software-Defined Perimeter 44
Trend #3—Micro-segmentation 44
Trend #4—Secure Access Service Edge 45
Trend #5—Security Operations, Automation and Response 46
Trend #6—Artificial Intelligence Operations 47
Trend #7—Network Managed Services (SD-WAN) 48
Trend #8—Internet of Things 49
Trend #9—Private 5G 50
Trend #10—Multi-Cloud Networking 51
Trend #11—Networking on Demand 51
Appendix B—Network and Security Roadmap 53
Appendix C—In-Flight Projects 54

1. Executive Summary

The Government of Canada (GC) is about to undertake one of its largest technology transformational changes in decades as it begins the process of consuming cloud-based services from both a computing and a software perspective. These transformation requirements are similar to what is taking place throughout industry. Industries such as retail chains, banks and hotel chains are all undertaking similar network and security transformations to leverage the advantages of using cloud-based solutions to support their core business. The reality that Shared Services Canada (SSC) must support a wide variety of businesses (40+) makes it even more challenging. Owing to this variety, SSC needs to focus its network and security strategy on those network and security requirements that are common to all businesses.

Today, general expectation is to be able to be online at any time, regardless of the demand and/or circumstances, since almost all government employees require information technology (IT) to provide their services. The variety of services requiring secure network connectivity is also expanding. The use of cloud, Internet, collaboration, video/web conferencing and secure-remote access services have exploded throughout the GC in recent years. Providing faster, secure and more reliable network infrastructure will be even more important as current and new services are expected to continue to grow in the future.

Recent events have raised awareness of the need to support flexibility in working requirements to support significant percentage of employees working from home and using other remote access options.

The growing use of these new cloud-based services will increase the attack surface for government infrastructure and applications and therefore, SSC must review how it approaches its delivery of network and security services to support GC departments and agencies in delivering their services to Canadians.

The key business drivers for the updated SSC Network and Security strategy are:

- Increase the operational efficiency of the delivery and management of network and security services moving forward.
- Define a network platform that allows for seamless end user mobility—anytime/anywhere from GC-approved devices with special consideration for secure remote access and work from home.
- Enhance the overall security posture of network services.
- Increase network performance to enable the next generation of network services.
- Improve resiliency of the overall network platform, thereby reducing the number of incidents and outages.
- Define an open-standards approach to the future-state network, reducing vendor lock-in.
- Extend the life cycle of existing assets through optimization of IT asset refresh cycles.

- Enhance stewardship of security by providing visibility and control over network assets and services.
- Implement the fundamentals to gradually implement the concept of Network-as-a-Service.

The need for the revised strategy is further reinforced by looking at the data that traverses the government networks—everything from personal information the Canada Revenue Agency keeps for every Canadian, to the Royal Canadian Mounted Police's policing information, and beyond. The advent of foreign state-sponsored actors undertaking sophisticated attacks on government assets requires the Canadian government to undertake a fundamental redesign of how they secure networks and transport data to employees and Canadians alike.

The future design and provision of network services will also require SSC to take a different approach to security. Organizations globally are moving to a new model of securing the network based on the premise of "don't trust but verify", referred to as Zero Trust Architecture (ZTA), which alters the security paradigm from the old protect-the-perimeter (also known as castle-and-moat) to the newer idea of protecting the data flow from end to end or user to application.

SSC is refreshing its Network and Security Strategy to align with current best practices, and to be adaptable to future requirements for its network and security services. Technologies, such as cloud computing, Internet of Things (IoT), and 5th Generation Digital Cellular (5G) Network services, are examples of the emerging technologies with which government infrastructure needs to integrate. These technology trends will require SSC to rethink how it architects, provides, manages and secures its network services, and must be agile enough to integrate any technology that is deemed necessary to government operations.

To develop this Network and Security Strategy, new approaches focused on automation, software-defined infrastructure (SDI) and a zero trust concept are required. The foundational pillars in this document are the underpinning for these new approaches, and are the focus of this strategy.

The foundational pillars are:

1. **Connectivity**—featuring the technology components (e.g., switches, routers, firewalls and load balancers) that make up the fabric of SSC networks, and covering internal and external access to these networks.
2. **Identity and Access Control**—featuring the authentication and authorization needed for users and devices to interact with and connect to GC resources.
3. **Monitoring**—featuring both performance- and security-related needs for continuous monitoring to enable different monitoring capabilities to drive eventual automated response.

A new **Provisioning Approach** must also be adopted to meet advances in technology and user expectations for timely service delivery. Services are expected to be provided in hours or days, and not weeks or months. Leveraging SDI to enable provisioning of network and security infrastructure is a key enabler of this approach.

Underpinning this recommendation is the need for advanced skills in areas including cloud management, cloud security, artificial intelligence, networking, security and automation. SSC will need to consider how it can create a valuable proposition that attracts resources with valued skillsets and enables their retention.

The Network and Security Strategy defines the approach SSC will need to undertake to enable the government to meet the demands of today, and adapt to the demands of the future by leveraging a progressive adoption and migration overall strategy.

To implement this strategy, the following strategic principles are recommended:

1. 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.
2. Commence, prioritize and sequence critical foundational capabilities for early delivery. What initiatives will get SSC to its desired end state?
3. Do not try to implement a big bang solution. This will be an evolution using current projects and refresh cycles, starting small and starting to use technology SSC already has.
4. Consider investing in automation and orchestration of technology SSC already supports.
5. Address the need for integration between security and network functions early as a critical change management activity.
6. Address skills gap within workforce to keep up with the ever -hanging technologies and skill requirements (e.g., programming).

1.1. Connectivity

The foundations of this pillar feature the technology components (e.g., switches, routers, firewalls and load balancers) that make up the fabric of the GC networks, and covers internal and external access to these networks. SSC will see several emerging technologies become a major part of its connectivity strategy moving forward:

- 5G, which is poised to fundamentally change how network services are delivered to consumers and enterprises. 5G has significantly higher bandwidth (capacity) and lower latency than older wireless technologies, such as 4G or LTE.
- Redesigned remote access services, moving to better support the anywhere/anytime network access concepts evolving in the modern workplace.
- The need for high-speed, low-latency and secure access to cloud services being enabled through SSC's Secure Cloud Enablement and Defence (SCED) program.
- Implementing new ways of providing access to GC wide-area network (WAN) and Internet services through software-defined WAN (SD-WAN).
- Software-defined local-area network (LAN) technologies will enable the efficient and timely instantiation of new workplaces and the effective segmentation of the various GC-user networks.

Progressive integration of these technologies, the emerging ones in particular, will establish the foundation for the "go-forward" network SSC is looking to build.

1.2. Identity and Access Control

Identity and access control refers to the authentication and authorization required for users and devices to interact with, and connect to, GC technology resources. Identity and access control will integrate with ZTA to fundamentally change how platforms and data are secured. In the ZTA model, everyone is viewed as a threat unless proven otherwise. The core benefit of this framework is that it enables organizations to secure internal and external users across the network. The complexity is that this model requires SSC to fundamentally redesign the core network and technology components and consolidate the identity services within GC networks with the objective of moving to a single identity for employees and another for external users.

1.3. Monitoring

Continuous monitoring and how it addresses both performance and security-related needs means the future network services will also require different monitoring capabilities. SSC will need to adopt a suite of tools to enable effective monitoring of its network, platform and data assets. This will include how SSC leverages products from cloud and third-party technology providers to create a pool of data for predictive analysis of threats, performance and availability challenges. Leveraging platforms such as Artificial Intelligence Operations platforms (AIOps) will enable SSC to derive deep insights and drive automated response to incidents. SDI / software-designed network (SDN) will be a critical enabler for adopting AIOps.

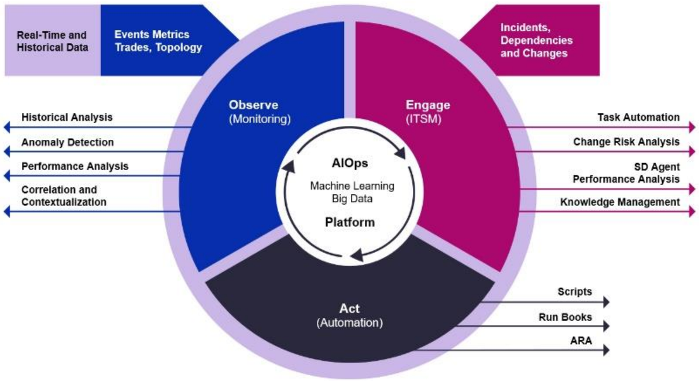


Figure 1: AIOps Platform Enabling Continuous Insights Across IT Operations and Monitoring

1.4. Provisioning Approach

The way the GC currently provisions infrastructure needs to adapt to meet advances in technology and user expectations of timely service delivery. Increasingly, partner departments will expect, based on comparable public offerings, services to be stood up in hours, not weeks or months. SSC will need to leverage SDI/SDN to enable the provisioning of network resources to meet expected demands.

The Network and Security Strategy defines the approach SSC will need to undertake to enable the government to meet the demands of today, and to adapt to the demands of the future by leveraging a progressive adoption and migration overall strategy. To implement this strategy, SSC will need to develop a cohesive set of requirements and reference architectures for the enabling technologies and frameworks defined within this document, and accelerate the procurement of products and services to enable the strategy.

2. Introduction

2.1. Purpose

The purpose of this document is to expand on the *SSC Future Network and Security Vision*, which establishes the future vision for SSC, essentially outlining the integration of SDI and ZTA. This document will attempt to elaborate on that premise, and consider the strategy and roadmap that SSC should undertake to uplift network and security services, address emerging technology and security trends, and operationalize the principles outlined in SSC 3.0.

This document was developed leveraging a number of key inputs from both within SSC and the broader GC, security trends and emerging practices, and through interviews with SSC and Treasury Board of Canada Secretariat (TBS) stakeholders.

2.2. Audience

The audience for this document includes the IT Security Tripartite, departmental chief information officers (CIO), the Canadian Centre for Cyber Security's (CCCS) executives and SSC service lines.

3. Strategy Rationale

With the rapid pace of infrastructure technology advancement, SSC requires a new approach to managing and operating the SSC network and security environment. The current approach will not scale to meet these demands. It is challenging for the workforce to keep pace with these changes as technology advancements are outpacing the available skills required.

Not only is technology evolving too quickly to keep pace, new threat vectors and security breaches are occurring so often that information technology (IT) staff cannot respond quickly enough to address them. Increased user mobility and connectivity from outside of the physical data centre (DC) lends itself to even more challenging security containment, not to mention workloads that are migrating to the public cloud, raising the bar even higher. IT staff cannot respond quickly enough, since they don't have the right information available to make informed decisions. Better monitoring, encompassing broader data collection (including security events, network events, identity/access management and network performance metrics) is required to ensure sufficient visibility across the enterprise.

IT as a whole has become much more complex. This increased complexity has resulted in negative impacts on the provisioning times of services for SSC customers and overall reduced service levels. IT operations staff are tasked with learning new software and tools constantly to keep pace with the changes in technology. The high rate of change has resulted in, and the increase in, heightened risks related to the manual effort involved, further eroding reliability of SSC's services to its customers.

To meet these challenges, new approaches are required focusing on automation, SDI and a zero-trust concept. The pillars described in Section 1 will be the foundation for these approaches, and will be the focus of this strategy document.

This Future Network and Security Strategy document is an extension of the SSC Future GC Network and Security Vision document and aligns with SSC 3.0 and the GC Digital Operations Strategic Plan 2018-2022[1]. This document is intended to be a dynamic, strategic description of a future GC network and security direction. The strategy laid out is a critical step toward achieving the GC's long-term digital government objectives through the development of a "modern, sustainable, reliable and robust technology infrastructure [that] enables horizontal digital service delivery, collaboration and information-sharing across government and with citizens, external business, stakeholders and partners."

This strategy will provide a future state and roadmap that will enable SSC to evolve into a more modern service delivery organization with best-of-breed technology and practice to meet the needs of the GC partner departments into the future.

[1] https://www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html#ToC1

4. Business Drivers and Other Challenges

SSC provides a range of services to Government of Canada departments and agencies. The organization plays a key role in the GC's ability to deliver a secure digital network that enables a positive user experience. The table below lists the key drivers for a modern network and security strategy that supports the emerging demands of digital government. While all are critical, there is no specific order for prioritization, dependencies or implementation sequencing. Some drivers are more relevant to SSC, some more so to GC, and the distinction is indicated in brackets with the Business Driver.

No.	Business Driver	Description
1	Seamless end-user mobility (GC)	Enables users to connect securely, seamlessly and simply to their departmental network resources and the Internet/cloud. Anytime/anywhere access from any GC-approved device.
2	Enhanced security (GC)	Ensures GC assets are properly protected and GC network connections to the Internet/cloud are adequately monitored.
3	Enhanced network performance (GC)	Supports existing and emerging demands for bandwidth and fast response times. Improves reliability through reduced outage times and performance degradation.
4	Network resiliency (GC)	Enables self healing, auto recovery and automation to build a more resilient network.
5	Support more remote work (GC)	Considers how with current events there are more employees working remotely than there has ever been.
6	Operational efficiency (SSC)	Reduces manual effort and overhead, develops scalable solutions to improve time to deliver, integrates teams and breaks down silos.
7	Manage vendor lock-in (SSC)	Supports a movement toward open standards with a vendor agnostic mindset.
8	Extend life cycle of existing assets (SSC)	Optimizes IT asset refresh cycles.
9	Stewardship of security (SSC, TBS, CCCS and other departments)	Provides visibility and control over network assets and services.

Table 1 – Business Drivers

The listed Business Drivers comprise some of the key motivating forces behind digital transformation for the GC and within IT in general. For SSC to plan its network strategy, it is important to understand the trends driving change in the IT industry. The aforementioned Digital Operations Strategic Plan is about building on those early steps and charting the path forward. This Network and Security Strategy document works to align with the change drivers and challenges that were considered as part of the basis for the strategic vision, digital standards and action items identified in the Digital Operations Strategic Plan.

No.	Other Challenges	Description
1	Aging workforce	Resulting in a decreased number of available human resources.
2	Resource competition	Skilled resources being sought by private sector, further limiting resources availability.
3	Compliance issues	Preventing quicker uptake of evolving technologies (e.g., cloud services).
4	Dated processes	Government procurement cycles unable to keep pace with technological disruption and innovation.

Table 2 – Other Challenges

Similar to the Business Drivers, the Other Challenges present real and significant obstacles to the successful completion of this initiative. Contrary to the Business Drivers, Other Challenges are less tangible than technical issues. Staffing, compliance and processes will contribute as many trials toward this project’s success, but as these issues fall into the people/process category, they can have a more political impact, and thus impose their own requirements.

5. Current State of Networking and Security within the GC

The GC network includes approximately 50 logical networks, spanning approximately 4,000 sites and approximately 5,000 buildings. It reaches over 400,000 users in Canada and around the world. Predictably, this network includes many diverse physical devices, vendors, and different levels of integration. 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. This lack of consistency has led to manageability challenges, reduced reliability and higher operational overhead. Changes to network and security infrastructure and software are slow and expensive, often requiring replacement of incorrectly sized hardware as well as rework for lack of alignment with a long-term vision. Adjusting current network technology and topology to accommodate the demand of agility and flexibility by modern multi-cloud-based services is also unmanageable. There are also costs associated with these inefficiencies:

> "A recent Gartner study[2] has identified that SSC's network and security model is expensive to operate with a 19 percent or $427 million greater cost than peers."

This network design relies on traditional security models, such as the secure perimeter concept. In this concept, most security efforts go toward defending the perimeter. This has worked well historically, when there was only "one door to defend"— essentially the "door" to the DC. However, today there are many "doors to defend", including but not limited to:

- Wireless/mobile devices
- Public cloud
- Remote sites
- Regional hubs

Cyber threats must also be monitored from within the organization as organizations are experiencing an increase in insider threats, such as users downloading an infected file (inadvertently) or a disgruntled employee exfiltrating data (intentionally). A well-known example is the data breach at Desjardins[3] leaking personal information of more than 4.2 million members.

Inconsistency in device monitoring and support teams working in silos further add to the layers of complexity that hinder timely and cost-effective problem resolution. Given the on-going growth of cross-domain integration within technologies, the silo-based team model of the past will prove incompatible with this new paradigm. Engineering, security and support teams need to work together to meet these new demands of network and security services of the future. Cross-domain integration also has training implications, and this should be considered as training plans are developed. The role of the

[2] *SSC sponsored review report - Gartner 2018*

[3] [3] *4.2 million Desjardins members affected by data breach, credit union now says | CBC News*

“Hybrid Engineer” is emerging—this individual will have an in-depth understanding of new consumption models for network, security and operations. They will have new skills that are critical to successfully implement the next generation of network and security infrastructure.

Another key requirement is real-time visibility into the network and security health of the entire infrastructure. Continuous monitoring is foundational to understanding not only historical data for forensic review and trend analysis, but also the point-in-time status of the environment, notwithstanding the ability to detect and respond to threats in a timely manner. To effectively manage changes, whether manual or programmatic, understanding the current state is essential. Only then can informed changes be planned and implemented.

The final consideration is the geo-distant nature of the GC network. Spanning beyond national boundaries, GC users can be located around the world, and existing solutions fall short. While the complex nature of the distributed-services requirement will not change, a focus on opportunities of optimization and traffic-shaping will be most advantageous for the future.

In short, the growing risk of cyber threats, the complexity of the current network and security infrastructure, and the lack of cross-functional monitoring and skills will lead to a reduction in operational efficiency, an inability to respond to growth demands and service availability issues.

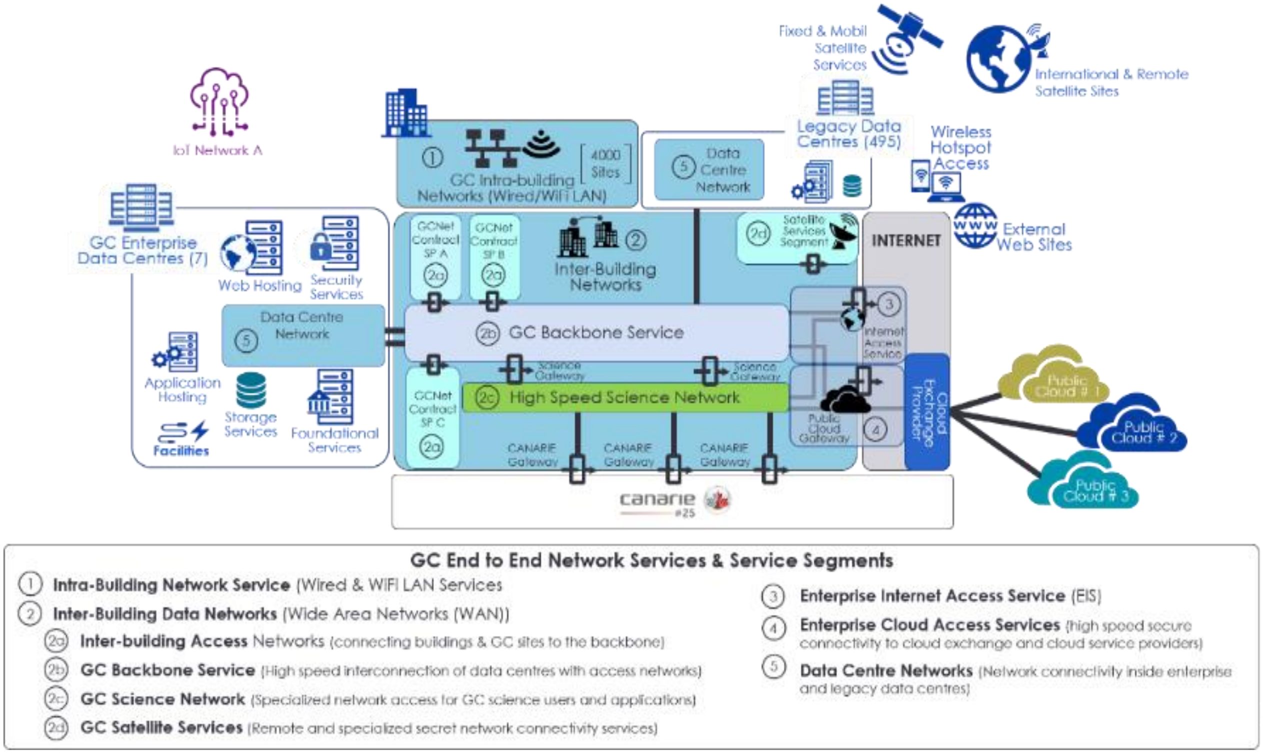

Fixed & Mobil Satellite Services
International & Remote Satellite Sites
IoT Network A
① GC Intra-building Networks (Wired/WiFi LAN)
4000 Sites
⑤ Data Centre Network
Legacy Data Centres (495)
Wireless Hotspot Access
GC Enterprise Data Centres (7)
Web Hosting
Security Services
GCNet Contract SP A
2a
GCNet Contract SP B
2a
② Inter-Building Networks
2d Satellite Services Segment
INTERNET
External Web Sites
Data Centre Network ⑤
2b GC Backbone Service
③ Internet Access Service
Application Hosting
Storage Services
Foundational Services
Facilities
Science Gateway
Science Gateway
GCNet Contract SP C
2a
2c High Speed Science Network
Public Cloud Gateway ④
Cloud Exchange Provider
Public Cloud # 1
Public Cloud # 2
Public Cloud # 3
CANARIE Gateway
CANARIE Gateway
CANARIE Gateway
canarie #25
GC End to End Network Services & Service Segments
① Intra-Building Network Service (Wired & WIFI LAN Services
② Inter-Building Data Networks (Wide Area Networks (WAN))
2a Inter-building Access Networks (connecting buildings & GC sites to the backbone)
2b GC Backbone Service (High speed interconnection of data centres with access networks)
2c GC Science Network (Specialized network access for GC science users and applications)
2d GC Satellite Services (Remote and specialized secret network connectivity services)
③ Enterprise Internet Access Service (EIS)
④ Enterprise Cloud Access Services (high speed secure connectivity to cloud exchange and cloud service providers)
⑤ Data Centre Networks (Network connectivity inside enterprise and legacy data centres)

Figure 2—SSC Current-State Network

6. Emerging Industry Trends

Over the past decade, the move to cloud is well underway and adoption rates are still rising. Cloud offers the enterprise the platform to support the agility and accelerated pace demanded by their users. Along with cloud and the unprecedented allure of change, there is also an expectation of how users want to work. The idea of "work" is no longer seen as a location, but an activity, as it is becoming the norm in many enterprises, and is becoming an expected trait of the workplace. Lastly, IoT brings devices into the network that would have recently been inconceivable. Coupled with cloud Infrastructure-as-a-Service (IaaS)/Platform-as-a-Service (PaaS)/Software-as-a-Service (SaaS) adoption of services, it is ever increasingly difficult to define, let alone manage, the perimeter for the security defences to contain.

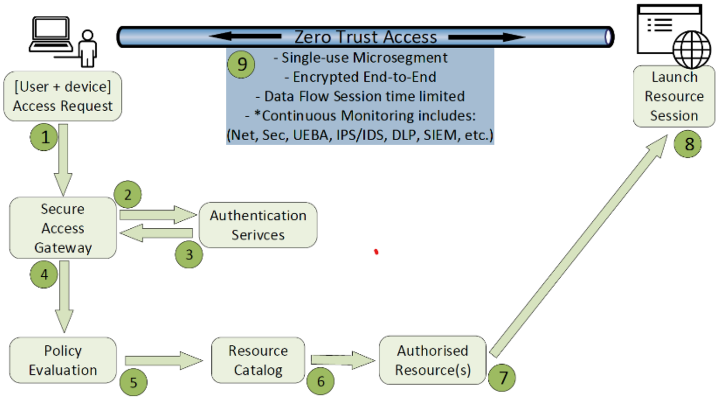
These trends require SSC to examine new approaches to providing network services and information security to the GC. Collectively, these industry changes affect further changes to enterprise infrastructure as organizations no longer control the location or boundary of the collection of services used for business. No longer is the traditional perimeter security model (castle-and-moat) sufficient; the perimeter is no longer within control of one organization.

6.1. Zero Trust Architecture (ZTA)

The emerging industry trends, and the risks they inherently impose, require adoption of a new paradigm in approach to security; that paradigm is Zero Trust Architecture (ZTA). This new approach renounces any implied trust (of users or location), assumes hostility within the network replaces the dated ideas of security based on physical location, and moves to a dynamic user/device/application policy driven model. Historically, Internet Protocol (IP) networks were designed with the intent of easy discovery of devices on the network. This approach is no longer sufficient for security, and the ZTA concept of no-implied-privilege (also known as a dark network) enables a user to see only devices/applications that they are intended to see/access. This drastically reduces many of the risks associated with the typical security breach. Most significantly, this approach accommodates public, hybrid and private cloud, and access to legacy physical systems. Figure 2 shows the complexity of the modern enterprise environment—hosting multiple compute stacks, including mixed-vendor solutions or private cloud stack.

Zero Trust Access – Connect/Communciations Process

Zero Trust: re-allocates the focus off 'location' (subnet), and on to 'Identity with Context'.



ZTA '*brings the network to the user*'; the user has no access to 'discover' other elements on the network.

Figure 3: Zero Trust Access process

6.2. Work from Home and Secure Remote Access

Recent events have pushed technology services in almost every industry to rapidly adapt to a change in work location. In response to COVID-19, most organizations were forced to adopt a work-from-home and a remote access work model. This shift of locale has stressed these services to the breaking point, and at the same time sees opportunity for innovative implementations to grow and shine in servicing these needs. Traditional virtual private network (VPN) or remote desktop applications, while functional, were typically not scaled for the majority of the workforce to leverage simultaneously. Secure Access Services Edge (SASE) has been thrust into mainstream with growing visibility from the main research groups (e.g., Gartner, Deloitte and KPMG), and have seen exponential growth in the adoption of their services. What was seen as fringe not long ago is now mainstream and central to many "road map" strategies.

6.3. Software-Defined Infrastructure

Legacy networks have served well in their time. However, new and changing demands on these installations are exposing their shortcomings. Long to implement, slow to change and expensive are a few of the common faults identified by stakeholders. Fixed design, while highly performant and predictable, is also the root cause of the static nature of the infrastructure. Additionally, it has been observed that the traffic pattern within the enterprise network has changed. Historically, most traffic was from the business to the consumer or other business (north/south traffic). More recently, the majority of data flow stays within the enterprise organization (east/west traffic). This evolution of traffic flow shifts the security risks and exposure that require additional diligence within the enterprise. In the past, internal data flow was considered trusted based solely on its location within the enterprise. Recent statistics on data breaches show upwards of 80 percent [4] are from internal exposure or compromise. Additionally, as the demand for access from outside the organization accelerates, ability to shift to a model that addresses each data access request equally, regardless of location, is essential. Much like virtualization has revolutionized the compute and storage paradigms, now the network and security devices are undergoing a similar shift. Abstraction of network and security devices allows for a flexibility in design that better suits the new distributed technologies model.

Software-designed infrastructure (SDI) will have considerable influence on technology infrastructure and operational models. SDI represents a collection of software-defined services—the local-area network (SD-LAN), commonly found in "Edge" buildings, intelligent routing over WAN link options (SD-WAN), software-designed data centres (SDDC) (including compute, storage) within a virtual context, SDN (encompasses both Network and Security)—that leverages the new paradigm of separation of software. SDI changes traditional functional models, with networking hardware running dedicated specialized software.

[4] *ClearSwift Insider Threat Index - https://www.clearswift.com/about-us/pr/press-releases/cybersecurity-incidents-insider-threat-falls-uk-and-germany-post-gdpr*

SDI represents a collection of software-defined services including the following:

- **SD-LAN**—the LAN or metropolitan-area network (MAN) aspect of Enterprise Network
- **Software-defined perimeter (SDP)**— extending SD to Remote Access to ensure flexibility for work-from-home / Remote Access following the connect Anywhere concept
- **SD-WAN**—transport from branch/regional/remote users to EDCs, to National Capital Region headquarters, or to cloud services
- **SDDC**—(virtualized compute, storage, network and security), typically within the context of a Hypervisor
- **SDN—**generic term most commonly associated within a DC

SDI will change the way technologies are deployed in the future, no longer requiring specific hardware for new or improved functionalities. Also, the benefits of SDI will far outweigh the potential throughput impact that is sometimes observed when highly optimized, hardware-based, devices (operating at near line speed) are replaced with software-based devices.

SDI facilitates the elasticity of resources through the application of SDI-specific functions. On-demand changes in infrastructure characteristics, such as capacity, speed, quality of service and security are enacted using SDI technologies. This type of functionality enables fast and efficient provisioning of resources resulting in operational efficiencies, cost effective resource utilization and ultimately, customer satisfaction through improved service offerings.

SDI decouples the hardware and software. This brings additional functionality and flexibility to infrastructure that previously were relatively static throughout their 3-5 year life cycle. SDI enables multiple software components to coexist on a given hardware component resulting in multi-function devices (e.g., a router coexisting with a firewall providing advanced integrated networking and security functionality).

6.3.1. SD-LAN - Edge Network - Office / Building LAN Services

Corresponding technology focus: Software-Defined Access (SD-LAN)

SD-LAN defines how offices (vs individuals) will connect with the future-state local network. Technologies such as Wi-Fi 6 and 5G will provide an opportunity to modernize and enhance the user experience as they are leveraged as a more flexible means of connectivity. Edge Network—Office/Building Services include considerations for connecting end-user devices to the network through Wi-Fi/Wi-Fi 6 and 5G. While the strategy/approach of "wireless first" will simplify user connectivity, reduce fit-up costs and enhance user experience, some devices (e.g., printers and videoconference stations) are not practical for wireless connectivity. This approach will also accommodate more predictability in the traffic routing to/from these devices, providing traffic optimization.

Network performance is critically important for Edge Building—Office/Building Services and direct internet connectivity (SD-WAN) for user access (vs backhaul to centralized firewalls) and should be planned as a means of improving network efficiency and effectiveness. Considering that up to 60+ percent of network traffic relates to "office" documents (which will be destined to O365), Direct Internet Access (DIA) links and SD-WAN can measurably reduce network traffic across the GC Backbone, while simultaneously improving typical user experience. As a part of the SDI strategy, with enhanced design and policy changes in both the network and the security domains, this will serve to improve application performance, and thereby user experience. Given the adoption of cloud services, the expectation of onboarding IoT devices and the growing call for "bring your own device" (BYOD), it is reasonable to assume the legacy approach to perimeter protection will not suffice. The Zero Trust model provides the flexibility and manageability that will be required for the future state, and therefore, should be considered for early integration as part of the fulfillment of the network and security strategy.

6.3.2. Remote Access—Software-Designed Perimeter

Remote Access focuses on how users connect remotely to GC services.

Corresponding technology focus: SDP

In this context, remote access is defined as any connection where a user is not directly connected to a GC network using traditional wired infrastructure or using a Wi-Fi service with direct corporate network access.

New technologies such as 5G and Wi-Fi 6 will change the users' "last-mile" services in the medium term. Changes are already occurring in the way end-remote-users devices are secured in areas such as user authentication and end-point protection for laptops, mobile phones and tablets. These changes and the impact on the security requirements for these devices impose new constraints on how remote access services will be implemented going forward. Strong user authentication is critical in a ZTA environment, with GC-wide Multi-Factor Authentication (MFA) being an essential part. With the adoption of BYOD, IoT, and cloud-hosted applications and services, it becomes clear that control over the perimeter is no longer easily definable. Given this "loss of control", new mitigation measures must be put in place to secure the enterprise. ZTA provides this function. By focusing on security between the end-user/session and the application, regardless of where it resides, the data-flow can be secured and made compliant to policy. This affects two key aspects of security—first, the user gets access only to those applications to which they are allowed to use, and second, the Zero Trust model implies limited visibility. Limited visibility implies that a user or system cannot see or discover other devices on the network outside if its policy-based isolation (see micro-segmentation).

6.3.3. Software-Defined Wide Area Network (SD-WAN)

SD-WAN is a specific application of SDN technology applied to WAN connections such as legacy point-to-point, broadband internet, 4G, LTE or Multi-protocol label switching (MPLS). SD-WAN intelligently connects enterprise networks across multiple links via optimal traffic routing. It does this by considering factors such as link availability, load, response time, traffic type and priority. For example, this approach manages and directs network traffic from branch offices destined to external services, whether they are in the cloud or in an EDC. The goal of SD-WAN is to optimize network flow and enhance the user experience over larger geographic distances.

SD-WAN has seen several applications since its inception, but the biggest impact it has had is in the replacement of costly point-to-point or MPLS WAN connections with a Dedicated Internet Access-based (DIA) connection.

6.3.4. GC Backbone and Cloud/Internet Access –SD-WAN

Corresponding technology focus: SD-WAN

SD-WAN encompasses all connections to and within the enterprise. The connections between edge network and the EDCs, cloud services, and internet services would all be augmented by an SD-WAN implementation. External Network Connectivity describes how EDC will connect to the cloud, Internet and GC-WAN connected partners and services. Efforts are currently underway to re-align the external connectivity with the existing and near-future cloud-based SaaS applications such as Office 365. Activities to migrate from traditional ISP services to Internet Exchange Point (IXP) and Cloud Exchange Point (CXP) services will open opportunities to integrate SD-WAN with controlled access to external resources.

As SSC looks to SD-WAN, it can derive significant benefits from its deployment:

- Optimize traffic flow to enhance user experience
- Provide lower cost options for connectivity to GC WAN from smaller or remote government locations
- Drive enhanced network security through enhanced embedded security capabilities within SD-WAN solutions
- Leverage the software-defined capabilities of SD-WAN to rapidly provision configuration changes or new services
- Provide the ability to deliver (in select instances) secure local Internet connectivity without the need to backhaul internet traffic to GC DCs, which will improve future performance of internet-facing solutions such as Office 365
- Better network throughput than solutions based solely on MPLS as the SD-WAN platforms will leverage “intelligent path” selection to optimize network performance
- Routing protocols that are application-aware optimize network usage and performance
- There are several potential use cases for SD-WAN within the government network environment both in the current and future state (e.g., small- to medium-sized government locations using costly MPLS circuits)
- Remote locations (especially out of country) have to backhaul Internet traffic back to a GC DC, then “hair-pin” the traffic out to the Internet for Internet services imposing significant round-trip delays, worsening remote user experience

- Resiliency – Considering SD-WAN's nature of shaping traffic over multiple lines/routes, interruption or delay on one route is automatically detected and traffic is routed to an alternative path
- Rapidly provisioning capabilities as a failover mechanism such as 4G, LTE, or in the future, 5G should the primary circuit fail

As SSC starts considering an SD-WAN strategy, the current landscape of SD-WAN providers must be examined. Many providers are still in the early stages of defining their SD-WAN solutions and may not have the capabilities that SSC requires. Some organizations, however, are now also offering fully managed SD-WAN-based solutions that should be considered as part of a broader network operations strategy.

6.3.5. Enterprise Data Centre and Core Network Services (SDDC and SDN)

Corresponding technology focus: SDDC and SDN

SDDC and SDN technologies provide the means for providing inter and intra EDC connectivity services as well as the interconnections between the virtual, physical, storage devices, security appliances, and any other DC platform. In the DC, SDDC refers to the collection of SDI services (e.g., compute, network and storage) used as part of the DC topology.

6.3.5.1. Software-Defined Data Centre

SDDC (using underlay and overlay architecture) is the next logical evolution from the traditional three-tier architecture for highly-virtualized DCs where virtual machine (VM) mobility, Zero Trust perimeters, on-demand network services and cloud computing are high priorities. This next-generation architecture provides consistent hop count, latency and bandwidth between all devices on the network. Some of the key requirements for a modern SDDC include:

- simplified automation by an application-driven policy model;
- centralized management, automation and orchestration;
- mixed workload and migration optimization/load balancing;
- secure and scalable multi-tenant environment;
- zero-trust perimeters; and
- extensibility and openness–open source, open application protocol interfaces (API), and open software flexibility for DevOps teams and ecosystem partner integration.

The SDDC fabric delivers integrated network virtualization for all workloads connected, and the controller can manage not only physical devices but also virtual switches.

The new software design infrastructure model will be moving from a single enterprise model to a service provider model supporting multiple tenants. Because the architecture is evolving to a service provider model, the new DC will also evolve to that same model, and will adopt a lot of its architecture from cloud providers. The physical DC locations will influence the DC design in two main ways—proximity to IXP/CXP, and distance from EDC. In the first, the closer proximity to either an IXP or CXP, will allow for earlier off-loading of SaaS traffic (M365 ~60 percent of network traffic). For distance from an EDC, greater distance will impose greater latency. This is a simple matter of physics—limited to the “speed of light”.

6.3.5.2. Software-Defined Network (SDN)

In common terms, SDN provides separation of the Control Plane from the Data Plane, with some solutions adding Management Plane as an additional separation. These layers of separations allow changes to the control plane (instructions layer) while no impact on the data plane (i.e. packets continue to move). This approach allows the physical underlay to be treated independently from the “overlay” layers. These overlays at the core network level in the EDC accommodate one or more overlays that can interface with different designs. For example, a typical DC has a collection of physical hardware making up the underlay. On this underlay, a first layer overlay would relate to the management of the physical layer. As an option, SDDC could provide another separate overlay for Network and Security device control within.

As previously outlined, SDN virtualizes and separates the functional services of the network devices into the Control Plane and the Data Plane. In the core network this can offer significant advantages for change/adds/deletes of resources. Interaction with the SDDC can take on more automation reducing the need to manually intervene to expand the SDDC physical resource footprint, thus eliminating complexities of multi-team planning and scheduling for routine activities. Similar interactions with SD-WAN can leverage efficiencies and optimize traffic routes in and out of the EDC.

7. Adoption Roadmap

This document uses strategic pillars to break down the strategy in consumable parts—Connectivity, Identity and Access Control, and Monitoring. Connectivity encompasses the traditional networking devices as the underlying infrastructure (e.g., switches, routers, firewalls and load balancers). In this context Connectivity also introduces software-defined "X" to enhance the traditional services such that adaptability and optimization of the infrastructure allows for cascading optimization of the application services. Identity and Access Control integrates contemporary identity and security services toward evolving the more advanced options including passwordless intrinsic authentication, centralized privileged access management (PAM) and identity governance, and Contextual Adaptive Single Sign-on Authentication. Monitoring in this case also encompasses collection, processing and dissemination of the collective of data from Network (performance and availability), Security (users, device context, access, authentication and incidents), and Application Data (use, distribution) to empower the future solutions which will leverage AI and machine learning (ML) to optimize user experience in accessing the information required using automation and orchestration. Additionally, a new provisioning approach must be adopted to meet advances in technology and user expectations for timely service delivery. Expectations are for services to be provided in hours—not weeks or months. Leveraging SDI to enable the provisioning of network and security infrastructure is a key enabler of this approach.

Figure 4 shows the Strategic Pillars and how their evolution along with a new provisioning approach is required for SDI, ZTA and eventually moving toward enhanced application/services innovation, AIOps, and Security, Orchestration, Automation and Response (SOAR).

7.1. Strategic Pillars

This section of the document describes the three key strategic pillars that provide the basis for the Network and Security Strategy. These three capabilities support SSC's Future Network and Security Vision, and are aligned with SSC 3.0 and the Digital Operations Strategic Plan 2018-2022. The focus of this section is to describe the desired target state for SSC in each of these areas. Although not all of these capabilities will be achievable in the near term, the subsequent roadmap and related activities describe the medium-term path toward achieving the future state set out in this section.

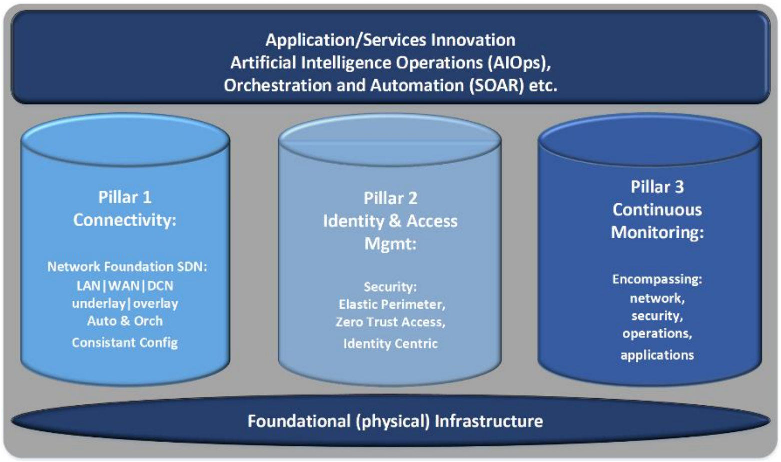


Figure 4: Strategic Pillars

7.2. Pillar 1: Connectivity

7.2.1. Overview

Connectivity as a pillar, builds upon the underlying foundational physical infrastructure to provide software-defined services on the LAN / WAN / data centre network (DCN) aspects of the network. This allows the SD underlay/overlay segregation of the Control Plane from the Data Plane providing isolation of the network management from the packet-forwarding layer. This centralized approach not only allows better consistency of the device configuration via Automation of Orchestration, but also less impeding services causing performance impacts.

Network connectivity within the GC network and security strategy can be categorized into four broad areas:

1) Edge Network—Office/Building Services—LAN
2) GC Backbone and cloud/Internet access—WAN
3) DCN—EDC and core network services
4) Remote Access

Each area encompasses its own complexity, and each area presents opportunities for improvements in communications within the GC integrating the myriad of network and security services required, such as identity and access management, zero trust, "cloud-first", wireless-first, and other competencies. SDI will also make these networks more flexible and more efficient.

7.2.2. Current State

The GC currently manages a complex legacy network, providing the backbone for IT services to approximately 4,000 sites and 5,000 buildings, and connects hundreds of thousands of devices for GC employees, contractors and Canadians.

Intra-building networks

Currently, there is no infrastructure standard. Each department has different physical and logical configurations, operating procedures, service levels and use cases. As a result, there is a need for a "standard service development" effort.

The majority of intra-building infrastructure existing in both single and multi-tenant buildings utilizes traditional hard-wired cabling to end-point devices. Usage of hard-wired infrastructure for end-user devices has been steadily decreasing with the ongoing acceptance and deployment of wireless access (Wi-Fi)-based connectivity.

Intra-building network infrastructure, equipment and cabling have multiple custodians, leading to a complexity of operational models with disparate strategies for technologies, vendors, deployment, maintenance and operations. There are hundreds of individual projects planned or in progress to maintain, refresh or replace these environments with no comprehensive nor integrated strategy.

Inter-Building Networks

Inter-building networks consist of a collection of networking components and services that provide data transportation between buildings and DCs, both domestic and international, and often span external networks (e.g., Internet and cloud), including:

- Inter-building transport that provides the "last mile" transport to over 4,000 sites, over 400 of which are multi-tenant;
- Inter-building backbone services that provide dark fibre transport services to over 220 sites (NCR-centric) and Network-to-Network Interfaces (NNI) for intranet and extranet connectivity;
- Satellite network connections that are used in over 30 departments for secret and mission-critical communication with over 6,000 mobile terminals; and
- International networks that are deployed to hundreds of Canadian missions and deployed to military worldwide as private GC networks—including technologies such as a combination of terrestrial and satellite (VSAT) deployments.

Most of the above services have been catalogued and outsourced as long-term contracts to various telecom service providers. Stewardship of the network architecture has been retained by SSC.

EDC Networks

In addition to SSC's four new EDCs, partner departments have approximately 500 legacy DCs that will be consolidated as part of SSC's ongoing efforts to consolidate DCs. Over 50 of these DCs are considered large deployments[5].

Most of these DCs were deployed before common infrastructure standards were adopted, therefore there is little commonality in network structures and underlying configurations. There have been past projects targeting DC consolidation that have proved challenging.

In addition to production environments, integrated pre-production or laboratory environments should also be considered as part of this strategy. Currently, testing labs are not integrated with all components, and many are restricted by departmental boundaries. This setup, combined with network segmentation, makes it a difficult task to test and validate future-state deployments, thus resulting in added project risk. There are currently hundreds of applications scheduled for development, and with no standardized pre-production testing facility for software, hardware, and infrastructure, integration consistency is a challenge.

[5] *SSC-Digital Operations Strategic Plan 2018-2022*

The current challenges across these areas of network connectivity result in several general challenges for the GC:

- Manual processes are required to manage the network and are executed on a per-device basis. As a result, changes to the network can require significant time and effort.
- Poor telemetry and a lack of standardized instrumentation limits reporting capabilities, with network optimization occurring via "best guesses."
- Lack of standardization owing to technology silos and procurement policies increases the complexity of support and integration.
- Vendor "lock-in" at various levels of the network impacts the GC's ability to adopt future technologies as the IT industry evolves and leads to sole-source procurements.

External Network Connectivity—Traditional

SSC partners are being connected to public cloud services in the following ways:

- Tunnelling over existing SSC-provided Virtual Private Networks (VPN), essentially creating a tunnel within a tunnel;
- Leveraging Telco-provided lines such as Digital Subscriber Line (DSL) and cable;
- Using site-to-site VPN solutions where a VPN is established on the customer-managed firewall into the public cloud; and
- OpenVPN solutions (such as OpenVPN Access Server) if supported by public cloud supplier.

The only SSC-sanctioned solution that customers can use is OpenVPN solutions where SSC provides a secure, dedicated workstation for the customer to establish connectivity to the public cloud supplier. The connectivity is supported for Unclassified and Protected A data only, and does not include Protected B or higher classification levels. SSC partners also currently leverage MPLS and VPN solutions for connectivity to GC WAN services.

At the time of writing, efforts are underway to expand the GC egress/ingress footprint to cloud services. This will include Office365 and other cloud SaaS-type services. Direct access without VPN will be enacted to optimize the traffic and reduce the latency, ultimately enhancing user experience.

7.2.3. Future State

In the GC target state, networks are based on open system standards, highly automated, and ultimately offered as a service through a web portal, with changes to network connectivity taking seconds or minutes, as opposed to days or weeks. Intent-based networking, coupled with network analytics, will enable dynamic network optimization to meet changing connectivity and performance requirements.

Additionally, GC as an enterprise will have a common place to build, test, integrate, stage and fix underlays, overlays and applications. Using virtualization and common underlays, building a common component pre-production facility will be an on-demand service. Developers will no longer be isolated by departmental boundaries and network segments, which will enable improved abilities to test and validate (de-risk) future-state deployments.

Intra-Building Network

For intra-building connectively, the GC has adopted a wireless-first strategy for end user and IoT devices. In addition, LAN and WAN architecture will be constantly expanding to incorporate IoT devices. Over time, the adoption of 5G technologies will change connectivity models for end-point devices accessing GC resources. This may have a significant impact on the connectivity usage between a building and GC Network (GCNet) services, lessening the reliance on traditional building connectivity, while increasing dependence on the external resources and gateways. In the medium term, devices will continue to rely on both Wi-Fi and cellular (3G/LTE/4G) connectivity as 5G technology reaches maturity, and pricing is analyzed to determine the value-add potential.

Network security must move instep with the new connectivity model, with the ability to confidently identify devices and users accessing GCNet resources, providing trusted any-platform, any-device connectivity and services (see “Identity and Access Control” section for additional details).

Inter-Building Networks

While inter-building networks will begin to leverage the aforementioned SDI technologies, in the short and medium term, the underlying inter-building transport layer will continue to be primarily an insourced model leveraging the infrastructure investments currently in place. However, over time, as new connectivity models (hosted 5G) become more viable, the dependence on traditional building infrastructure will lessen.

Inter-building backbone services will likely remain the same for the connectivity within the NCR, as this is a cost-effective solution with the majority of GC buildings located in the region.

Stewardship of the technology architecture should remain within SSC. Current contracts will need to be reviewed to ensure services are in line with SSC 3.0 future state.

EDCs

The major transformational change within the DCs from a network perspective will be the move to SDN. SDN will enable the rapid provisioning of new network services and changes. AIOps will also provide the ability to make automated changes based on elements such as threat remediation and performance management.

SD-WAN will also play a role in small- to medium-sized DCs acting as the new transport layer for access to Internet and GC WAN services, offloading or replacing legacy (and costly) MPLS-based solutions.

External Network Connectivity

It is expected that many customers will continue to leverage the option previously described in the Current State section for accessing Unclassified/Protected A data. Protected B data will be accessed leveraging the Secure Cloud Enablement for Defence (SCED) connectivity solution. SSC stated that customers are now able to leverage SCED for Protected-B-level connectivity. To leverage SCED, customers were advised to ensure they meet all security requirements prior to being provided with connectivity.

As SD-WAN solutions evolve, we will see more and more customers leverage SD-WAN solutions to enable access to Internet and cloud SaaS services as a replacement for legacy MPLS-based solutions.

7.2.4. Implications and Dependencies

To successfully enable the target state for connectivity a single organization (i.e. SSC) needs to have the authority to ensure compliance and availability of appropriate funding. The Enterprise Perimeter Security (EPS) project may need to be re-visited to take into account a “virtualized” perimeter that spans outside boundaries of the traditional perimeter. Full ZTA will need to be phased in over time to take into account how the EPS project will be aligned with the ZTA approach.

7.3. Pillar 2: Identity and Access Control

7.3.1. Overview

One of the key tenets of a Zero Trust security posture is the implementation of least-privilege access and fine-grained security controls to strengthen information security inside the GCNet perimeter. Access to resources is granted using a policy-based approach to securing access rather than depending on manually configuring firewall rules, which is cumbersome, static and prone to error. Lateral movement within the perimeter is secured using micro-segmentation. Micro-segmentation minimizes and contains the breach when it inevitably occurs. Instead of using IP addresses and security zones to establish segmentation policies, the policies are based on logical attributes as opposed to physical ones, and provide granular application access control to authorized users.

The intention of access controls is to ensure that an authorized user has access to the right resources, such as databases, applications and/or networks, and that these resources are inaccessible to unauthorized users. Access controls include both physical and logical controls. Physical access controls limit access to network closets, rooms and buildings where physical assets or equipment are located. Logical access controls grant or prevent access to resources (e.g., information, networks and applications and systems) once the identity of a user, entity or a device has been verified. Logical or physical access privileges are typically tied to the unique identities of the user/entity/device. As the network technology landscape undergoes significant transformation, this further elevates the importance of logical access controls to protect GC networks and information flows.

7.3.2. Current State

The GC has traditionally applied the castle-and-moat approach to access control, aimed at securing the perimeter by authenticating and granting access to authorized users at secure entry-points. Networks have expanded to include a vast number of end points and adversaries continue to find new ways to circumvent perimeter security. This is further complicated by the growing adoption of mobile technologies that enable a remote workforce and the use of outsourced services. The GC has traditionally mitigated these threats by establishing network zones and deploying an increased number of firewalls to filter network access. However, this approach has become cumbersome and costly as firewall rulesets must be continually adjusted to account for both new threats and new authorized traffic.

Today, Canadians securely access GC online services by signing in with an online banking credential (such as username and password) from Canadian financial institutions through the Credential Broker Service, or they can use the GC-branded credential service, known as GCKey.

GC users authenticate with different user stores including built-in ones, departmental Active Directory and Federated Active Directory, and also with a multitude of different multi-factor authentication services including Internal Credential Management and other departmental solutions. A trusted digital identity system is fundamental to access control and a key enabler to seamless and frictionless security in digital systems.

7.3.3. Trends

The legacy approach to access control was that of a defence-in-depth posture that uses a series of defensive mechanisms layered to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This approach is no longer seen as a viable means of preventing and mitigating against current security threats.

Access control trends are primarily shaped by proliferation of connected devices, connection options, increased end-user mobility and heightened expectation of consistent and customized experience, regardless of connection channel, location, or type of device used to initiate the connection. These expectations extend beyond the traditional definition of an end user (typically viewed as a consumer of the service) and include privileged users (e.g., service administrators) and non-human users (e.g., bots and smart connected devices).

As a result, next-generation network access controls should be able to support and enable the following:

- **Cross-entity identities**—End users expect seamless connectivity to on-premises and off-premises data and services with the device and location of their choosing. Access controls must allow for user authentication processes that are seamless, resilient, and efficient.

- **End user furnished or trusted identities**—Next-generation access controls need to account for the predicted implementation of BYOD emergence of “Bring Your Own Credentials” (BYOC) and various trusted identity schemes. This includes the evolution of a trusted digital identity for public-facing services to facilitate connections with various levels of government throughout Canada.
- **Multi-Factor Authentication**—No longer is a simple username/password combination considered acceptable to well-qualify a user. In the new paradigm, the addition of extra factors is essential. The addition of bio-metric data, hard tokens or device-installed ID, provides the added layer of assurance—something you are (bio-metric), you have (token/device) and you know (password or PIN).
- **Customized, but consistent experience**—Providing a high level of customization and consistency will result in increased user profile and metadata sharing, requiring increased data protection controls.

7.3.4. Future State

As security threats have increased in recent years, there has been a paradigm shift in architectural thinking on how to balance protection and availability while supporting the evolution of a new, information-centric security model for GC networks. The future-state network model will account for end-user needs while also ensuring security of their data.

From an access control point of view, the most influential change will be associated with the move from a traditional perimeter security approach to a “virtual perimeter”; an approach relying on the concept of Zero Trust and micro-segmentation applied to GC networks and resources. Zero Trust is based on the premise that we “never trust and always verify”. The associated Zero Trust Network Access (ZTNA) architecture dictates that verification is required for all access to resources, even from traditionally trusted sources. Traditional perimeter security may still serve as the first line of defence, but both device and user will be continually verified, authenticated and authorized to gain access to assets and resources, thus the need for micro-segmentation, a more granular view into network resources. This will have significant implications for the design and operation of access control mechanisms.

7.3.5. Implications and Dependencies

The following implications and dependencies will have to be considered in order for the next generation network to meet end user and digital government usability and security expectations:

- **Elevated need for PAM**—As delivery of network services and resources will become increasingly controlled by software, a number of new high-profile security targets will emerge (e.g., control panels for network components, policy engines). These need to be accounted for and properly managed via PAM solutions. PAM helps organizations restrict privileged access within an existing Active Directory environment. PAM accomplishes two goals:
    - Re-establish control over a compromised Active Directory environment by maintaining a separate bastion environment that is known to be unaffected by malicious attacks; and

    - Isolate the use of privileged accounts to reduce the risk of those credentials being stolen.

- **Elevated need for Secrets Management (Passwords and Secret Keys)**—Proper Continuous Integration / Continuous Delivery Pipeline, development and deployment processes must be in place to support just-in-time delivery of resources and the move to Network-as-a-Utility. A Secrets Management service must be provided to enable automation and orchestration, and be tightly coupled with access control mechanisms.
- **Higher focus on capacity/capability of access control mechanisms**—The move to ZTA will drive increased capacity requirements for all components of access control mechanisms as the process of end-user/entity/device authentication and authorization becomes continuous and multi-modal. Increased shift to "smart" risk engines will result in additional capacity requirements to enable the collection and processing of end-user and device metadata in a seamless and efficient manner.
- **Higher focus on data governance and data leakage protections**—As additional end-user and device metadata is collected and processed, externally-trusted user identity attributes are acquired and utilized to enable verification, authentication, authorization and policy development processes. Having proper data governance, master data management and data leakage protections in place will be even more important.

7.4. Pillar 3: Monitoring

7.4.1. Special Consideration Regarding Security

Given the Canadian Centre for Cyber Security (CCCS) owns the Security Operations Centre (SOC) and the security information and event management (SIEM) process, many overlaps of interest and responsibility will show in this section. While this document does not attempt to delineate tasks or specific responsibility, it will be essential to evaluate any overlaps and consider operational impacts/changes for the optimization of the process model. Mention of the SIEM solution is only to acknowledge that a SIEM is indeed required, and should not be interpreted as a function of SSC.

According to research by Gartner and Forrester and others, the future state of networks will demonstrate a convergence or alignment of functional areas. This will impose an alignment of operations centres, both the SOC and the Network Operations Centre, such that it has been proposed that a Security and Network Operations Centre (SNOC) model may be the way of the future. As SSC and the GC progress into this new paradigm, intermediary steps will pave the way to the final convergence.

While user and system-related security events will remain under the purview of the SOC (as part of CCCS), security interests relating to the infrastructure components will be integrated into the Continuous Monitoring solution. This will facilitate the automated response capabilities of the SDI.

7.4.2. Overview

Monitoring proactively manages the performance and security of the GC's IT infrastructure. The scope of monitoring capabilities extends across network devices and traffic, servers and end-user devices, and the applications running on these devices. Effective monitoring enables proactive identification of events related to network devices, and it enables the ability to remediate those events to improve the security, reliability and performance.

7.4.3. Current State

Throughout the GC there is a combination of partner-managed and SSC-managed monitoring tools and data. This results in a lack of clarity, accountability and coverage of monitoring functions. Specific skillsets and solution configurations have been tailored to individual departmental requirements. Monitoring tools are used for basic alerting and reporting. An example would be Microsoft System Center Operations Manager (SCOM).

SSC has a decentralized and non-standard SIEM capability (varying levels of maturity and configurations) that provides partial coverage. This means that SSC does not have full visibility over the GC environment to identify risks and to respond quickly to incidents.

The configuration of these solutions allows for the automation of several simple operational tasks. However, human intervention is required for anything more complex. The lack of automation and orchestration capabilities and event correlation leads to irrelevant and non-actionable information that IT operations teams must review. This causes longer analysis and resolution times, and erodes service delivery. Furthermore, SSC's current operating model is making the upkeep of the infrastructure resources cost-intensive, time-consuming and prone to human error.

7.4.4. Trends

Increasingly, organizations are implementing technologies that ingest and correlate monitoring/logging sources, aggregate this data, and apply both human and machine logic to detect and execute actions to investigate and resolve incidents/events. These platforms include Security Orchestration, Automation and Response (SOAR), behavioural analytics, and AI. The product market for these solutions continues to evolve and solutions have yet to reach their intended potential (see Appendix A).

Additionally, organizations are taking an "assumed breach" position. In doing so, organizations are incorporating threat hunting into security monitoring capabilities to continuously search for anomalies that could indicate a cyber-event.

7.4.5. Target State

In the target state, SSC will need to move from stand-alone monitoring tools and processes to an integrated set of technologies that are supported by a centralized data repository—here on referred to as SSC Data Lake—and provides improved visibility. 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 AIOps.

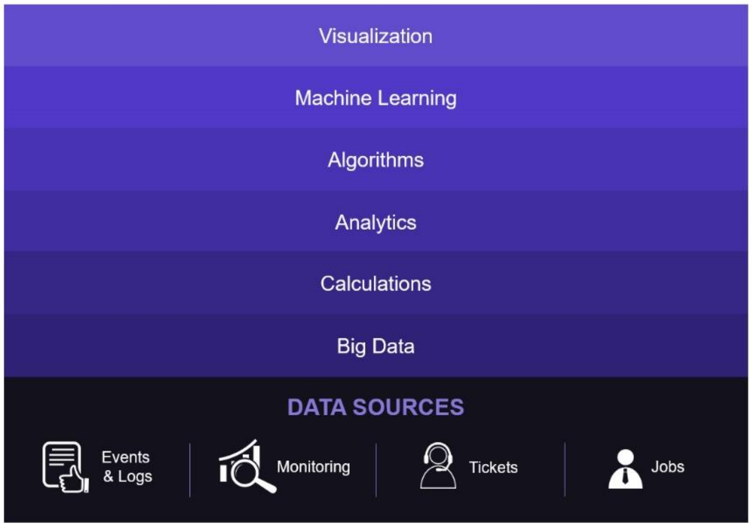


Figure 5: AIOps Multi-Layer Technology

SSC, in coordination with partners, will work to reduce the number of monitoring solutions in the future state, taking a 70/30 approach, whereby a single tool achieves 70 percent of the monitoring requirements and the remaining 30 percent will be multiple-point solutions. Seventy percent of the tools should be domain agnostic "full-stack solutions" for the broadest use cases. The 30 percent of these "point solutions", which are focused on one specific domain (e.g., network, security, endpoint systems or application performance monitoring), should be domain centric.

DC 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 EDCs that will form the foundation of a centralized monitoring capability for the GC.

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, the adoption of advanced use case content to detect events (using a combination of rules-based and user/entity behavioural analytics), and SOAR capabilities to improve threat detection and automate response. It will be critical to adopt a situational awareness capability to anticipate IT asset exposure levels to cyber threats and make risk-based remediation decisions.

To support the aggregation and correlation of data, the SSC Data Lake will be created and used to store and analyze logging data. The more data that is fed into the system, the more intelligent decisions can be made through emerging technologies, such as machine learning, SOAR and AI. To achieve better economies of scale for analytics, SSC should investigate the use of public cloud IaaS and/or PaaS solutions for the SSC Data Lake, whereby a hybrid cloud model is used for connectivity back to the EDCs.

The above technologies and solutions will continue to improve auto-remediation, self-healing infrastructure, event correlation and predictive analytics. The diagram below illustrates a proposed next generation SIEM supported by a centralized SSC Data Lake.

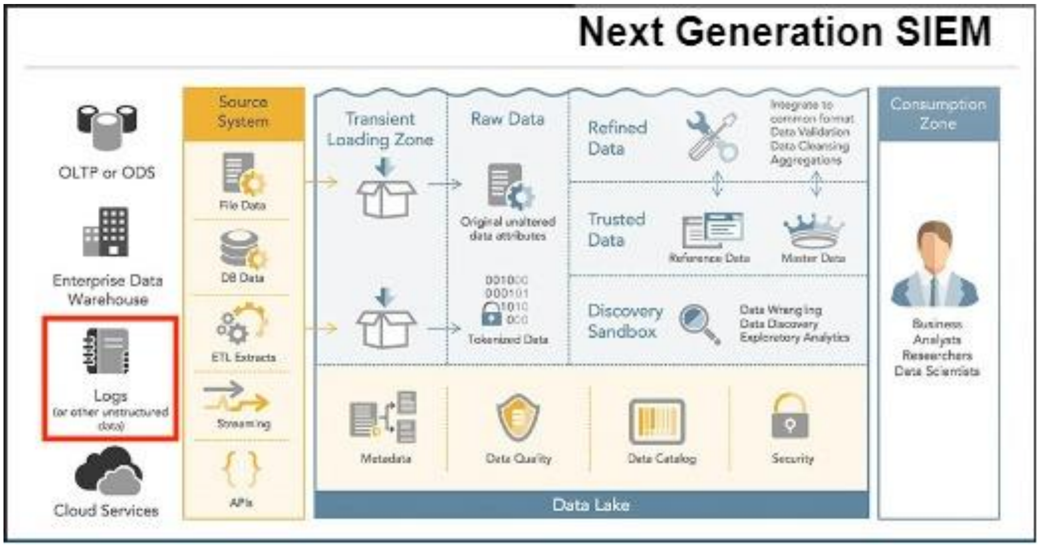


Figure 6: Next Generation SIEM with SSC Data Lake

7.4.6. Implications and Dependencies

Monitoring infrastructure suites have broad and integrated functionalities, while best-of-breed monitoring tools have deep domain-specific functionalities. The key dependency to achieve the future monitoring strategy will be for all partners to share logging data across the technology stack with SSC (including application performance data), and for this data to be stored within a centralized repository (SSC Data Lake). This integration will provide visibility into the overall GC security posture, enable advanced use cases and accelerate incident response. It will also be critical for SSC to work with partners and CCCS to ensure roles and responsibilities for incident detection, response and remediation are clear.

7.5. Provisioning

7.5.1. Overview

Provisioning refers to the ability of the technology platform and solution to implement the components of the overall solution. In the context of networking and security, provisioning provides the ability to implement components of the network and security, such as adding or changing network configurations or adding/changing firewalls rules. Provisioning should be looked at holistically across networking, compute and security, leveraging capabilities like SDI as enablers to enhanced provisioning capabilities.

7.5.2. Current State

Currently, the GC has a number of vendors providing networking, compute and security services (hardware, software and service providers). This has led to a proliferation of platforms throughout the GC that, in many cases, require unique technology solutions and skills across these platforms to manage and monitor.

Provisioning time is one of the main concerns of Chief Information Officers (CIO). CIOs are dependent on SSC for the delivery of compute, storage and network services to implement new applications that enable GC program delivery. SSC's provisioning time is, therefore, one of the critical enablers of agile program delivery. The target is to reduce provisioning time for infrastructure services from weeks/months to hours/days. Also, many of the legacy network, compute and security platforms are nearing—or have exceeded— their end of life, and need to be replaced to effectively secure and manage the GC's technical assets.

The advent of new technology capabilities, such as ZTA and SDN, will require most of the legacy networking and security platforms be either replaced, or at a minimum, upgraded, to enable these new operating paradigms.

7.5.3. Trends

The area of networking, compute and security is going through a fundamental overhaul as organizations move to enabling technologies, such as cloud computing. Cloud is driving the need for the provision of networking, compute and security services to happen immediately to support the dynamic demands of cloud services. Use of AI operations also enables the speed of provisioning by automating many of the operational tasks for IT service delivery.

7.5.4. Future State

Enhanced provisioning capabilities will enable network, compute and security services to be provisioned in minutes (vs days/weeks). The trends that are driving the need to enhance provisioning are:

- Innovation requiring new capabilities;
- Cyber threats requiring automated network changes to mitigate threats; and
- CIOs requiring the rapid provisioning of new technology environments and associated network and security services.

The future state will see the implementation of enabling technologies, such as SDN/SDI, integrated with on-premises infrastructure, such as hyper-converged infrastructure, software-defined-based network and security platforms. Off-premise cloud will enable rapid provisioning of network, security and compute services.

There are multiple approaches to be considered for the delivery of software-defined capabilities, including the selection of a vendor-based ecosystem solution (e.g., Cisco Application Centric Infrastructure, Juniper Contrail, Arista EOS) or an open-source-based solution (e.g., OpenDayLight SDN).

In the future state, SSC will be able to dynamically provision network, compute and security solutions through a software-enabled platform improving provisioning times and customer satisfaction with departmental CIOs.

7.5.5. Implications and Dependencies

The strategy for achieving enhanced provisioning capabilities will need to consider the following implications/questions:

- How do the various network and security solutions enable capabilities (e.g., ZTA)?
- What is the process to define and implement an integrated provisioning competency, especially if SSC undertakes a multi-vendor approach to network and security?
- Does SSC begin the process of vendor standardization to provide an integrated enhanced provisioning capability, or select the path of multi-vendor- or open-source-based solutions?
- Will self-provisioning be offered as part of the strategy, especially in the areas of compute?
- How will SSC support integrating automation and AI operations into provisioning?

7.6. Considerations

7.6.1. Re-skilling and Re-tooling the Organization

Given the accelerated rate of change created by rapid advancement in technology, and future ways of working, the current SSC workforce will need to adapt its operating model, skills and operations to support the future-state network and security platform.

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; and
- Vendor management capabilities.

The operating model will need to fundamentally change how SSC is oriented for network and security services from day-to-day technical support right up to the leadership team.

Skills

The changes to network and security will require a new set of skills and capabilities within SSC, such as:

- Zero Trust networking to design, implement and operate the future-state environment;
- SDN/SDI, which will be the future operating model for the design and delivery of network and security services;
- DevOps capabilities with Infrastructure-as-Code experience;

- Shifting to advanced threat hunting and creating advanced content for security event monitoring, including using behavioural analytics and combining organizational and security content to detect anomalies;
- Re-skilling the organization to enhance and grow skills around vendor management as SSC moves toward more of a vendor management role for certain areas of responsibility as the organization expands its use of managed services; and
- Leveraging vendor partners and consultants to close the defined skills gaps with a plan focused on either hiring for these skills or defining long-term outsourcing contracts for such skills.

Roles and Responsibilities

Changes to the operating model will also require new roles be defined within SSC to support the future-state model. New roles will be required, such as:

- Software-Defined Architect;
- ZTA Architect;
- Vendor Management; and
- Additional partner relationship management focus in all roles.

The questions facing the future of the SSC workforce are:

- What future skills are needed?
- What tasks could we automate or give to alternative talent?
- How can we transition the workforce?
- How will SSC address ongoing skills modification/upgrade needs?
- How big will the impact be?
- What will it cost?

To answer these questions, a separate target operating model program will need to be undertaken by SSC:

- Understand external trends, internal priorities and pressures impacting the Department’s workforce
- Identify key skills and tasks that are new, increasing and/or diminishing, and then map the skills/tasks to roles for prioritization
- Define an approach to close prioritized skills gap—digitalization/automation, hire externally, borrow short-term talent or develop internally
- Develop the future-state IT Operating Model
- Define the required roles and responsibilities
- Develop the change management processes to manage the operational change (highly important), following ITSM best practices

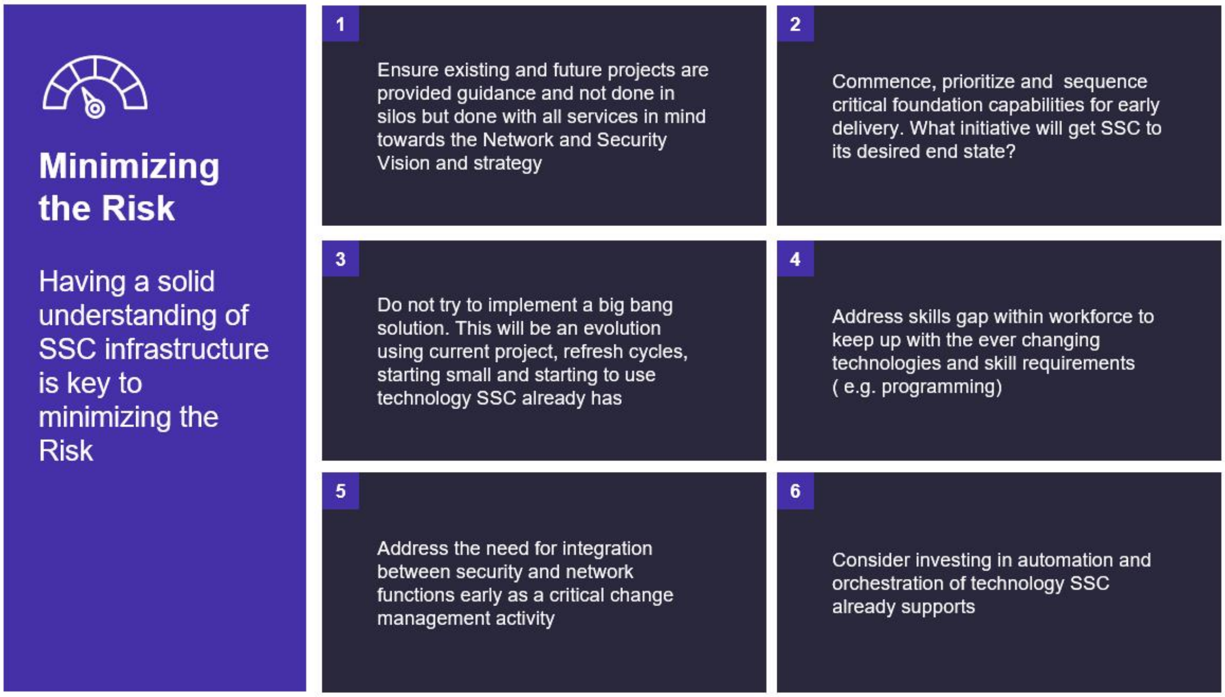
The results of this program should drive skill and role gap mitigation strategies at the Department- and enterprise-wide levels, and estimate costs to upskill and size the impact to the overall workforce.

7.7. Recommended Next Steps

In the previous sections, future-state pillars were detailed to describe where SSC needs to go to move to SDI and ZTA. This section will describe the recommended necessary next steps to get there in terms of principles, projects and initiatives.

7.8. The Principles

To implement this strategy, core principles needed to be developed owing to the complexity of the SSC network and security infrastructure. It is impossible to procure and implement in one shot a fully-functional SDI and ZTA infrastructure, therefore, the following strategic principles are recommended:



Minimizing the Risk

Having a solid understanding of SSC infrastructure is key to minimizing the Risk

1 Ensure existing and future projects are provided guidance and not done in silos but done with all services in mind towards the Network and Security Vision and strategy

2 Commence, prioritize and sequence critical foundation capabilities for early delivery. What initiative will get SSC to its desired end state?

3 Do not try to implement a big bang solution. This will be an evolution using current project, refresh cycles, starting small and starting to use technology SSC already has

4 Address skills gap within workforce to keep up with the ever changing technologies and skill requirements (e.g. programming)

5 Address the need for integration between security and network functions early as a critical change management activity

6 Consider investing in automation and orchestration of technology SSC already supports

Figure 7: Foundation Steps

7.9. Communication Plan

A comprehensive communication plan is essential and needs to be executed to share the Network and Security Vision, Strategy and plan moving forward. This needs to be done throughout SSC at both executive levels and at working levels to ensure there is buy-in and understanding throughout the organization. However, this is not just an SSC initiative—for this initiative to succeed, assistance and buy-in will be required from all SSC partners, as this extends to the business services and applications SSC provides to those partners.

7.10. Reference Architectures

Reference Architecture Documents (RAD) must be developed to provide an architecture, methodology, guidelines and principles for the different technologies at a high level and be broken down into different service levels. The RADs will:

1. Show relations to the SSC Network and Security Vision and Strategy.
2. Compare, contrast and align SSC requirements against emerging industry technologies.
3. Provide guidelines and principles for services/products/projects to follow.
4. Focus on function over technologies.

An overarching Master RAD will be developed first and will be an architecture that interconnects all sub-RADs to ensure that the overall goals are consistent between interrelated functions and technologies.

The sub-RADs will be developed and will link back to the Overarching Master RAD. The sub-RADs initially proposed to be developed include:

1. SD-LAN
2. SD-WAN
3. SDDC
4. Cloud, Internet and Remote Access Connectivity
5. EDC/DCN core network
6. ZTA

7.11. Support Existing Initiatives

Existing projects and initiatives are currently in progress that have been planned and ongoing for some time. Several of these would have been identified even before the concepts of SDI or ZTA were well known. However, many of these projects/initiatives are important pieces of the core infrastructure for moving SSC toward SDI and ZTA.

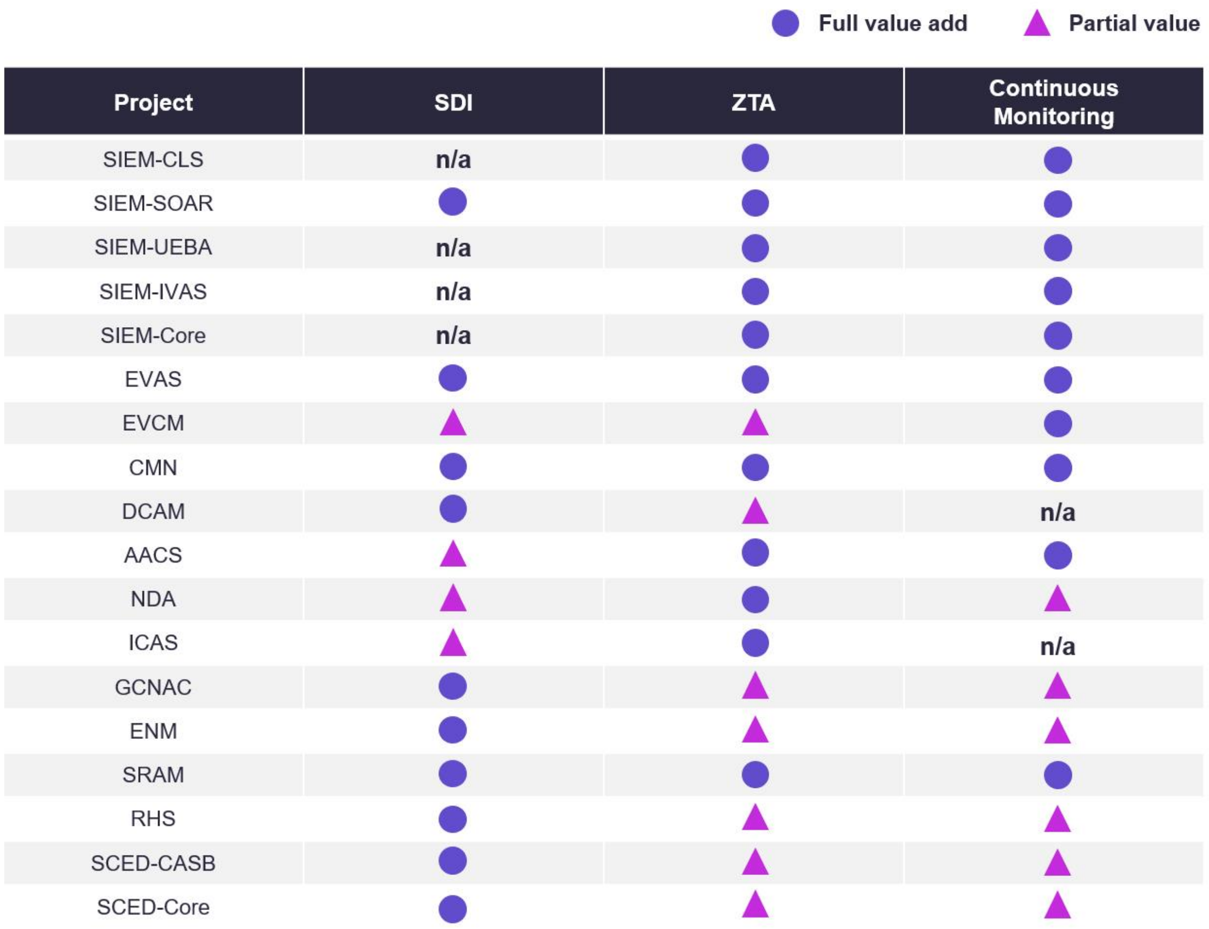
It is recommended that in-flight and new projects take time to reflect on the SSC Network and Security Vision and Strategy—and The Principles identified earlier—and work with SSC to identify opportunities to align activities even further than was originally scoped in the projects.

The following table identifies a list of the SSC projects and significant sub-initiatives that support the Network and Security Vision and Strategy moving forward, and should continue to be supported with guidance from SSC.

Project	Description	Sub Projects/Initiatives
SIEM	Security Information and Event Management	• Central Logging Service (CLS) • Security Orchestration, Automation and Response (SOAR) • SIEM (Traditional) • User and Entity Behaviour Analytics (UEBA) • Infrastructure Visibility, Awareness and Security (IVAS))
EVAS	Endpoint Visibility Awareness and Security	N/A
EVCM	Enterprise Vulnerability and Compliance Management	N/A
CMN	Centralized Management Network	N/A
DCAM	Directory Credential Account Management	N/A
AACS	Administrative Access Controls Service	N/A
NDA (now CLM)	Network Device Authentication / Crypto Life Cycle Management	N/A
ICAS	Internal Centralized Authentication Service	N/A
GCNAC	Government of Canada Network Access Control	N/A
ENM	Edge Network Modernization	N/A
EPS	Enterprise Perimeter Security	N/A
SRAM	Secure Remote Access Management	N/A
RHS	Regional Hub Strategy	N/A
SCED	Secure Cloud Enablement for Defence	• SCED Core • Cloud Access Security Broker (CASB)

Table 3 – Supporting SSC Projects and Initiatives

The following heatmap demonstrates how each of the projects align with Network and Security Vision.



● Full value add ▲ Partial value

Project	SDI	ZTA	Continuous Monitoring
SIEM-CLS	n/a	●	●
SIEM-SOAR	●	●	●
SIEM-UEBA	n/a	●	●
SIEM-IVAS	n/a	●	●
SIEM-Core	n/a	●	●
EVAS	●	●	●
EVCM	▲	▲	●
CMN	●	●	●
DCAM	●	▲	n/a
AACS	▲	●	●
NDA	▲	●	▲
ICAS	▲	●	n/a
GCNAC	●	▲	▲
ENM	●	▲	▲
SRAM	●	●	●
RHS	●	▲	▲
SCED-CASB	●	▲	▲
SCED-Core	●	▲	▲

Table 4 – Project Alignment Heatmap

7.12. Required Future Initiatives

The Network and Security Roadmap summary below outlines the progressive steps necessary to migrate from current state to the projected to SDI and ZTA end state. This evolution will require some specific steps and technologies put in place for each of those disciplines along with supplementing/evolving Identity services and Security. The following diagram summarizes the recommended progressive adoption of future required initiatives that will need to be supported to continue to evolve SSC to SDI and ZTA. For the full details, please see the full Roadmap document in Appendix B.

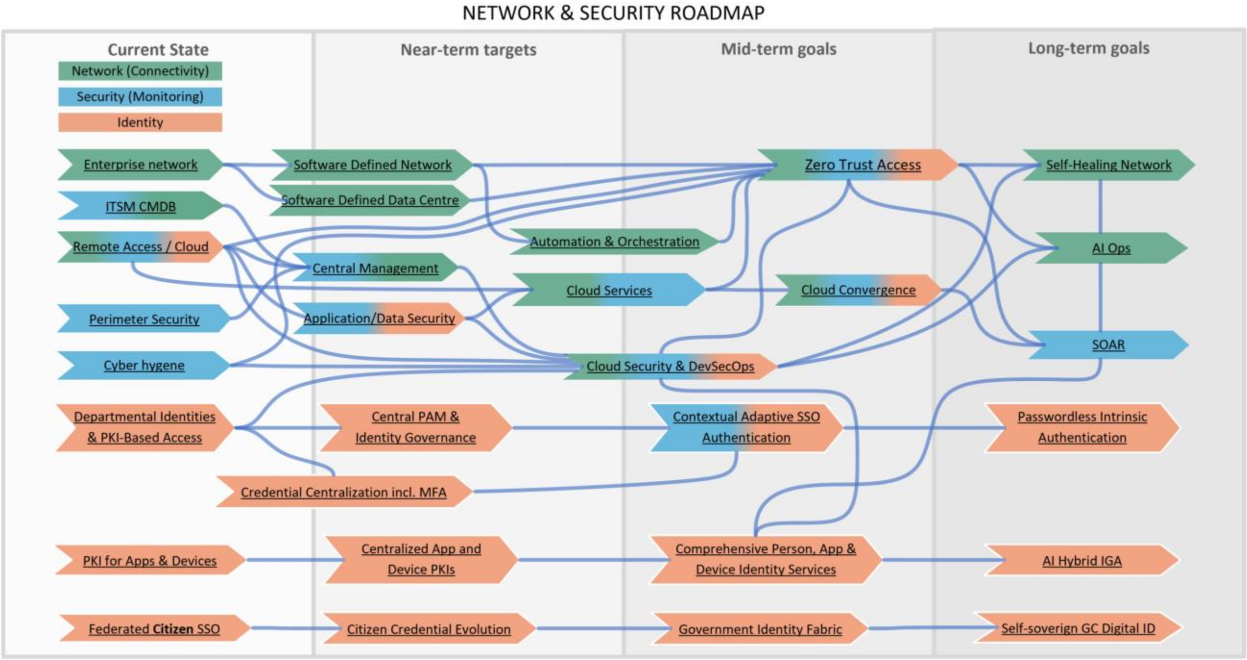

NETWORK & SECURITY ROADMAP
Current State
Near-term targets
Mid-term goals
Long-term goals
Network (Connectivity)
Security (Monitoring)
Identity
Enterprise network
ITSM CMDB
Remote Access / Cloud
Perimeter Security
Cyber hygene
Departmental Identities & PKI-Based Access
PKI for Apps & Devices
Federated Citizen SSO
Software Defined Network
Software Defined Data Centre
Central Management
Application/Data Security
Central PAM & Identity Governance
Credential Centralization incl. MFA
Centralized App and Device PKIs
Citizen Credential Evolution
Zero Trust Access
Automation & Orchestration
Cloud Services
Cloud Convergence
Cloud Security & DevSecOps
Contextual Adaptive SSO Authentication
Comprehensive Person, App & Device Identity Services
Government Identity Fabric
Self-Healing Network
AI Ops
SOAR
Passwordless Intrinsic Authentication
AI Hybrid IGA
Self-soverign GC Digital ID

Figure 8: Future Initiatives

8. Conclusion

Throughout this document three persistent themes emerge:

1) The ongoing acceleration of change.
2) The need to keep up with these changes while maintaining security and control.
3) The criticality of gathering and using monitoring/analytics data.

The saying “Change is inevitable” has long been a mantra within IT circles. However the breadth and pace of change continues to challenge. Adoption and integration of cloud services and the acceptance of IoT expansion of technologies’ footprint—not only in the DC, but across the board in personal and business life—changes user expectations on how, when and where access to GC systems is needed.

Establishing and adopting technologies, (including network, security, compute, storage), that can continually evolve is paramount, but equally critical is the modernization of the processes and policies that define the use and function of the technology. Social acceptance must precede the adoption of this substantially new technology paradigm.

Monitoring or “Continuous Monitoring”, as has been outlined throughout this document, proposes to go beyond traditional functional/performance/security monitoring. These will—and must—remain integrated in any solution. However, what has begun as device and functional convergence will continue and predictably include user/device security information and policy engine authorization. This enhanced model will gather much more monitoring data than previously available, allow the various teams to get data relevant to their needs, and further allow integration of AI-driven solutions to leverage the capabilities of the SDI of tomorrow.

9. Acronyms

Acronym	Description
AI	Artificial intelligence
AIOps	Artificial intelligence in support of system operations activities
BYOC	Bring Your Own Credentials
BYOD	Bring Your Own Device
CI/CD	Continuous Integration/Continuous Development
IoT	Internet of Things
MAN	Metropolitan Area Network
ML	Machine Learning
PAM	Privileged Access Management
SCED	Secure Cloud Enablement for Defence
SDI	Software-Defined Infrastructure
SDN	Software-Defined Network
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SRA	Secure Remote Access
TCP/IP	Transport Control Protocol / Internet Protocol
Wi-Fi	Trademark referring to the wireless 802.11 family of standards for wireless network access
ZTA	Zero Trust Architecture / Zero Trust Access – architectural framework alternative to traditional "defence in depth"
ZTNA	Zero Trust Networking Access

10. References

1. Information Technology Security Guidance Number 33 (ITSG-33): IT Security Risk Management: A Lifecycle Approach.
2. Cloud First Strategy, SSC 3.0 Strategy
3. Government of Canada (“GC”) Digital Operations Strategic Plan 2018-2022

Appendix A—Network and Security Trends

The following tables describe various trends that are most relevant to SSC's strategic vision. A number of these trends are mainstream, while others are not quite as mature, but are gaining market traction. A definition, analysis and applicability for SSC are provided for each trend.

Trend #1—Zero Trust Architecture

What is Zero Trust Architecture (ZTA)?

ZTA leverages a software-defined approach to establishing a perimeter, and 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. This removes the application assets from public visibility and significantly reduces the surface area for attack.

Although ZTA offerings differ in their technical approaches, they generally provide the same fundamental value proposition:

- Removing applications and services from direct visibility on the Internet.
- Enabling granular application access either programmatically or through role-based access, and applying a least privilege approach.
- Enabling access independent of the user's physical location. Access policies are based on user, device and application identities.
- Granting access only to the specific application, not the underlying network infrastructure. This limits the need for excessive access to all ports and protocols or all applications, some of which the user may not be entitled to.
- Providing end-to-end encryption of network communications.
- Providing optional inspection of the traffic stream for excessive risks in the form of sensitive data handling and malware.
- Enabling optional monitoring of the session for indications of unusual activity, duration or bandwidth requirements.

Trend Analysis

The ZTA market is still immature, but it is growing quickly—interest is based primarily on organizations seeking a more flexible alternative to VPNs and those seeking more granular application access control.

Applicability to SSC

- Updates their existing dated network security framework
- Aligns with the GC's "cloud-first" strategy—new perimeters being established
- Provides a consistent user experience for accessing applications—clientless or via ZTA client regardless of network location
- Incorporates automation techniques into the security framework

Trend #2—Software-Defined Perimeter

What is Software-Defined Perimeter (SDP)?
ZTA is typically implemented through the use of SDP and micro-segmentation. SDP is a new, very versatile technology providing confidential, secure access to enterprise applications. The technology is implemented in software on end-user devices, gateways, controllers or servers. An SDP may be acquired either as a stand-alone product (operated by the network team) or as a service.

Trend Analysis
SDP is a newer technology, with vendors rapidly adding new features or form factors. New features specifically include management portal interfaces and flexibilities in attestation and policies. Additional form factors include turnkey virtual gateway appliances, virtual network functions (VNF) and software images on public cloud marketplaces. SDP and software-defined technologies in general will upend the traditional hardware vendor market. SDP is generally not used to access Software-as-a-Service (SaaS) applications such as Microsoft Office 365, Salesforce or ServiceNow. Thus, SDPs do not overlap with cloud access security brokers (CASB).

Applicability to SSC
• Updates its existing dated network security framework • In line with mandate to offer secure, remote access for end users • As networking components age out, this can facilitate network consolidation

Trend #3—Micro-segmentation

What is Micro-segmentation?
Micro-segmentation is a foundational capability that supports ZTA. Historically, customers were paranoid about breaches from external access into their corporate DC perimeters. They assumed that if a breach occurred from a north-south perspective, they had lost the battle. The mindset has now changed, and customers are coming to terms with the fact that breaches can and do occur, and they need to look at ways to minimize the damage. With the advent of automation and more capable software, micro-segmentation has gained a wide audience in its ability to mitigate damage from a breach once the DC perimeter has been compromised. Micro-segmentation minimizes and contains the breach when it inevitably occurs. Instead of using IP addresses and security zones to establish segmentation policies, policies are based on logical attributes (not physical) and provide granular application access control.

Trend Analysis

Network virtualization has been mainstream for a number of years now, thereby acting as the enabler for micro-segmentation. It is becoming more mainstream and seems to be the best answer to address east-west traffic containment.

More advanced network micro-segmentation solutions monitor and baseline flows, and alert on anomalies. They also continuously assess the relative levels of risk/trust of the network session behavior observed (for example, unusual connectivity patterns, excessive bandwidth, excessive data transfers, and communication to URLs or IP addresses with low levels of trust). If a network session represents too much risk, an alert can be raised or the session can be terminated.

Applicability to SSC

- Containment of breaches occurring from within the DC (east-west traffic)
- Fits well into a microservices architecture
- In line with automation requirements
- Much easier to implement and manage
- Enables enforcement of consistent segmentation policies across on-premises and cloud-based workloads
- Well suited to workloads that host containers meeting compliance requirements

Trend #4—Secure Access Service Edge

What is Secure Access Service Edge (SASE)?

The requirements of digital business and edge computing are turning traditional traffic patterns upside down, fundamentally transforming this model and forcing a convergence of the WAN edge and network security markets into the SASE (pronounced sassy). SASE typically combines products and services to deliver multiple capabilities such as SD-WAN, WOC, SWG, CASB, NGFW and ZTA/SDP.

Trend Analysis

Over the next few months, there will be a number of offerings in this area, but they will be based on purpose-built appliances built for scale-out, cloud-native and cloud-based delivery, and optimized to deliver very low latency services.

Be aware that during this transition there will be a great deal of slideware and marketing content, especially from incumbents that are not well prepared for the cloud-based delivery model from distributed POPs.

The inversion of networking and network security patterns established by this technology will transform the competitive landscape and create opportunities for enterprises to reduce complexity and allow their IT staff to eliminate mundane aspects of the network and network security operations.

SASE will allow for consolidation across CASB, SWG and SDP solutions, providing a seamless way for users to connect to SaaS applications, internet websites and private applications (whether hosted on-premises or in public cloud IaaS) based on context and policy.

Applicability to SSC
• Aligned with SSC 3.0—better end user experience • Ability to provide more secure and performant international connectivity • Better scalability—less reliance on point solutions and long lead times for hardware procurement • Consolidation across CASB, SWG and SDP solutions, providing a unified way for GC users to connect to SaaS applications, internet websites and private applications (whether hosted on-premises or in public cloud IaaS)

Trend #5—Security Operations, Automation and Response

What is Security Operations, Automation and Response (SOAR)?

The term SOAR is another one of those new buzz words floating around. The security vendor community proudly promotes this term when marketing their products. The fact of the matter is that full automation and remediation is not yet available in the industry and won't be for a few years to come. The vendors tout their capabilities as being fully automated, but the fact of the matter is that they are doing one of two things:

- Leveraging external scripts as add-ons to their core offerings for remediation; and
- Integrating with other products to provide a more robust automation solution set.

SOARs are technologies that enable organizations to take inputs from a variety of sources (mostly from SIEM systems) and apply workflows aligned to processes and procedures. Additional capabilities include case and incident management features; the ability to manage threat intelligence, dashboards and reporting; and analytics that can be applied across various functions. SOAR tools significantly enhance security operations activities like threat detection and response by providing machine-powered assistance to human analysts to improve the efficiency and consistency of people and processes.

The following are aspects of SOAR—in the context of security operations:

- Aggregation: The ability to aggregate/ingest data across multiple sources.
- Enrichment: Whether after incident identification or during data collection and processing, SOAR solutions can help integrate external threat intelligence, perform internal contextual look-ups or run processes to gather further data according to defined actions.
- Orchestration: The complexity of combining resources involves coordination of workflows with manual and automated steps, involving many components and affecting information systems and often humans as well.
- Automation: This concept involves the capability of software and systems to execute functions on their own, typically to affect other information systems and applications.
- Response: Manual or automated response provides canned resolution to programmatically defined activities.

Trend Analysis

The SOAR market is still an emerging one. There have been numerous acquisitions over the last few years and this is expected to continue as vendors try to enhance their existing platforms capability or replace it altogether. Customers should be aware of this trend and plan for contingency should their current SOAR platform be acquired by another company.

A number of organizations implement SOAR tools with use cases primarily focused on making their SOC analysts more efficient, such that they can process more incidents while having more time to apply human analysis and drive response actions much quicker.

Applicability to SSC

- Aligned with SSC movement to more automation and orchestration
- SOC optimization
- Augment staff shortages and skill gaps
- Threat monitoring and response
- Threat investigation and response
- Threat intelligence management

Trend #6—Artificial Intelligence Operations

What is Artificial Intelligence Operations (AIOps)?

AIOps platforms provide the ability to augment—and in some cases replace—traditional IT operations platforms primarily in the areas of event correlation and analysis. They leverage big data and machine learning functionality to analyze large data sets in response to digital transformation.

Some of the core capabilities of AIOps platforms include:

- Ingesting data from multiple sources including infrastructure, networks, applications, cloud or existing monitoring tools (for cross-domain analysis);
- Enabling data analytics using machine learning at two points:
  - Real-time analysis at the point of ingestion (streaming analytics);
  - Historical analysis of stored data;
- Storing and providing access to the data;
- Suggesting prescriptive responses to analysis; and
- Initiating an action or a next step based on the prescription (result of analysis).

Trend Analysis

The trend for AIOps platforms is one toward a manager of managers (MoM) approach, whereby other ITOps platforms send their data to the AIOps platform for aggregate analysis and reporting, leading to more simplified and efficient operational management. Ideally, organizations are looking for a domain-agnostic approach to AIOps that can cover most of their requirements. However, there are no platforms currently available to meet all customer needs, and a domain-centric-solutions approach is taken to fill the gap.

Since these platforms leverage AI technologies, they rely on very large data sets to show their effectiveness, and are not intended to be deployed in an "island" or "siloed" manner. In other words, the more data the platform has access to, the better it provides value. With the advent of big data, AIOps will show better value over time.

Applicability to SSC

- More simplified and centralized reporting service
- Better visibility into partner infrastructures—better Service-Level Agreements (SLA)
- Good use case for centralized data lake—data from partner departments can feed into the solution to provide better value

Trend #7—Network Managed Services (SD-WAN)

What is SD-WAN?

SD-WAN is a software-defined approach to managing WANs. Key advantages include:

- Providing agnostic transport across multiple protocols such as MPLS, 3G/4G LTE.
- Improving business application performance and increases agility and cost reduction.
- Optimizing the user experience and efficiency for SaaS and public cloud applications.
- Simplifying operations with automation and cloud-based management.

Managed SD-WAN providers operationally manage customer SD-WAN products, which are physical appliances or software instances that are either enterprise-owned or included with the service. Managed SD-WAN products typically reside on the customer premises, are governed by an SLA and are priced on a recurring monthly basis. Providers offer managed SD-WAN services independently of, or in conjunction with, WAN transport. To be considered a managed SD-WAN services provider, the provider must offer an SPOC for all management inclusive of WAN transport, SD-WAN customer premises equipment and required software functions.

Trend Analysis
SD-WAN solutions are now mainstream and the options available to enterprises for managed SD-WAN services are expanding in parallel to the growth of SD-WAN technology. Hybrid WAN design options will continue to expand, and will continue to be affected by managed SD-WAN service). SD-WAN's security capabilities will continue expanding beyond basic firewall as more providers are including unified threat management (UTM) such as SWG and IDS/IPS. Additionally, WAN optimization and acceleration capabilities will grow as more providers incorporate engineered network features to improve quality of service (QoS) and throughput.

Applicability to SSC

- Good cost alternative to consider when existing MPLS contracts are up for renewal
- Potential for outsourcing as a managed service
- Path diversity for availability and cost reduction
- Aligns well with SSC's move to SDI
- Good alternative for non-latency sensitive applications
- Considered for new site builds at remote locations

Trend #8—Internet of Things

What is the Internet of Things (IoT)?

IoT is defined as:

"A network of physical objects (things) that contain embedded technology to sense or interact with their internal state or external environment, and can send and receive data to or from a remote digital platform."

Trend Analysis

Five high impact IoT trends:

- **AI:** AI will be applied to a wide range of IoT information, including video, still images, speech, network traffic activity and sensor data.
- **Social/legal/ethical IoT**: As IoT matures, ownership issues and bias in interpretation of that data will be a concern.
- **Data brokering:** IoT system data can be sold or used to others than the device or owner that created it.
- **IoT mesh:** Edge architecture layers will dissolve to create a more unstructured architecture consisting of a wide range of "things" and services connected in a dynamic, flexible mesh.
- **IoT governance**: Governance encompasses the operational management of IoT devices and the information and services that IoT systems deliver.

Applicability to SSC

- Real property utility and security monitoring
- Performance monitoring for GC smart devices
- Cost savings
- Security
- Canadian Food Inspection Agency’s remote inspection
- Border-crossing inspection equipment
- National video surveillance systems

Trend #9—Private 5G

What is Private 5G?

A private 5G network, also known as a local or non-public 5G network, is a LAN that provides dedicated bandwidth using 5G technology. 5G is the next revision of 4G/LTE wireless data networks. 5G introduces a higher bandwidth using a different radio spectrum that will also enable more devices to connect simultaneously. It is currently being rolled-out by all major service providers in Canada. A private 5G (local) network is a LAN that provides dedicated bandwidth using 5G technology.

Both private and public 5G deployments are enabling the IoT. It is envisioned that service providers will offer overlays on the public 5G network, enabling the creation of VPNs routed back to private networks. This is an alternative to deploying private 5G equipment and provides the opportunity to outsource this connectivity model instead of a built-in-Canada solution.

Trend Analysis

With Release 16, 5G has the potential to become the world’s predominant LAN and WAN technology over the next 10 to 20 years, especially in greenfield builds. New buildings, factories, ports or campuses may significantly reduce their usage of wired connections by implementing private 5G. The next five years will likely see a boom in private 5G implementations at locations that would greatly benefit from better wireless technology in terms of speed, capacity, latency.

In the short term, 5G will deliver higher bandwidth and lower latency connections, in many cases, in the form of fixed wireless access networks and early IoT networks.

Applicability to SSC

- IoT communications
- New site builds in remote locations, i.e. International
- High-definition video
- GC building upgrades

Trend #10—Multi-Cloud Networking

What is Multi-Cloud Networking?

As more customers opt for a multi-cloud approach to providing IT services, they are looking for a more seamless way to manage and operate them. Multi-Cloud Networking refers to the network infrastructure to support the use of cloud services from multiple public cloud providers, including connectivity to, between and within providers.

Multi-Cloud Networking solutions are software-based and provide consistent network policy across multiple cloud providers. They include overlays, management of cloud provider APIs or other mechanisms. Multi-Cloud Networking is similar to an ethernet fabric where multiple components are managed as a single construct and policy is created centrally.

Trend Analysis

Although multi-cloud compute has become more mainstream, Multi-Cloud Networking is in its early stages of adoption. A number of organizations can implement multi-cloud computing without Multi-Cloud Networking, and most are doing that.

However, in the interim, organizations looking to implement Multi-Cloud Networking solutions should use multi-cloud network virtualization solutions (NFV) such as with Cisco ACI and VMware (NSX) to fill gaps or address mission-critical business functionality when cloud-native capabilities do not provide the capability.

Applicability to SSC

- Seamless connectivity and central management interface across multiple providers
- Centralized reporting capabilities
- Reduces vendor lock-in
- The ability to move storage resources among providers as prices change

Trend #11—Networking on Demand

What are Network on Demand (NoD) Services?

NoD services are WAN transport services provided from network service providers (NSP) and managed service providers (MSP). They are typically offered through a portal or a provider's API. Capacity and configuration changes can be made on-the-fly in real time and are not fixed. Changes can be made by the customer on demand and do not require a lengthy order process to fulfill.

These services are often based on software-defined technology and allow real-time changes to port allocations and bandwidth allocations. Customers can even add and delete network endpoints such as connection to cloud and extranet connections.

Trend Analysis

In support of cloud connectivity and IoT, there is a new generation of network on-demand services that provide greater agility and flexibility. Currently, the primary use case of these new offerings are for connectivity to new endpoints such as cloud services. They can also support a migration of network traffic from MPLS to internet services.

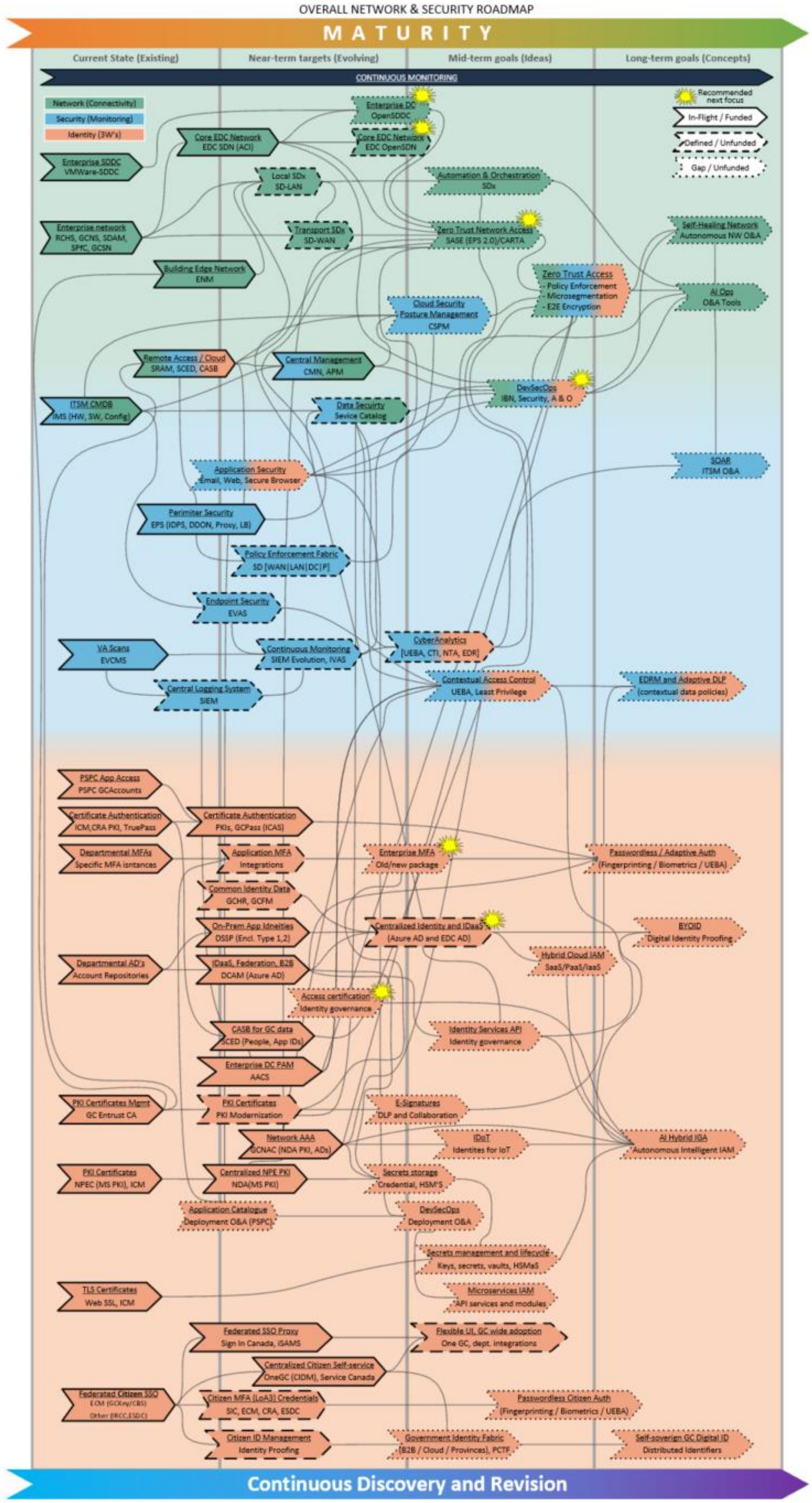
Organizations that seek these services are primarily looking for cost optimization and agility. Network on demand solutions will start to show higher adoption rates especially related to dynamic bandwidth services as they continue to evolve and add greater value to enterprises in terms of speed and flexibility.

Voice and data services should be a key consideration when evaluating NoD services.

Applicability to SSC

- Simplified network migration and consolidation
- On-demand provisioning of edge site and cloud connectivity
- Better user experience for voice and data services
- Cost optimization
- Better capacity planning

Appendix B—Network and Security Roadmap



Appendix C—In-Flight Projects

*See Section 3 for the Business Drivers table

SCED—Secure Cloud Enablement and Defence

Provides secure cloud connectivity for Protected B workloads. Must be considered as part of any external network connectivity requirements as described in Connectivity section. SSC is still determining whether trusted interconnection point (TIP) / cloud access points (CAP) components of SCED will reside on-premise or in the cloud, which will have an impact on monitoring solution.

Outcome:

- GC trusted interconnection point (GC-TIP): network perimeter for cloud connectivity to meet cloud demand on the GC WAN
- GC cloud access points (GC-CAP): centralized public cloud security perimeters to provide private/public DMZ capabilities for internet-bound communications
- Dedicated CXP connection: high speed, low latency connection of cloud service providers (CSP)
- Implementation of a cloud access security broker (CASB) to provide security policy enforcement points
- Central logging and management for all components implemented in support of the perimeter and CSB service, capturing security events for cloud traffic and forward to SIEM

Dependencies:

- SSC and Communications Security Establishment Canada (CSEC) personnel to develop/deploy/operate SCED
- CSEC-deployed services to inspect high volume of network traffic
- SIEM to provide cyberthreat prediction/detection
- Centralized Management Network (CMN) project to provide enterprise network management solution
- Identity and Credential Management (ICAM) strategy by SSC to provide access control solution for cloud
- Enterprise Perimeter Security (EPS) project: leverage GCNet perimeters solution
- CSEC CCCS to develop/operate solution
- SSC to develop strategies for: IP Address Management (IPAM), Domain Name Server (DNS), systems management/CSP policy management enforcement

Pillar: Connectivity

Timeline: Year 1

EVAS—Endpoint Visibility, Awareness and Security

Enterprise approach to endpoint security improving visibility and awareness of all endpoint devices on GC/SSC networks to provide cyber situational awareness across the GC/SSC enterprise. Automated asset discovery and assessment to support Operating System and application patch and currency management and hardening requirements.

Outcome:

- Visibility/monitoring of up to 900,000 GC endpoints, offering protection at host level
- Enables enterprise to obtain and consolidate data from individual departments and partners to create enterprise view
- Data to assist with patching/hardening Operating System and applications, identify unmanaged devices
- Mitigate threat posed by zero-day vulnerabilities
- Assist with IT business planning, forecasting and life cycle management: identify outdated systems, unused licences

Dependencies:

- Resource/staffing availability to build/deploy/run EVAS
- Sufficient infrastructure to host/run EVAS tools
- Stakeholder/partner organizations to provide requirements and acceptance
- IT Security Tripartite to act as signatories of project artefacts
- TBS to create GC policy surrounding reporting/remediation timeframes relating to EVAS

Pillar: Access Control

Timeline: Year 1

EVCM—Enterprise Vulnerability and Compliance Management

Enterprise vulnerability and compliance services and capability providing a unified approach and technology solution for vulnerability management.

Outcome:

- Vulnerability and compliance scanning for EDC, IT infrastructure and perimeter, Wi-Fi, networks, and workstations
- Automated and integrated enterprise vulnerability and compliance assessment, including reporting, to continually assess exposure of IT systems and infrastructure for weaknesses
- Scan up to 500,000 internet-facing IP addresses, ability to support up to 2,000,000 IPs in the future

- Establish Compliance Management Service within SSC Security Management and Governance team

Dependencies:

- Resource/staffing availability to build/deploy/run EVCM solution
- Partner organization to provide requirements
- IT Security Tripartite (TBS, CSEC, SSC) provide response as signatories
- IT infrastructure to securely run/host tools
- TBS create GC policy for VM altering/reporting, response timeframes
- Security Management Network rollout, network bandwidth to support Partner EVCM deployment

Pillar: Access Control

Timeline: Year 1

NDA—Network Device Authentication

NDA is part of SSC's Infrastructure Security Enterprise Program to implement an enterprise network device authentication service which includes certificate-based network authentication.

Centralizes life cycle management of non-person entity (NPE) certificates and provides reporting on authentication, authorization, and auditing (AAA) transactions for security auditing, compliance and service improvement.

Outcome:

- Automate Provisioning of NPE certificates and provides AAA services to GC, certificate-based network authentication capabilities to provide multifactor authentication
- Service provides GC-wide device credentials and a standard authentication mechanism
- Central trusted Public Key Infrastructure (PKI) to provision NPE certificates consolidating 52+ legacy certificate solutions
- Improves access controls, management, auditing, and forensic analysis of data/network access history associated with users, devices
- Central management of authentication of NPEs to network access points with a central remote authentication dial-in user service (RADIUS)
- Enables network access control (NAC) and enhances auditing/report of network certificate usage
- Allows for further adoption of encryption of data in transit on GC networks improving defense in depth

Dependencies:

- Procure licences on Enterprise Microsoft agreement and vendor participation/support
- Connectivity/adequate throughput between SSC DCs and partner networks
- IAM privilege management/identity management services access controls in place

Pillar: Access Control

Timeline: Year 2

SRAM—Secure Remote Access Migration

Fully integrate and rationalize existing secure remote access (SRA) infrastructure and consolidate process of SRA connections at EDCs. Transform SRA services to an enterprise data service from a departmental-based service.

Outcome:

- Consolidate client-to-gate remote access solutions (largely unstructured) across GC and ever-greening gate-to-gate remote access solutions for remote offices off GCNet
- Provide full scope of log collection, analytics, and processing to meet SSC SOC mandate to timely provide data for threat detection/incident response
- Rationalize and move legacy SRA gateways from legacy DCs into the EDC, installing gateways at the EDCs to support traffic volume of an aggregate of departmental services
- Enable increased teleworking, reducing office space costs and increase employment opportunities and presence in remote communities

Dependencies:

- Staffing: availability of qualified resources to build, deploy, and run the SRAM
- SSC DC Consolidation Program
- EDCs physical space to house SRAM solution
- Directory Services: ensure new gateway can authenticate users
- SRA end user departments need to configure endpoints to migrate to new SRAM
- Network bandwidth: adequate throughput connection speeds required

Pillar: Access Control

Timeline: Year 2

ENM—EDGE Network Modernization

The ENM Pathfinder Project will define a repeatable network service that can be used to deploy enterprise network structure and services throughout the GC. The standard physical infrastructure should be of the highest quality and latest technology to support any GC department or user and enable true mobility. The ENM Pathfinder Project will lay the groundwork to enable all GC workers to have access to the 3,500 plus GC locations as potential worksites. It will provide the foundational components for network virtualization and automation.

Outcome:

- Service standardization resulting in simplified service offerings and improved service delivery: by undertaking the pathfinder project will be able to understand the service catalogue that will be offered through the ENM Pathfinder Project deployment and the best method of service delivery for the GC customers.
- Established network infrastructure required to enable the delivery of other services and solutions: by utilizing a pathfinder approach, the project will be able to deliver an enterprise network infrastructure that can then be repeated successfully across the remaining 3,500 plus sites, rather than trying to design, create and deploy at the same time.

Dependencies: See ENM Business Case for full list of dependencies

Pillar: Connectivity

Timeline: Year 3-5

CMN—Central Management Network

Improve support resource experience by providing a single window to securely manage all partner infrastructure/ services located in DCs (EDCs and legacy), improving service availability and reliability.

Outcome:

- Reduce user complexity by standardizing tools and a single laptop to manage partner legacy networks.

Dependencies: How will connectivity occur?

Pillar: Provisioning

Timeline: Year 3-5

EPS—Enterprise Perimeter Security

ZTA is a key architectural approach for the future network and security strategy and assumes that the network perimeter has moved to a "virtual" perimeter. SSC will need to ensure that the design and architecture of the EPS project is aligned to the key tenets of a ZTA.

Outcome:

- Modernized network perimeter able to withstand current threat landscape and absorb DDoS attacks
- Protects the GC's perimeter regardless of physical and virtual boundaries
- Enables secure end user connectivity from any location
- Leverages ZTA architectural principles with least privilege access in mind

Dependencies: CMN, EPS, IPAM, DNS and SCED projects

Pillar: Access Control

Timeline: Year 1 (Current)

SIEM—

Fully integrated GC enterprise SIEM solution providing visibility and automated response to cyberattacks. Enables accelerated threat detection and security incident response.

Outcome:

- Enables SSC SOC to improve prediction of cyberthreats, increase detection capability, and detect and identify more complex threats
- Supports SSC SOC's mandate to provide timely/accurate information to support threat detection and security incident response
- AI-based system to analyze User and Entity Behaviour Analytics (UEBA) to enhance rule-based SIEM capabilities
- Leverages cyber threat intelligence (CTI) feeds to obtain contextual information to assist in updating protective countermeasure prior to an attack
- Centralized log collection capability to assist in threat detection, investigations, and access to information, increasing SIEM coverage and log visibility

Dependencies:

- To build, deploy, and run the SIEM
- IT Security Tripartite provide timely responses as signatories of project artefacts
- Infrastructure to securely host SIEM
- Project to follow SSC Cyber and IT security Assessment and Authorization processes
- Align with CCCS requirements and methodologies

Pillar: Access Control

Timeline: Year 1

ICAS— Internal Centralized Authentication Service

ICAS provides a centralized authentication capability that will offload end-user authentication from individual GC enterprise applications, providing a whole-of-government authentication solution.

The move to ZTA will drive increased capacity requirements for all components of ICAS as the process of end user/entity/device centralized authentication and authorization becomes continuous and multi-modal. This program will need to be aligned with the ZTA.

Outcome:

- Enables a consolidated and centralized authentication platform for the GCe
- Reduces point solutions currently in use
- Reduces overall security risk through a standard and controlled authentication framework

Dependencies:

- Next generation network architecture
- Understanding of future services / use cases to support with some capacity estimates (e.g., IoT).

Pillar: Access Control

Timeline: Year 1

GC Digital Workspace Profiles

A standard set of employee experience profiles for standard digital workspace and related employee-centric IT services to be mapped and delivered against, which are function-based.

There are two activities that are coalescing around defining the Digital Workspace:

- Public Services and Procurement Canada’s Real Property branch is defining the workplace of the future including collaborative hubs
- A standardized service offering to reduce lead times for delivery and better align to the physical workplace of the future

Outcome:

- Enables any GC employee to work from any building without departmental barriers
- Improved user experience
- Avoidance of overages

- Optimized tool selection
- Better managed departmental purchases

Dependencies: N/A

Pillar: Access Control

Timeline: Year TBD