

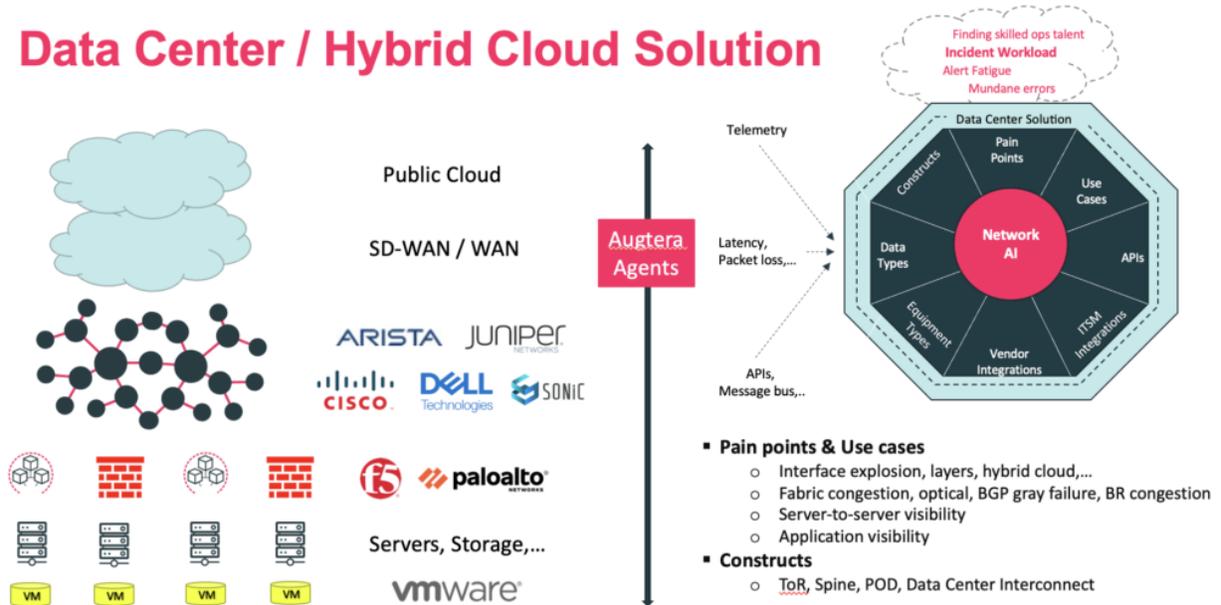
Solution Brief

Augtera Networks Data Center Solution

Introduction

Augtera's Network AI Data Center Solution covers the major equipment types and suppliers in Data Center Environments. Importantly it addresses the relevant pain points, use cases, integrations, and constructs. The result is a purpose-fit Data Center solution that results in faster detection, mitigation, and remediation, reduced overall incident workload, and prevention of incidents before they occur.

Data Center / Hybrid Cloud Solution

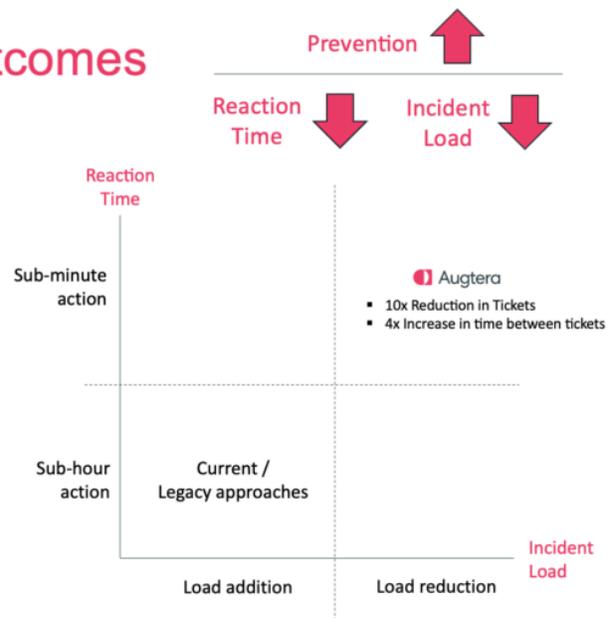
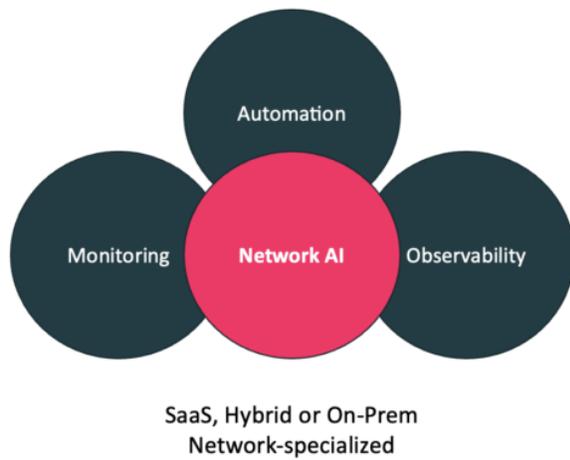




Network Operations tools are being disrupted and consolidated. Network AI incorporates monitoring, observability, and automation of ingestion, detection, incident root identification, and noiseless notification (alert console, trouble ticket creation, and automation systems).

The result for customers is a dramatic reduction in detection / action, from over 40 minutes to under a minute, a reduction in trouble tickets / actioned incidents by a factor of 10, and in increase in the time between incidents by a factor of 4.

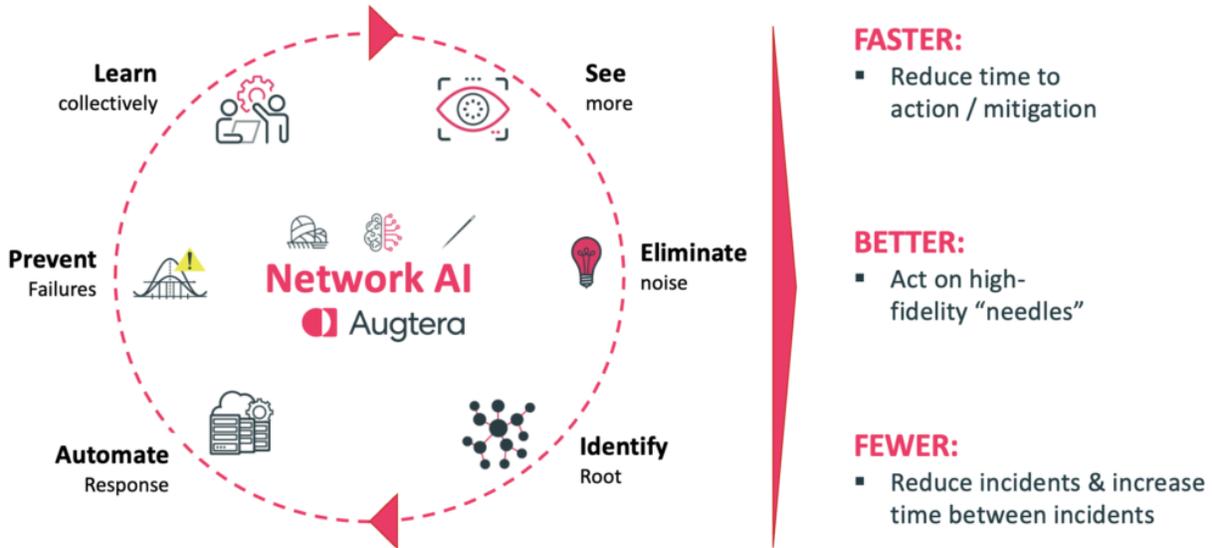
Fundamental Shift: Technology & Customer Outcomes



The Augtera Networks Data Center Solution is based on our core Network AI platform which creates a virtuous circle across the entire customer base.



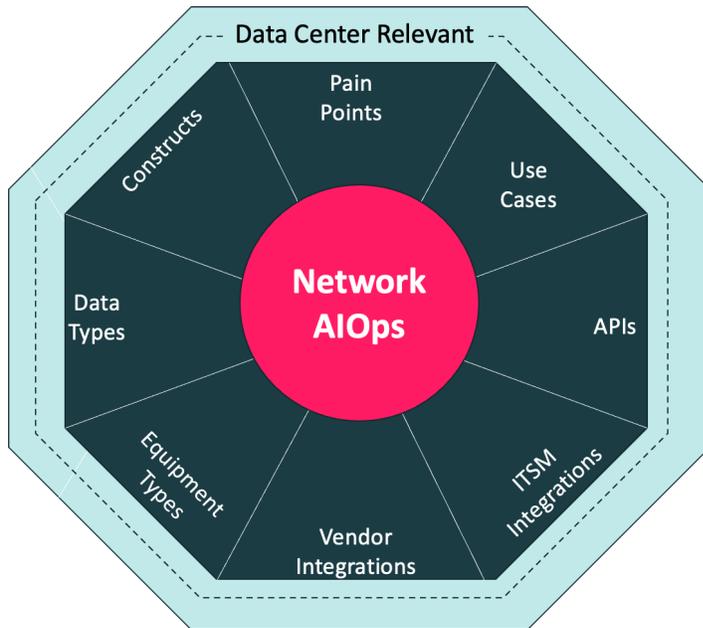
Faster, Better, Fewer



Network AI sees more anomalies than other tools, it has better insights than other tools, it eliminates noise, identifies incident root, automates mitigation / remediation, detects degradation and other gray failures so future failures can be prevented, and shares anomaly signatures across the entire customer base, effectively accelerating learning for each customer. Incidents are acted on faster, the insights for the incidents are better, and there are fewer overall incidents / tickets to be acted on.

Data Center Solution Engineering

The Augtera Networks Data Center Solution extends Augtera's Network AIOps platform to address the specific pain points, use cases, constructs, and integrations required to enable customers to realize the potential of Network AIOps in Data Center deployments.



Data Center Relevant

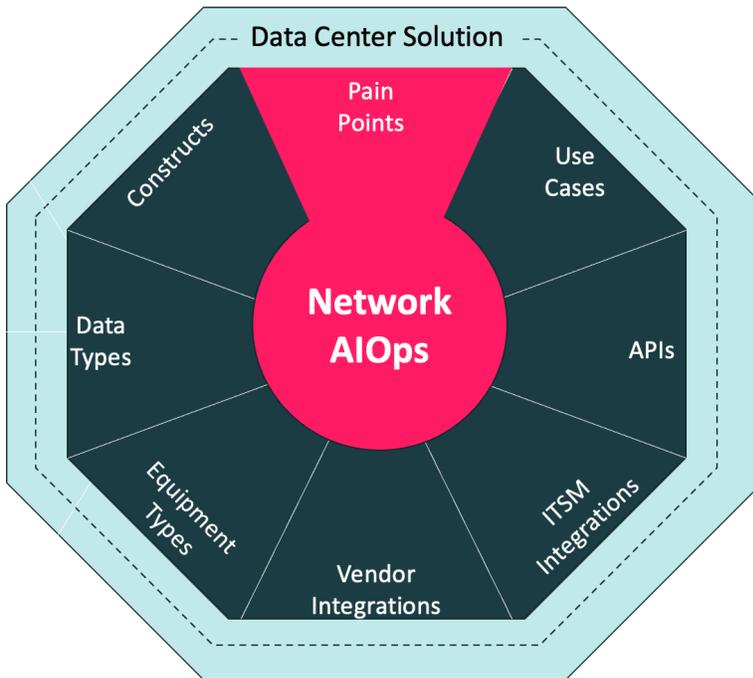
- Pain Points
- Use Cases
- APIs
- ITSM Integrations
- Vendor Integrations
- Equipment Types
- Data Types
- Constructs

The solution is the result of three years of development and close partnership with customers to understand, develop, and mature the capabilities specifically relevant to Data Center Network Operations teams.

Pain Points

Nowhere in networking are the issues of scale and complexity more acute than in Data Centers. There are numerous contributors to this. The complexity inherent in large modular chassis equipment has been replaced by the simplicity of fixed form factor switches and routers deployed in L3 Clos topologies.

However, this has led to new Network Operations challenges. An explosion in the number of interfaces has led to new scaling challenges for operations tools and the explosion in paths between sources and destinations has created new anomaly detection challenges, not just at the physical layer, but all the way up to the application flow layer.



Pain Points

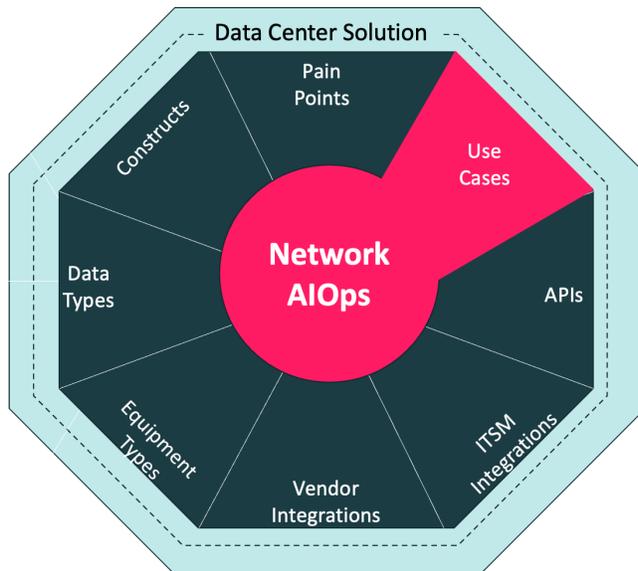
- Interface explosion
- Path explosion
- Layer complexity
- Application performance
- Hybrid Cloud

Another area of complexity is the number of layers in modern Data Center Architectures. Physical layer, optical, Ethernet, IP underlay (commonly BGP-based), IP Overlay (commonly EVPN/VXLAN-based), and for Hybrid/Multi-cloud scenarios, there can also be SD-WAN.

The Augtera Networks Data Center Solution uses an auto-discovered Network Model that understands all the elements/objects, layers, and constructs in Data Center environments. Leveraging the Network Model, multi-layer, topology-aware auto-correlation is able to reduce noise and identify the root of an incident.

Use Cases

There are many use cases a Network AIOps solution needs to address in a Data Center environment. Here we discuss a few.



Use Cases

- Fabric/server latency & packet loss
- Fabric congestion impact on application flows
- Optical anomaly
- BGP gray failure
- Border router congestion
- ...

Fabric / Server, Hybrid Cloud Latency & Packet Loss

In the Data Center, the network does not end at ToR (Top of Rack) switches, it extends all the way to servers. Detecting changes in latency and packet loss within the fabric, and all the way to servers is critical today. However, while other solutions stop at measurements, the Augtera Data Center Solution inputs the measurements, into Machine Learning (ML) based anomaly detection to find operationally relevant anomalies in latency and loss. The solution further inputs these anomalies along with other data sources, and performs multi-layer, topology-aware auto-correlation. The Augtera Data Center Solution uses Machine Learning (ML) models instead of static thresholds to reduce anomaly detection noise. Less noise, better insights. Augtera Networks latency and packet loss anomaly detection is also supported for Hybrid / Multi-Cloud.

Fabric Congestion Impact on Application Flows

It is one thing to know or suspect there is fabric congestion, it is another to know if that congestion is impacting applications. The Augtera Data Center Solution can determine if specific applications are experiencing performance degradation. It is critical today that network operations teams be able provide answers to application teams on the impact or innocence of the network with respect to Data Center / Cloud-based applications.

Auto-Remediation



While some problems require a skilled engineer to diagnose the ultimate remediation, there are a class of anomalies that occur often, and for which there are well known responses. These responses can be easily automated. Augtera Networks has been working closely with customers and continues to add to this capability. Some examples of anomalies that can be auto-mitigated/remediated include:

- Optical anomalies
- Link flaps or anomalous errors
- BGP gray failures
- Border router congestion

Augtera Networks works with customers to notify automation systems developed/managed by the customer, that perform the auto-mitigation/remediation action triggered by an Augtera notification.

NetOps / DevOps Friendly APIs

There are numerous short and long-term drivers for APIs. In the short-term, an operations team may not be able to provide direct access to a data source for a Network Operations tool. Sometimes the export of data to a file is explored, and maybe the only option. However, this is far from optimal. It is not dynamic for one. In these cases, Augtera provides its own APIs and support for other APIs. In the long-term, the transition to NetOps and DevOps-friendly Network Operations is the main driver for supporting and providing APIs.

Augtera Networks is always exploring with customers what APIs to support and what APIs to provide for the Data Center Solution. Two APIs that have been powerful in Data Center Solutions are:

- Meta-Information API
- Topology API

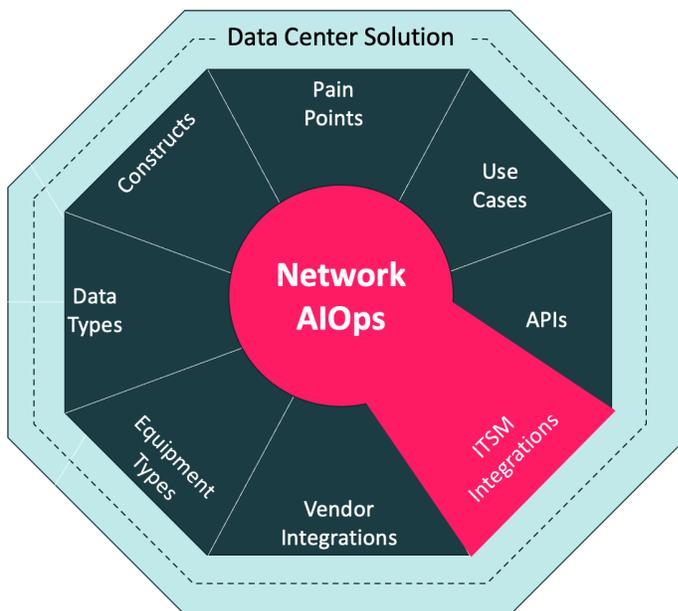
There are many powerful uses of Meta-Information, including data / alert enrichment. Of particular concern to Network Operations teams is communicating to Network Operations tools when to suppress alarms. For example, a Network Operations team may know that it is performing maintenance, so it does not need alarms for impacted elements.

Augtera believes strongly that auto-correlation needs to be topology-aware to effectively identify the root of an incident, which is why topology auto-discovery is provided in the base platform. However, there are times that Network Operations teams cannot provide use of the protocols needed to do auto-discovery. For these occasions, using an API is a good alternative.



ITSM Integrations

All Network Operations teams have a “job to be done”, and that job cannot be done unless tools are integrated into / aware-of processes and workflows. Any tool vendor can say they support an API. The “rubber meets the road” on the question of whether a tool is enabling the network operations team to get their job done.



ITSM Integrations

- ServiceNow
(customer workflow, not just API call)
- Slack

There are numerous ways in which Augtera has worked with Data Center Network Operations teams to support workflows and processes.

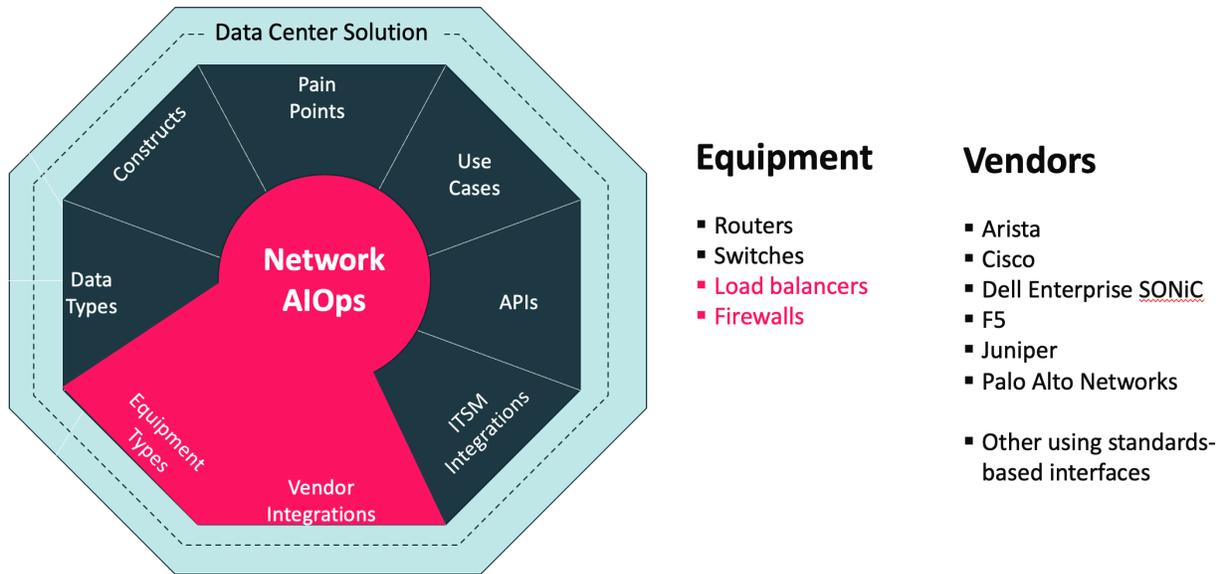
ServiceNow tickets are often the trigger for scheduling skilled engineers to act on an incident. As skilled engineers are a scarce resource, it is critical that no noise is injected into ServiceNow. The Augtera Networks Data Center Solution eliminates noise from anomaly detection and ingestion of multiple data sources, suppresses maintenance incidents, de-duplicates, and provides customer policy definition that indicates what is operationally relevant and what is high or low priority.

As Network Operations teams seek to be more collaborative, tools like Slack have been adopted. Augtera Networks provides alerts / visualizations within Slack.

Equipment and Vendor Integrations



Augtera Networks is inherently differentiated from single-vendor / single-vendor-oriented solutions by broad multi-vendor support. While equipment vendors are often motivated to provide better support for their own equipment, Augtera Networks is motivated to provide robust multi-vendor support. In the context of the Data Center Solution, this includes prominent suppliers like Arista Networks, Cisco Systems, Juniper Networks and Dell Enterprise SONiC, as well as several other switch and router vendors

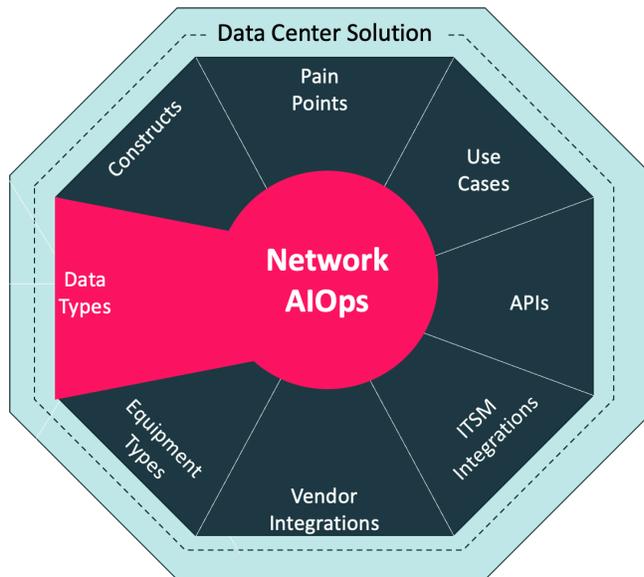


However, there is more to Data Centers than Routers and Switches. Load-balancers and Firewalls are also critical equipment types which is why the Data Center solution has integrations with F5, Palo Alto Networks, and other suppliers in these areas.



Data Types

Network AIOps begins with ingesting the data needed to develop the insights and actions that transform Network Operations. Any Data Center Solution must support the needed data.



Data Types

- SNMP
- Syslog
- sFLOW
- IPFIX
- VPC Flow Logs
- gRPC / gNMI / OpenConfig
- Mirror on Drop (MOD)
- Dell SONiC streaming telemetry
- Augtera synthetic probe agent for latency and loss
- Kafka

Augtera Networks has found SNMP and Syslog is fundamental to most solutions. In fact, some solutions can be provided with Syslog only. For the Data Center Solution, sFLOW and IPFIX are important for anomaly detection involving flows and application performance degradation. For some SD-WAN offerings, IPFIX is the only flow data supported.

OpenConfig and gRPC/gNMI are emerging approaches. While implementations are still maturing in many cases, support is critical for some Data Center equipment and customer preferences. VPC Flow Log support extends the Data Center Solution to cloud environments.

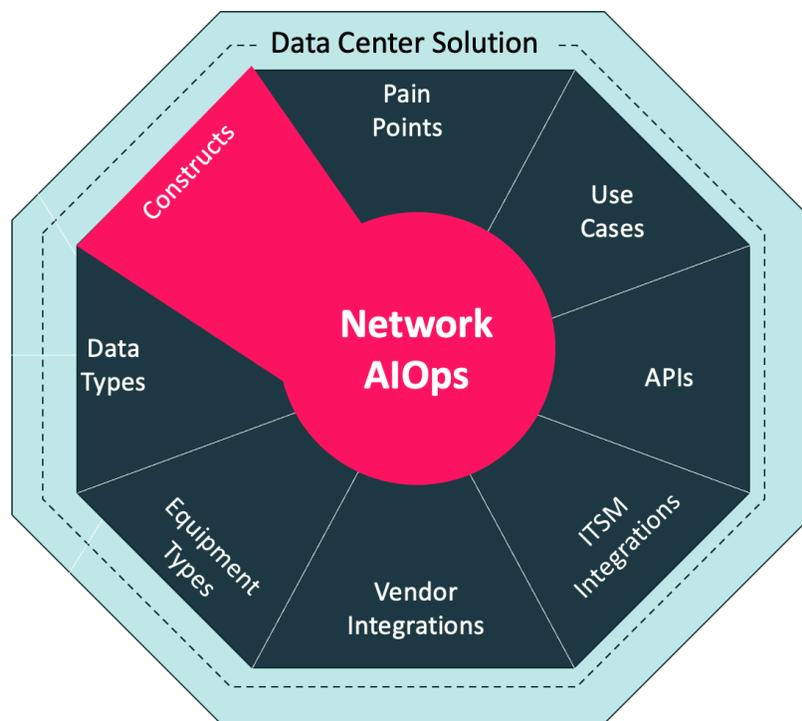
Synthetic agents for latency and loss are critical because other telemetry data does not provide this information. Kafka is an increasingly important transport for many data types.

The Augtera Data Center Solution also supports the Mirror on Drop (MOD) Broadcom chip capability enabled on Dell Enterprise SONiC, in addition to Dell Enterprise SONiC streaming telemetry.



Constructs

Every networking environment has potentially different constructs that need to be supported, because of network architecture and design considerations inherent to that environment.



Constructs

- Physical
- Optical
- Ethernet

- BGP underlay
- EVPN / VXLAN
- SD-WAN
- TORs
- PODs
- Fabrics
- DCIs

For Data Center environments, there are numerous constructs that need to be supported. Some already mentioned in this paper include physical, optical, Ethernet, underlays, overlays, and SD-WAN. The Data Center has other unique constructs like Top of Rack, spine switches, PODs, L3 Clos Fabrics, and Data Center Interconnects (DCIs).

Why does this matter? What if a network operations team decides they want to understand anomalies at the POD aggregate level? Then the POD construct must be supported by the solution. What if a network operations team decides links from a ToR to a server are not high priority from a notification perspective, but ToR uplinks are? Then the ToR construct must be supported and understood.



If the constructs important to data center environments are not understood and integrated into the solution, then important noise reduction, notification, and analysis policies cannot be realized.

Conclusion

A solution must address the specific needs of a customer's environment. Networking and Network Operations are not like other IT domains. The networking domain is differentiated by pain points, use cases, required API support, the workflows / process support needed for ITSM integration, vendor / equipment integrations, data type, and constructs. An industry-leading Data Center Solution requires holistic support for all of these, within a Data Center Networking context.

The Augtera Network AIOps Data Center solution – the first and leading solution.

Related Links

- [Data Center Solution](#)
- [Fortune 500 Case Study](#)
- [Actionable Insights for Data Center](#)
- [Flow Path Demo](#)
- [Proactive Multicloud Performance Visibility](#)
- [Multicloud Performance Insights](#)